

TP-LINK®

РЪКОВОДСТВО НА ПОТРЕБИТЕЛЯ

TL-WR841N

TL-WR841ND

300Mbps безжичен N рутер



АВТОРСКИ ПРАВА И ТЪРГОВСКИ МАРКИ

Спецификациите подлежат на промяна без предизвестие. **TP-LINK**[®] е регистрирана търговска марка на TP-LINK TECHNOLOGIES CO., LTD. Други марки и продуктови имена са търговски марки или регистрирани търговски марки на техните съответни притежатели.

Никоя част от спецификациите не може да се възпроизвежда по никакъв начин или с никакви средства или да се използва за изготвяне на такива дериватни продукти като трансляции, трансформации или адаптации без разрешението от TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2012 TP-LINK TECHNOLOGIES CO., LTD. Всички права запазени.

<http://www.tp-link.com>

ДЕКЛАРАЦИЯ НА FCC



Настоящото оборудване е тествано и отговаря на ограниченията за цифрово устройство от клас В съгласно част 15 на Правилника на Федералната комисия по комуникации. Тези ограничения имат за цел да осигурят добра защита срещу вредните въздействия при инсталации в жилищни сгради. Това оборудване генерира, използва и може да излъчва радиочестотна енергия и, ако не се инсталира и използва съгласно инструкциите, може да причини вредно въздействие на радиокомуникациите. Все пак няма гаранция, че никаква намеса няма да възникне в конкретна инсталация. Ако това оборудване оказва вредни смущения на радио или телевизионния сигнал, което може да се определи чрез включване и изключване на оборудването, съветваме потребителя да се опита да коригира смущението посредством една или повече от следните мерки:

- Да промени ориентацията или мястото на приемателната антена.
- Да увеличи разстоянието между оборудването и приемника.
- Да включи оборудването към верига, различна от тази, към която е свързан приемника.
- Да се свърже с продавача или опитен радио или телевизионен техник с молба за съдействие.

Това устройство съответства на част 15 от Правилника на FCC. Работата му се определя от следните две условия:

- (1) Това устройство не причинява вредни смущения.
- (2) Това устройство трябва да приема получавани смущения, включително смущения, които могат да причинят нежелан начин на работа.

Всички промени или модификации, които не са изрично одобрени от страната, отговорна за съответствието, може да лишат потребителя от правото да работи с оборудването.

Забележка: Производителят не носи отговорност за радио и телевизионни смущения, причинени от неупълномощени модификации по това оборудване. Такива модификации може да лишат потребителя от правото да работи с оборудването.

Декларация на FCC за излагане на въздействието на радиочестотно излъчване

Настоящото оборудване съответства на ограниченията за излагане на въздействието на радиочестотно излъчване, определено за неконтролирана среда. Това устройство и неговата антена не трябва да бъдат разположени заедно или да работят заедно с друга антена или предавател.

“За спазване на изискванията за съответствие с излагане на радиочестотно въздействие на FCC RF, това разрешително е валидно само за мобилни конфигурации. Използваните антени за този предавател трябва да се инсталират така, че да са на разстояние поне 20 см от всички лица и не трябва да се разполагат заедно или да работят заедно с друга антена или предавател.

Предупреждение за CE знак

CE 1588 !

Този продукт е от клас B. В домашна среда, този продукт може да причини радиосмущения като в този случай потребителят трябва да вземе адекватни мерки.

Национални ограничения

Това устройство е предназначено за използване в дома и в офиса във всички държави от ЕС (и всички други страни спазващи директивата на ЕС 1999/5/ЕС) без никакви ограничения освен за страните, посочени по-долу:

| Страна | Ограничение | Причина/ забележка |
|-----------------|--|--|
| България | Няма | Общо разрешение, изисквано за използване на открито и в обществени зони. |
| Франция | Употребата навън е ограничена до 10 mW e.i.r.p. в рамките на 2454-2483.5 MHz | Военна радиолокация . В последните години тече преразпределение на 2.4 GHz честотната лента, за да се осигури текущата облекчена регулация. Пълното въвеждане е планирано за 2012 г. |
| Италия | Няма | Изисква се общо разрешение, ако се използва извън собствените помещения. |
| Люксембург | Няма | Изисква се общо разрешение за мрежа и доставка на услуга (не за спектър) |
| Норвегия | Въведено | Този подраздел не се прилага за географската зона в радиус от 20 км от центъра на Ny-Ålesund. |
| Руска федерация | Няма | Само за приложения на закрито |

Забележка: Моля не използвайте продукта на открито във Франция.

Това устройство е проектирано за работа с долупосочените антени и с максимално усилване от 5 dBi. Антените, които не са посочени в списъка или с усилване по-голямо от 5 dBi, са строго забранени за употреба с това устройство. Изискваният импеданс на антената е 50 ома.

За да се намалят радиосмущенията към други потребители, типът на антената и нейното усилване трябва да бъдат избрани така, че еквивалентната изотропично излъчвана мощност (е.и.г.р.) да не е повече от разрешената за успешна комуникация.

Индустриална декларация на Канада:

Настоящото устройство е в съответствие с RSS-210 на Индустиалните правила на Канада. Работата е предмет на следните две условия:

(1) Това устройство не трябва да причинява вредно смущение, и

(2) Това устройство трябва да приема получавани смущения, включително смущения, които могат да причинят нежелан начин на работа.

ВАЖНА ЗАБЕЛЕЖКА:

Декларация за радиационно излагане:

Настоящото оборудване е в съответствие с канадските ограничения за радиационно излагане, зададени за неконтролирана среда. Това оборудване трябва да бъде инсталирано и да работи с минимално разстояние от 20 см между радиатора и вашето тяло.

ДЕКЛАРАЦИЯ ЗА СЪОТВЕТСТВИЕ

За следното оборудване:

Описание на продукта: **300Mbps безжичен N рутер**

Модел No.: **TL-WR841N/TL-WR841ND**

Търговска марка: **TP-LINK**

Декларираме на своя собствена отговорност, че горните продукти отговарят на всички технически наредби, приложими за продукта в рамките на обхвата на следните Директиви на Съвета:

Директива 1999/5/EC, Директива 2004/108/EC, Директива 2006/95/EC, Директива 1999/519/EC, Директива 2011/65/EU

Горепосоченият продукт е в съответствие със следните стандарти или други нормативни документи

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN60950-1:2006+A11:2009+A1:2010

EN62311:2008

Продуктът има CE маркировка:

CE 1588 !

Отговорно лице за издаването на настоящата декларация:



Янг Хонглианг

Продуктов мениджър "Международни операции"

Дата на издаване: 2012

TP-LINK TECHNOLOGIES CO., LTD.

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park,
Shennan Rd, Nanshan, Shenzhen, China

СЪДЪРЖАНИЕ

| | |
|--|-----------|
| Съдържание на пакета..... | 1 |
| Раздел 1. Въведение..... | 2 |
| 1.1 Обща информация за рутера..... | 2 |
| 1.2 Конвенции | 3 |
| 1.3 Основни характеристики | 3 |
| 1.4 Разположение на панела | 4 |
| 1.4.1 Преден панел | 4 |
| 1.4.2 Заден панел | 5 |
| Раздел 2. Свързване на рутера | 6 |
| 2.1 Системни изисквания | 6 |
| 2.2 Изисквания за средата на инсталация..... | 6 |
| 2.3 Свързване на рутера | 6 |
| Раздел 3. Указания за бърза инсталация..... | 9 |
| 3.1 TCP/IP конфигурация | 8 |
| 3.2 Указания за бърза инсталация | 10 |
| Раздел 4. Конфигуриране на рутера | 16 |
| 4.1 Регистрация | 16 |
| 4.2 Статус | 16 |
| 4.3 Бърза настройка..... | 18 |
| 4.4 QSS..... | 18 |
| 4.5 Мрежа | 25 |
| 4.5.1 LAN | 25 |
| 4.5.2 WAN | 25 |
| 4.5.3 MAC Clone | 35 |
| 4.6 Безжична връзка | 36 |
| 4.6.1 Настройки за безжична връзка..... | 36 |
| 4.6.2 Сигурност на безжична връзка..... | 39 |
| 4.6.4 Безжично MAC филтриране | 42 |
| 4.6.4 Разширена безжична връзка | 45 |
| 4.5.6 Статистика на безжична връзка..... | 46 |
| 4.7 DHCP | 47 |
| 4.7.1 DHCP настройки | 47 |

| | | |
|--------|---|----|
| 4.7.2 | Списък DHCP клиенти..... | 48 |
| 4.7.3 | Резервиране на адрес | 49 |
| 4.8 | Препращане | 50 |
| 4.8.1 | Виртуални сървъри | 50 |
| 4.8.2 | Задействащ порт | 52 |
| 4.8.3 | DMZ..... | 54 |
| 4.8.4 | UPnP | 54 |
| 4.9 | Сигурност | 55 |
| 4.9.1 | Базова сигурност..... | 56 |
| 4.9.2 | Разширена сигурност..... | 57 |
| 4.9.3 | Локално управление | 58 |
| 4.9.4 | Дистанционно управление | 59 |
| 4.10 | Родителски контрол | 60 |
| 4.11 | Контрол на достъпа | 63 |
| 4.11.1 | Правило | 63 |
| 4.11.2 | Хост | 66 |
| 4.11.3 | Цел..... | 68 |
| 4.11.4 | Схема..... | 70 |
| 4.12 | Разширено маршрутизиране..... | 72 |
| 4.12.1 | Списък за статично маршрутизиране..... | 72 |
| 4.12.2 | Таблица за системно маршрутизиране..... | 73 |
| 4.13 | Контрол на честотна лента..... | 74 |
| 4.13.1 | Настройки за контрол | 74 |
| 4.13.2 | Списък правила..... | 75 |
| 4.14 | Настройка за IP & MAC свързване | 76 |
| 4.14.1 | Настройки за свързване..... | 76 |
| 4.14.2 | ARP списък..... | 78 |
| 4.15 | Динамична DNS..... | 79 |
| 4.15.1 | Comexe.cn DDNS | 79 |
| 4.15.2 | Dyndns.org DDNS | 80 |
| 4.15.3 | No-ip.com DDNS | 81 |
| 4.16 | Системни инструменти..... | 82 |
| 4.16.1 | Настройка за време..... | 83 |
| 4.16.2 | Диагностика..... | 84 |
| 4.16.3 | Надграждане на фърмуер..... | 85 |
| 4.16.4 | Заводски настройки | 86 |

| | |
|---|------------|
| 4.16.5 Архивиране & възстановяване | 87 |
| 4.16.6 Рестартиране | 87 |
| 4.16.7 Парола | 88 |
| 4.16.8 Системен журнал..... | 88 |
| 4.16.9 Статистика | 91 |
| Приложение А: Най-често задавани въпроси | 93 |
| Приложение В: Конфигуриране на компютри..... | 121 |
| Приложение С: Спецификация | 102 |
| Приложение D: Речник | 103 |

Съдържание на пакета

В пакета трябва да откриете следните елементи:

- TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер
- DC захранващ адаптер за TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер
- Ръководство за бърза инсталация
- CD за TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер, включващ:
 - Настоящото ръководство
 - Друга полезна информация

Забележка:

Уверете се, че пакетът съдържа горните елементи. Ако някой от горепосочените елементи е повреден или липсва, моля свържете се с дистрибутора.

Раздел 1. Въведение

Благодарим Ви, че избрахте TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер.

1.1 Обща информация за рутера

TL-WR841N/TL-WR841ND 300Mbps Wireless N рутер включва 4-портов превключвател, защитна система, NAT-рутер и безжична точка за достъп. Захранван с 2x2 MIMO технология 300Mbps безжичният N рутер осигурява изключителен обхват и скорост, които напълно покриват нуждата от мрежа за малък офис/ дом (SOHO) и за потребители, изискващи по-добро мрежово изпълнение.

Невероятна скорост

TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер осигурява до 300Mbps безжична връзка с други 802.11n безжични клиенти. Невероятната скорост позволява работа с множество информационни потоци по едно и също време, което гарантира стабилна и сигурна мрежа. Изпълнението на този 802.11n безжичен рутер ще ви предостави неочаквано мрежово изпълнение при скорост 650% по-голяма от 802.11g. Съвместим е и с всички IEEE 802.11g и IEEE 802.11b продукти.

Множество защиты за сигурност

С множеството мерки за сигурност, включително SSID контрол на излъчването и безжично LAN 64/128/152-bit WEP кодиране, Wi-Fi защитен достъп (WPA2- PSK, WPA-PSK), както и усъвършенствани защиты на защитна стена, TL-WR841N/TL-WR841ND 300Mbps Wireless N рутер осигурява пълна неприкосновеност на данните.

Гъвкав контрол на достъп

TL-WR841N/TL-WR841ND 300Mbps безжичният N рутер осигурява гъвкав контрол на достъп, така че родители или мрежови администратори могат да въвеждат политики на ограничен достъп за деца или персонал. Поддържа виртуален сървър и DMZ хост за прехвърляне на порт, така че мрежовите администратори да могат да управляват и наблюдават мрежата в реално време с функцията за дистанционно управление.

Лесна инсталация

Тъй като рутерът е съвместим с буквално всички основни операционни системи, той е лесен за управление. Налична е програма за бърза настройка, а подробни инструкции, стъпка по стъпка, са дадени в настоящото ръководство. Преди да инсталирате рутера, моля прочетете ръководството, за да се запознаете с всички функции на рутера.

1.2 Конвенции

Рутерът или TL-WR841N/TL-WR841ND, посочен в настоящото ръководство, ще означава TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер.

➔ Забележка:

Две устройства TL-WR841N и TL-WR841ND ползват едно и също ръководство - настоящото ръководство на потребителя. За улеснение в ръководството ще посочване само TL-WR841ND.

Разликите между двете устройства са:

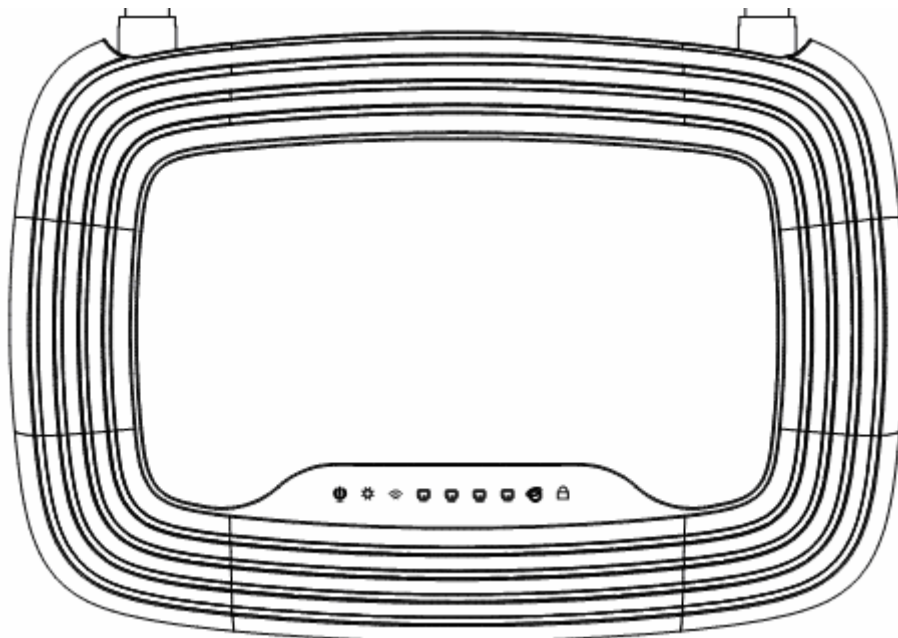
- TL-WR841N рутер с 2 фиксирани антени.
- TL-WR841ND рутер с 2 подвижни антени.

1.3 Основни характеристики

- Отговаря на IEEE 802.11n за осигуряване на безжична скорост на данни до 300Mbps
- Един 10/100M Auto-Negotiation RJ45 WAN порт, четири 10/100M Auto-Negotiation RJ45 LAN порта, поддържащи Auto MDI/MDIX.
- Осигурява WPA/WPA2, WPA-PSK/WPA2-PSK аутентификация, TKIP/AES кодиране за сигурност.
- Споделя данни и Интернет достъп за потребители, поддържащи Dynamic IP/Static IP/PPPoE Интернет достъп.
- Поддържа Virtual Server, Special Application и DMZ host.
- Поддържа UPnP, динамична DNS, статично маршрутизиране.
- Осигурява автоматично свързване и планирано свързване в определен момент към Интернет.
- Вграден NAT и DHCP сървър, поддържащ статично разпределение на IP адреси.
- Поддържа родителски контрол и контрол на достъпа.
- Свързва Интернет при поискване и прекъсва връзката към Интернет при бездействие за PPPoE.
- Осигурява 64/128/152-bit WEP кодиране за сигурност и безжичен LAN ACL (Списък за контрол на достъпа).
- Поддържа статистика на потока.
- Поддържа надграждане на фърмуера и уеб управление.

1.4 Разположение на панела

1.4.1 Преден панел



Фигура 1-1 Схема на преден панел

Светлинните индикатори на рутера се намират на предния панел (изглед от ляво на дясно).

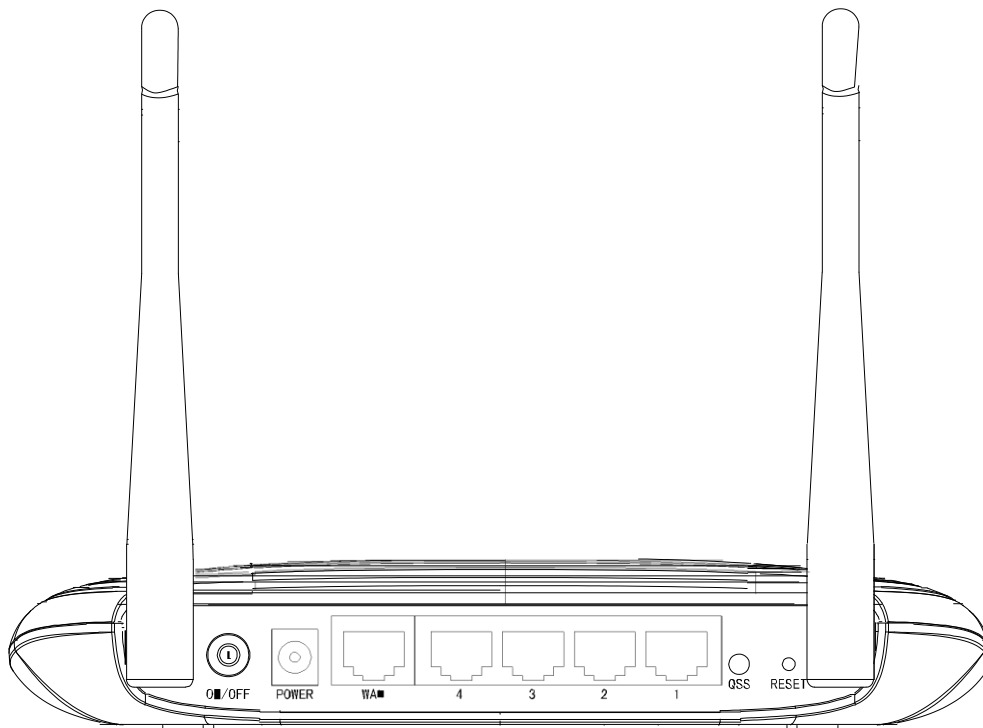
| Име | Статус | Индикац |
|----------------------|--------------|--|
| ⏻ (Захранване) | Изкл. | Захранването е изключено. |
| | Вкл. | Захранването е включено. |
| ⚙️ (Система) | Мигане | Рутерът работи нормално. |
| | Вкл/ Изкл | Има системна грешка. |
| 📶(WLAN) | Изкл. | Функцията за безжична връзка е изключена. |
| | Мигане | Функцията за безжична връзка е включена. |
| 🌐(WAN), (LAN 1-4) | Изкл. | Няма устройство, свързано към кореспондиращия |
| | Вкл. | Има устройство, свързано към кореспондиращия порт, но няма активност. |
| | Мигане | Има активно устройство, свързано към |
| 🔒 (QSS) | Бавно мигане | Безжично устройство се свързва към мрежата чрез QSS функция. Този процес ще продължи в първите 2 |
| | Вкл. | Безжично устройство е успешно добавено към мрежата чрез QSS функция. |
| | Бързо мигане | Неуспех на добавяне на безжично устройство към мрежата чрез QSS функцията. |

Таблица 1-1 Описание на светлинни индикатори

→ Забележка:

След като устройството е успешно добавено към мрежата чрез QSS функция, QSS светлинният индикатор ще свети за около 5 минути и след това ще се изключи.

1.4.2 Заден панел



Фигура 1-2 Схема на заден панел

Следните елементи са разположени на задния панел (Изглед от ляво на дясно).

- ON/OFF:** Превключвател за захранване.
- POWER:** Гнездото за захранване е това, в което включвате адаптера за захранване. Моля, използвайте адаптерът, доставен заедно с този TL-WR841N/TL-WR841ND 300Mbps безжичен N рутер.

- WAN:** Това е портът, в който включвате DSL/кабелен модел или Ethernet.
- 4,3,2,1 (LAN):** Тези портове (4,3,2,1) свързват рутера към локалните компютри.
- RESET:**

Има два начина за възстановяване на заводските настройки на рутера:

1) Използвайте функцията **Factory Defaults** от страница **“System Tools → Factory Defaults”** в програмата на рутера.

2) Използвайте бутон **RESET**: При включен рутер натиснете с топлика и задръжте бутон **RESET** (приблизително 5 секунди) докато SYS LED премине в бързо мигане от бавно мигане. След това отпуснете бутона и изчакайте рутерът да се възстанови до заводски настройки.

- Wireless antenna:** За получаване и изпращане на безжични данни.

Раздел 2. Свързване на рутера

2.1 Системни изисквания

- Широколентов Интернет достъп (DSL/Cable/Ethernet)
- Един DSL/кабелен модел с RJ45 конектор (което не е необходимо, ако рутерът е свързан директно към Ethernet)
- Компютри с работещ Ethernet адаптер и Ethernet кабел с RJ45 конектори
- TCP/IP протокол на всеки компютър
- Уеб браузър, като Microsoft Internet Explorer, Mozilla Firefox или Apple Safari

2.2 Изисквания за среда на инсталация

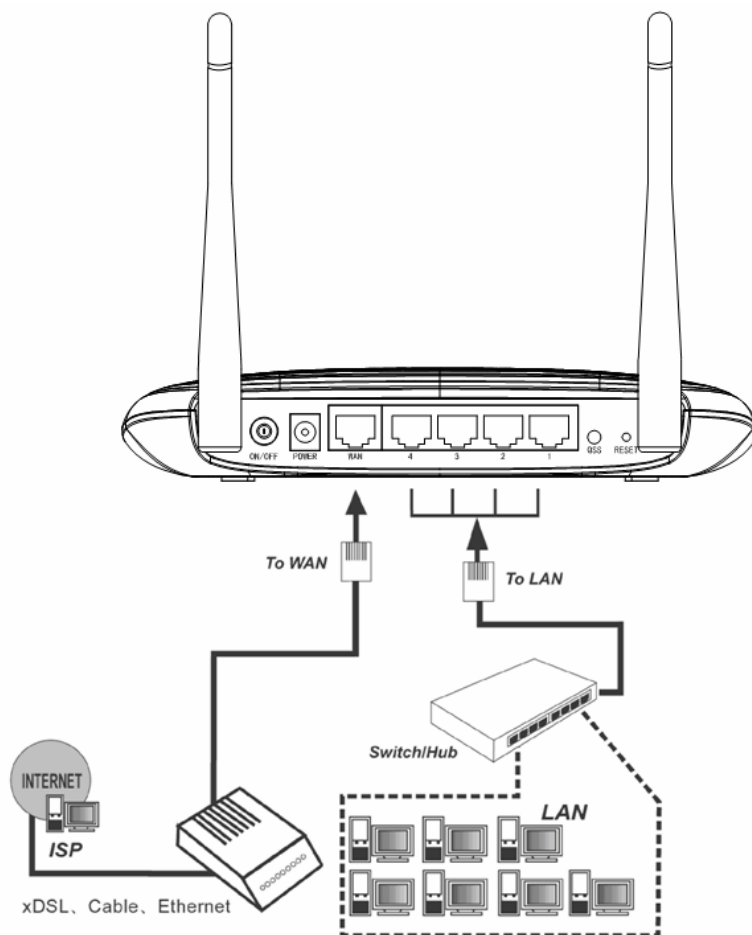
- Поставете рутера в добре вентилирано помещение далеч от отоплителни уреди или отоплителна вентилация
- Избягвайте директно облъчване от силна светлина (напр. слънчева светлина)
- Оставете поне 2 инча (5 см) свободно пространство около рутера
- Работна температура: 0°C~40°C (32°F~104°F)
- Работна влажност: 10%~90%RH, без конденз

2.3 Свързване на рутера

Преди инсталиране на рутера се уверете, че вашият компютър е успешно свързан към Интернет чрез широколентова връзка. Ако има проблем, свържете се с вашия ISP. След това моля инсталирайте рутера като следвате долупосочените стъпки. Не забравяйте да извадите захранващия щепсел и пазете ръцете си сухи.

1. Изключете вашия кабелен/DSL модем и рутера.
2. Намерете оптималното място на рутера. Най-доброто място обикновено е в центъра на вашата безжична мрежа.
3. Нагласете посоката на антената. Обикновено това е посока нагоре.
4. Свържете компютъра/ите и всеки комутатор/ концентратор във вашата LAN към LAN портовете на рутера, както е показано на Фигура 2-1. (Ако имате безжична NIC и желаете да ползвате безжичната функция, можете да пропуснете тази стъпка.)
5. Свържете DSL/кабелният модел към WAN порта на рутера, както е показано на Фигура 2-1.

6. Свържете захранващия адаптер към захранващото гнездо на рутера, а другият край към електрически извод. Рутерът трябва да започне автоматично да работи.
7. Включете кабелния/ DSL модем към захранването.



Фигура 2-1 Хардуерна инсталация на TL-WR841ND 300Mbps безжичен N рутер

Раздел 3. Указания за бърза инсталация

Този раздел ще ви покаже как да конфигурирате само за минути основните функции на своя TL-WR841ND 300Mbps безжичен N рутер с помощта на **Quick Setup Wizard**.

3.1 TCP/IP конфигурация

По подразбиране домейн името на TL-WR841ND 300Mbps безжичен N рутер е <http://tplinklogin.net>, IP адресът по подразбиране е 192.168.0.1, маската на подмрежа е 255.255.255.0). Тези стойности могат да бъдат променяни по ваше желание. В тези инструкции ние използваме за целите на описанието зададените по подразбиране стойности.

Свържете компютъра към LAN портовете на рутера. След това можете да конфигурирате IP адреса на вашия компютър по следните два начина.

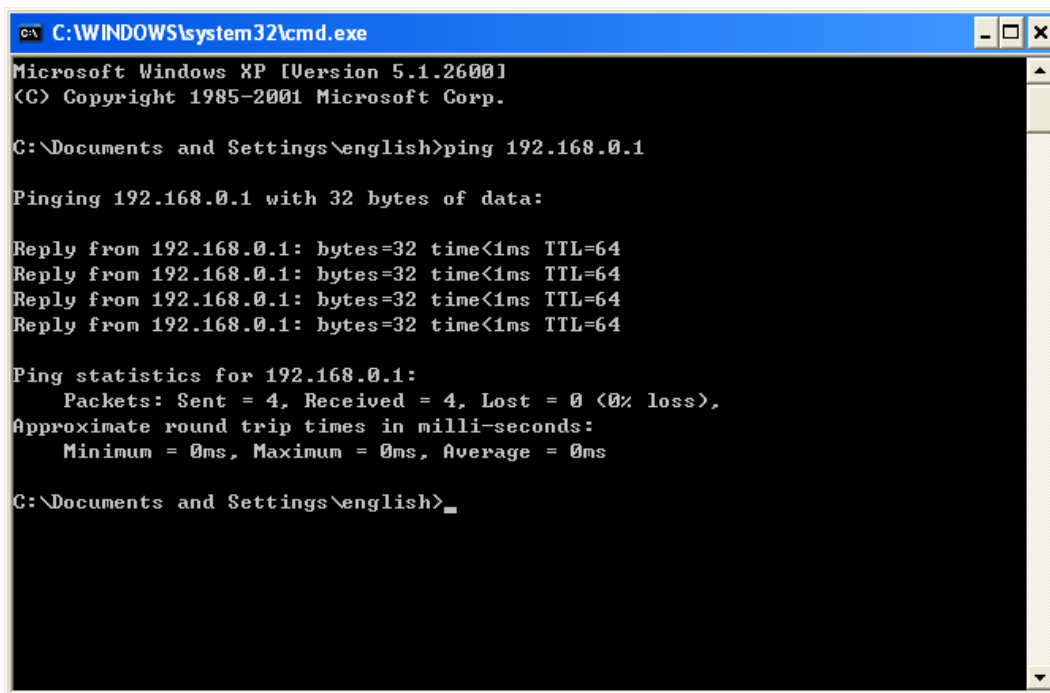
- Ръчно конфигуриране на IP адрес
 - 1) Задайте TCP/IP протокол за вашия компютър. Ако се нуждаете от указания как да направите това, моля вижте Приложение В: "[Конфигуриране на компютър](#)".
 - 2) Конфигурирайте мрежовите параметри. IP адресът е 192.168.0.xxx ("xxx" е всяко число от 2 до 254), маската на подмрежа е 255.255.255.0, а шлюзът е 192.168.0.1 (IP адресът по подразбиране на рутера)
- Автоматично получаване на IP адрес
 - 1) Настройте TCP/IP протокола в режим "Obtain an IP address automatically" (автоматично получаване на IP адрес) на вашия компютър.

Ако се нуждаете от указания как да направите това, моля вижте Приложение В: "[Конфигуриране на компютъра](#)".
 - 2) След това вграденият DHCP сървър ще зададе IP адрес за компютъра.

Сега можете да пуснете команда Ping в command prompt, за да проверите връзката между компютъра и рутера. Долният пример е за конфигурация в операционна система Windows 2000.

Отворете command prompt и напишете ping 192.168.0.1, след това натиснете Enter.

- Ако показаният резултат е подобен на Фигура 3-1, това означава, че връзката между вашия компютър и рутера е установена.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\english>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

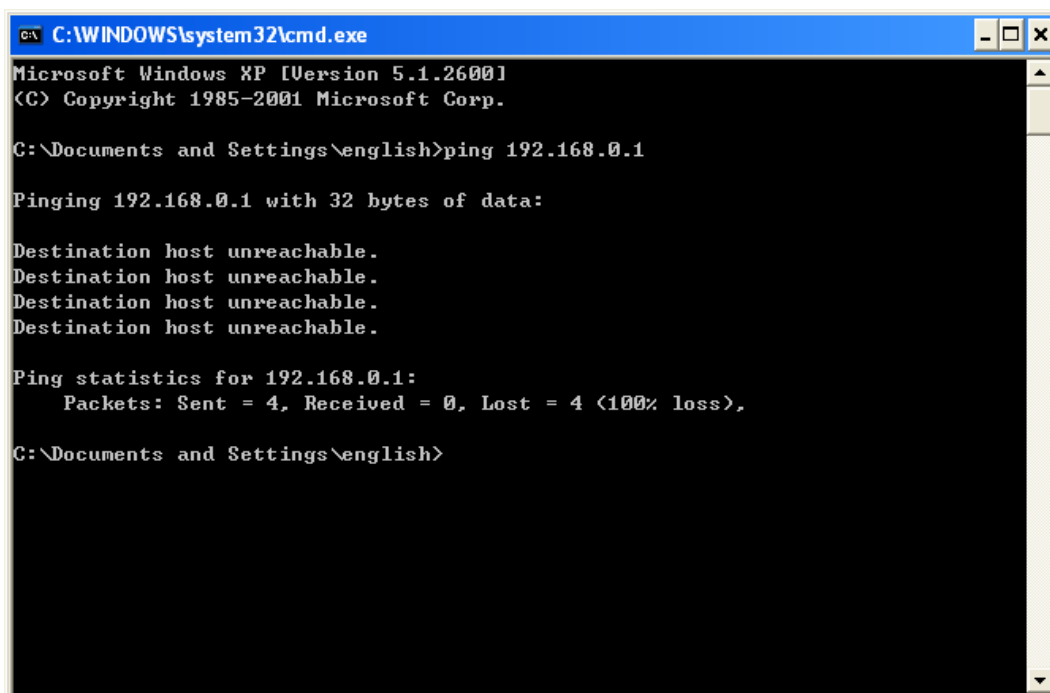
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\english>
```

Фигура 3-1 Успешен резултат след команда Ping

□ Ако показаният резултат е подобен на Фигура 3-2, това означава, че връзката между вашия компютър и рутера не е установена.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\english>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\english>
```

Фигура 3-2 Неуспешен резултат след команда Ping

Моля проверете връзката като следвате долните стъпки:

1. Правилна ли е връзката между вашия компютър и рутера?

➔ **Забележка:**

Светлинните индикатори 1/2/3/4 на LAN портове, които свързвате на рутера и светлинните индикатори на вашия адаптер за компютър трябва да светят.

2. Правилна ли е TCP/IP конфигурацията на вашия компютър?

➔ **Забележка:**

Ако IP адреса на рутера е 192.168.0.1, IP адресът на вашия компютър трябва да е в границите на 192.168.0.2 ~ 192.168.0.254.

3. Правилен ли е зададения LAN IP на рутера?

➔ **Забележка:**

Ако LAN IP на модема, свързан към вашия рутер е 192.168.0.x, зададеният LAN IP на рутера автоматично ще превключи от 192.168.0.1 на 192.168.1.1, за да избегне IP конфликт. Следователно, за да проверите мрежовата връзка между компютъра и рутера, можете да отворите command prompt (команден ред) и да напишете ping 192.168.1.1, след което натискате Enter.

3.2 Указания за бърза инсталация

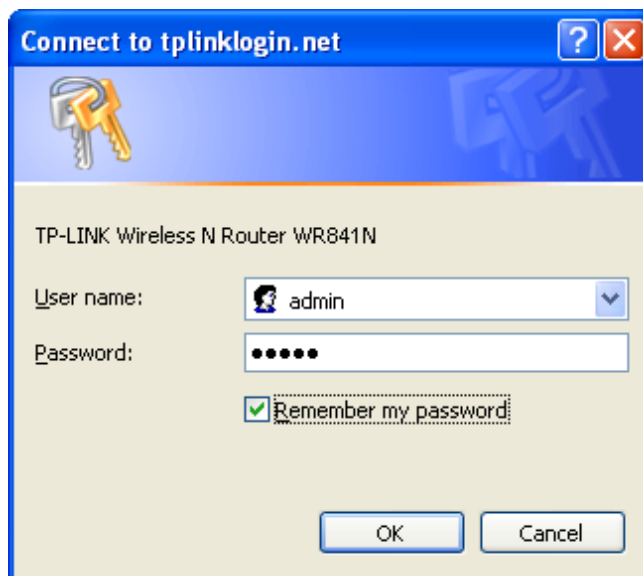
С помощта на уеб-базирана сервисна програма можете лесно да конфигурирате и управлявате TL-WR841ND 300Mbps безжичен N рутер. Уеб-базирана сервисна програма може да се използва за всяка Windows, Macintosh или UNIX ОС с уеб браузър като Microsoft Internet Explorer, Mozilla Firefox или Apple Safari.

1. За достъп до програма за конфигурация отворете браузера и напишете <http://tplinklogin.net> в полето за адреси.



Фигура 3-3 Вход с регистрация в рутера

След секунди ще се появи прозорец за регистрация, подобен на този, показан на Фигура 3-4. Въведете **admin** за потребителско име и парола, и двете с малки букви. След това натиснете бутон ОК или Enter.

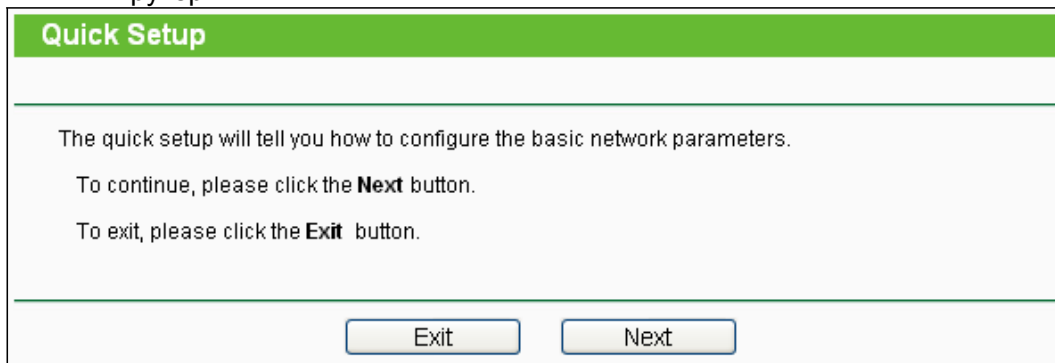


Фигура 3-4 Прозорец за регистрация

➔ **Забележка:**

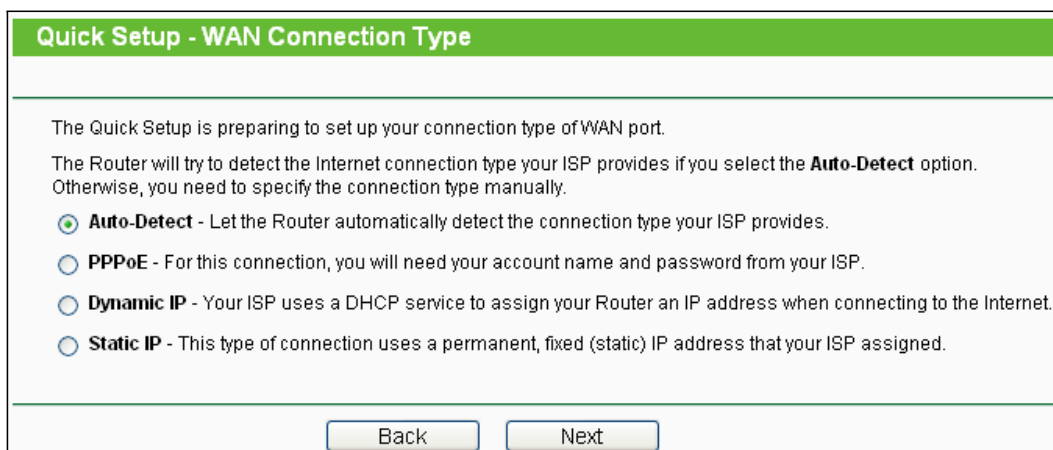
Ако горният прозорец не се покаже, това означава, че вашият уеб-браузер е настроен към прокси. Отидете в Tools menu>Internet Options>Connections>LAN Settings, в прозорецът, който се появи, махнете маркировката на Using Proxy и натиснете ОК, за да завършите.

1. След успешна регистрация натиснете меню **Quick Setup** за бързо конфигуриране на вашия рутер.



Фигура 3-5 Бърза настройка

2. Натиснете Next и ще се появи страница WAN Connection Type, показана на Фигура 3-6.



Quick Setup - WAN Connection Type

The Quick Setup is preparing to set up your connection type of WAN port.

The Router will try to detect the Internet connection type your ISP provides if you select the **Auto-Detect** option. Otherwise, you need to specify the connection type manually.

- Auto-Detect** - Let the Router automatically detect the connection type your ISP provides.
- PPPoE** - For this connection, you will need your account name and password from your ISP.
- Dynamic IP** - Your ISP uses a DHCP service to assign your Router an IP address when connecting to the Internet.
- Static IP** - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.

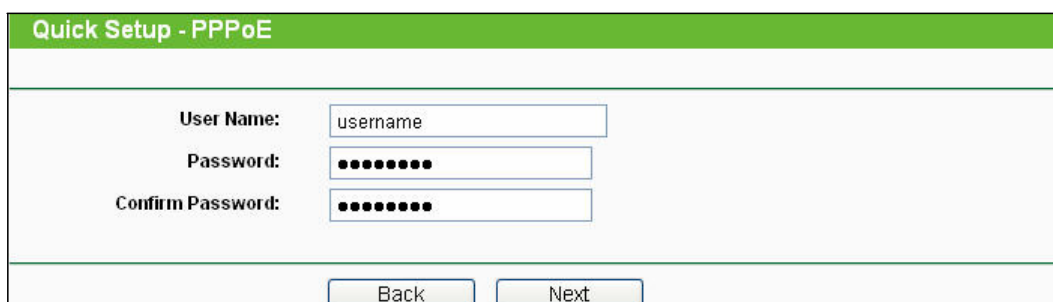
Back Next

Фигура 3-6 Тип WAN връзка

Рутерът осигурява функция Auto-Detect (автоматично откриване) и поддържа три популярни начина Dynamic IP, Static IP и PPPoE за свързване към Интернет. Препоръчваме Ви да използвате функцията Auto-Detect. Ако н сте сигурни какъв тип връзка предоставя вашия доставчик, можете да изберете всеки от типовете и след това натиснете **Next**, за да продължите с конфигурирането.

3. Ако изберете Auto-Detect, рутерът автоматично ще открие типа връзка, която вашия ISP осигурява. Уверете се, че кабелът е добре поставен в WAN порта преди началото на откриването. Когато активна Интернет връзка бъде успешно открита от рутера, ще се покаже подходяща страница за конфигуриране.

- 1) Ако типът връзка е PPPoE, ще се появи екран, както е показан на Фигура 3-7.



Quick Setup - PPPoE

User Name:

Password:

Confirm Password:

Back Next

Фигура 3-7 Бърза настройка - PPPoE

- User Name/Password** - Въведете, предоставените от вашия ISP потребителско име и парола. Тези полета са с точно определен формат. Ако имате проблеми с този процес, моля свържете се в вашия Интернет доставчик.
- Confirm Password** - Въведете отново паролата, предоставена от вашия ISP, за да сте сигурни, че това е правилната парола. Ако паролата е различна от посочената в Confirm Password, ще се появи следния екран. Натиснете **OK** и въведете отново паролата в Password и Confirm Password.



2) Ако откритият тип връзка е Dynamic IP, ще се покаже следния екран, както е показан на Фигура

Фигура 3-9. Тогава можете да продължите с конфигурацията на безжична връзка.

- Ако влизате в рутера от главен компютър, моля изберете Yes, и след това натиснете **Clone MAC Address**.

A screenshot of a web-based configuration page titled "Quick Setup - MAC Clone". The page has a green header bar. Below the header, there is a red instruction: "Please read help carefully on the right." Two radio button options are present: "Yes, I am connected by the main computer (clone MAC address)" which is selected, and "No, I am connected by another computer (do NOT clone MAC address)". Below these are two rows of input fields. The first row is labeled "WAN MAC Address:" and contains the text "F8-D1-11-61-E3-8B" and a button labeled "Restore Factory MAC". The second row is labeled "Your PC's MAC Address:" and contains the text "40-61-86-FC-74-93" and a button labeled "Clone MAC Address". At the bottom of the form are two buttons: "Back" and "Next".

Фигура 3-8 Бърза настройка – MAC разделяне

- Ако влизате в рутера от друг компютър, а не от главния, моля изберете **No**, и след това въведете MAC на главния компютър в полето **WAN MAC Address**.

A screenshot of a web-based configuration page titled "Quick Setup - MAC Clone". The page has a green header bar. Below the header, there is a red instruction: "Please read help carefully on the right." Two radio button options are present: "Yes, I am connected by the main computer (clone MAC address)" and "No, I am connected by another computer (do NOT clone MAC address)" which is selected. Below these are two rows of input fields. The first row is labeled "WAN MAC Address:" and contains the text "F8-D1-11-61-E3-8B" and a button labeled "Restore Factory MAC". The second row is labeled "Your PC's MAC Address:" and contains the text "40-61-86-FC-74-93" and a button labeled "Clone MAC Address". At the bottom of the form are two buttons: "Back" and "Next".

Фигура 3-9 Бърза настройка – MAC разделяне

3) Ако откритият тип връзка е Static IP, ще се покаже следния екран, както е показан на Фигура 3-8.

Quick Setup - Static IP

IP Address:

Subnet Mask:

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Фигура 3-8 Бърза настройка - Static IP

- IP Address** - Това е WAN IP адреса, който се вижда от външни потребители в Интернет (включително вашия ISP). Въведете IP адреса в полето.
- Subnet Mask** - Маската на подмрежа се използва за WAN IP адрес, обикновено тя е 255.255.255.0).
- Default Gateway** - Въведете IP адреса на шлюза в позицията, ако се изисква.
- Primary DNS** - Въведете IP адрес на DNS сървъра в позицията, ако е необходимо.
- Secondary DNS** - Ако вашият ISP осигурява и друг DNS сървър, въведете го тук.

4. Натиснете **Next**, за да продължите, ще се появи страница Настройки за безжична връзка, както е показано на Фигура 3-9.

Quick Setup - Wireless

Wireless Radio: (dropdown)

Wireless Network Name: (Also called the SSID)

Region: (dropdown)

Channel: (dropdown)

Mode: (dropdown)

Channel Width: (dropdown)

Max Tx Rate: (dropdown)

Wireless Security:

Disable Security


WPA/WPA2 - Personal

Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

No Change

Фигура 3-9 Бърза настройка – Безжична връзка

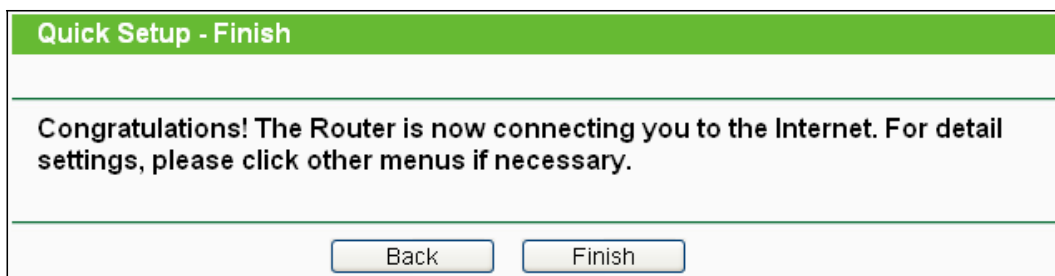
- Wireless Radio** - Активиране или деактивиране на безжично радио, с избор от падащо меню.
- Wireless Network Name** - Въведете стойност до 32 символа. Същото име SSID (мрежов идентификатор) трябва да бъде зададено на всички безжични устройства във вашата мрежа. Във връзка със сигурността на вашата безжична мрежа SSID по подразбиране трябва да е TP-LINK_XXXXXX (XXXXXX указва последните уникални шест цифри на всеки MAC адрес на рутер). Тези стойности имат точно определен формат за изписване. Например, TEST не е същото като test.
- Region** - Изберете своя регион от падащия списък. Това поле показва района, където може да се ползва безжичната функция на рутера. Може да е незаконно да ползвате безжичната функция на рутера в район, различен от този, посочен в това поле. Ако вашата страна или регион не са посочени, моля свържете се в вашата местна държавна агенция за съдействие.
 **Забележка:**
Поради местни законови ограничения версията за Северна Америка няма опция за избор на регион.
- Channel** - Това поле определя, коя работна честота ще се използва. По подразбиране каналът е зададен на Auto, така че AP ще избере автоматично най-добрия канал. Не е необходимо да променяте безжичния канал, освен ако забележите намеса с друга близкостояща точка за достъп.
- Mode** - Това поле определя безжичния режим, на който работи рутера.
- Channel Width** - Изберете ширина на канала от падащия списък. Настройката по подразбиране е автоматична, което позволява автоматично настройване на каналната ширина за вашите клиенти.
- Max Tx Rate** - В това поле можете да ограничите максималната скорост на предаване на рутера.
- Disable Security** - Функцията за безжична сигурност може да бъде включвана или изключвана. Ако е изключена, безжичните станции ще могат да се свързват с рутера без кодиране. Силно препоръчване да изберете една от следните опции за активиране на сигурността.
- WPA-PSK/WPA2-PSK** - Избор на WPA на база на предварително определен код/фраза.
 - ◆ **PSK Password** - Можете да въведете **ASCII** или **Hexadecimal** символи.
За **ASCII** ключът може да се състои от числата от 0 до 9 и всяка буква от А до Z, дължината трябва да е между 8 и 63 символа.
За **Hexadecimal** ключът може да се състои от числата от 0 до 9 и букви от А до F, дължината трябва да е между 8 и 64 символа.
Моля имайте предвид, че ключът има определен формат, като това означава, че главни или малки букви оказват влияние. Добра идея е да запишете ключа и всички настройки за безжична сигурност.

- ◆ No Change - Ако изберете тази опция, конфигурацията за безжична сигурност няма да се промени!

Тези настройки са само за базови безжични параметри. За допълнителни настройки, моля вижте [4.6 Безжична връзка](#).

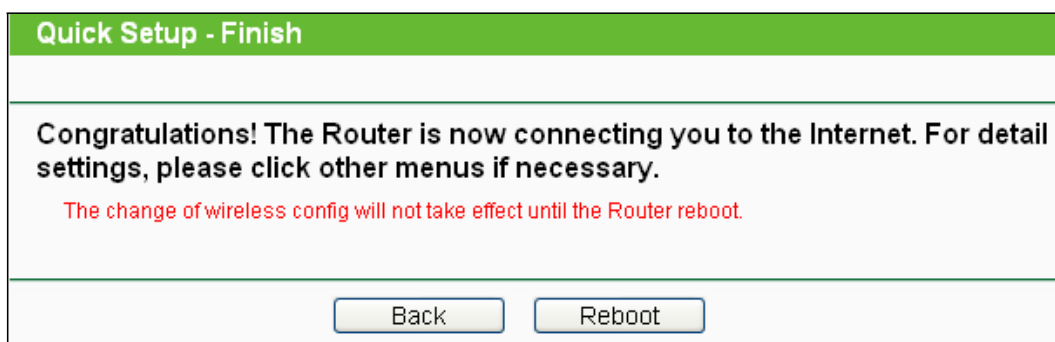
5. Натиснете бутон **Next**. Ще се отвори страница **Finish**.

- Ако не правите промени в страница Wireless, страница Finish ще изглежда както е показано на Фигура 3-10. Натиснете бутон Finish, за да завършите Бързата настройка.



Фигура 3-10 Бърза настройка - Завършване

- Ако има промени по страница Wireless, страница Finish ще е като тази, показана на Фигура 3-11. Натиснете бутон Reboot, за да потвърдите безжичната конфигурация и да завършите Бързата настройка.



Фигура 3-11 Бърза настройка – Завършване

Раздел 4. Конфигуриране на рутера

Този раздел показва най-важните функции на всяка уеб страница и начина на конфигуриране.

4.1 Регистрация за вход

След успешна регистрация ще видите петнадесет основни менюта вляво на уеб-базираната сервисна програма. Вдясно има съответни обяснения и инструкции.

| |
|--------------------|
| Status |
| Quick Setup |
| QSS |
| Network |
| Wireless |
| DHCP |
| Forwarding |
| Security |
| Parental Control |
| Access Control |
| Advanced Routing |
| Bandwidth Control |
| IP & MAC Binding |
| Dynamic DNS |
| System Tools |

Подробните обяснения за основните функции на всяка уеб страница са описани по-долу.

4.2 Статус

Страница Статус ви дава информация за текущия статус на рутера. Цялата информация може да се ползва само за четене.

| Status | | |
|---------------------------|--------------------------------|--|
| Firmware Version: | 3.13.4 Build 111108 Rel.32821n | |
| Hardware Version: | WR841N v6/V7 00000000 | |
| LAN | | |
| MAC Address: | F8-D1-11-61-E3-8A | |
| IP Address: | 192.168.0.1 | |
| Subnet Mask: | 255.255.255.0 | |
| Wireless | | |
| Wireless Radio: | Enable | |
| Name (SSID): | TP-LINK_61E38A | |
| Channel: | Auto (Current channel 5) | |
| Mode: | 11bgn mixed | |
| Channel Width: | Automatic | |
| Max Tx Rate: | 300Mbps | |
| MAC Address: | F8-D1-11-61-E3-8A | |
| WDS Status: | Disable | |
| WAN | | |
| MAC Address: | F8-D1-11-61-E3-8B | |
| IP Address: | 0.0.0.0 | Dynamic IP |
| Subnet Mask: | 0.0.0.0 | |
| Default Gateway: | 0.0.0.0 | <input type="button" value="Renew"/> |
| DNS Server: | 0.0.0.0 , 0.0.0.0 | |
| Traffic Statistics | | |
| | Received | Sent |
| Bytes: | 0 | 0 |
| Packets: | 0 | 0 |
| System Up Time: | 0 days 00:01:33 | <input type="button" value="Refresh"/> |

Фигура 4-1 Статус на рутера

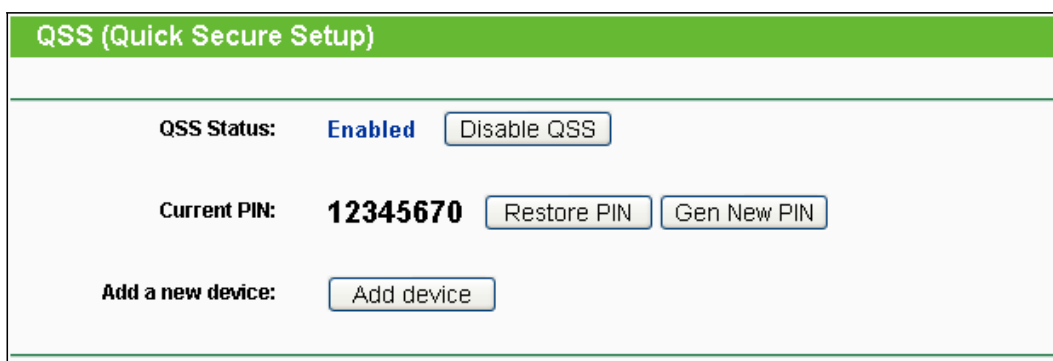
4.3 Бърза настройка

Моля вижте [3.2 Указания за бърза инсталация](#).

4.4 QSS

Тук ще получите указания за добавяне на ново безжично устройство към съществуваща мрежа като изберете функцията **QSS (Quick Secure Setup)**.

а). Изберете меню “QSS” и ще се покаже следния екран (вижте Фигура 4-2).



Фигура 4-2 QSS

- QSS Status** - Тук активирате и деактивирате QSS функцията.
- Current PIN** - Показва се текущата стойност на PIN на рутера. По подразбиране PIN на рутера можете да видите на етикета или в Ръководството на потребителя.
- Restore PIN** - Възстановяване на PIN на рутера до стойността по подразбиране.
- Gen New PIN** - Натиснете този бутон и тогава можете да генерирате нова, случайна стойност за PIN на рутера. Можете да осигурите мрежовата сигурност чрез генерирането на нов PIN.
- Add device** - Можете да добавите ново устройство към съществуваща мрежа ръчно чрез избор на този бутон.

б) За добавяне на ново устройство:

Ако безжичен адаптер поддържа Wi-Fi Protected Setup (WPS), можете да установите безжична връзка между безжичен адаптер и рутер като използвате или Push Button Configuration (PBC) метод или PIN метод.

→ **Забележка:**

За изграждане на успешна връзка от QSS трябва да направите и съответната конфигурация на новото устройство за QSS функция.

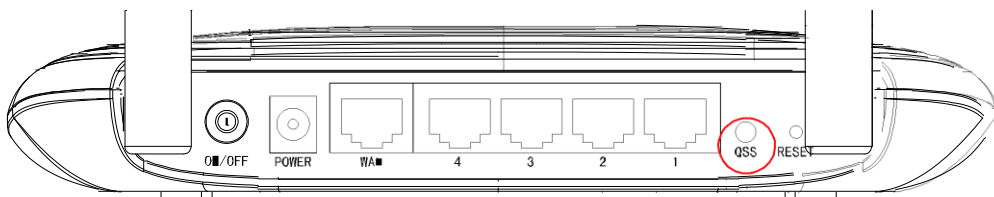
За конфигурация на ново устройство, вземаме за пример безжичен адаптер.

I. Чрез PBC

Ако безжичният адаптер поддържа Wi-Fi Protected Setup и Push Button Configuration (PBC) метод, можете да го добавите към мрежата чрез PBC по следните два начина:

Първи начин:

Стъпка 1: Натиснете бутон QSS на предния панел на рутера.

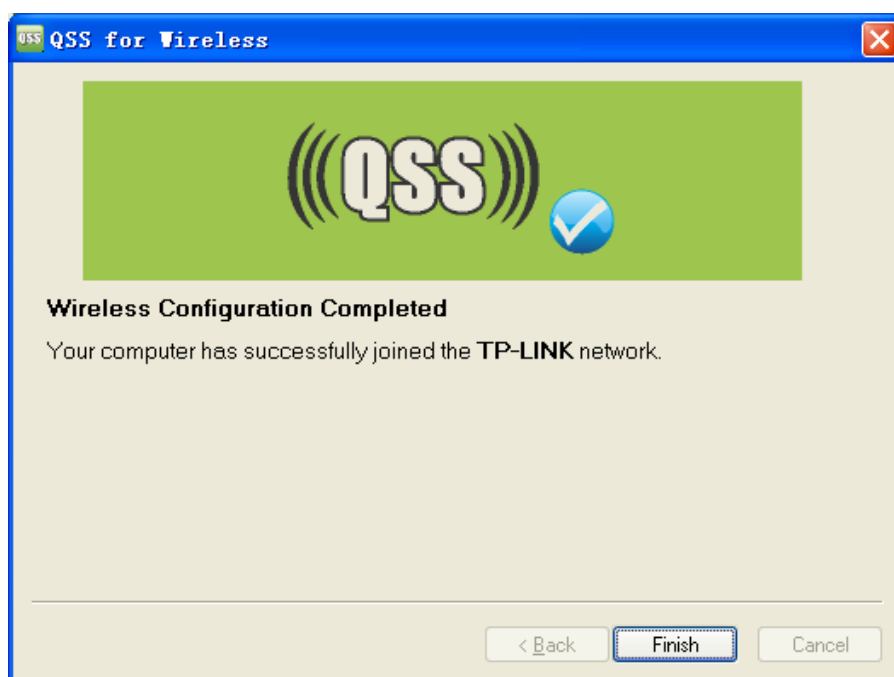


Стъпка 2: Натиснете и задръжте бутон QSS на адаптера за 2 или 3 секунди.



Стъпка 3: Изчакайте малко до появяването на следния екран. Натиснете **Finish** за завършване на QSS

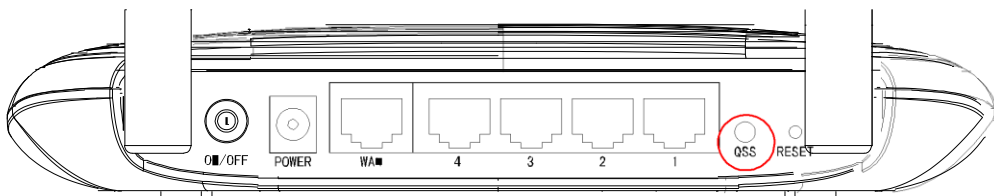
конфигурацията.



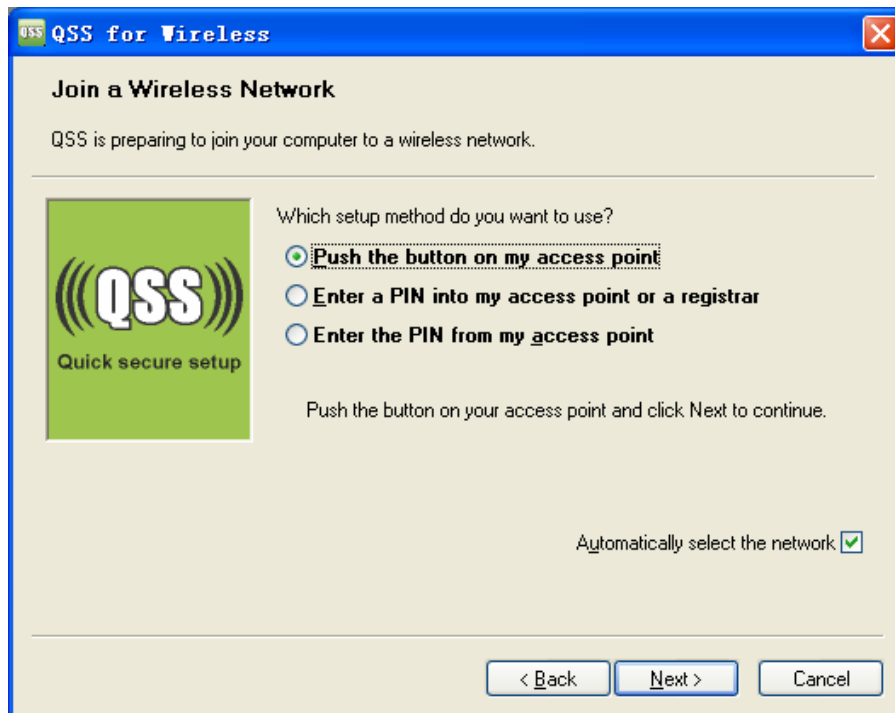
Екран за QSS конфигурация на безжичен адаптер

Втори начин:

Стъпка 1: Натиснете бутон QSS на предния панел на рутера.

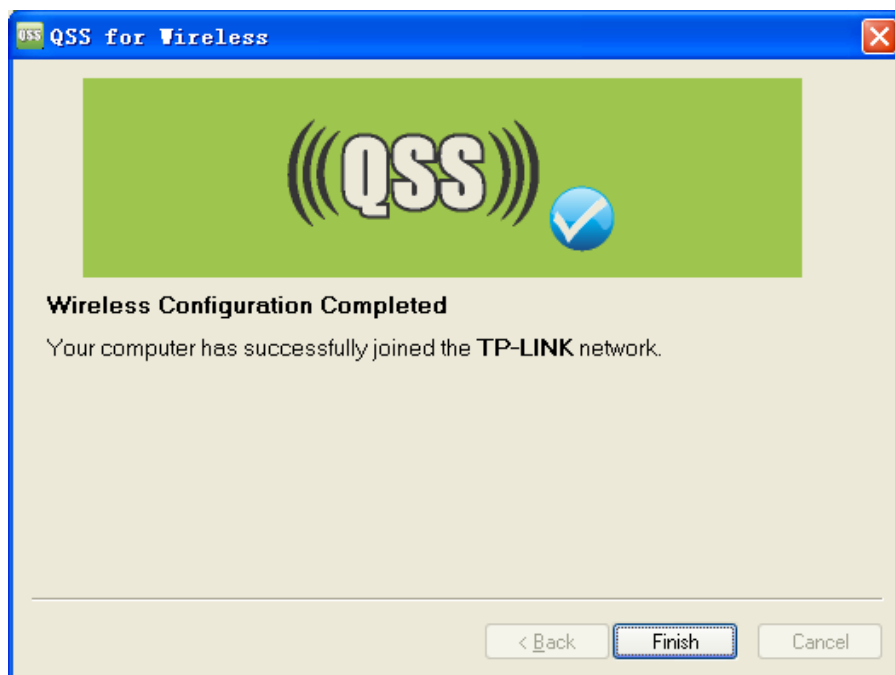


Стъпка 2: За конфигуриране на безжичния адаптер, моля изберете **“Push the button on my access point”** в програмата за конфигурация на QSS, както е показано по-долу и натиснете **Next**.



Екран за QSS конфигурация на безжичен адаптер

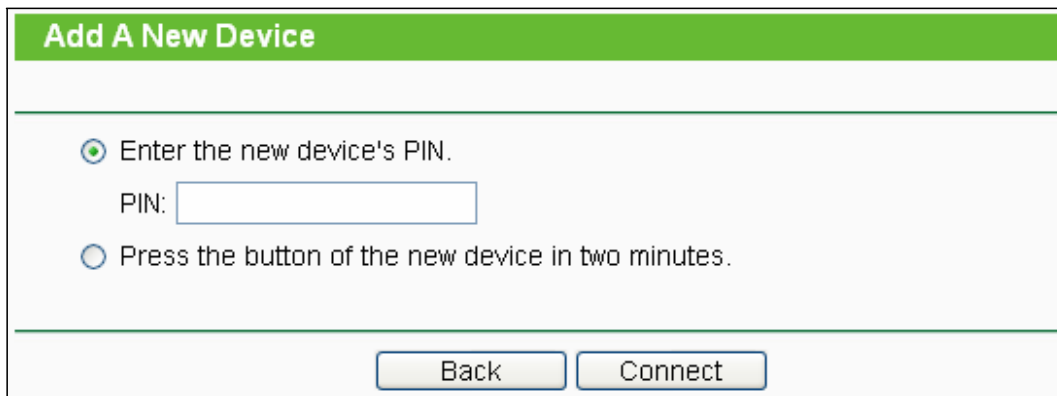
Стъпка 3: Изчакайте до появата на следния екран. Натиснете **Finish** за завършване на QSS конфигурацията.



Екран за QSS конфигурация на безжичен адаптер

Трети начин

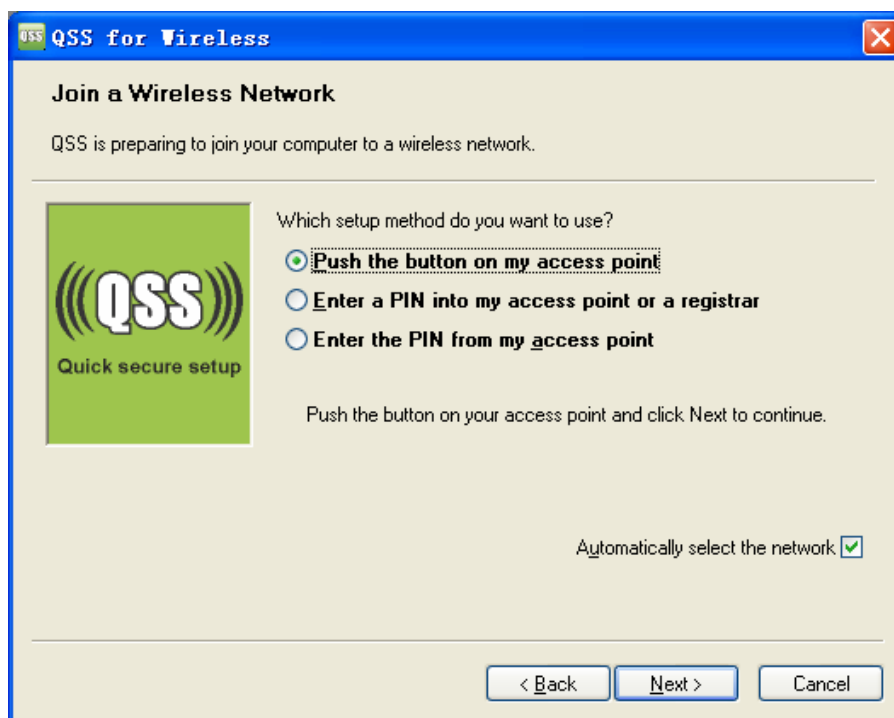
Стъпка 1: Запазете QSS статуса по подразбиране като Enabled и натиснете бутон Add device както на Фигура 4-2, ще се появи следния екран.



Фигура 4-3 Добавяне на ново устройство

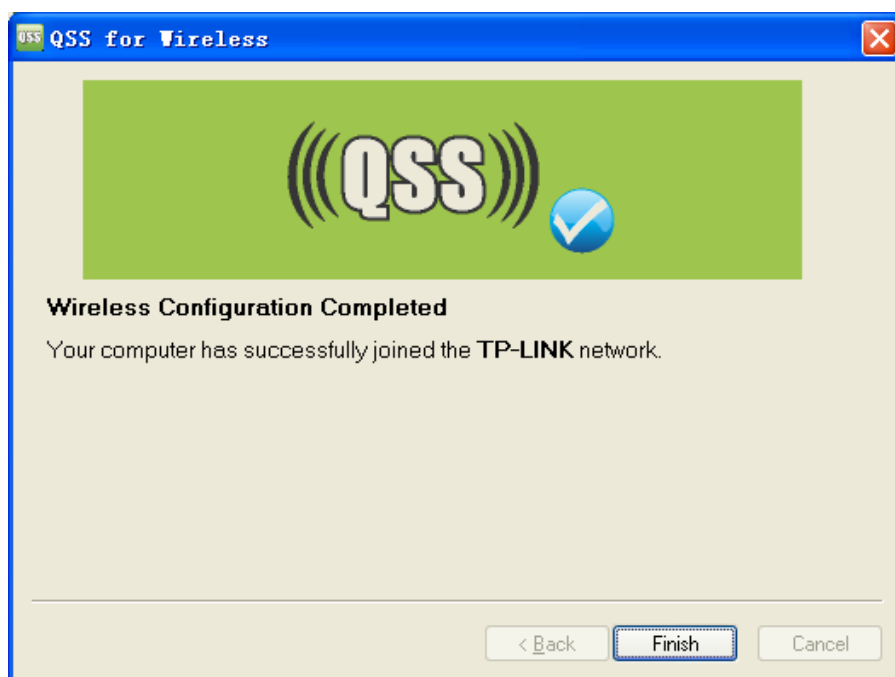
Стъпка 2: Изберете “Press the button of the new device in two minutes” и натиснете Connect.

Стъпка 3: За конфигуриране на безжичния адаптер, моля изберете “**Push the button on my access point**” в програмата за конфигурация на QSS, както е показано по-долу и натиснете **Next**.



Екран за QSS конфигурация на безжичен адаптер

Стъпка 4: Изчакайте до появата на следния екран. Натиснете **Finish** за завършване на QSS конфигурацията.



Екран за QSS конфигурация на безжичен адаптер

II. Чрез PIN

Ако новото устройство поддържа Wi-Fi Protected Setup и PIN метод, можете да го добавите към мрежата чрез PIN по следните два начина.

Първи начин: Въведете PIN в рутера

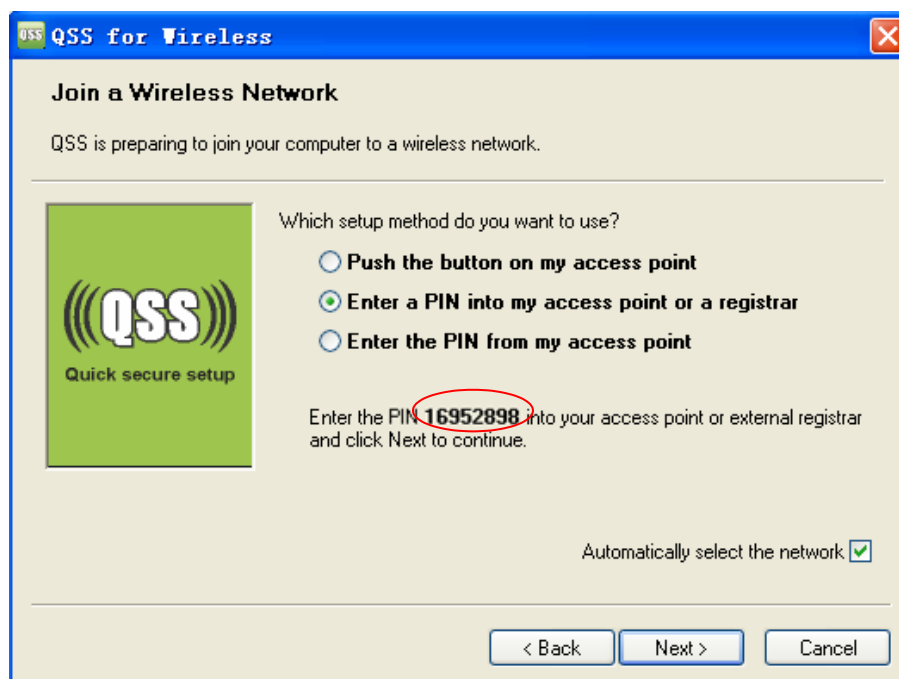
Стъпка 1: Запазете QSS статуса по подразбиране като Enabled и натиснете бутон Add device както на Фигура 4-2, ще се появи следния екран.

Стъпка 2: Изберете “**Enter the new device's PIN**” и въведете PIN кода на безжичния адаптер в полето след **PIN**, както е показано на горната фигура. След това натиснете бутон Connect.

➔ **Забележка:**

PIN кодът на адаптера винаги е показана на екрана за QSS конфигурация.

Стъпка 3: За конфигурация на безжичния адаптер, моля изберете “**Enter a PIN into my access point or a registrar**” в програмата за конфигурация на QSS и натиснете **Next**.



Екран за QSS конфигурация на безжичен адаптер



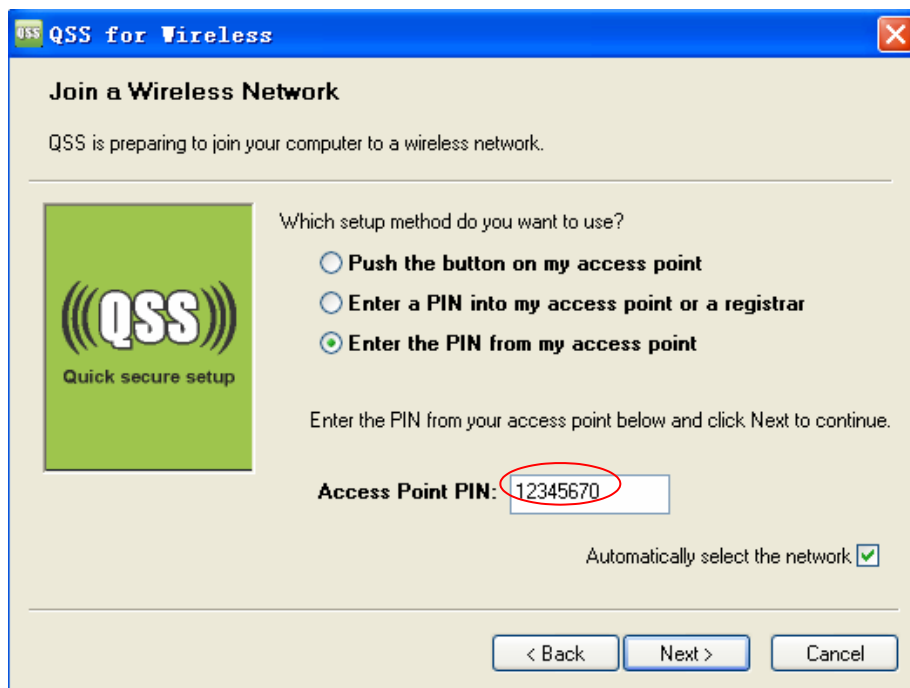
Забележка:

В този пример PIN кодът на този адаптер е 16952898, както е показано на горната фигура.

Втори начин: Въведете PIN от рутера

Стъпка 1: Вижте текущия PIN код на рутера на Фигура 4-2 (всеки рутер има свой уникален PIN код. Тук PIN кодът е 12345670, на рутера от примера).

Стъпка 2: За конфигуриране на безжичен адаптер, моля изберете “**Enter a PIN from my access point**” в програмата за конфигурация на QSS, както е показано по-долу и въведете PIN кода на рутера в поле “**Access Point PIN**”. След това натиснете **Next**.



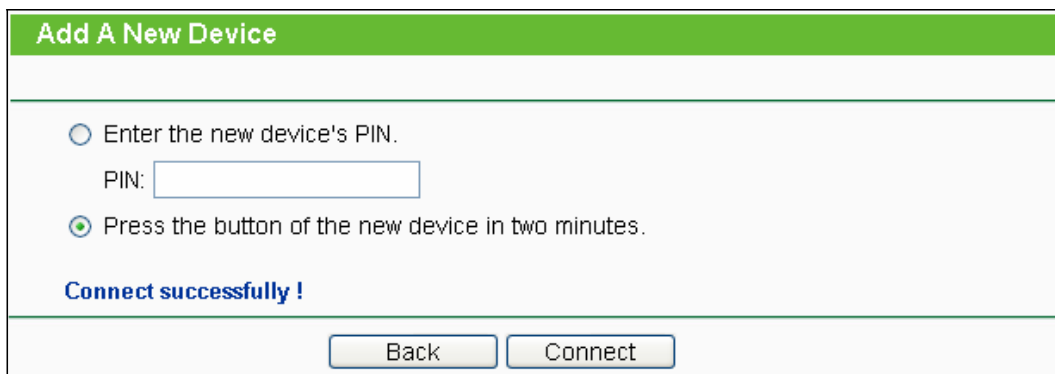
Екран за QSS конфигурация на безжичен адаптер



Забележка:

PIN кодът по подразбиране на рутера може да бъде намерен на табелката или на екрана за QSS конфигурация, показан на Фигура 4-2.

с). Ще видите следния екран при успешно свързване на новото устройство към мрежата.

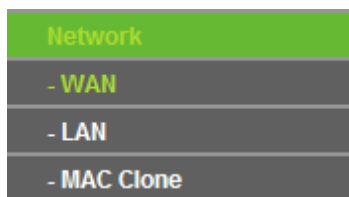


Забележка:

- 1) Светлинният индикатор за QSS на рутера ще свети зелено за пет минути, ако устройството е успешно добавено към мрежата.
- 2) QSS функцията не може да бъде конфигурирана, ако функцията за безжична връзка на рутера е де-активирана.

Уверете се, че тази функция е активирана преди за започнете конфигуриране на QSS.

4.5 Мрежа



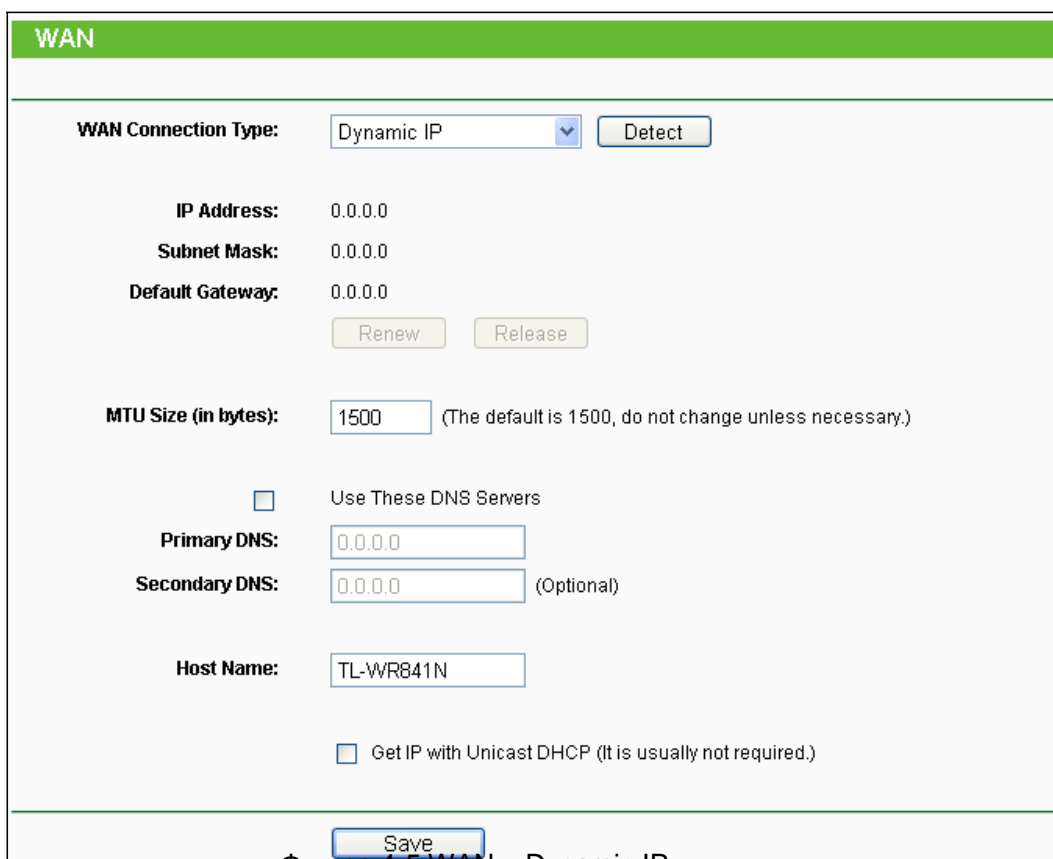
Фигура 4-4 Меню Мрежа

Има три подменюта под меню Network (показани на Фигура 4-4): **LAN**, **WAN** и **MAC Clone**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция.

4.5.1 WAN

Като изберете меню “Network → WAN”, можете да конфигурирате IP параметрите на WAN в показания по-долу екран.

1. Ако вашия ISP предоставя DHCP услугата, моля изберете тип Dynamic IP и рутерът автоматично ще получи IP параметрите от вашия ISP. Ще видите долната страница (Фигура 4-5):

A screenshot of the WAN configuration page. The title is 'WAN'. The 'WAN Connection Type' is set to 'Dynamic IP' with a 'Detect' button. Below are fields for 'IP Address', 'Subnet Mask', and 'Default Gateway', all set to '0.0.0.0'. There are 'Renew' and 'Release' buttons. The 'MTU Size (in bytes)' is set to '1500' with a note: '(The default is 1500, do not change unless necessary.)'. There is a checkbox for 'Use These DNS Servers' which is unchecked. Below are fields for 'Primary DNS' and 'Secondary DNS', both set to '0.0.0.0' with '(Optional)' next to the secondary field. The 'Host Name' is set to 'TL-WR841N'. At the bottom, there is a checkbox for 'Get IP with Unicast DHCP (It is usually not required.)' which is unchecked, and a 'Save' button.

Фигура 4-5 WAN – Dynamic IP

Тази страница показва WAN IP параметрите, зададени динамично от вашия ISP, включително IP адрес, маска на подмрежа, шлюз и др. Натиснете бутон **Renew** за обновяване на IP параметрите от вашия ISP. Натиснете бутон Release, за да освободите IP параметрите.

- **MTU Size** - Нормалната MTU (максимален размер на предаваем блок данни) стойност за повечето Ethernet мрежи е 1500 байта. Не се препоръчва да промените зададения MTU Size освен ако това не се изисква от вашия ISP.
- **Use These DNS Servers** - Ако вашият ISP ви дава един или два DNS адрес, изберете Use These DNS Servers и въведете първичен и вторичен адрес в правилните полета. В противен случай DNS сървърите ще бъдат зададени динамично от вашия ISP.

➔ **Забележка:**

Ако откриете грешка, когато отидете на уеб сайт след влизане в DNS адреси, е вероятно вашите DNS сървъри да не са правилно настроени. Трябва да се свържете с вашия ISP, за да получите адреса на DNS сървър.

- **Host Name** - Тази опция определя хост името на рутера.
- **Get IP with Unicast DHCP** - Някои DHCP сървъри на доставчици не поддържат приложения за излъчване. Ако не можете да получите IP адрес нормално, можете да изберете тази опция. (Много рядко се налага.) Натиснете бутон Save, за да запазите настройките.

2. Ако вашия ISP предоставя статичен или фиксиран IP адрес, маска за подмрежа, шлюз и DNS настройка, изберете Static IP. Ще се появи страница Static IP settings, както е показана на Фигура 4-6.

The screenshot shows the WAN configuration interface. At the top, there is a green bar with the text 'WAN'. Below this, the 'WAN Connection Type' is set to 'Static IP' with a dropdown arrow and a 'Detect' button. The 'IP Address' field contains '0.0.0.0'. The 'Subnet Mask' field contains '0.0.0.0'. The 'Default Gateway' field contains '0.0.0.0' with '(Optional)' next to it. The 'MTU Size (in bytes)' field contains '1500' with a note '(The default is 1500, do not change unless necessary.)'. The 'Primary DNS' field contains '0.0.0.0' with '(Optional)' next to it. The 'Secondary DNS' field contains '0.0.0.0' with '(Optional)' next to it. At the bottom of the form, there is a 'Save' button.

Фигура 4-6 WAN - Static IP

- **IP Address** - Въведете IP адреса в десетичен формат с разделителни точки, предоставен от вашия ISP.
- **Subnet Mask** - Въведете маска за подмрежа в десетичен формат с разделителни точки, предоставена от вашия доставчик, обикновено това е 255.255.255.0.
- **Default Gateway** - (По избор) Въведете IP адрес на шлюз в десетичен формат с

разделителни точки, предоставен от вашия ISP.

- MTU Size** - Обичайната MTU (максимален размер на предаваем блок данни) стойност за повечето Ethernet мрежи е 1500 байта. Не се препоръчва да промените зададения MTU Size освен ако това не се изисква от вашия ISP.
- Primary/Secondary DNS** - (По избор) Въведете един или два DNS адреса в десетичен формат с разделителни точки, предоставен от вашия ISP.

Натиснете бутон Save, за да запазите настройките.

3. Ако вашия ISP осигурява PPPoE връзка, изберете опция PPPoE/Russia PPPoE. И трябва да въведете следните параметри (Фигура 4-7):

WAN

WAN Connection Type: PPPoE/Russia PPPoE Detect

PPPoE Connection:

User Name: username

Password: ●●●●●●

Secondary Connection: Disabled Dynamic IP Static IP (For Dual Access/Russia PPPoE)

Wan Connection Mode: Connect on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting
Period of Time: from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

Connect Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)

Connect Disconnect Disconnected!

Save Advanced

Фигура 4-7 WAN - PPPoE

- User Name/Password** - Въведете, предоставените от вашия ISP потребителско име и парола. Тези полета са имат точно определен формат за изписване.
- Secondary Connection** - наличен е само за PPPoE връзка. Ако вашия ISP осигурява допълнителен тип връзка, като Dynamic/Static IP за свързване към локална мрежа, тогава можете да маркирате радио-бутона на Dynamic/Static IP, за да активирате тази вторична връзка.
 - ◆ **Disabled** - Вторичната връзка е изключена по подразбиране, затова има само PPPoE връзка. Това се и препоръчва.
 - ◆ **Dynamic IP** - Можете да маркирате този радио-бутон, за да използвате Dynamic IP като вторична връзка за свързване към локалната мрежа, предоставена от ISP.
 - ◆ **Static IP** - Можете да маркирате този радио-бутон, за да използвате Static IP като

вторична връзка за свързване към локалната мрежа, предоставена от ISP.

- Connect on Demand** - В този режим Интернет връзката може да бъде прекратена автоматично след определен период на бездействие (Max Idle Time) и да бъде възстановена, когато се опитате да получите отново достъп до Интернет. Ако искате вашата Интернет връзка да се запази активна през цялото време, въведете "0" в поле **Max Idle Time**. В противен случай въведете броя минути, които искате да изминат преди вашия Интернет достъп да прекъсне.
- Connect Automatically** - Връзката може да бъде възстановена автоматично след пропадането ѝ.
- Time-based Connecting** - Връзката ще се създава в период от начално до крайно зададено време (и двете във HH:MM формат).

→ **Забележка:**

Само когато сте конфигурирали системното време на страница "System Tools → Time Settings", функцията Time-based Connecting може да се включи.

- Connect Manually** - Можете да натиснете бутон Connect/Disconnect за незабавно свързване/ прекъсване. Този режим поддържа и функция Max Idle Time като режим Connect on Demand. Интернет връзката може да се прекъсва автоматично след определен период на бездействие и възстановяване при опит за достъп до Интернет. Натиснете бутон Connect за незабавно свързване. Натиснете бутон Disconnect за незабавно прекъсване.

Внимание: Понякога връзката не може да бъде прекъсвана, въпреки че сте посочили време в Max Idle Time, тъй като някои приложения "посещават" Интернет постоянно на заден план.

Ако искате да направите по-специална конфигурация, моля натиснете бутон Advanced и ще се покаже страницата, показана на Фигура 4-8:

Фигура 4-8 PPPoE специални настройки

- MTU Size** - Зададеният размер за MTU е "1480" байта, което обикновено е добре. Не се препоръчва да промените зададения MTU Size освен ако това не се изисква от вашия ISP.
- Service Name/AC Name** - Сервизното име и AC (Концентратор за достъп) името не трябва да бъдат конфигурирани освен ако не сте сигурни, че вашия ISP изисква това. В повечето случаи можете да оставите тези полета празни.
- ISP Specified IP Address** - Ако вашият ISP не зададе автоматично IP адреси на рутера по време на регистрацията, моля отбележете позицията "Use IP address specified by ISP" и въведете IP адрес, предоставен от вашия ISP в десетичен формат с разделителни точки.
- Detect Online Interval** - Рутерът ще открие Access Concentrator онлайн на всеки интервал. Зададената стойност е "0". Можете да въведете стойност между "0" и "120". Стойността "0" означава, че няма откриване.
- Primary DNS/Secondary DNS** - Ако вашият ISP не задава автоматично DNS адреси на рутера по време на регистрацията, моля натиснете "Use the following DNS servers" и въведете IP адреса в десетичен формат с разделителни точки, отнасящ се до първичния DNS сървър на вашия доставчик. Ако има и адрес на вторичен DNS сървър, въведете и него. Натиснете бутон Save, за да запазите настройките.

4. Ако вашия ISP доставя BigPond кабелна (или Heart Beat Signal) връзка, моля изберете

BigPond Cable. И трябва да въведете следните параметри (Фигура 4-9):

The screenshot shows the WAN configuration interface. At the top, there is a green header with the text "WAN". Below the header, the "WAN Connection Type" is set to "BigPond Cable" in a dropdown menu. The "User Name" field contains "username" and the "Password" field is masked with dots. The "Auth Server" field contains "sm-server" and the "Auth Domain" field is empty. The "MTU Size (in bytes)" is set to "1500" with a note: "(The default is 1500, do not change unless necessary.)". There are three radio button options for connection mode: "Connect on Demand" (selected), "Connect Automatically", and "Connect Manually". Each option has a "Max Idle Time" field set to "15" minutes, with a note: "(0 means remain active at all times.)". At the bottom, there are three buttons: "Connect" (blue), "Disconnect" (yellow), and "Disconnected!" (blue text). A "Save" button is located at the very bottom of the form.

Фигура 4-9

- User Name/Password** - Въведете, предоставените от вашия ISP потребителско име и парола. Тези полета са имат точно определен формат за изписване.
- Auth Server** - Въведете IP адрес или хост име на сървър за аутентификация.
- Auth Domain** - Напишете името на сървъра на база на вашето място, напр.
NSW / ACT - nsw.bigpond.net.au
VIC / TAS / WA / SA / NT - vic.bigpond.net.au
QLD - qld.bigpond.net.au
- MTU Size** - Обичайната MTU (максимален размер на предаваем блок данни) стойност за повечето Ethernet мрежи е 1500 байта. Не се препоръчва да променяте зададения MTU Size освен ако това не се изисква от вашия ISP.
- Connect on Demand** - В този режим Интернет връзката може да бъде прекратена автоматично след определен период на бездействие (Max Idle Time) и да бъде възстановена, когато се опитате да получите отново достъп до Интернет. Ако искате вашата Интернет връзка да е активна през цялото време, моля въведете "0" в поле Max Idle Time. В противен случай въведете броя минути, които искате да изминат преди вашия Интернет достъп да прекъсне.
- Connect Automatically** - Връзката може да бъде възстановена автоматично след пропадането ѝ.
- Connect Manually** - Можете да натиснете бутон Connect/Disconnect за незабавно свързване/ прекъсване. Този режим поддържа и функция Max Idle Time като режим Connect on Demand. Интернет връзката може да се прекъсва автоматично след определен период на бездействие и възстановяване при опит за достъп до Интернет.

Натиснете бутон Connect за незабавно свързване. Натиснете бутон Disconnect за незабавно прекъсване.

Внимание: Понякога връзката не може да бъде прекъсвана, въпреки че сте посочили време в Max Idle Time, тъй като някои приложения "посещават" Интернет постоянно на заден план. Натиснете бутон Save, за да запазите настройките.

5. Ако вашият ISP осигурява L2TP връзка, моля изберете опцията L2TP/Russia L2TP. И трябва да въведете следните параметри (Фигура 4-10):

WAN

WAN Connection Type: L2TP/Russia L2TP

User Name: username

Password: ●●●●●●

Disconnected!

Dynamic IP Static IP

Server IP Address/Name: [Empty]

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): 1460 (The default is 1460, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

WAN Connection Mode: Connect on Demand
 Connect Automatically
 Connect Manually

Фигура 4-10

- **User Name/Password** - Въведете, предоставените от вашия ISP потребителско име и парола. Тези полета са имат точно определен формат за изписване.
- **Dynamic IP/ Static IP** - Изберете според това, което е предоставено от вашия ISP. Натиснете бутон Connect за незабавно свързване. Натиснете бутон Disconnect за незабавно прекъсване.
- **Connect on Demand** - Можете да конфигурирате рутера да прекъсва Интернет връзката след определен период на бездействие (Max Idle Time). Ако вашата Интернет връзка е прекъсната поради бездействие, Connect on Demand позволява на рутера да възстанови автоматично връзката веднага след като се опитате отново да получите достъп до Интернет. Ако искате да активирате Connect on Demand, натиснете радиобутона. Ако искате вашата Интернет връзка да остане активна през цялото време, въведете 0 в поле Max Idle Time. В противен случай въведете броя минути, които искате да изминат преди вашата Интернет връзка да бъде прекъсната.

- Connect Automatically** - Автоматично свързване след прекъсване на рутера. За да ползвате тази опция, изберете радио-бутон.
- Connect Manually** - Можете да конфигурирате рутера за ръчно свързване или прекъсване.

След определен период н бездействие (Max Idle Time) рутерът ще прекъсне Интернет връзката и няма да можете да възстановите връзката автоматично веднага след като опитате да получите отново достъп до Интернет. За да ползвате тази опция, изберете радио-бутон. Ако искате вашата Интернет връзка да остане активна през цялото време, въведете 0 в поле Max Idle Time. В противен случай въведете броя минути, през които искате да имате Интернет до поискване нов линк.

Внимание: Понякога връзката не може да бъде прекъсната дори да посочите време в Max Idle Time, тъй като някои приложения ползват Интернет постоянно. Натиснете бутон Save, за да запазите настройките.

6. Ако вашият ISP осигурява PPTP връзка, моля изберете опция PPTP/Russia PPTP. И трябва да въведете следните параметри (Фигура 4-11):

WAN

WAN Connection Type: PPTP/Russia PPTP

User Name: username

Password: ●●●●●●●●

Disconnected!

Dynamic IP Static IP

Server IP Address/Name: [Empty field]

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0 , 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): 1420 (The default is 1420, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

WAN Connection Mode:

Connect on Demand

Connect Automatically

Connect Manually

Фигура 4-11 PPTP настройки

- **User Name/Password** - Въведете, предоставените от вашия ISP потребителско име и парола. Тези полета са имат точно определен формат за изписване.
- **Dynamic IP/ Static IP** - Изберете посоченото ви от вашия ISP и въведете IP адреса на ISP или името на домейна.

Ако изберете статичен IP и въведете името на домейна, трябва да въведете и DNS, зададен от вашия ISP. И натиснете бутон Save.

Натиснете бутон Connect за незабавно свързване. Натиснете бутон Disconnect за незабавно прекъсване.

- **Connect on Demand** - Можете да конфигурирате рутера за прекъсване н Интернет връзката след определен период н бездействие (Max Idle Time). Ако вашата Интернет връзка е била прекъсната поради неактивност, **Connect on Demand** позволява на рутера

автоматично да възстанови връзката веднага след опит за достъп до Интернет. Ако искате да активирате Connect on Demand, натиснете радио-бутон. Ако искате вашата Интернет връзка да остане активна през цялото време, въведете 0 в поле Max Idle Time. В противен случай въведете броя минути, които искате да изминат преди вашата Интернет връзка да прекъсне.

Connect Automatically - Автоматично свързване след прекъсване на рутера. За да ползвате тази опция, изберете радио-бутон.

Connect Manually - Можете да конфигурирате рутера за ръчно свързване или прекъсване.

След определен период н бездействие (Max Idle Time) рутерът ще прекъсне Интернет връзката и няма да можете да възстановите връзката автоматично веднага след като опитате да получите отново достъп до Интернет. За да използвате тази опция, натиснете радио-бутон. Ако искате вашата Интернет връзка да остане активна през цялото време, въведете 0 в поле Max Idle Time. В противен случай въведете броя минути за запазване на Интернет връзката, освен ако бъде поискан нов линк.

Внимание: Понякога връзката не може да бъде прекъсната дори да посочите време в Max Idle Time, тъй като някои приложения ползват Интернет постоянно. Натиснете бутон Save, за да запазите настройките.

→ **Забележка:**

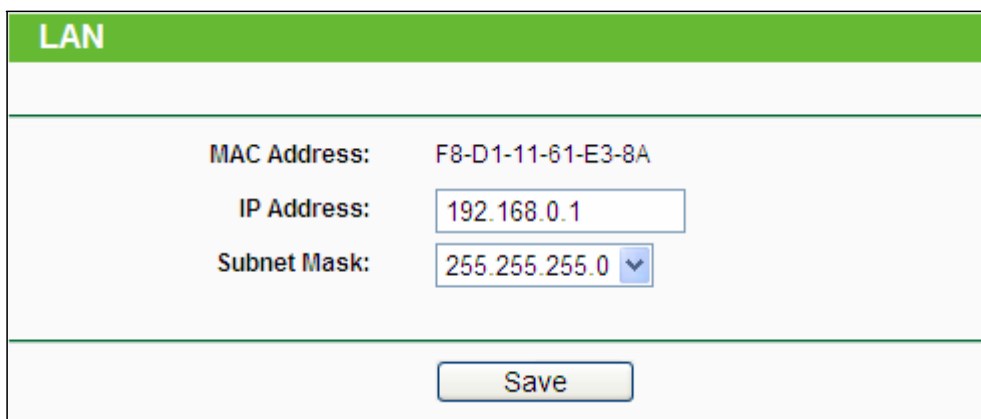
Ако не знаете как да изберете подходящия тип връзка, натиснете бутон Detect, за да може рутерът автоматично да потърси вашата Интернет връзка за сървъри и протоколи. Типът връзка ще се докладва, когато рутерът открие успешно активна Интернет връзка. Този доклад е само за ваша информация. За да се сигурни за типа връзка на вашия ISP, моля обърнете се към него. Различните видове Интернет връзка, които рутерът може да открие са следните:

- ◆ PPPoE - Връзките, които ползват PPPoE с изискване за потребителско име и парола.
- ◆ Dynamic IP - Връзки, които ползват динамично задаване на IP адрес.
- ◆ Static IP - Връзки, които ползват статично зададен IP адрес.

Рутерът не може да открива PPTP/L2TP/BigPond връзки с вашия ISP. Ако вашият ISP ползва един от тези протоколи, тогава трябва да конфигурирате ръчно вашата връзка.

4.5.2 LAN

Изберете меню "Network → LAN", можете да конфигурирате IP параметрите на LAN на екрана, както е показано по-долу.



Фигура 4-12 LAN

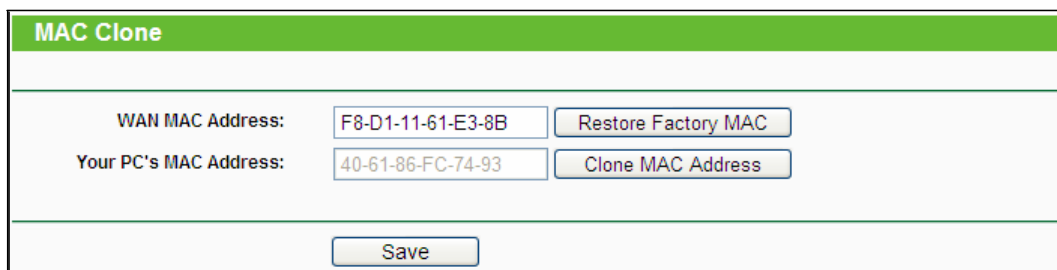
- MAC Address** - Физическият адрес на рутера, както се вижда от LAN. Стойността не може да бъде променена.
- IP Address** - Въведете IP адреса на вашия рутер или го рестартирайте в десетичен формат с разделителна точка (заводска настройка: 192.168.0.1).
- Subnet Mask** - Код на адрес, който определя размера на мрежата. Обикновено за подмрежова маска се ползва 255.255.255.0.

→ **Забележка:**

- 1) Ако промените IP адреса на LAN, трябва да ползвате новия IP адрес за регистрация на рутера.
- 2) Ако новият LAN IP адрес не е в същата подмрежа, IP адрес пулт на DHCP сървъра ще се промени съответно в същия момент, докато виртуалният сървър и DMZ хостът няма да се активират преди да бъдат преконфигурирани.

4.5.3 MAC Clone

Изберете меню “Network → MAC Clone”, и можете да конфигурирате MAC адреса на WAN на показания по-долу екран, Фигура 4-13:



Фигура 4-13 Клониран на MAC адрес

Някои доставчици изискват да регистрирате MAC адрес на вашия адаптер. Рядко са необходими промени тук.

- WAN MAC Address** - Това поле показва текущия MAC адрес на Интернет порта. Ако вашият ISP изисква да регистрирате MAC адреса, моля въведете правилния MAC адрес в това поле в XX-XX-XX-XX-XX-XX формат (X е всяко шестнадесетично число).
- Your PC's MAC Address** - Това поле показва MAC адреса на компютъра, който управлява рутера. Ако се изисква MAC адрес, можете да натиснете бутон Clone

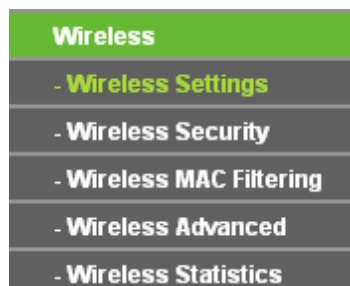
MAC Address То и този MAC адрес ще бъде посочен в поле WAN MAC Address.

Натиснете Restore Factory MAC, за да възстановите MAC адреса на Интернет порта до заводска настройка. Натиснете бутон Save, за да запазите настройките.

→ **Забележка:**

Само компютъра на вашата LAN може да ползва функцията MAC Address Clone.

4.6 Безжична връзка

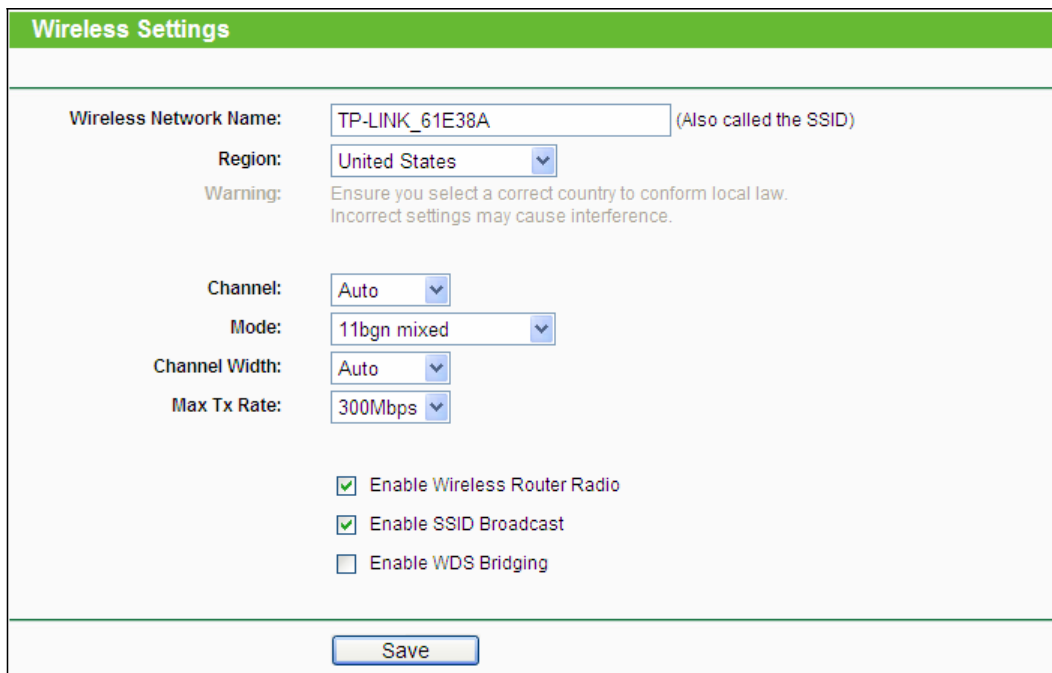


Фигура 4-14 Меню
Безжична връзка

Има пет подменюта под меню Wireless (показани на Фигури 4-14): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced** и **Wireless Statistics**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция.

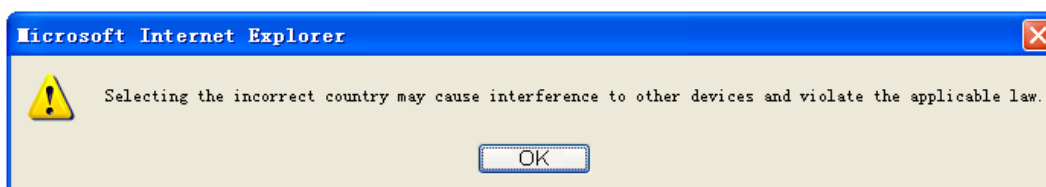
4.6.1 Настройки за безжична връзка

Изберете меню “Wireless → Wireless Settings” и можете да конфигурирате основните настройки за безжична мрежа.



Фигура 4-15 Статистика за безжична мрежа

- **Wireless Network Name** - Въведете стойност до 32 символа. Същото име за SSID (мрежов идентификатор) трябва да бъде зададено на всички безжични устройства във вашата мрежа. С оглед сигурността на безжичната мрежа, по подразбиране SSID е зададен като TP-LINK_XXXXXX (XXXXXX указва последните уникални шест цифри на MAC адреса на всеки рутер). Тези стойности имат точно определен формат за изписване. Например, TEST не е същото като test.
- **Region** - Изберете от падащия списък вашия регион. Това поле определя региона, където може да се ползва безжичната функция на рутера. Може да е незаконно ползването на безжичната функция на рутера в регион, различен от посочения в това поле. Ако вашата страна или регион не са посочени, моля свържете се в вашата местна държавна агенция за съдействие.
Когато изберете от падащия списък вашия локален регион, натиснете бутон Save, след това се появява Note Dialog. Натиснете **OK**.



Note Dialog

→ **Забележка:**

Поради местно законово ограничение версията за Северна Америка няма опция за избор на регион.

- **Channel** - Това поле определя, коя работна честота ще се използва. По подразбиране каналът е зададен на Auto, така че AP ще избере автоматично най-добрия канал. Не е необходимо да променяте безжичния канал, освен ако забележите

намеса с друга близкостояща точка за достъп.

- Mode** - Изберете желания режим. По подразбиране настройката е Disabled.
 - 11b only** - Изберете, ако всички ваши безжични клиенти са 802.11b.
 - 11g only** - Изберете, ако всички ваши безжични клиенти са 802.11g.
 - 11n only** - Изберете, ако всички ваши безжични клиенти са 802.11n.
 - 11bg mixed** - Изберете, ако използвате и 802.11b, и 802.11g безжични клиенти.
 - 11bgn mixed** - Изберете, ако ползвате 802.11b, 11g и 11n безжични клиенти. Изберете желания безжичен режим. Когато е избран режим 802.11g, само 802.11g безжични станции могат да се свързват към рутера. Когато бъде избран режим 802.11n, само 802.11n безжични станции могат да се свързват към точката за достъп. Силно препоръчваме да зададете режим 802.11b&g&n и всички 802.11b, 802.11g и 802.11n безжични станции могат да се свържат към рутера.
- Channel Width** - Изберете ширина на канала от падащия списък. Настройката по подразбиране е автоматична, което позволява автоматично настройване на каналната ширина за вашите клиенти.
 - **Забележка:**
Ако се избере 11b only, 11g only или 11bg mixed в полето Mode, Channel Width избраното поле ще стане сиво, а стойността 20M, което не може да се променя.
- Max Tx Rate** - Можете да ограничите максималната tx скорост на рутера от това поле.
- Enable Wireless Router Radio** - Безжичното радио на този рутер може да е активирано или деактивирано с цел разрешение за достъп на безжичните станции.
- Enable SSID Broadcast** - Когато безжични клиенти проучват локалната зона за безжични мрежи, с които да се свържат, те ще открият SSID предаване от рутера. Ако изберете Enable SSID Broadcast, безжичният рутер ще излъчи своето име (SSID).
- Enable WDS Bridging** - Маркирайте тази позиция за активиране на WDS. С тази функция рутерът може да свърже две или повече безжични мрежи. Ако бъде избрана тази позиция, трябва да зададете следните настройки, показани на Фигура 4-16. Уверете се, че следните настройки са правилните.

Enable WDS Bridging

S SID(to be bridged):

BSSID(to be bridged): Example:00-1D-0F-11-22-33

Key type:

WEP Index:

Auth type:

Password:

Фигура 4-16

- SSID(to be bridged)** - SSID на AP, с която вашият рутер ще се свърже като клиент. Може да ползвате и функцията за търсене за избор на SSID за присъединяване.
- BSSID(to be bridged)** - BSSID на AP, с която вашият рутер ще се свърже като клиент. Може да ползвате и функцията за търсене за избор на BSSID за свързване.
- Survey** - Като натиснете този бутон можете да търсите AP, която работи на текущия канал.
- Key type** - Тази опция трябва да бъде избрана съгласно конфигурацията за сигурност на AP. Препоръчва се типът сигурност да е същия като този на вашата AP.
- WEP Index** - Тази опция трябва да се избира, ако типът ключ е WEP(ASCII) или WEP(HEX). Тя указва индекса на WEP ключа.
- Auth Type** - Тази опция трябва да се избере, ако типът ключ е WEP(ASCII) или WEP(HEX). Тя указва типа аутентификация на Root AP.
- Password** - Ако AP, с която вашият рутер ще се свързва иска парола, трябва да попълните така в това поле.

4.6.2 Сигурност на безжична мрежа

Изберете меню “Wireless → Wireless Security” и можете да конфигурирате настройки за сигурност за вашата безжична мрежа.

Има пет режима за сигурност, поддържани от рутера: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA-PSK (Pre-Shared Key), WPA2-PSK (Pre-Shared Key).

Wireless Security

Disable Security

WEP

Type:

WEP Key Format:

| Key Selected | WEP Key (Password) | Key Type |
|---|----------------------|---------------------------------------|
| Key 1: <input checked="" type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 2: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 3: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 4: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |

WPA/WPA2 - Enterprise

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

WPA/WPA2 - Personal(Recommended)

Version:

Encryption:

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

Фигура 4-17 Сигурност на безжичната връзка

- Disable Security** - Ако не искате да ползвате сигурност на безжична мрежа, маркирайте този радио-бутон. Но ние силно препоръчваме да изберете един от следните режими за активиране на сигурност.
- WEP** - Стандарт, базиран на IEEE 802.11. Ако маркирате радио бутон, ще видите съобщение в червено като това, показано на Фигура 4-18.

WEP

Type:

WEP Key Format:

| Key Selected | WEP Key | Key Type |
|---|----------------------|---------------------------------------|
| Key 1: <input checked="" type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 2: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 3: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |
| Key 4: <input type="radio"/> | <input type="text"/> | <input type="text" value="Disabled"/> |

We do not recommend using the WEP encryption if the device operates in 802.11n mode due to the fact that WEP is not supported by Draft 11N specification.

Фигура 4-18

- **Туре** - можете да изберете тип за WEP сигурност от падащия списък. Настройката по подразбиране е **Automatic**, с което може да се избере **Shared Key** или **Open System** тип аутентификация, автоматично базирана на способността на безжичната станция.

- **WEP Key Format** - Hexadecimal и ASCII формати са предоставени тук. Hexadecimal формат означава всяка комбинация от шестнадесетични символи (0-9, a-f, A-F) в определената дължина. ASCII формат означава всяка комбинация от символите на клавиатурата в определената дължина.
- **WEP Key** - Изберете кои четири клавиша ще бъдат ползвани и въведе съответния WEP ключ, който създавате. Уверете се, че тези стойности са идентични на всички безжични станции във вашата мрежа.
- **Key Type** - Можете да изберете дължина на WEP ключ (64-bit или 128-bit или 152-bit.) за шифроване. "Disabled" означава, че този WEP ключ е невалиден.

64-bit - Можете да въведете 10 шестнадесетични символа (всяка комбинация от 0-9, a-f, A-F, нула не се приема) или 5 ASCII символа.

128-bit - Можете да въведете 26 шестнадесетични символа (всяка комбинация от 0-9, a-f, A-F, нула не се приема) или 13 ASCII символа.

152-bit - Можете да въведете 32 шестнадесетични символа (всяка комбинация от 0-9, a-f, A-F, нула не се приема) или 16 ASCII символа.

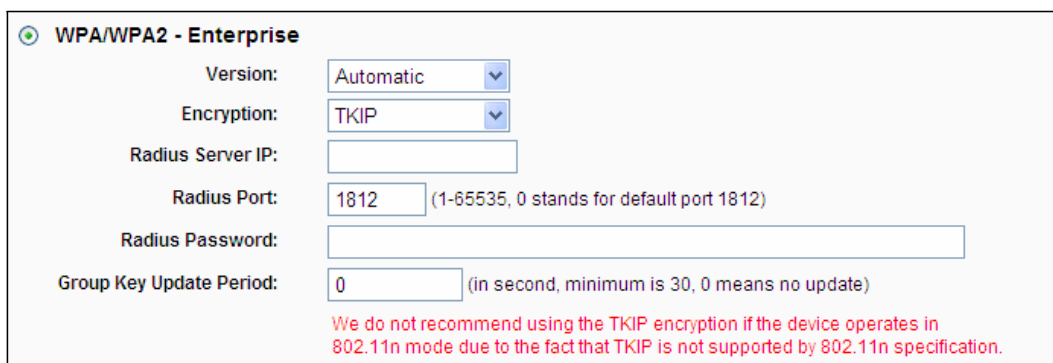
→ **Забележка:**

Ако не зададете ключ, функцията за безжична сигурност остава неактивна дори когато изберете Shared Key като Authentication Type.

- WPA/WPA2- Enterprise** - Базирана е на Radius сървър.
- **Version** - можете да изберете версията за WPA сигурност от падащия списък. Настройката по подразбиране е Automatic, с което може автоматично да се избере WPA (Wi-Fi защитен достъп) или WPA2 (WPA версия 2) на база на възможностите на безжичните станции и при поискване.
- **Encryption** - Можете да изберете или Automatic, или TKIP или AES.

→ **Забележка:**

Ако изберете радио бутон WPA/WPA2-Enterprise и TKIP шифроване, ще откриете съобщение в червено, както е показано на Фигура 4-19.



WPA/WPA2 - Enterprise

Version: Automatic

Encryption: TKIP

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

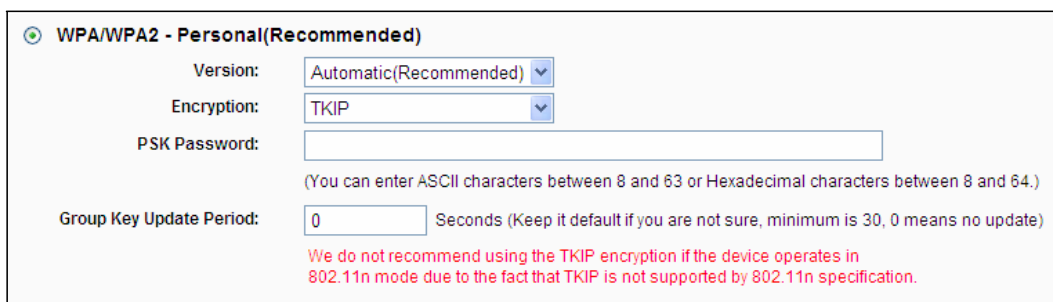
Фигура 4-19

- **Radius Server IP** - Въведете IP адрес на Radius сървър.

- **Radius Port** - Въведете номер на порт на Radius сървъра.
 - **Radius Password** - Въведете паролата за Radius сървъра.
 - **Group Key Update Period** - Посочете групов ключ за интервал на актуализация в секунди. Стойността трябва да е 30 и нагоре. Въведете 0, за да деактивирате функцията.
- **WPA-PSK/WPA2-PSK – Personal (Recommended)** - това е WPA/WPA2 тип аутентификация, базирана на предварително споделена фраза за идентификация.
- **Version** - можете да изберете версията за WPA-PSK сигурност от падащия списък. Настройката по подразбиране е Automatic, с което може автоматично да се избере WPA-PSK (предварително споделен ключ за WPA) или WPA2-PSK (предварително споделен ключ за WPA) на база на възможностите на безжичните станции и при поискване.
 - **Encryption** - Когато WPA-PSK или WPA е зададена като тип аутентификация, можете да изберете или Automatic, или TKIP или AES като шифроване.

→ **Забележка:**

Ако изберете **WPA-PSK/WPA2-PSK – Personal (Recommended)** радио бутон и TKIP кодиране, ще видите съобщение в червено, както е показано на Фигура 4-20.



WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended) ▾

Encryption: TKIP ▾

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

Фигура 4-20

- **PSK Password** - Можете да въведете ASCII символи между 8 и 63 знака или 8 до 64 шестдесетични знака.
- **Group Key Update Period** - Посочете групов ключ за интервал на актуализация в секунди. Стойността трябва да е 30 и нагоре. Въведете 0, за да деактивирате функцията.

Задължително натиснете бутон Save за запазване на настройките на тази страница.

4.6.3 Безжично MAC филтриране

Изберете меню “Wireless → MAC Filtering” и можете да контролирате безжичния достъп чрез конфигуриране на функцията Wireless MAC Filtering, показана на Фигура 4-21.

Wireless MAC Filtering

Wireless MAC Filtering: **Disabled**

Filtering Rules

Allow the stations not specified by any enabled entries in the list to access.

Deny the stations not specified by any enabled entries in the list to access.

| ID | MAC Address | Status | Description | Modify |
|----|-------------------|---------|--------------------|---|
| 1 | 00-0A-EB-B0-00-0B | Enabled | wireless station A | Modify Delete |

Фигура 4-21 MAC филтриране на безжична мрежа

За филтриране на безжични потребители чрез MAC адрес, натиснете Enable. По подразбиране настройката е Disabled.

- MAC Address** - MAC адресът на безжичната станция, която искате да филтрирате.
- Status** - Статусът на този запис, Enabled или Disabled.
- Description** - Кратко описание на безжичната станция.

За да добавите безжично филтриране на MAC адрес, натиснете бутон Add New.... Ще се появи страница "**Add or Modify Wireless MAC Address Filtering entry**", показана на Фигура 4-22:

Add or Modify Wireless MAC Address Filtering entry

MAC Address:

Description:

Status: ▼

Фигура 4-22 Add or Modify Wireless MAC Address Filtering

За добавяне или модифициране на филтриране на MAC адрес, следвайте долните инструкции:

1. Въведете необходимия MAC адрес в поле MAC Address. Форматът на MAC адреса е XX-XX-XX-XX-XX-XX (X е всеки шестнадесетичен символ). Например: 00-0A-EB-B0-00-0B.
2. Дайте просто описание за безжичната станция в поле Description. Например: Безжична станция A.

3. Изберете Enabled или Disabled за този запис от падащ списък Status.
4. Натиснете бутон Save за запазване на записа.

За промяна или изтриване на съществуващ запис:

1. Натиснете Modify в записа, който искате да промените. Ако искате да изтриете записа, натиснете **Delete**.
2. Променете информацията.
3. Натиснете бутон Save.

Натиснете бутон Enable All за активиране на всички записи. натиснете бутон Disabled All за деактивиране на всички записи. Натиснете бутон Delete All за изтриване на всички записи.

Натиснете бутон Next за преминаване към следваща страница.

Натиснете бутон Previous за връщане на предходната страница.

Например: Ако искате безжичната станция A с MAC адрес 00-0A-EB-B0-00-0B и безжичната станция B с MAC адрес 00-0A-EB-00-07-5F да могат да получат достъп до рутера, можете да конфигурирате Wireless MAC Address Filtering списъка като следвате следните стъпки:

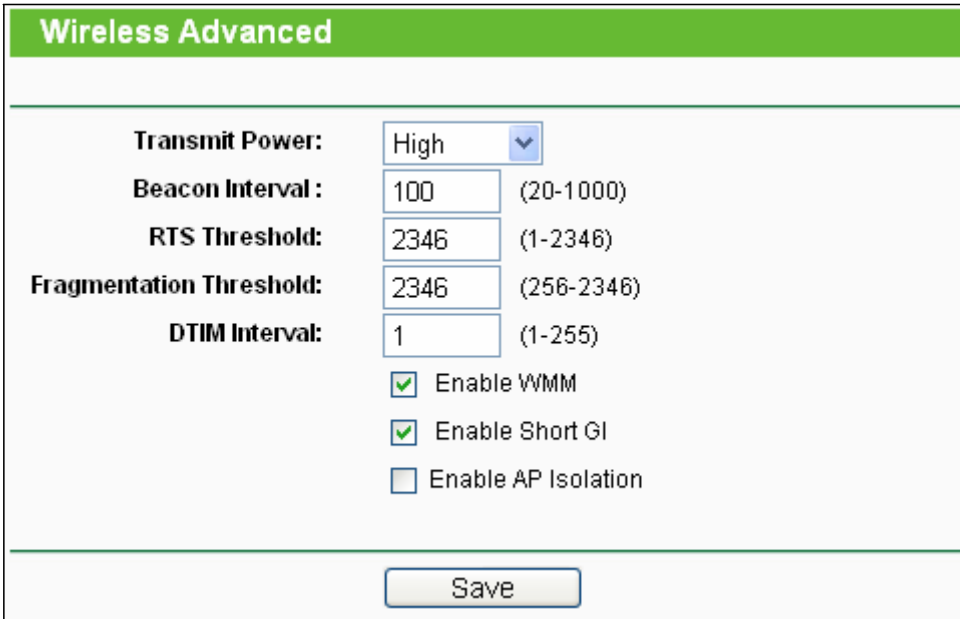
1. Натиснете бутон Enable за активиране на тази функция.
2. Изберете радио бутон "Deny the stations not specified by any enabled entries in the list to access" за **Filtering Rules** (правила за филтриране).
3. Изтрийте всички или деактивирайте всички записи, ако вече има направени такива.
4. Натиснете **Add New...** бутона.
 - 1) Въведете MAC адрес 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F в поле MAC Address.
 - 2) Въведете безжична станция A/B в поле Description.
 - 3) Изберете Enabled от падащ списък Status.
 - 4) Натиснете бутон Save.
 - 5) Натиснете бутон Back.

Така конфигурираните правила за филтриране трябва да са подобни на следния списък:

| Filtering Rules | | | | |
|-----------------|----------------------------------|---------|--|---|
| | <input type="radio"/> | Allow | the stations not specified by any enabled entries in the list to access. | |
| | <input checked="" type="radio"/> | Deny | the stations not specified by any enabled entries in the list to access. | |
| ID | MAC Address | Status | Description | Modify |
| 1 | 00-0A-EB-B0-00-0B | Enabled | wireless station A | Modify Delete |
| 2 | 00-0A-EB-00-07-5F | Enabled | wireless station A | Modify Delete |

4.6.4 Wireless Advanced

Изберете меню “Wireless → Wireless Advanced” и можете да конфигурирате подробни настройки за вашата безжична мрежа.



Фигура 4-23 Wireless Advanced

- **Transmit Power** - Тук можете да посочите силата на предаване на рутера. Можете да изберете висока, средна и ниска според желанието си. Настройката по подразбиране е висока сила и това е препоръчително.
- **Beacon Interval** - Въведете стойност между 20-1000 милисекунди за интервал за повикване. Повикванията са пакети, изпращани от рутера за синхронизиране на безжична мрежа. Стойността за интервал за повикване определя интервалите на повикванията. Стойността по подразбиране е 100.
- **RTS Threshold** - Тук можете да посочите праг за RTS (искане за изпращане). Ако пакетът е по-голям от посочения RTS, рутерът ще изпраща RTS фреймове на посочена приемаща станция и ще обработва изпращането на информационен фрейм. Стойността по подразбиране е 2346.
- **Fragmentation Threshold** - Тази стойност е максималния размер, определящ дали пакетите ще бъдат фрагментирани. Задаването на твърде нисък праг за фрагментация може да доведе до лошо изпълнение на мрежата поради прекомерен брой пакети. 2346 е настройката по подразбиране и това се препоръчва.
- **DTIM Interval** - Тази стойност определя интервала за съобщение за индикация за трафик на доставка (DTIM). Полето DTIM е поле с обратно броене, което информира клиентите на следващия прозорец за прослушване на излъчване и съобщения за групово предаване. Когато рутерът е буферизирал съобщения за излъчване и групово предаване, той изпраща следващо DTIM със стойност за DTIM Interval. Можете да посочите стойност между 1-255 интервалите за повикване. Стойността по подразбиране е 1, което указва, че DTIM Interval е същия като Beacon Interval.

- **Enable WMM** - WMM функцията може да гарантира, че пакетите със съобщения с висок приоритет се предават преференциално. Това е силно препоръчително.
- **Enable Short GI** - Тази функция се препоръчва, тъй като тя увеличава информационния капацитет чрез намаляване на защитното интервално време.
- **Enabled AP Isolation** - Тази функция може да изолира безжични станции на вашата мрежа един от друг. Безжичните устройства ще могат да комуникират с рутера, но не един с друг. За да използвате тази функция, маркирайте позицията. AP изолация е деактивирана по подразбиране.

→ **Забележка:**

Ако не познавате точките за настройка на тази страница, силно препоръчваме да запазите дадените стойности по подразбиране; в противен случай това може да понижи изпълнението на безжичната мрежа.

4.6.5 Статистика за безжична мрежа

Изберете меню “Wireless → Wireless Statistics” и можете да видите MAC адреса, текущия статус, получени пакети и изпратени пакети за всяка свързана безжична станция.

| Wireless Statistics | | | | | |
|--|-------------------|-------------------------------------|------------------|--------------|--|
| Current Connected Wireless Stations numbers: | | | | 1 | <input type="button" value="Refresh"/> |
| ID | MAC Address | Current Status | Received Packets | Sent Packets | |
| 1 | 00-0A-EB-88-34-75 | STA-ASSOC | 416 | 2 | |
| <input type="button" value="Previous"/> | | <input type="button" value="Next"/> | | | |

Фигура 4-24 Статистика за безжична мрежа

- **MAC Address** - MAC адрес на свързаната безжична станция
- **Current Status** - Текущият статус на свързаната безжична станция, един от STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected
- **Received Packets** - Пакетите, получени от станцията
- **Sent Packets** - Пакетите, изпратени от станцията

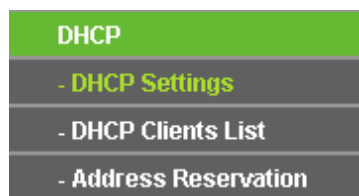
Не можете да промените стойностите на тази страница. За актуализиране на тази страница и за показване на текущите свързани безжични станции, натиснете бутон Refresh.

Ако броя свързани безжични станции излиза извън страницата, натиснете бутон Next, за да отидете на следваща страница и натиснете бутон Previous за връщане на предходна страница.

→ **Забележка:**

Тази страница се обновява автоматично на всеки 5 секунди.

4.7 DHCP

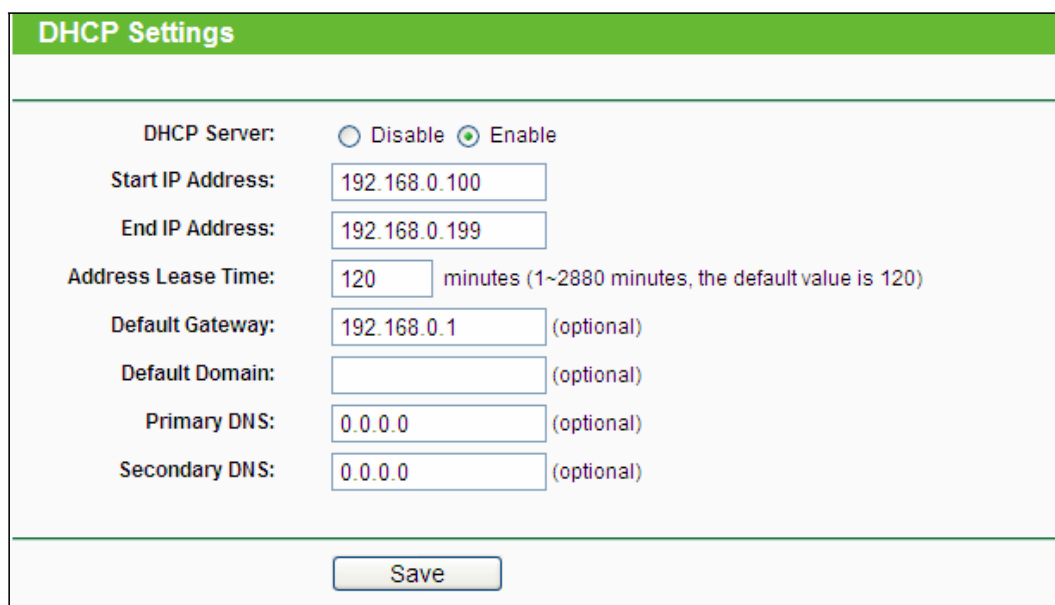


Фигура 4-25 Меню DHCP

Има три подменюта под меню DHCP (показано на Фигура 4-25), **DHCP Settings**, **DHCP Clients List** и **Address Reservation**. Натиснете върху някое от тях и ще можете да конфигурирате съответната функция.

4.7.1 DHCP настройки

Изберете меню “DHCP → DHCP Settings” и можете да конфигурирате DHCP сървър, както е показано на Фигура 4-26. Рутерът е настроен по подразбиране като DHCP (Dynamic Host Configuration Protocol) сървър, което осигурява TCP/IP конфигурацията за всички компютри, свързани към рутера в локалната мрежа.



Фигура 4-26 DHCP настройки

- DHCP Server** - Enable или Disable на DHCP сървър. Ако деактивирате сървъра, трябва да имате друг DHCP сървър във вашата мрежа или ще трябва да конфигурирате компютъра ръчно.
- Start IP Address** - Посочете IP адрес за DHCP сървъра, за да започнете със задаването на IP адреси. 192.168.0.100 е начален адрес по подразбиране.
- End IP Address** - Посочете IP адрес за DHCP сървъра, за да завършите със задаването на IP адреси. 192.168.0.199 е по подразбиране краен адрес.

- Address Lease Time** - Address Lease Time е периода от време, през който мрежов потребител ще има връзка към рутера със своя текущ динамичен IP адрес. Въведете периода от време в минути и потребителят ще получи този динамичен IP адрес. След изтичане на времето на потребителя автоматично се задава нов динамичен IP адрес. Период, който може да бъде зададен - 1 ~ 2880 минути. Стойността по подразбиране е 120 минути.
- Default Gateway** - (По избор) Предлагаме ви да въведете IP адреса на LAN порта на рутера. Стойността по подразбиране е 192.168.0.1.
- Default Domain** - (По избор) Въведете името на домейна на вашата мрежа.
- Primary DNS** - (По избор) Въведете DNS IP адрес, предоставен от вашия ISP или се консултирайте с вашия ISP.
- Secondary DNS** - (По избор) Въведете IP адрес на друг DNS сървър, ако вашият ISP осигурява два DNS сървъра.

→ **Забележка:**

За използване функцията DHCP сървър на рутера, трябва да конфигурирате всички компютри в LAN като "Obtain an IP Address automatically".

4.7.2 DHCP списък на клиенти

Изберете меню "DHCP → DHCP Clients List" и на екрана можете да видите информация за клиентите, прикачени към рутера, както е показано на Фигура 4-27.

| DHCP Clients List | | | | |
|-------------------|-----------------|-------------------|---------------|------------|
| ID | Client Name | MAC Address | Assigned IP | Lease Time |
| 1 | tp-113ea910272d | 40-61-86-FC-74-93 | 192.168.0.100 | 01:55:14 |

Refresh

Фигура 4-27 DHCP клиентски списък

- Client Name** - Името на DHCP клиент
- MAC Address** - MAC адресът на DHCP клиента
- Assigned IP** - IP адресът, който рутерът е разпределил за DHCP клиента
- Lease Time** - Разрешеното време на DHCP клиента. След изтичане на времето на динамичния IP адрес, на потребителят автоматично ще бъде зададен нов динамичен IP адрес.

Не можете да промените стойностите на тази страница. За актуализиране на тази страница и за показване на текущо прикачените устройства, натиснете бутон Refresh.

4.7.3 Резервиране на адрес

Изберете меню “DHCP → Address Reservation” и можете да видите и добавите резервиран адрес за клиенти с помощта на следващия екран (показан на Фигура 4-28). Когато посочвате резервиран IP адрес за компютър в локалната мрежа, този компютър винаги получава един и същ IP адрес, всеки път когато иска достъп до DHCP сървър. Резервирани IP адреси трябва да се задават на сървърите, които изискват постоянни IP настройки.

| Address Reservation | | | | |
|---------------------|-------------------|---------------------|---------|---|
| ID | MAC Address | Reserved IP Address | Status | Modify |
| 1 | 00-11-22-33-44-AA | 192.168.0.100 | Enabled | Modify Delete |

Фигура 4-28 Резервиране на адрес

- MAC Address** - MAC адресът на компютъра, за който искате да резервирате IP адрес.
- Reserved IP Address** - IP адресът, резервиран за компютъра от рутера.
- Status** - Статусът на този запис, Enabled или Disabled.

За да резервирате IP адрес:

1. Натиснете бутон Add New... . Ще се покаже Фигура 4-29.
2. Въведете MAC адреса (в XX-XX-XX-XX-XX-XX формат.) и IP адреса (в десетичен формат с разделителни точки) на компютъра, за който искате да резервирате IP адрес.
3. Натиснете бутон **Save**.

| Add or Modify an Address Reservation Entry | |
|--|--|
| MAC Address: | <input type="text"/> |
| Reserved IP Address: | <input type="text"/> |
| Status: | Enabled <input type="button" value="v"/> |

Фигура 4-29 Добавяне или промяна на запис за резервиране на адрес

За промяна или изтриване на съществуващ запис:

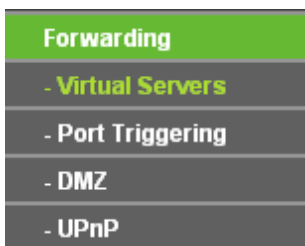
1. Натиснете **Modify** в записа, който искате да промените. Ако искате да изтриете записа, натиснете **Delete**.
2. Променете информацията.
3. Натиснете бутон **Save**.

Натиснете бутон **Enable/Disabled All** за активиране/ деактивиране на всички записи.

Натиснете бутон **Delete All** за изтриване на всички записи.

Натиснете бутон **Next**, за да отидете на следваща страница и натиснете бутон **Previous** за връщане на предходна страница.

4.8 Препращане



Фигура 4-30 Меню Препращане

Има четири подменюта под меню **Forwarding** (показано на Фигура 4-30), **Virtual Servers**, **Port Triggering**, **DMZ** и **UPnP**. Натиснете на някое от тях и ще можете да конфигурирате съответната функция.

4.8.1 Виртуални сървъри

Изберете меню “Forwarding→Virtual Servers” и можете да видите и да добавите виртуални сървъри в следния прозорец (показан на Фигура 4-31). Виртуалните сървъри могат да се ползват за задаване на публични услуги във вашата локална мрежа, като например DNS, Email и FTP. Виртуалният сървър се дефинира като обслужващ порт и всички запитвания от Интернет до този обслужващ порт ще бъдат пренасочвани към компютъра, посочен от IP на сървъра. Всеки компютър, който е бил използван за виртуален сървър трябва да има статичен или резервиран IP адрес, IP адресът може да се промени с използване на DHCP функцията.

| ID | Service Port | Internal Port | IP Address | Protocol | Status | Modify |
|----|--------------|---------------|---------------|----------|---------|---|
| 1 | 11130 | 11120 | 192.168.0.198 | ALL | Enabled | Modify Delete |

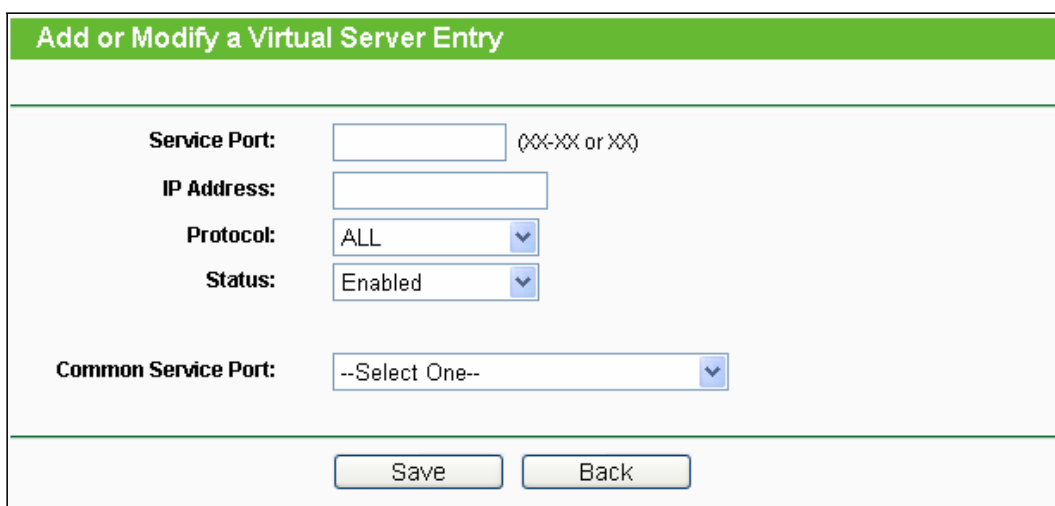
Фигура 4-31 Виртуални сървъри

- **Service Port** - Номерата на външни портове. Можете да въведете сервизен порт или серия сервизни портове (форматът е XXX – YYY; XXX е начален порт, а YYY е краен порт).

- IP Address** - IP адресът на компютъра, на който работи сервизното приложение.
- Protocol** - Протоколът, използван за това приложение, или TCP, UDP, или All (всички протоколи, поддържани от рутера).
- Status** - Статусът на този запис, Enabled или Disabled.

За настройка на запис за виртуален сървър:

1. Натиснете бутон Add New... , ще се появи екрана, показан на Фигура 4-32.
2. Изберете от Common Service Port списъка сервизен порт, който искате да ползвате. Ако менюто Common Service Port не включва услугата, която искате да ползвате, въведете номера на сервизния порт или серията сервизни портове в поле Service Port.
3. Напишете IP адреса на компютъра в позицията **IP Address**.
4. Изберете протокола, използван за това приложение, или **TCP**, **UDP** или **All**.
5. Изберете **Enable** за активиране на виртуалния сървър.
6. Натиснете бутон **Save**.



Фигура 4-32 Добавяне или промяна на запис за виртуален сървър

→ **Забележка:**

Ако вашият компютър или сървър има повече от един тип налична услуга, моля изберете друга услуга и въведете същия IP адрес за този компютър или сървър.

За промяна или изтриване на съществуващ запис:

1. Натиснете Modify в записа, който искате да промените. Ако искате да изтриете записа, натиснете **Delete**.
2. Променете информацията.
3. Натиснете бутон Save.

Натиснете бутон Enable/ Disabled All, за да активирате/ деактивирате всички записи. Натиснете бутон Delete All за изтриване на всички записи.

Натиснете бутон Next, за да отидете на следваща страница и натиснете бутон Previous за връщане на предходна страница.

→ Забележка:

Ако зададете сервисния порт на виртуален сървър като 80, трябва да зададете порт за уеб управление от System Tools → Remote Management, която да е друга стойност, различна от 80, например 8080. В противен случай ще конфликт за деактивиране на виртуалния сървър.

4.8.2 Прехвърляне на порт

Изберете меню “Forwarding→Port Triggering” и можете да виждате и добавяте прехвърляне на порт на следния екран (показан на Фигура 4-33). Някои приложения изискват множество връзки, например Интернет игри, видео конферентен разговор, Интернет телефония и др. Тези приложения не могат да работят с изцяло NAT рутер. Прехвърляне на порт се използва за някои от тези приложения, които могат да работят с NAT рутер.

| ID | Trigger Port | Trigger Protocol | Incoming Port | Incoming Protocol | Status | Modify |
|----|--------------|------------------|---------------|-------------------|---------|---|
| 1 | 554 | ALL | 8970-8999 | ALL | Enabled | Modify Delete |

Фигура 4-33 Прехвърляне на порт

След като рутерът е вече конфигуриран, той работи както следва:

1. Локален хост прави изходяща връзка като ползва номер на порт за дестинация, дефиниран в поле Trigger Port.
2. Рутерът записва тази връзка, отваря входящ порт или портове, свързани с този запис в таблица Port Triggering и ги асоциира с локалния хост.
3. Когато е необходимо, външният хост може да се свърже към локалния хост като използва един от портовете, дефинирани в поле **Incoming Ports**.

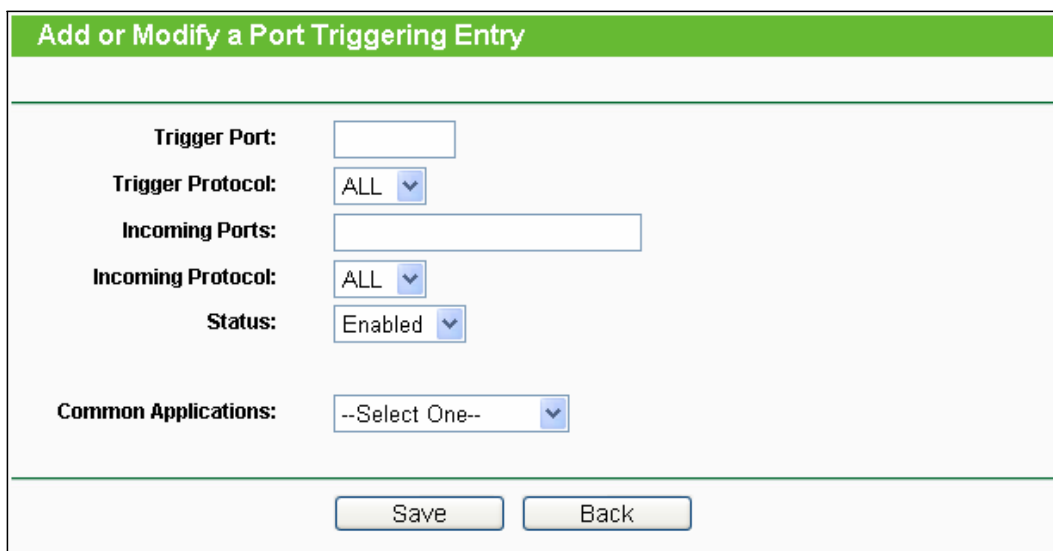
- Trigger Port** - Порт за изходящ трафик. Изходяща връзка, използваща този порт, ще задейства това правило.
- Trigger Protocol** - Протокол, използван за прехвърлящи портове, TCP, UDP или All (всички протоколи, поддържани от рутера).
- Incoming Ports Range** - Портът или серията портове, използвани от дистанционна система, когато тя отговаря на изходящо искане. Отговор, с използване на тези портове ще бъде прехвърлен на компютъра, който е задействал това правило. Можете да въведете най-много 5 групи портове (или порт секции). Всяка група портове трябва да бъде отделена с ",". Например, 2000-2038, 2050-2051, 2085, 3010-3030.
- Incoming Protocol** - Протоколът, използван за Incoming Ports Range, или TCP, или UDP, или

ALL (всички протоколи, поддържани от рутера).

- Status** - Статусът на този запис, Enabled или Disabled.

За добавяне на ново правило, следвайте долните стъпки.

1. Натиснете бутон Add New... , ще се появи екрана, показан на Фигура 4-34.
2. Изберете приложение от падащ списък Common Applications, след това поле Trigger Port и поле Incoming Ports ще бъдат автоматично попълнени. Ако Common Applications не включва приложението, от което се нуждаете, въведете ръчно Trigger Port и Incoming Ports.
3. Изберете протокола, използван за Trigger Port от падащ списък Trigger Protocol, TCP, UDP или All.
4. Изберете протокола, използван за Incoming Ports от падащ списък Incoming Protocol, TCP, UDP или All.
5. Изберете Enable в поле Status.
6. Натиснете бутон **Save** за запазване на новото правило.



Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL ▾

Incoming Ports:

Incoming Protocol: ALL ▾

Status: Enabled ▾

Common Applications: --Select One-- ▾

Save Back

Фигура 4-34 Добавяне или промяна на запис за прехвърляне

За промяна или изтриване на съществуващ запис:

1. Натиснете Modify в записа, който искате да промените. Ако искате да изтриете записа, натиснете **Delete**.
2. Променете информацията.
3. Натиснете бутон Save.

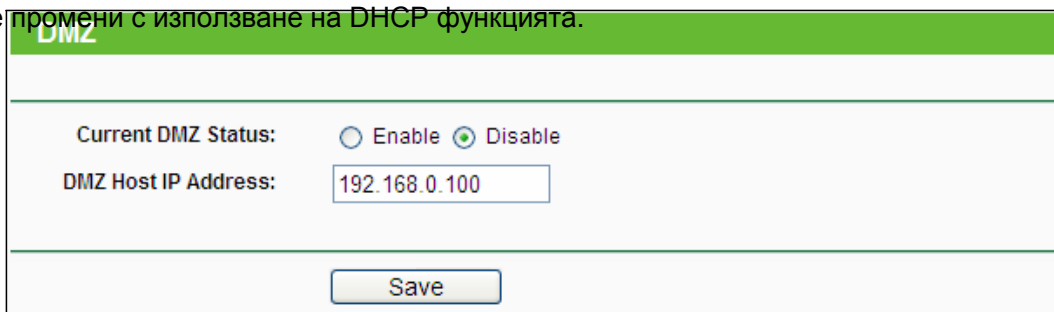
Натиснете бутон Enable All за активиране на всички записи. натиснете бутон Disabled All за деактивиране на всички записи. Натиснете бутон Delete All за изтриване на всички записи

→ Забележка:

1. Когато връзката за прехвърляне бъде освободена, съответно отворените портове ще бъдат затворени.
2. Всяко правило може да бъде използвано от един хост в LAN синхронизирано. Връзката за прехвърляне на други хостове от локалната мрежа ще бъде отказана.
3. Диапазонът на Incoming Ports не трябва да се припокрива.

4.8.3 DMZ

Изберете меню “**Forwarding** → **DMZ**” и можете да видите и конфигурирате DMZ хост в екрана, показан на Фигура 4-35. Характеристиката DMZ хост позволява един локален хост да бъде открит за Интернет за услуга със специална цел като Интернет игра или видеоконферентен разговор. DMZ хостът прехвърля всички портове едновременно. Всеки компютър, чийто порт се прехвърля трябва да има своя DHCP деактивирана клиентска функция и трябва да има нов статичен IP адрес, зададен за него, тъй като IP адресът може да се промени с използване на DHCP функцията.



| DMZ | |
|-------------------------------------|---|
| Current DMZ Status: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| DMZ Host IP Address: | <input type="text" value="192.168.0.100"/> |
| <input type="button" value="Save"/> | |

Фигура 4-35 DMZ

За задаване на компютър или сървър като DMZ сървър:

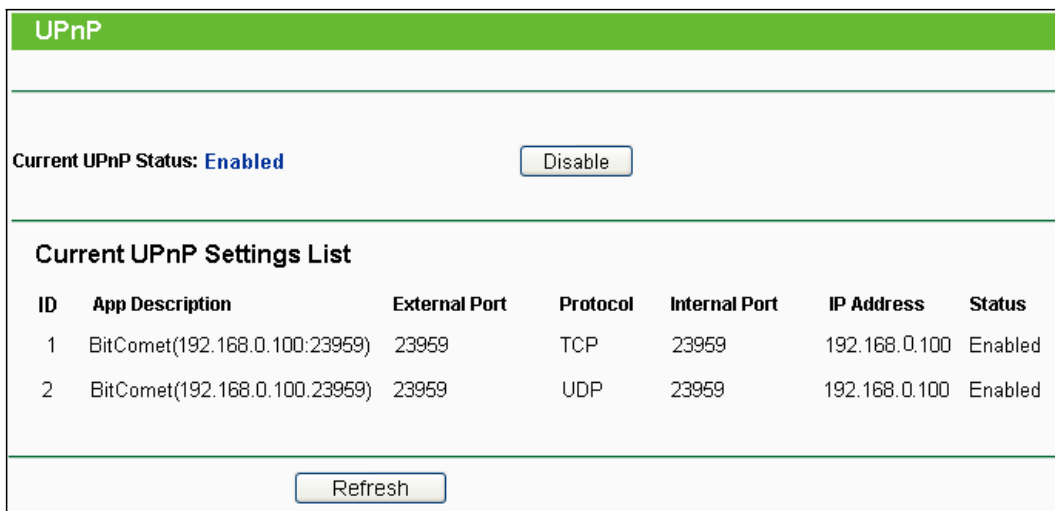
1. Изберете радио бутон **Enable**
2. Въведете IP адреса на локален хост в поле **DMZ Host IP Address**
3. Натиснете бутон **Save**.

→ Забележка:

След като зададете DMZ хост защитната стена за хоста няма да работи.

4.8.4 UPnP

Изберете “Forwarding→UPnP” и след това можете да видите информация за UPnP (Universal Plug and Play) в екрана (показан на Фигура 4-36). Характеристиката UPnP позволява на устройствата, като Интернет компютри, да имат достъп до ресурсите или устройствата на локалния хост, според необходимостта. UPnP устройства могат да бъдат автоматично откривани от UPnP сервизното приложение в LAN.



Фигура 4-36 UPnP

- **Current UPnP Status** - UPnP може да бъде активиран или деактивиран чрез избор на бутон Enable или Disable.
- **Current UPnP Settings List** - Тази таблица показва текущата UPnP информация.
 - **App Description** - Описанието, осигурявано от приложението в UPnP искането.
 - **External Port** - Портът, който рутерът отваря за приложението.
 - **Protocol** - Типът протокол, който рутерът отваря за приложението.
 - **Internal Port** - Порт, който рутерът е отворил за локален хост.
 - **IP Address** - IP адресът на UPnP устройството, което в момента иска достъп до рутера.
 - **Status** - Тук се показва статуса на порта. "Enabled" означава, че портът все още е активен; в противен случай, той е неактивен.

Натиснете бутон Refresh за актуализиране на текущия списък с UPnP настройки.

4.9 Сигурност



Фигура 4-37 Меню Сигурност

Има четири подменюта под меню Сигурност както е показано на Фигура 4-37: **Basic Security**, **Advanced Security**, **Local Management** и **Remote Management**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция.

4.9.1 Базова сигурност

Изберете меню “Security → Basic Security” и можете да конфигурирате базова сигурност, както е показано на Фигура 4-38.

| Basic Security | |
|-------------------------------------|---|
| Firewall | |
| SPI Firewall: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| VPN | |
| PPTP Passthrough: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| L2TP Passthrough: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| IPSec Passthrough: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ALG | |
| FTP ALG: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| TFTP ALG: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| H323 ALG: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| <input type="button" value="Save"/> | |

Фигура 4-38 Базова сигурност

- **Firewall** - Защитна стена, която защитава вашата мрежа от външния свят. Тук можете да активирате или деактивирате защитната стена на рутера.
 - ♦ **SPI Firewall** - SPI (Stateful Packet Inspection, известна като динамично филтриране на пакети) помага за предотвратяване на кибер атаки чрез проследяване на повече състояния на сесия. Тя валидира, че трафикът, преминаващ през сесията отговаря на протокола. SPI Firewall е активирана по заводска настройка. Ако искате всички компютри от локалната мрежа да са отворени към външния свят, можете да я деактивирате.
- **VPN** - VPN транзит трябва да бъде активиран, ако искате да разрешите VPN тунели с използване на IPSec, PPTP или L2TP протоколи да преминават през защитната стена на рутера.
 - ♦ **PPTP Passthrough** - Протокол за тунели от точка до точка (PPTP), който позволява протокол от точка до точка (PPP) да бъде тунелиран през IP мрежа. За да позволите PPTP тунели да преминават през рутера, запазете настройката по подразбиране - Enable.
 - ♦ **L2TP Passthrough** - Слои две протокол за тунелирани (L2TP) е метод, използван за активиране на сесии Point-to-Point през Интернет на ниво Слои две. За да

позволите L2TP тунели да преминават през рутера, запазете настройката по подразбиране - Enable.

- ◆ **IPSec Passthrough** - Интернет протокол сигурност (IPSec) е пакет протоколи за осигуряване на частни, сигурни комуникации през Интернет протокол (IP) мрежи, чрез използване на криптографски услуги за сигурност. За да позволите IPSec тунели да преминават през рутера, запазете настройката по подразбиране - Enable.
- **ALG** - Препоръчва се да активирате шлюз приложно ниво (ALG), тъй като ALG позволява специални Network Address Translation (NAT) обходни филтри да бъдат включени към шлюза за подпомагане на трансляцията на адрес и порт за някои "control/data" приложно ниво протоколо, като FTP, TFTP, H323 и др.
 - ◆ **FTP ALG** - За да могат FTP клиенти и сървъри да прехвърлят данни през NAT, натиснете Enable.
 - ◆ **TFTP ALG** - За позволите TFTP клиенти и сървъри да прехвърлят данни през NAT, запазете настройката по подразбиране - **Enable**.
 - ◆ **H323 ALG** - За да могат Microsoft NetMeeting клиенти да комуникират през NAT, запазете настройката по подразбиране - Enable.

Натиснете бутон Save, за да запазите настройките.

4.9.2 Повишена сигурност

Изберете меню “**Security** → **Advanced Security**” и можете да защитите рутера от атаки от TCP-SYN Flood, UDP Flood и ICMP-Flood, в екрана, показан на Фигура 4-39.

Фигура 4-39 Повишена сигурност

- Packets Statistics Interval (5~60)** - Стойността по подразбиране е 10. Изберете стойност между 5 и 60 секунди, от падащия списък. Стойността на Packets Statistics Interval указва времеви интервал на пакетната статистика. Резултатът от статистиката се използва за анализ от SYN Flood, UDP Flood и ICMP-Flood.
- DoS Protection** - Защита Отказ от обслужване. Натиснете бутон Enable или Disable за активиране или деактивиране на функцията DoS защита. Само когато е активирана, ще се активират и филтрите.

→ **Забележка:**

DoS Protection действа само, когато е активирана Traffic Statistics в "System Tool → Traffic Statistics".

- Enable ICMP-FLOOD Attack Filtering** - Активиране или деактивиране на ICMP-FLOOD Attack Filtering.
- ICMP-FLOOD Packets Threshold (5~3600)** - Стойността по подразбиране е 50. Въведете стойност между 5 ~ 3600. Когато текущият номер на ICMP-FLOOD пакети е над зададената стойност, рутерът ще включи веднага функцията за блокиране.
- Enable UDP-FLOOD Filtering** - Активира или деактивира UDP-FLOOD филтриране.
- UDP-FLOOD Packets Threshold (5~3600)** - Стойността по подразбиране е 500. Въведете стойност между 5 ~ 3600. Когато текущият номер на UDP-FLOOD пакети е над зададената стойност, рутерът ще включи веднага функцията за блокиране.
- Enable TCP-SYN-FLOOD Attack Filtering** - Активира или деактивира TCP-SYN-FLOOD Attack Filtering.
- TCP-SYN-FLOOD Packets Threshold (5~3600)** - Стойността по подразбиране е 50. Въведете стойност между 5 ~ 3600. Когато текущият номер на TCP-SYN-FLOOD пакети е над зададената стойност, рутерът ще включи веднага функцията за блокиране.
- Ignore Ping Packet From WAN Port** - Активира или деактивира Ignore Ping Packet From WAN Port. По подразбиране настройката е деактивирана. Ако бъде активирана, пакетът за проверка от Интернет не може да осъществи достъп до рутера.
- Forbid Ping Packet From LAN Port** - Активиране или деактивиране на Forbid Ping Packet From LAN Port. По подразбиране настройката е деактивирана. Ако е активирана, пакетът за проверка от локалната мрежа, не може да осъществи достъп до рутера. Тази функция може да бъде използвана за защита срещу някои вируси. Натиснете бутон Save за запазване на настройките.

Натиснете бутон Blocked DoS Host List за показване на таблица DoS host чрез блокиране.

4.9.3 Локално управление

Изберете меню "**Security** → **Local Management**" и можете да конфигурирате правило за управление, както е показано на Фигура 4-40. Характеристиката за управление ви позволява да отхвърлите компютри в локалната мрежа за достъп до рутера.

Local Management

Management Rules

All the PCs on the LAN are allowed to access the Router's Web-Based Utility

Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address:

Фигура 4-40 Локално управление

По подразбиране, радио бутон “All the PCs on the LAN are allowed to access the Router's Web-Based Utility” е маркиран. Ако искате да позволите компютри със специфичен MAC адрес да имат достъп до страница Setup на уеб-базирана програма на рутера, локално, маркирайте радио бутон “Only the PCs listed can browse the built-in web pages to perform Administrator tasks” и ще можете да въведете всеки MAC адрес в отделно поле. Форматът за MAC адреса е XX-XX-XX-XX-XX-XX (X е всяко шестдесетично число). Само компютри с посочен MAC адрес могат да ползват паролата за преглеждане на вградени уеб страници за изпълнение на задачи на Администратор, докато всички други ще бъдат блокирани.

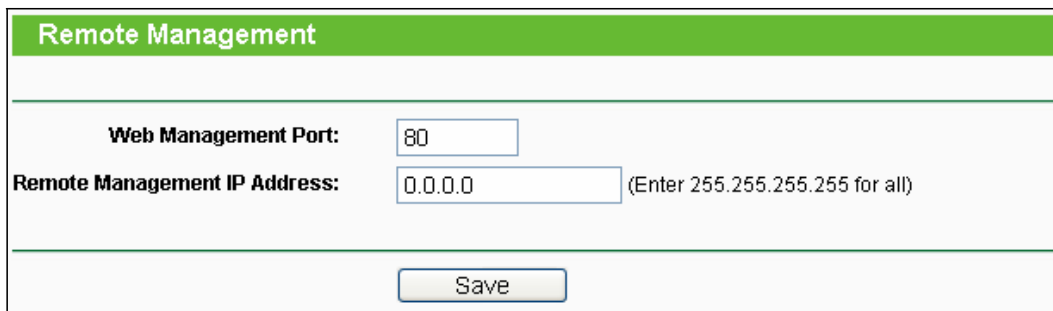
След натискане на бутон Add MAC адресът на вашия компютър ще бъде включен към горния списък. Натиснете бутон Save, за да запазите настройките.

→ **Забележка:**

Ако компютърът ви е блокиран, но искате отново достъп до рутера, използвайте топлийка, за да натиснете и задържите бутон Reset (отвор) отзад на панела за около 5 секунди, за да върнете заводските настройки на рутера на уеб-базирана програма на рутера.

4.9.4 Дистанционно управление

Изберете меню “Security → Remote Management” и можете да конфигурирате функцията Remote Management на екрана, показан на Фигура 4-41. Тази характеристика ви позволява да управлявате вашия рутер от отдалечено място през Интернет.



| Remote Management | |
|-------------------------------------|--|
| Web Management Port: | <input type="text" value="80"/> |
| Remote Management IP Address: | <input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all) |
| <input type="button" value="Save"/> | |

Фигура 4-41 Дистанционно управление

- **Web Management Port** - Уеб браузър достъпът обикновено ползва стандартен HTTP сервизен порт 80. Този уеб порт за отдалечено управление на рутера по подразбиране е номер 80. За по-голяма сигурност можете да промените уеб порта за дистанционно управление с друг като въведете номера му в съответната позиция. Изберете номер между 1 и 65534, но не използвайте номер на общ сервизен порт.
- **Remote Management IP Address** - Това е текущият адрес, който ще ползвате, когато получавате достъп до рутера през Интернет. Тази функция е деактивирана, когато IP адресът е зададен със стойност 0.0.0.0. За активиране на функцията, променете 0.0.0.0 с валиден IP адрес. Ако зададете 255.255.255.255, тогава всички хостове могат да имат достъп до рутера през Интернет.

→ **Забележка:**

- 1) За достъп до рутера трябва да напишете WAN IP адреса на вашия рутер в браузера (в IE) или в позицията за място (в Navigator), последван от двоеточие и съответния номер на порт. Например, ако WAN адресът на рутера е 202.96.12.8, а номерът на ползвания порт е 8080, моля въведете в браузера <http://202.96.12.8:8080> . След това може да бъде поискана парола за рутера. След успешно въвеждане на потребителско име и парола, ще можете да имате достъп до уеб-базираната програма на рутера.
- 2) Сменете паролата по подразбиране на рутера с друга, много по-сигурна парола.

4.10 Родителски контрол

Изберете меню "Parental Control" и можете да конфигурирате родителски контрол в екрана, показан на Фигура 4-42. Функцията Родителски контрол може да бъде използвана за контролиране на дейностите на детето в Интернет, за ограничаване на достъпа до определени сайтове и за задаване на определен срок от време за сърфиране.

Фигура 4-42 Настройки за родителски контрол

- Parental Control** - Маркирайте Enable, ако искате да активирате тази функция; в противен случай, маркирайте Disable.
- MAC Address of Parental PC** - В това поле въведете MAC адреса на контролирания компютър или използвайте бутон Copy To Above.
- MAC Address of Your PC** - Това поле показва MAC адреса на компютъра, който управлява този рутер. Ако MAC адресът на вашия адаптер е регистриран, можете да натиснете бутон Copy To Above, за да попълните този адрес в поле MAC Address of Parental PC.
- Website Description** - Описание на позволен уебсайт за контролирания компютър.
- Schedule** - Период от време с позволен достъп до Интернет за контролирания компютър. За подробна информация, моля вижте "Access Control → Schedule".
- Modify** - Тук можете да редактирате или изтривате запис.

За добавяне на нов запис, моля следвайте долните стъпки.

1. Натиснете бутон Add New... и ще се покаже прозореца, който виждате на Фигура 4-43.
2. Въведете MAC адреса на компютъра (напр. 00-11-22-33-44-AA), който искате да контролирате, в поле MAC Address of Child PC. Или може да изберете MAC адреса от падащ списък All Address in Current LAN.
3. Опишете (напр. позволи Google) уебсайт, който е позволен за посещение, в поле Website Description.
4. Въведете името на сайта, или пълно име или само ключова дума (напр. google) в поле Allowed Domain Name. Всяко домейн име с ключови думи в него (www.google.com, www.google.com.cn) ще бъде позволено.
5. Изберете от падащ списък Effective Time схемата (напр. Schedule_1), която искате да активирате. Ако няма подходящи за вас схеми, натиснете Schedule в червено отдолу, за да отидете на страницата за подробни настройки за схема и създайте схема (разрешено време), каквото ви е необходимо.

6. В поле Status, можете да изберете Enabled или Disabled за активиране или деактивиране на записа.

7. Натиснете бутон Save.

Натиснете бутон Enable All за активиране на всички правила от списъка. Натиснете бутон Disable All за деактивиране на всички правила от списъка. Натиснете бутон Delete All за изтриване на всички записи в таблицата.

Натиснете бутон Next за преминаване към следваща страница или бутон Previous за връщане на предходна страница.

Add or Modify Parental Control Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time settings](#)".

MAC Address of Child PC:

All MAC Address In Current LAN:

Website Description:

Allowed Domain Name:

Effective Time:

The time schedule can be set in "Access Control->[Schedule](#)"

Status:

Фигура 4-43 Добавяне и промяна на настройки за родителски контрол

Например: Ако искате компютър на дете с MAC адрес 00-11-22-33-44-AA да има достъп до www.google.com само в събота, а родителският компютър с MAC адрес 00-11-22-33-44-BB да е без ограничение, трябва да следвате долните настройки.

1. Изберете меню "Parental Control" отляво, за да влезете в страница Parental Control Settings. Маркирайте Enable и въведете MAC адрес 00-11-22-33-44-BB в поле MAC Address of Parental PC.

2. Натиснете "Access Control → Schedule" отляво, за да влезете в страница Schedule Settings.

Натиснете бутон Add New... за създаване на нова схема с Schedule Description на Schedule_1, ден - събота и време - цял ден, 24 часа.

3. Изберете меню “Parental Control” отляво, за да се върнете обратно на страница Add or Modify Parental Control Entry:

- ◆ Натиснете **Add New...** бутона.
- ◆ Въведете 00-11-22-33-44-AA в поле **MAC Address of Child PC**.
- ◆ Въведете “Allow Google” в поле **Website Description**.
- ◆ Въведете “www.google.com” в поле **Allowed Domain Name**.
- ◆ Изберете “Schedule_1”, която създадохте току-що, от падащ списък **Effective Time**.
- ◆ В поле **Status**, изберете Enable.

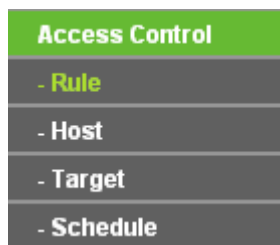
4. Натиснете Save за запазване на настройките.

След това отивате обратно н страница Parental Control Settings и ще видите следния списък, както е показан на Фигура 4-44.

| ID | MAC address | Website Description | Schedule | Status | Modify |
|----|-------------------|---------------------|------------|---------|---|
| 1 | 00-11-22-33-44-AA | Allow Google | Schedule_1 | Enabled | Edit Delete |

Фигура 4-44 Настройки за родителски контрол

4.11 Контрол на достъпа



Фигура 4-45 Контрол на достъпа

Има четири подменюта под меню Access Control, както са показани на Фигура 4-45: **Rule**, **Host**, **Target** и **Schedule**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция.

4.11.1 Rule (правило)

Изберете меню “Access Control → Rule” и можете да видите и да задавате правила за контрол на достъпа, както е показано на Фигура 4-46.

Access Control Rule Management

Enable Internet Access Control

Default Filter Policy

Allow the packets not specified by any access control policy to pass through the Router

Deny the packets not specified by any access control policy to pass through the Router

| ID | Rule Name | Host | Target | Schedule | Action | Status | Modify |
|----|-----------|------------------------|--------------------------|----------------------------|--------|---------|---|
| 1 | Rule_1 | Host_1 | Target_1 | Schedule_1 | Allow | Enabled | Edit Delete |

ID To ID

Page

Фигура 4-46 Управление на правило за контрол на достъпа

- Enable Internet Access Control** - Маркирайте, за да активирате функцията Internet Access Control, така че зададената политика за филтриране да влезе в сила.
- Rule Name** - Тук се показва името на правилото и това име е уникално.
- Host** - Тук се показва хост, избран в съответстващото правило.
- Target** - Тук се показва таргета, избран в съответстващото правило.
- Schedule** - Тук се показва избраната схема за съответното правило.
- Action** - Тук се показва действието, което рутерът предприема за работа с пакетите. Може да е **Allow** или **Deny**. **Allow** означава, че рутерът разрешава на пакетите да преминат през рутера. **Deny** означава, че рутерът отказва преминаването на пакетите през рутера.
- Status** - Това поле показва статуса на правилото. **Enabled** означава, че правилото ще действа, **Disabled** означава, че правилото няма да се прилага.
- Modify** - Тук можете да редактирате или изтриете съществуващо правило.

За добавяне на нов запис, моля следвайте долните стъпки.

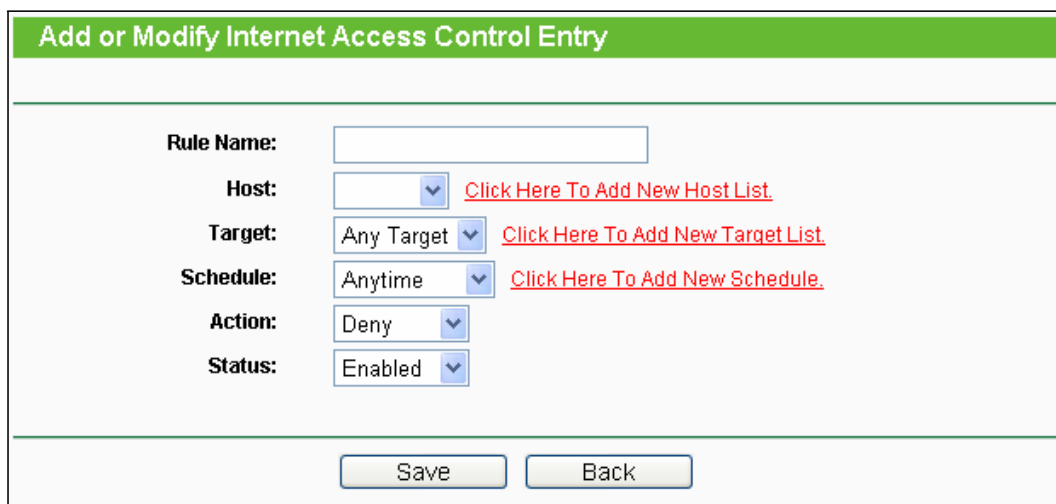
1. Натиснете бутон Add New... и ще се покаже прозореца, който виждате на Фигура 4-47.
2. Задайте име (напр. Rule_1) за правилото в поле Rule Name.
3. Изберете хост от падащ списък Host или изберете "Click Here To Add New Host List".
4. Изберете таргет от падащ списък Target или изберете "Click Here To Add New Target List".

5. Изберете схема от падащ списък Schedule или изберете “Click Here To Add New Schedule”.
6. В поле **Action** изберете **Deny** или **Allow**.
7. В поле Status изберете Enabled или Disabled за активиране или деактивиране на вашия запис.
8. Натиснете бутон Save.

Натиснете бутон Enable All за активиране на всички правила от списъка. Натиснете бутон Disable All за деактивиране на всички правила от списъка. Натиснете бутон Delete All за изтриване на всички записи в таблицата.

Move - Можете да промените реда на записите. Предни записи са преди задни. Въведете ID номерът в първата позиция и друг ID номер във втората позиция и след това натиснете бутон **Move**, за да промените реда на записите.

Натиснете бутон Next за преминаване към следваща страница, или натиснете бутон Previous за връщане на предходна страница.



The screenshot shows a web interface titled "Add or Modify Internet Access Control Entry". It contains the following fields and options:

- Rule Name:** An empty text input field.
- Host:** A dropdown menu with a blue arrow, next to a red link: [Click Here To Add New Host List](#).
- Target:** A dropdown menu with "Any Target" selected and a blue arrow, next to a red link: [Click Here To Add New Target List](#).
- Schedule:** A dropdown menu with "Anytime" selected and a blue arrow, next to a red link: [Click Here To Add New Schedule](#).
- Action:** A dropdown menu with "Deny" selected and a blue arrow.
- Status:** A dropdown menu with "Enabled" selected and a blue arrow.

At the bottom of the form are two buttons: "Save" and "Back".

Фигура 4-47 Добавяне или промяна на запис за достъп на таргет

Например: Ако желаете да позволите на хост с MAC адрес 00-11-22-33-44-AA достъп до www.google.com само от 18:00 до 20:00 ч. в събота и неделя и да забраните достъпа до Интернет на други хостове в локалната мрежа, трябва да следвате долните настройки:

1. Натиснете “**Access Control** → **Host**” отляво, за да влезете в страница Host Settings. Добавете нов запис с описание на хост Host_1 и MAC адрес - 00-11-22-33-44-AA.
2. Натиснете “**Access Control** → **Target**” отляво и влезте в страница Target Settings. Добавете нов запис с описание на таргета - Target_1 и име на домейн - www.google.com.

3. Натиснете **“Access Control → Schedule”** отляво , за да влезете в страница Schedule Settings. Добавете нов запис с описание за схема - Schedule_1, ден - Sat and Sun, начално време -1800 и край - 2000.
4. Натиснете **“Access Control → Rule”** отляво за връщане в страница Access Control Rule Management. Изберете **“Enable Internet Access Control”** и изберете "Deny the packets not specified by any access control policy to pass through the Router".
5. Натиснете бутон Add New... за добавяне на ново правило, както следва:
 - ♦ В поле **Rule Name** създайте име на правилото. Това име трябва да е уникално, например Rule_1.
 - ♦ В поле **Host** изберете Host_1.
 - ♦ В поле **Target** изберете Target_1.
 - ♦ В поле **Schedule** изберете Schedule_1.
 - ♦ В поле **Action** изберете Allow.
 - ♦ В поле **Status**, изберете Enable.
 - ♦ Натиснете Save за потвърждение на настройките.

След това ще се върнете на прозореца за управление на правило за контрол на достъпа и ще видите следния списък.

| ID | Rule Name | Host | Target | Schedule | Action | Status | Modify |
|----|-----------|------------------------|--------------------------|----------------------------|--------|---------|---|
| 1 | Rule_1 | Host_1 | Target_1 | Schedule_1 | Allow | Enabled | Edit Delete |

4.11.2 Хост

Изберете меню **“Access Control → Host”** и можете да видите и зададете списък за хост на екрана, показан на Фигура 4-48. Този списък е необходим за правилото за контрол на достъпа.

| Host Settings | | | |
|--|------------------|--------------------------------|---|
| ID | Host Description | Information | Modify |
| 1 | Host_1 | IP: 192.168.0.1 - 192.168.0.23 | Edit Delete |
| <input type="button" value="Add New..."/> <input type="button" value="Delete All"/> | | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> Current No. <input type="text" value="1"/> <input type="button" value="Page"/> | | | |

Фигура 4-48 Настройки за хост

- Host Description** - Тук се показва описанието на хост, което трябва е уникално.
- Information** - Тук се показва информация за хоста. Може да е IP или MAC.
- Modify** - Промяна или изтриване на съществуващ запис.

За добавяне на нов запис, моля следвайте долните стъпки.

1. Натиснете бутон Add New... .
2. В поле Mode изберете IP Address или MAC Address.
 - 1) Ако изберете IP адрес, ще се покаже екрана от Фигура 4-49.
 - ♦ В поле Host Description създайте уникално описание на хоста (напр. Host_1).

2) В поле LAN IP Address въведете IP адреса.

- ♦ Ако изберете MAC адрес ще се покаже екрана от Фигура 4-50.

1) В поле Host Description създайте уникално описание на хоста (напр. Host_1).

2) В поле MAC Address въведете MAC адреса.

3. Натиснете бутон Save за потвърждение на настройките.

Натиснете бутон Delete All за изтриване на всички записи в таблицата.

Натиснете бутон Next за преминаване към следваща страница, или натиснете бутон Previous за връщане на предходна страница.

The screenshot shows a web form titled "Add or Modify a Host Entry". It has a green header bar. Below the header, there are three input fields: "Mode" is a dropdown menu set to "IP Address"; "Host Description" is a text box containing "Host_1"; "LAN IP Address" is a range input box containing "192.168.0.1" and "192.168.0.23" separated by a hyphen. At the bottom of the form are two buttons: "Save" and "Back".

Фигура 4-49 Добавяне или промяна на запис за хост

The screenshot shows the same "Add or Modify a Host Entry" form. In this version, the "Mode" dropdown menu is set to "MAC Address". The "Host Description" text box still contains "Host_1". The "MAC Address" text box contains "00-11-22-33-44-AA". The "Save" and "Back" buttons are still present at the bottom.

Фигура 4-50 Добавяне или промяна на запис за хост

Например: Ако искате да ограничите Интернет дейността на хост с MAC адрес 00-11-22-33-44-AA, трябва да направите следните настройки:

1. Натиснете бутон Add New... както е на Фигура 4-48, за да влезете в страница за добавяне или промяна на хост.
2. В поле Mode изберете MAC адрес от падащия списък.
3. В поле Host Description създайте уникално описание на хоста (напр. Host_1).
4. В поле MAC Address въведете 00-11-22-33-44-AA.
5. Натиснете Save за запазване на настройките.

След това ще се върнете на прозореца за настройки на хост и ще видите следния списък.

| ID | Host Description | Information | Modify |
|----|------------------|------------------------|---|
| 1 | Host_1 | MAC: 00-11-22-33-44-AA | Edit Delete |

4.11.3 Таргет

Изберете меню “Access Control → Target” и ще видите и зададете списък за таргет на екрана, показан на Фигура 4-51. Този списък е необходим за правилото за контрол на достъпа.



| ID | Target Description | Information | Modify |
|----|--------------------|-----------------------------------|---|
| 1 | Target_1 | 192.168.0.2 - 192.168.0.23/21/TCP | Edit Delete |

Фигура 4-51 Настройки за таргет

- Target Description** - Тук се показва описанието на таргета, като то трябва да е уникално.
- Information** - Таргетът може да е IP адрес, порт или име на домейн.
- Modify** - Промяна или изтриване на съществуващ запис.

За добавяне на нов запис, моля следвайте долните стъпки.

1. Натиснете бутон Add New... .
 2. В поле Mode изберете IP Address или Domain Name.
 - ♦ Ако изберете IP адрес, ще се покаже екрана от Фигура 4-52.
 - 1) В поле Target Description създайте уникално описание за таргета (напр. Target_1).
 - 2) В поле IP Address въведете IP адреса на таргета.
 - 3) Изберете обща услуга от падащ списък Common Service Port, така Target Port ще бъде автоматично попълнен. Ако падащият списък Common Service Port не включва услугата, която желаете, посочете ръчно Target Port.
 - 4) В поле Protocol изберете TCP, UDP, ICMP или ALL от падащия списък.
 - ♦ Ако изберете Domain Name ще се появи екрана от Фигура 4-53.
 - 1) В поле Target Description създайте уникално описание за таргета (напр. Target_1).
 - 2) В поле Domain Name въведете име на домейн, или пълно име или ключови думи (например, google). Всяко име на домейн с ключови думи в него (www.google.com, www.google.cn) ще бъде блокирано или позволено. Можете да въведете 4 имена на домейни.
 3. Натиснете бутон Save.
- Натиснете бутон Delete All за изтриване на всички записи в таблицата.

Натиснете бутон Next за преминаване към следваща страница, или натиснете бутон Previous за връщане на предходна страница.

The screenshot shows a web form titled "Add or Modify an Access Target Entry". The form has a green header bar with the title. Below the header, there are several input fields and dropdown menus:

- Mode:** A dropdown menu with "IP Address" selected.
- Target Description:** A text input field.
- IP Address:** Two text input fields separated by a hyphen, representing IP address ranges.
- Target Port:** Two text input fields separated by a hyphen, representing port ranges.
- Protocol:** A dropdown menu with "ALL" selected.
- Common Service Port:** A dropdown menu with "--please select--" selected.

At the bottom of the form, there are two buttons: "Save" and "Back".

Фигура 4-52 Добавяне или промяна на запис за достъп на таргет

The screenshot shows a web form titled "Add or Modify an Access Target Entry". The form has a green header bar with the title. Below the header, there are several input fields and dropdown menus:

- Mode:** A dropdown menu with "Domain Name" selected.
- Target Description:** A text input field.
- Domain Name:** Four stacked text input fields for entering domain information.

At the bottom of the form, there are two buttons: "Save" and "Back".

Фигура 4-53 Добавяне или промяна на запис за достъп на таргет

Например: Ако искате да ограничите Интернет дейността на хост с MAC адрес 00-11-22-33-44-AA в локалната мрежа само за достъп до www.google.com, трябва първо да направите следните настройки:

1. Натиснете бутон Add New... както е показано на Фигура 4-51, за да влезете в страница Добавяне или промяна на запис за достъп на таргет.
2. В поле Mode, от падащия списък изберете име на домейн.
3. В поле Target Description създайте уникално описание на таргета (напр. Target_1).
4. В поле Domain Name въведете www.google.com.
5. Натиснете Save за запазване на настройките.

След това ще се върнете обратно на страницата с настройки за таргет и ще видите следния списък:

| ID | Target Description | Information | Modify |
|----|--------------------|--|---|
| 1 | Target_1 | www.google.com | Edit Delete |

4.11.4 Схема

Изберете меню “Access Control → Schedule” и можете да видите и да зададете списък за схеми в екрана, показан на Фигура 4-54. Този списък ви е необходим за правилото за контрол на достъпа.

| Schedule Settings | | | | |
|-------------------|----------------------|-----|---------------|---|
| ID | Schedule Description | Day | Time | Modify |
| 1 | Schedule_1 | Sat | 00:00 - 24:00 | Edit Delete |

Page

Фигура 4-54 Настройки за схема

- Schedule Description** - Тук се показва описанието на схемата, което трябва да е уникално.
- Day** - Тук се посочва ден (дни) в седмицата.
- Time** - Посочва се определен период време от деня.
- Modify** - Редактирате или изтривате съществуваща схема.

За добавяне на нова схема следвайте долните стъпки:

1. Натиснете бутон Add New... показан на Фигура 4-54, появява се екрана от Фигура 4-55.
 2. В поле Schedule Description създайте уникално описание на схемата (напр. Schedule_1).
 3. В поле Day изберете ден или дни, които желаете.
 4. В поле Time можете да изберете цял ден - 24 часа или да въведете начално и крайно време в съответните полета.
 5. Натиснете Save за запазване на настройките.
- Натиснете бутон Delete All за изтриване на всички записи в таблицата.
- Натиснете бутон Next за преминаване към следваща страница, или натиснете бутон Previous за връщане на предходна страница.

| Advance Schedule Settings | |
|---|--|
| Note: The Schedule is based on the time of the Router. | |
| Schedule Description: | <input type="text"/> |
| Day: | <input checked="" type="radio"/> Everyday <input type="radio"/> Select Days <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun |
| Time: | all day-24 hours: <input checked="" type="checkbox"/> |
| Start Time: | <input type="text"/> (HHMM) |
| Stop Time: | <input type="text"/> (HHMM) |
| <input type="button" value="Save"/> <input type="button" value="Back"/> | |

Фигура 4-55 Подробни настройки за схема

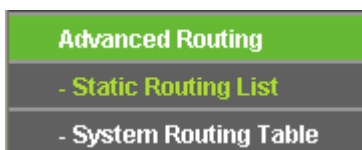
Например: Ако искате да ограничите Интернет дейността на хост с MAC адрес 00-11-22-33-44-AA за достъп www.google.com само от 18:00 до 20:00 ч. в събота и неделя, трябва първо да направите следните настройки:

1. Натиснете бутон Add New... както е показано на Фигура 4-54, за да влезете в страница Подробни настройки за схема.
2. В поле Schedule Description създайте уникално описание на схемата (напр. Schedule_1).
3. В поле Day изберете радио бутон Select Days и след това маркирайте събота и неделя (Sat и Sun).
4. В поле Time въведете 1800 в поле Start Time и 2000 в поле Stop Time.
5. Натиснете Save за запазване на настройките.

След това ще се върнете на страницата за настройки на схема и ще видите следния списък.

| ID | Schedule Description | Day | Time | Modify |
|----|----------------------|---------|---------------|---|
| 1 | Schedule_1 | Sat Sun | 18:00 - 20:00 | Edit Delete |

4.12 Подробна маршрутизация

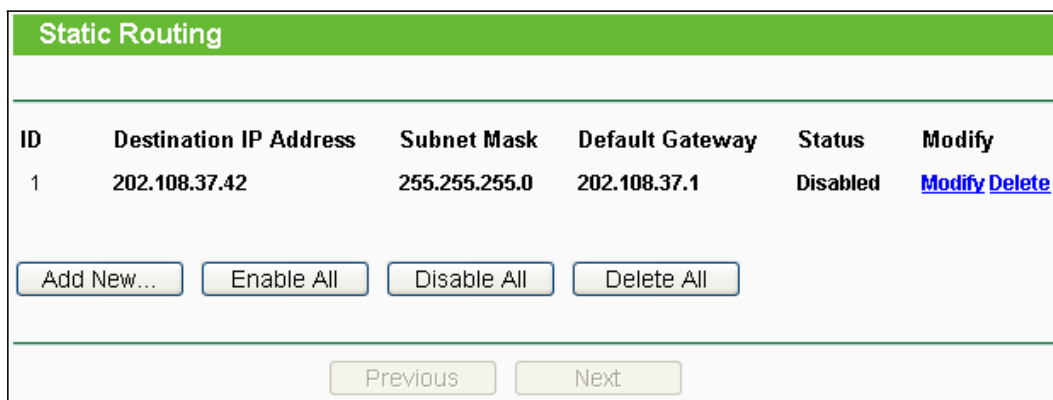


Фигура 4-56 Подробно маршрутизиране

Има две подменюта под меню Network (показани на Фигура 4-56): **Static Routing List** и **System Routing Table**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция.

4.12.1 Статична маршрутизация

Изберете меню “**Advanced Routing** → **Static Routing**” и можете да конфигурирате статичен маршрут в екрана, показан на Фигура 4-57. Статичният маршрут представлява предварително определен път, по който трябва да пътува мрежовата информация, за да достигне даден порт или мрежа.



| ID | Destination IP Address | Subnet Mask | Default Gateway | Status | Modify |
|----|------------------------|---------------|-----------------|----------|---|
| 1 | 202.108.37.42 | 255.255.255.0 | 202.108.37.1 | Disabled | Modify Delete |

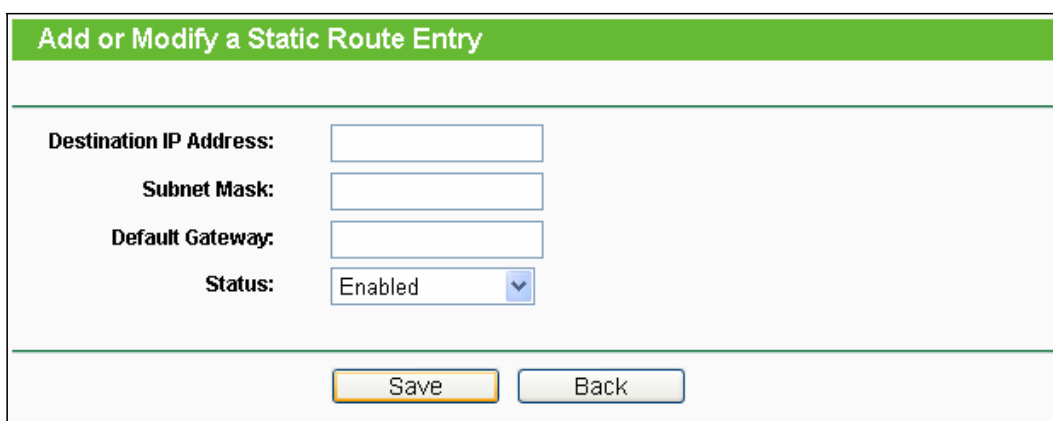
Buttons: Add New..., Enable All, Disable All, Delete All

Navigation: Previous, Next

Фигура 4-57 Статична маршрутизация

За добавяне на записи за статична маршрутизация следвайте долните стъпки.

1. Натиснете **Add New...**, виж Фигура 4-57, и ще видите следния екран - Фигура 4-58.



Add or Modify a Static Route Entry

Destination IP Address:

Subnet Mask:

Default Gateway:

Status:

Buttons: Save, Back

Фигура 4-58 Добавяне или промяна на запис за статичен маршрут

2. Въведете следните данни:

- Destination IP Address - Destination IP Address** е адреса на мрежата или хоста, който искате да зададете на статичен маршрут.
- Subnet Mask** - Subnet Mask определя, коя част от IP адрес е мрежовата част и коя част е за хоста.
- Default Gateway** - Това е IP адреса на шлюза, който позволява осъществяването на контакт между рутера и мрежата или хоста.

3. Изберете Enabled или Disabled за този запис от падащ списък Status.

4. Натиснете бутон Save за активиране на записа.

Натиснете бутон Delete за изтриване на запис.

Натиснете бутон Enable All за активиране на всички записи. Натиснете бутон Disable All за деактивиране на всички записи. Натиснете бутон Delete All за изтриване на всички записи.

Натиснете бутон Previous, за да видите информацията на предходния екран или натиснете бутон Next, за да видите информацията на следващия екран.

4.12.2 Таблица за маршрутизация на системата

Изберете меню “**Advanced Routing** → **System Routing Table**” и можете да видите всички валидни и използвани записи за маршрут. Destination IP address, Subnet Mask, Gateway и Interface са показани за всеки запис.

| System Routing Table | | | | |
|----------------------|------------------------|---------------|---------|------------|
| ID | Destination IP Address | Subnet Mask | Gateway | Interface |
| 1 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | LAN & WLAN |
| 2 | 1.0.0.0 | 255.0.0.0 | 0.0.0.0 | WAN |
| 3 | 239.0.0.0 | 255.0.0.0 | 0.0.0.0 | LAN & WLAN |
| 4 | 0.0.0.0 | 0.0.0.0 | 1.0.0.1 | WAN |

Refresh

- Destination IP Address - Destination IP Address** е адреса на мрежата или хоста, на който е зададен статичен маршрут.

- Subnet Mask** - определя, коя част от IP адрес е мрежовата част и коя част е за хоста.
- Gateway** - Това е IP адресът на шлюза, който позволява контакт между рутера и мрежата или хост.
- Interface** - Този интерфейс ви казва дали Destination IP Address е в **LAN & WLAN** (вътрешна кабелна или безжична мрежа), или **WAN(Internet)**.

Натиснете бутон Refresh за обновяване на всички елементи.

4.13 Контрол на честотна лента



Фигура 4-59

Има две подменюта под меню Bandwidth Control, както е показано на Фигура 4-59: Кликнете върху някое от тях и ще можете да конфигурирате съответната функция. Подробни обяснения за всяко подменю са дадени по-долу.

4.13.1 Настройки за контрол

Изберете меню “**Bandwidth Control** → **Control Settings**” и можете да конфигурирате Egress Bandwidth и Ingress Bandwidth (изходна и входна честотна лента) в показания екран. Стойностите, които задавате трябва да са под 100000Kbps. За оптимален контрол на честотна лента, моля изберете правилния тип линия и попитайте вашия доставчик за общо честотна лента за вход и изход.

The image shows a web form titled 'Bandwidth Control Settings'. It contains the following fields and options:

- Enable Bandwidth Control:** An unchecked checkbox.
- Line Type:** Two radio buttons: 'ADSL' (which is selected) and 'Other'.
- Egress Bandwidth:** A text input field containing '512' followed by 'Kbps'.
- Ingress Bandwidth:** A text input field containing '2048' followed by 'Kbps'.
- Save:** A button at the bottom of the form.

Фигура 4-60 Настройки за контрол на честотна лента

- Enable Bandwidth Control** - Маркирайте тази позиция, за да активирате настройките за контрол на честотна лента.
- Line Type** - Изберете правилния тип за вашата мрежова връзка. Ако не знаете какво да изберете, попитайте вашия Интернет доставчик.
- Egress Bandwidth** - Скоростта на качване през Интернет порта.

- Ingress Bandwidth** - Скоростта на изтегляне през Интернет порта.

4.13.2 Списък на правилата

Изберете меню “**Bandwidth Control** → **Rules List**” и можете да видите и конфигурирате правила за контрол на честотна лента

на показания по-долу екран.

| Bandwidth Control Rules List | | | | | | | |
|------------------------------|-------------------------------|------------------------|------|-------------------------|------|-------------------------------------|---|
| ID | Description | Egress Bandwidth(Kbps) | | Ingress Bandwidth(Kbps) | | Enable | Modify |
| | | Min | Max | Min | Max | | |
| 1 | 192.168.0.2 - 192.168.0.23/21 | 0 | 1000 | 0 | 4000 | <input checked="" type="checkbox"/> | Modify Delete |

Now is the page

Фигура 4-61 Списък правила за контрол на честотна лента

- Description** - Това е информация за правилата, като например обхванати адреси.
- Egress bandwidth** - Това поле показва максимална и минимална честотна лента за качване през WAN порта; по подразбиране е 0.
- Ingress bandwidth** - Това поле показва максимална и минимална честотна лента за изтегляне през WAN порта; по подразбиране е 0.
- Enable** - Показва статуса на правилото.
- Modify** - Натиснете Modify за промяна на правилото. Натиснете Delete за изтриване на правилото.

За добавяне/ промяна на правило за контрол на честотна лента, следвайте долните стъпки.

Стъпка 1: Натиснете Add New... , показан на Фигура 4-61, ще видите екрана, показан на Фигура 4-62.

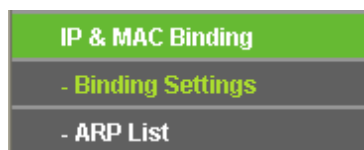
Стъпка 2: Въведете информацията, както е показано по-долу.

| Bandwidth Control Rule Settings | |
|---|--|
| Enable: | <input checked="" type="checkbox"/> |
| IP Range: | <input type="text" value="192.168.0.2"/> - <input type="text" value="192.168.0.23"/> |
| Port Range: | <input type="text" value="21"/> - <input type="text"/> |
| Protocol: | <input type="text" value="ALL"/> |
| | Min Bandwidth(Kbps) Max Bandwidth(Kbps) |
| Egress Bandwidth: | <input type="text" value="0"/> <input type="text" value="1000"/> |
| Ingress Bandwidth: | <input type="text" value="0"/> <input type="text" value="4000"/> |
| <input type="button" value="Save"/> <input type="button" value="Back"/> | |

Фигура 4-62 Настройки за правило за контрол на честотна лента

Стъпка 3: Натиснете бутон Save.

4.14 Настройка за свързване на IP & MAC



Фигура 4-63 Меню IP & MAC свързване

Има две подменюта под меню IP&MAC свързване (показани на Фигура 4-63): **Binding Settings** и **ARP List**. Натиснете някое от тях и ще можете да сканирате или конфигурирате съответната функция. Подробни обяснения за всяко подменю са дадени по-долу.

4.14.1 Настройки за свързване

Тази страница показва таблица IP & MAC Binding Setting; можете да работите с нея според вашето желание (вижте Фигура 4-64).

 A screenshot of the 'Binding Settings' page. At the top, there's a green header 'Binding Settings'. Below it, 'ARP Binding:' is set to 'Disable' (selected with a radio button) and 'Enable' (unselected). A 'Save' button is to the right. Below this is a table with the following data:

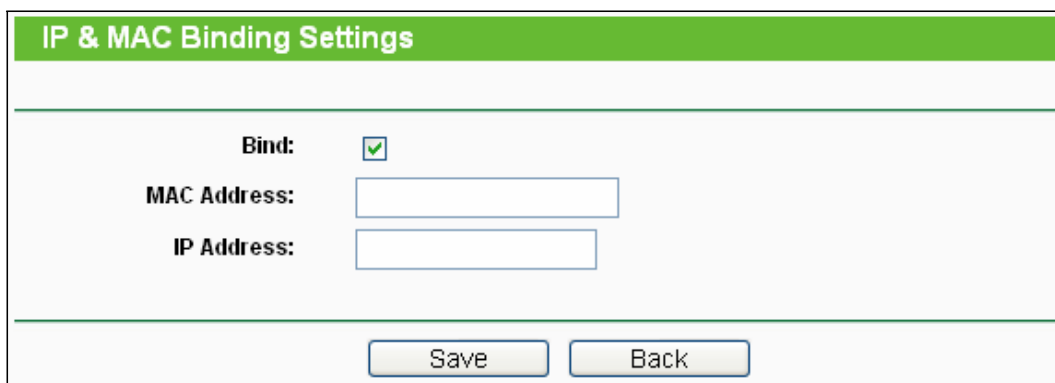
| ID | MAC Address | IP Address | Bind | Modify |
|----|-------------------|---------------|-------------------------------------|---|
| 1 | 00-11-22-33-44-BB | 192.168.0.100 | <input checked="" type="checkbox"/> | Modify Delete |

 Below the table are buttons: 'Add New...', 'Enable All', 'Disable All', 'Delete All', and 'Find'. At the bottom, there are 'Previous' and 'Next' buttons, and a 'Current No. 1' dropdown menu followed by 'Page'.

Фигура 4-64 Настройка за свързване

- MAC Address** - MAC адресът на контролиран компютър в локалната мрежа.
- IP Address** - Зададеният IP адрес на контролиран компютър в локалната мрежа.
- Bind** - Маркирайте тази опция за активиране на ARP свързване за дадено устройство.
- Modify** - Промяна или изтриване на съществуващ запис.

Когато искате да добавите или промените запис за IP & MAC свързване, можете да натиснете бутон Add New... или бутон Modify и ще преминете на следващата страница. Тази страница се използва за добавяне или промяна на запис за IP & MAC Binding, вижте Фигура 4-65.



IP & MAC Binding Settings

Bind:

MAC Address:

IP Address:

Save Back

Фигура 4-65 Меню IP & MAC свързване

За добавяне на записи за IP & MAC свързване изпълнете следните стъпки.

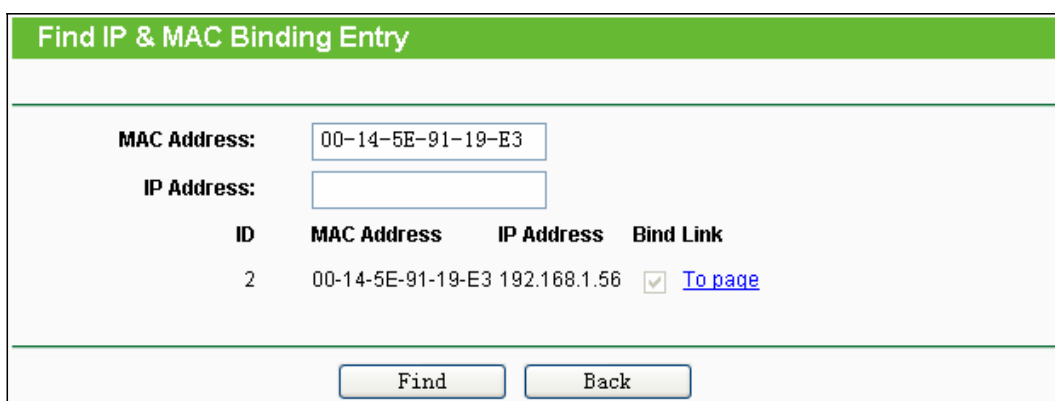
1. Натиснете бутон Add New... както е показано на Фигура 4-64.
2. Въведете MAC адрес и IP адрес.
3. Маркирайте позиция Bind.
4. Натиснете бутон Save за запазване.

За промяна или изтриване на съществуващ запис, изпълнете следните стъпки.

1. Намерете желанния запис в таблицата.
2. Натиснете Modify или Delete според желанието ви, в колона Modify.

За откриване на съществуващ запис изпълнете следните стъпки.

1. Натиснете бутон Find, както е показано на Фигура 4-64.
2. Въведете MAC адрес или IP адрес.
3. Натиснете бутон **Find** в страницата, показана на Фигура 4-66.



Find IP & MAC Binding Entry

MAC Address:

IP Address:

| ID | MAC Address | IP Address | Bind Link |
|----|-------------------|--------------|---|
| 2 | 00-14-5E-91-19-E3 | 192.168.1.56 | <input checked="" type="checkbox"/> To page |

Find Back

Фигура 4-66 Откриване на запис за свързване на IP & MAC

Натиснете бутон Enable All за активиране на всички записи. Натиснете бутон Delete All за изтриване на всички записи.

4.14.2 ARP списък

За управление на компютъра можете да наблюдавате компютрите в LAN като маркирате

връзката на MAC адрес и IP адрес в ARP list и така да конфигурирате и елементи в ARP списъка. Тази страница показва ARP списъка; показва всички съществуващи записи за IP & MAC свързване както е показано на Фигура 4-67.

| ARP List | | | | |
|----------|-------------------|---------------|---------|---|
| ID | MAC Address | IP Address | Status | Configure |
| 1 | 40-61-86-FC-74-93 | 192.168.0.100 | Unbound | Load Delete |

Фигура 4-67 ARP списък

- MAC Address** - MAC адресът на контролиран компютър в локалната мрежа.
- IP Address** - Зададеният IP адрес на контролиран компютър в локалната мрежа.
- Status** - Указва дали MAC и IP адресите са свързани или не.
- Configure** - Зареждане или изтриване на елемент.
 - ◆ **Load** - Зареждане на елемент в списък IP & MAC свързване.
 - ◆ **Delete** - Изтриване на елемент.

Натиснете бутон Bind All за свързване на всички текущи елементи, налични след активиране. Натиснете бутон Load All за зареждане на всички елементи в списъка за IP & MAC свързване.

Натиснете бутон Refresh за обновяване на всички елементи.

→ Забележка:

Даден елемент не може да бъде качен в списък за IP & MAC свързване, ако IP адресът на елемента е бил зареждан преди. Ще се появи екран със съобщение за грешка. По подобен начин "Load All" зарежда само елемент без смущение по списъка за IP & MAC свързване.

4.15 Динамична DNS

Изберете меню "Dynamic DNS" и можете да конфигурирате функцията динамична DNS.

Рутерът предлага характеристиката DDNS (динамична система за имена на домейни), която позволява хостван на уебсайт, FTP сървър или пощенски сървър с фиксирано име на домейн (посочено от вас) и динамичен IP адрес, след това вашите приятели ще могат да се свързват към вашия сървър чрез въвеждане на вашето домейн име, без значение какъв е вашия IP адрес. Преди да използвате тази характеристика, трябва да заявите това пред доставчици на DDNS услугата, като www.comexe.cn, www.dyndns.org, или www.no-ip.com. Доставчикът на клиентска услуга за динамична DNS ще ви даде парола или ключ.

4.15.1 Comexe.cn DDNS

Ако доставчикът на услуга за динамична DNS, който сте избрали е www.comexe.cn, ще се появи страницата, показана на Фигура 4-68.

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

Фигура 4-68 Comexe.cn DDNS настройки

За настройка на DDNS изпълнете следните инструкции:

1. Въведете Domain Name, което сте получили от вашия доставчик на динамична DNS.
2. Въведете User Name за вашия DDNS акаунт.
3. Въведете Password за вашия DDNS акаунт.
4. Натиснете бутон Login за вход в DDNS услугата.

Connection Status - Тук се показва статуса на DDNS връзката. Натиснете Logout за изход от DDNS услугата.

4.15.2 Dyndns.org DDNS

Ако доставчикът на динамична DNS, който сте избрали е www.dyndns.org, ще се появи страницата, показана на Фигура 4-69.

DDNS

Service Provider: Dyndns (www.dyndns.org) [Go to register...](#)

User Name: username

Password: ●●●●●●●●

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Login Logout

Save

Фигура 4-69 Настройки за Dyndns.org DDNS

За настройка на DDNS изпълнете следните инструкции:

5. Въведете User Name за вашия DDNS акаунт.
6. Въведете Password за вашия DDNS акаунт.
7. Въведете Domain Name, което сте получили от вашия доставчик на динамична DNS.
8. Натиснете бутон Login за вход в DDNS услугата.

Connection Status - Тук се показва статуса на DDNS връзката. Натиснете Logout за изход от DDNS услугата.

4.15.3 No-ip.com DDNS

Ако доставчикът на динамична DNS услуга, който сте избрали, е www.no-ip.com, ще се появи страницата, показана на Фигура 4-70.

DDNS

Service Provider: No-IP (www.no-ip.com) [Go to register...](#)

User Name: username

Password: ●●●●●●●●

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Login Logout

Save

Фигура 4-70 No-ip.com DDNS настройки

За настройка на DDNS изпълнете следните инструкции:

1. Въведете User Name за вашия DDNS акаунт.
2. Въведете Password за вашия DDNS акаунт.
3. Въведете Domain Name, което сте получили от вашия доставчик на динамична DNS.
4. Натиснете бутон Login за вход в DDNS услугата.

Connection Status - Тук се показва статуса на DDNS връзката. Натиснете Logout за изход от DDNS услугата.

4.16 Системни инструменти



Фигура 4-71 Меню Системни инструменти

Изберете меню “System Tools” и можете да видите подменютата: **Time Settings, Diagnostic, Firmware Upgrade, Factory Defaults, Backup & Restore, Reboot,**

Password, System Log и **Statistics**. Кликнете върху някое от тях и ще можете да конфигурирате съответната функция. Подробни обяснения за всяко подменю са дадени по-долу.

4.16.1 Настройка за време

Изберете меню “System Tools→Time Setting” и можете да конфигурирате време на следния екран.

The screenshot shows the 'Time Settings' configuration interface. It includes a dropdown for 'Time zone' set to '(GMT+08:00) Beijing, Hong Kong, Perth, Singapore'. The 'Date' field is set to '1/1/2000' (MM/DD/YY) and the 'Time' field is set to '0/1/4' (HH/MM/SS). There are two 'NTP Server' fields, both set to '0.0.0.0'. A 'Get GMT' button is present. The 'Enable Daylight Saving' checkbox is unchecked. The 'Start' field is set to 'Mar 3rd Sun 2am' and the 'End' field is set to 'Nov 2nd Sun 3am'. The 'Daylight Saving Status' is 'daylight saving is down'. A note at the bottom states: 'Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server(IP Address or Domain Name) in the above frames.' A 'Save' button is at the bottom.

Фигура 4-72 Настройка за време

- Time Zone** - Изберете вашата времева зона от падащия списък.
- Date** - Въведете дата с формат MM/DD/YY в позициите отдясно.
- Time** - Въведете час с формат HH/MM/SS в позициите отдясно.
- NTP Server I / NTP Server II** - Въведете адрес или домейн на NTP Server I или NTP Server II, след това рутерът ще вземе преференциално времето от NTP сървъра. В допълнение рутерът има някои общи NTP сървъри, така че може автоматично да актуализира часа след свързване към Интернет.
- Enable Daylight Saving** - маркирайте позицията, за да активирате функцията "спестяване от прилагане на лятно часово време".
- Start** - Времето за начало на Daylight Saving. Изберете месеца в първото поле, седмицата във второто поле, деня в третото поле и час в последното поле.
- End** - Времето за край на Daylight Saving. Изберете месеца в първото поле, седмицата във второто поле, деня в третото поле и час в последното поле.
- Daylight Saving Status** - Указва дали се използва Daylight Saving.

За ръчно задаване на време:

1. Изберете вашата местна часова зона.
2. Въведете Дата във формат месец/ден/година.
3. Въведете Час във формат час/минута/секунда.
4. Натиснете Save.

За автоматично задаване на време:

1. Изберете вашата местна часова зона.
2. Въведете адрес или домейна на NTP Server I или NTP Server II.
3. Натиснете бутон Get GMT, за да получите системно време от Интернет, ако имате връзка към Интернет.

За задаване на Daylight Saving:

1. Маркирайте позицията за активиране на Daylight Saving.
2. Изберете начален час от падащия списък в поле Start.
3. Изберете краен час от падащия списък в поле End.
4. Натиснете бутон **Save** за запазване на настройките.

| | |
|-------------------------|--|
| | <input checked="" type="checkbox"/> Enable Daylight Saving |
| Start: | Mar ▾ 2nd ▾ Sun ▾ 2am ▾ |
| End: | Nov ▾ 1st ▾ Sun ▾ 3am ▾ |
| Daylight Saving Status: | daylight saving is up. |

→ Забележка:

1. Тази настройка ще се използва за някои базирани на време функции, като защитна стена например. Трябва да посочите вашата часова зона след успешна регистрация в рутера, в противен случай тези функции няма да работят.
2. Часът се загубва, ако рутерът бъде изключен.
3. Рутерът автоматично получава GMT от Интернет, ако е правилно конфигуриран.
4. Функцията Daylight Saving ще се активира една минута след завършване на конфигурацията.

4.16.2 Диагностика

Изберете меню **“System Tools → Diagnostic”** и можете да използвате Ping или Traceroute функцията за проверка на свързаността на вашата мрежа. Вижте долния екран.

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP Address/ Domain Name:

Ping Count: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Timeout: (100-2000 Milliseconds)

Traceroute Max TTL: (1-30)

Diagnostic Results

The Router is ready.

Фигура 4-73 Инструменти за диагностика

- Diagnostic Tool** - Маркирайте радио бутона за избор на диагностика.
 - ◆ Ping - Този инструмент за диагностика проверява свързаността, достижимост и резолюция на има за даден хост или шлюз.
 - ◆ Traceroute - Този инструмент за диагностика тества изпълнението на връзката.

→ **Забележка:**

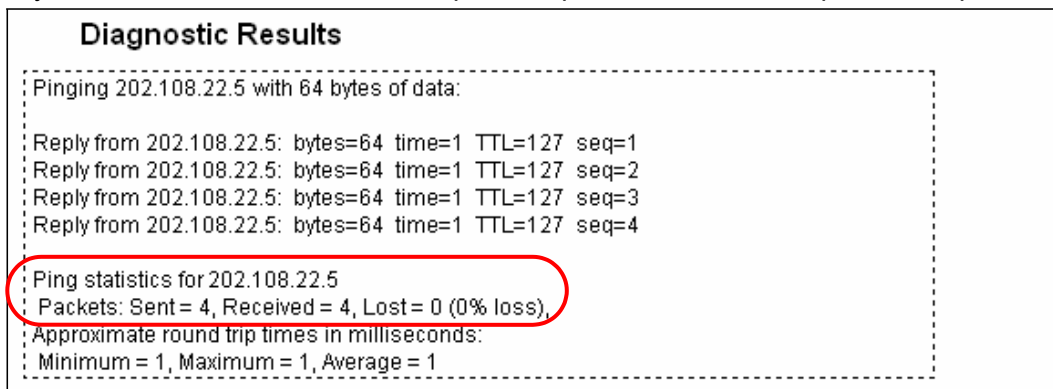
Можете да ползвате ping/traceroute за тестване на числов IP адрес и за име на домейн. Ако pinging/tracerouting проверката на IP адреса е успешна, но pinging/tracerouting проверката на име на домейн не е, може да имате проблем по резолюция на името. В този случай се уверете, че името и домейна, което се посочили може да бъде анализирано с използване на запитвания на система за имена на домейни (DNS).

- IP Address/Domain Name** - Напишете IP адреса на дестинация (например 202.108.22.5) или име на домейн (например http://www.tp-link.com).
- Pings Count** - Броя Ping пакети за Ping връзка.
- Ping Packet Size** - Размерът на Ping пакет.
- Ping Timeout** - Задайте време за изчакване за отговор на всеки Ping пакет. Ако няма отговор в рамките на определеното време, връзката се разпада.
- Traceroute Max TTL** - Максималният брой сегменти за Traceroute връзка.

Натиснете Start за проверка на свързаността към Интернет.

Страница Diagnostic Results показва резултата от диагностиката.

Ако резултатът е подобен на долния екран, свързаността към Интернет е добра.



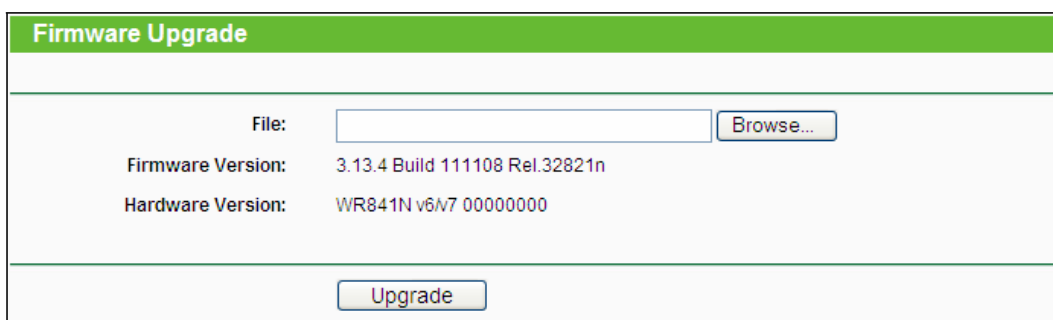
Фигура 4-74 Резултати от диагностика

→ Забележка:

Само един потребител може да ползва инструментите за диагностика в даден момент. Опциите “Number of Pings”, “Ping Size” и “Ping Timeout” се използват за **Ping** функция. Опция “Tracert Hops” се използва за функция **Tracert**.

4.16.3 Надграждане на фърмуер

Изберете меню “System Tools → Firmware Upgrade” и след това можете да актуализирате последната версия на фърмуера за рутера, както е показано на долния екран.



Фигура 4-75 Надграждане на фърмуер

- **Firmware Version** - Показва текущата версия на фърмуера.
- **Hardware Version** - Показва текущата версия на хардуера. Версията на хардуера на файла за надграждане трябва да отговаря на текущата версия на хардуера.

За надграждане на фърмуера на рутера изпълнете следните инструкции:

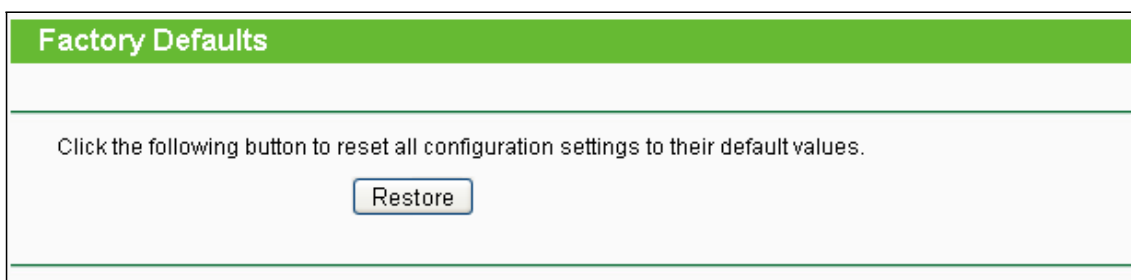
1. Изтеглете последният файл за надграждане на фърмуера от нашия уебсайт (www.tp-link.com). (<http://www.tp-link.com>).
2. Напишете пътя и името на файла за актуализиране в поле **File**. Или натиснете бутон **Browse** за локализиране на файла за актуализация.
3. Натиснете бутон Upgrade.

→ Забележка:

- 1) Нови версии на фърмуер са налични за бесплатно изтегляне на <http://www.tp-link.com>. Няма нужда от надграждане на фърмуера освен ако новият фърмуер има нова функция, която искате да ползвате. Но, когато има проблеми, причинени от рутера, различни от конфигурацията, може да опитате да надградите фърмуера.
- 2) При надграждане на фърмуера на рутера може да загубите текущите конфигурации, затова преди начало на надграждане, запишете си някои от специалните настройки, за да избегнете загуба на важни настройки.
- 3) Не изключвайте рутера и не натискайте бутон Reset по време на надграждане на рутера. Рутерът ще се рестартира след приключване на надграждането.

4.16.4 Заводски настройки

Изберете меню “System Tools → Factory Defaults” и можете да възстановите конфигурациите на рутера до заводски настройки, както е показано на следния екран



Фигура 4-76 Възстановяване на заводски настройки

Натиснете бутон Restore за възстановяване на всички настройки до стойностите им по подразбиране.

- **User Name** по подразбиране: admin
- **Password** по подразбиране: admin
- **IP Address** по подразбиране: 192.168.0.1
- **Subnet Mask** по подразбиране: 255.255.255.0

→ Забележка:

Всички настройки, които сте направили и запазили до сега, ще бъдат загубени с връщането на заводските настройки.

4.16.5 Архивиране и възстановяване

Изберете меню “System Tools → Backup & Restore” и можете да запазите текущата конфигурация на рутера като архивиран файл и да възстановите конфигурацията чрез архивиран файл, както е показано на Фигура 4-77.



Фигура 4-77 Архивиране и възстановяване на конфигурация

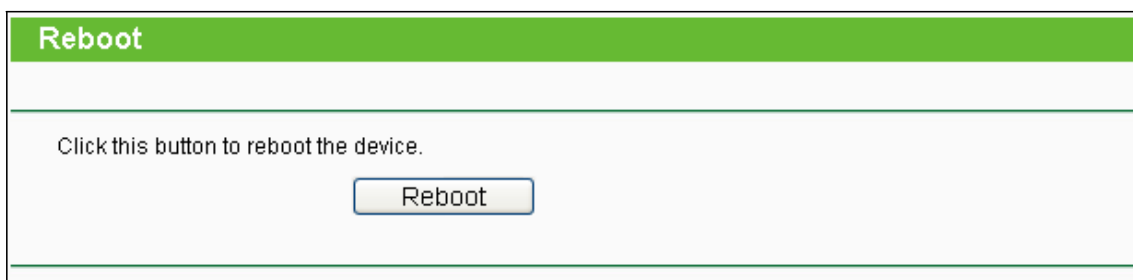
- Натиснете бутон Backup за запазване на всички настройки за конфигурация като архивиран файл на ваш компютър.
- За надграждане на конфигурацията на рутера изпълнете следните инструкции.
 - Натиснете бутон **Browse...** за локализиране на файл за актуализация за рутера или въведете точния път до файл Setting в текстовата позиция.
 - Натиснете бутон **Restore**.

→ **Забележка:**

Текущата конфигурация ще бъде заменена с качването на конфигурационния файл. Процесът по възстановяване продължава 20 секунди и след това рутерът автоматично се рестартира. Рутерът трябва да е включен по време на процеса по надграждане с цел да се избегне повреда.

4.16.6 Рестартиране

Изберете меню “System Tools → Reboot” и тогава можете да натиснете бутон Reboot за рестартиране на рутера чрез следващия екран.



Фигура 4-78 Рестартиране на рутера

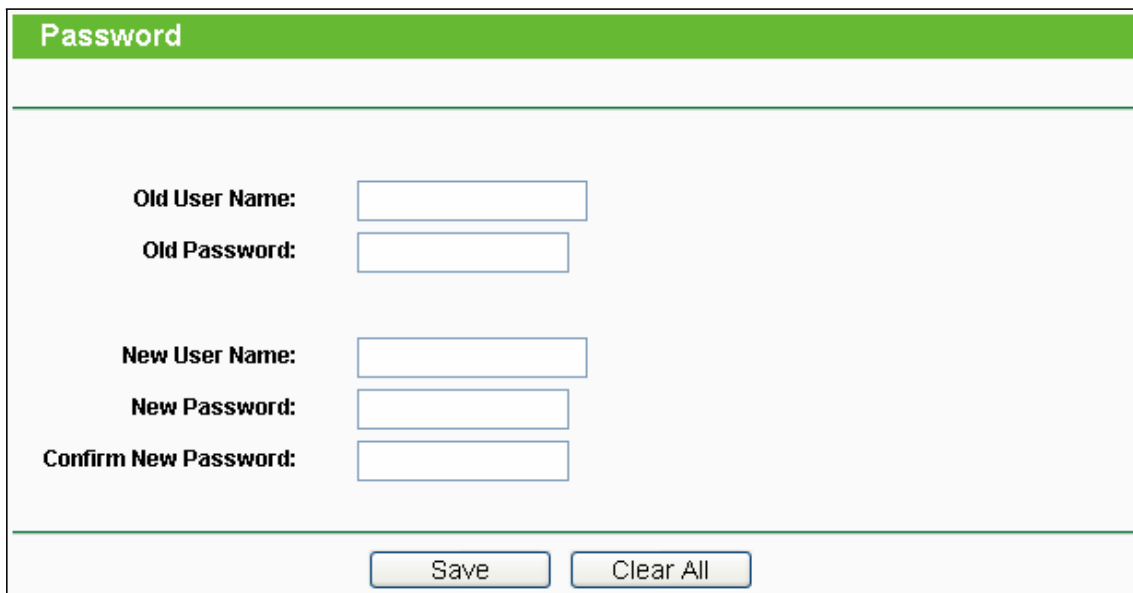
Някои настройки на рутера влизат в сила само след рестартиране, което включва

- Променете LAN IP адреса (системата се рестартира автоматично).
- Промяна на DHCP настройки.
- Промяна на конфигурации за безжична връзка.
- Промяна на порт за уеб управление.
- Надграждане на фърмуера на рутера (системата се рестартира автоматично).
- Възстановяване на рутера до заводски настройки (системата се рестартира автоматично).

- Актуализация на конфигурацията с файл (системата се рестартира автоматично).

4.16.7 Парола

Изберете меню “System Tools → Password” и можете да промените заводските настройки за потребителско име и парола на рутера в следния екран, показан на Фигура 4-79.



The screenshot shows a web interface for changing the router's password. It features a green header with the text "Password". Below the header, there are five input fields arranged in two columns. The left column contains the labels "Old User Name:", "Old Password:", "New User Name:", "New Password:", and "Confirm New Password:". The right column contains five empty text input boxes corresponding to these labels. At the bottom of the form, there are two buttons: "Save" and "Clear All".

Фигура 4-79 Парола

Силно препоръчваме да промените заводските настройки за потребителско име и парола на рутера, тъй като всички потребители, които се опитват да получат достъп до уеб-базираната програма на рутера или бързи настройки, ще бъдат питани за потребителско име и парола по подразбиране на рутера.

→ **Забележка:**

Новото потребителско име и парола не трябва да са с повече от 14 символа и не трябва да има празно разстояние между тях. Въведете новата парола два пъти за потвърждение.

Натиснете бутон Save при завършване. Натиснете бутон Clear All за премахване на всичко.

4.16.8 Системен журнал

Изберете меню “System Tools → System Log” и след това можете да видите записите на рутера.

System Log

Auto Mail Feature: Disabled Mail Settings

Log Type: All **Log Level:** ALL

| Index | Time | Type | Level | Log Content |
|-------|------------------|------|-------|---|
| 1 | 1st day 00:40:37 | PPP | INFO | sent [PADI Host-Uniq(0x000002b7)] |
| 2 | 1st day 00:40:37 | PPP | INFO | rcvd [PADO AC-Name:SOHOROUTER AC-MAC:00:19:66:77:51:81] |
| 3 | 1st day 00:40:37 | PPP | INFO | sent [PADR Host-Uniq(0x000002b7)] |
| 4 | 1st day 00:40:37 | PPP | INFO | rcvd [PADS sess-id(16567)] |
| 5 | 1st day 00:40:37 | PPP | INFO | sent [LCP Req mru=1480 magic=0x604caa8c] |
| 6 | 1st day 00:40:37 | PPP | INFO | rcvd [LCP Req mru=1492 auth=chap-MS-v2 magic=0x374c5cd0 callback=CBCP mrru=1614 endpoint] |
| 7 | 1st day 00:40:37 | PPP | INFO | sent [LCP Rej callback=CBCP mrru=1614] |

Time = 2000-01-01 0:58:43 3524s

H-Ver = WR841N v6/v7 00000000 : S-Ver = 3.11.6 Build 100524 Rel.33810n

L = 192.168.1.1 : M = 255.255.255.0

W1 = PPPoE : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Refresh
Save Log
Mail Log
Clear Log

Previous
Next
Current No. 1 Page

Фигура 4-80 Системен журнал

- Auto Mail Feature** - Указва дали функцията за автоматична поща е активирана или не.
- Mail Settings** - Задайте адрес на пощенска кутия за получаване и изпращане, адрес на сървър, информация за валидация, както и график за характеристика автоматична поща, както е показано на Фигура 4-81.

Mail Account Settings

From:

To:

SMTP Server:

Authentication

User Name:

Password:

Confirm The Password:

Enable Auto Mail Feature

Everyday, mail the log at :

Mail the log every hours

Фигура 4-81 Настройки за пощенски акаунт

- ♦ **From** - Адрес на вашата поща. Рутерът ще го свърже за изпращане на записи.
- ♦ **To** - Адрес на получател. Поща на дестинацията, където да се получават записите.
- ♦ **SMTP Server** - Вашият smtp сървър. Той съответства на пощата, попълнена в поле From. Можете да влезете в съответния уебсайт за помощ, ако не сте сигурни за адреса.
- ♦ **Authentication** - Повечето SMTP сървъри изискват аутентификация. Това се изисква за повечето пощи, за които трябва потребителско име и парола за вход.

→ **Забележка:**

Само когато изберете Authentication е необходимо да въведете потребителско име и парола в следните полета.

- ♦ **User Name** - Името на вашия пощенски акаунт, както е попълнено в поле From. Частта след @ се изключва.
- ♦ **Password** - Паролата за вашия пощенски акаунт.
- ♦ **Confirm The Password** - Въведете паролата още веднъж за потвърждение.

- ◆ **Enable Auto Mail Feature** - Изберете, ако искате автоматично изпращане на записи. Можете да изпращате текущите записи или в определено време всеки ден, или през определени интервали, но само едно от двете може да бъде текущо приложимо правило. Въведете желаното време или интервали в съответното поле, както е показано на Фигура 4-81.

Натиснете Save за запазване на настройките.
Натиснете Back за връщане на предходна страница.

- Log Type** - С избора на тип запис, само този тип записи ще бъдат показвани.
- Log Level** - С избор на ниво запис, ще се показват само записи от това ниво.
- Refresh** - Обновете страницата, за да се покаже последния списък записи.
- Save Log** - Натиснете, за да запазите всички записи в txt файл.
- Mail Log** - Натиснете за ръчно изпращане на електронно писмо с текущи записи съгласно адреса и информацията за валидация, посочени в Mail Settings.
- Clear Log** - Всички записи ще бъдат изтрети изцяло от рутера, не само от страницата.

Натиснете бутон Next за преминаване към следваща страница, или натиснете бутон Previous за връщане на предходна страница.

4.16.9 Статистика

Изберете меню “System Tools → Statistics” и можете да видите статистиката на рутера, включително целия трафик и стойността за последния интервал за статистика на пакети в секунди.

The screenshot shows the 'Statistics' page with the following details:

- Current Statistics Status:** Disabled (with an 'Enable' button)
- Packets Statistics Interval(5-60):** 10 Seconds (with an 'Auto-refresh' checkbox and a 'Refresh' button)
- Sorted Rules:** Sorted by IP Address (with 'Reset All' and 'Delete All' buttons)
- Table:**

| IP Address/ MAC Address | Total | | Current | | | | | Modify |
|----------------------------|---------|-------|---------|-------|---------|--------|--------|--------|
| | Packets | Bytes | Packets | Bytes | ICMP Tx | UDP Tx | SYN Tx | |
| The current list is empty. | | | | | | | | |
- Footer:** Per page 5 entries Current No. 1 page (with 'Previous' and 'Next' buttons)

Фигура 4-82 Статистика

- Current Statistics Status** - активиране или деактивиране. По подразбиране е деактивирана. За активиране, натиснете бутон Enable. Ако е деактивирана, функцията DoS защита в настройки за сигурност ще се деактивира.
- Packets Statistics Interval (5-60)** - Стойността по подразбиране е 10. Изберете стойност между 5 и 60 секунди от падащия списък. Packets Statistic interval указва времевия интервал на статистиката за пакети.

Sorted Rules - Изберете как да бъде сортирана показваната статистика. Изберете позиция Auto-refresh за автоматично обновяване.

Натиснете бутон Refresh за незабавно обновяване.

Натиснете Reset All за зануляване на стойностите за всички записи. Натиснете Delete All за изтриване на всички записи в таблицата.

Таблица на статистиката:

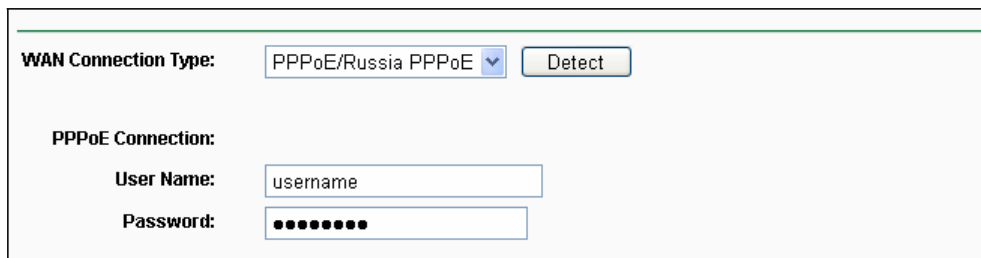
| | | |
|-----------------------|-------------------|--|
| IP/MAC Address | | IP и MAC адресът се показват със свързаната статистика. |
| Total | Packets | Общият брой пакети, получени и предадени от рутера. |
| | Bytes | Общият брой байтове, получени и предадени от рутера |
| Current | Packets | Общият брой пакети , получени и предадени с последния интервал за статистика на пакети в секунди. |
| | Bytes | Общият брой байтове, получени и предадени с последния интервал за статистика на пакети, в секунди. |
| | ICMP Tx | Броят ICMP пакети, предадени на WAN на секунда за определен интервал за статистика на пакети. Показва се като "текуща скорост на предаване/ максимална скорост на предаване". |
| | UDP Tx | Броят UDP пакети, предадени към WAN на секунда за определен интервал статистика за пакети. Показва се като "текуща скорост на предаване/ максимална скорост на предаване". |
| | TCP SYN Tx | Броят TCP SYN пакети, предадени към WAN на секунда за определения интервал статистика за пакети. Показва се като "текуща скорост на предаване/ максимална скорост на предаване". |
| Modify | Reset | Занулява стойността на записа. |
| | Delete | Изтрива съществуващ запис в таблицата. |

Ще има 5 записа на всяка страница. Натиснете бутон Previous за връщане на предходна страница и бутон Next за преминаване на следваща страница.

Приложение А: Най-често задавани въпроси

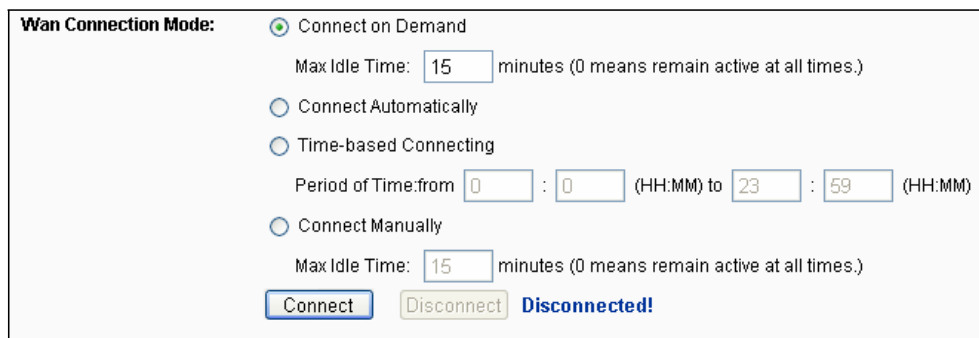
1. Как да конфигурирам рутера за достъп до Интернет от ADSL потребители?

- 1) Първо конфигурирайте ADSL модема, конфигуриран в RFC1483 мостов/ свързващ модел.
- 2) Свържете Ethernet кабела от вашия ADSL модем към Интернет порта на рутера. Телефонният кабел влиза в линейния порт на ADSL модема.
- 3) Влезте с регистрацията си в рутера, натиснете меню "Network" отляво на рутера и изберете подменю "WAN". На страница WAN изберете "PPPoE" за WAN тип връзка. Напишете потребителско име в поле "User Name" и парола в поле "Password", завършете с натискане на **Connect**.



Фигура А-1 PPPoE тип връзка

- 4) Ако вашият ADSL е в режим "заплащане според времето", изберете "Connect on Demand" или "Connect Manually" за Интернет режим връзка. Напишете съответното число за "Max Idle Time" за избягване на излишно платено време. В противен случай изберете "Auto-connecting" за режим Интернет връзка.



Фигура А-2 Режим PPPoE връзка

→ Забележка:

- 1) Понякога връзката не може да бъде прекъсната дори да посочите време в Max Idle Time, тъй като някои приложения ползват Интернет постоянно.
- 2) Ако сте на кабелна връзка, моля конфигурирайте рутера като следват горните стъпки.

2. Как да конфигурират рутера за достъп от Ethernet потребители?

- 1) Влезте с регистрацията си в рутера, натиснете меню "Network" отляво на рутера и изберете

подменю "WAN". На страница WAN изберете "Dynamic IP" за "WAN Connection Type", завършете като натиснете "Save".

- 2) Някои Интернет доставчици изискват да регистрирате MAC адрес на вашия адаптер, който е свързан към вашия кабелен/DSL модем по време на инсталацията. Ако вашият доставчик изисква MAC регистрация, влезте в рутера и изберете меню "Network" отляво на браузера и след това натиснете подменю "MAC Clone". На страница "MAC Clone", ако MAC адресът на вашия компютър е правилния MAC адрес, натиснете бутон "Clone MAC Address" и MAC адреса на вашия компютър ще бъде попълнен в поле "WAN MAC Address". Или напишете MAC адреса в поле "WAN MAC Address". Форматът на MAC адреса е XX-XX-XX-XX-XX-XX. След това натиснете бутон **Save**. Настройката ще влезе в сила след рестартиране.

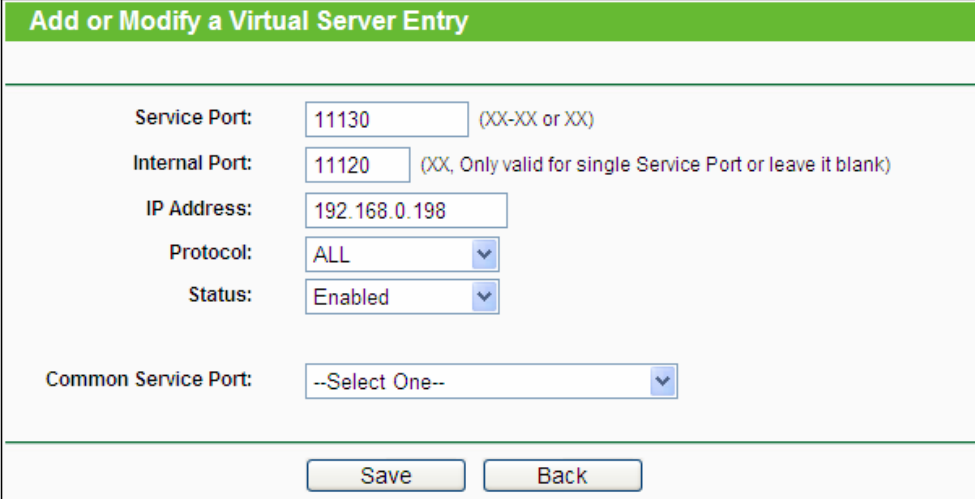
Фигура А-3 MAC Clone

3. Искам за ползвам Netmeeting, какво трябва да направя?

- 1) Ако стартирате Netmeeting като хост, не е необходимо да правите нищо по рутера.
- 2) Ако стартирате като отговор, трябва да конфигурирате виртуален сървър или DMZ хост и се уверете, че H323 ALG е активиран.
- 3) Как се конфигурира виртуален сървър: Влезте с регистрацията си в рутера, изберете меню "Forwarding" отляво на браузера и натиснете подменю "Virtual Servers". На страница "Virtual Servers", натиснете Add New.... След това на страница "Add or Modify a Virtual Server Entry" въведете "11130" в поле "Service Port" и вашия IP адрес в поле "IP Address", в случая като пример 192.168.0.198, не забравяйте да изберете **Enable** и **Save**.

| ID | Service Port | Internal Port | IP Address | Protocol | Status | Modify |
|----|--------------|---------------|---------------|----------|---------|---|
| 1 | 11130 | 11120 | 192.168.0.198 | ALL | Enabled | Modify Delete |

Фигура А-4 Виртуални сървъри



Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)

Internal Port: (XX, Only valid for single Service Port or leave it blank)

IP Address:

Protocol:

Status:

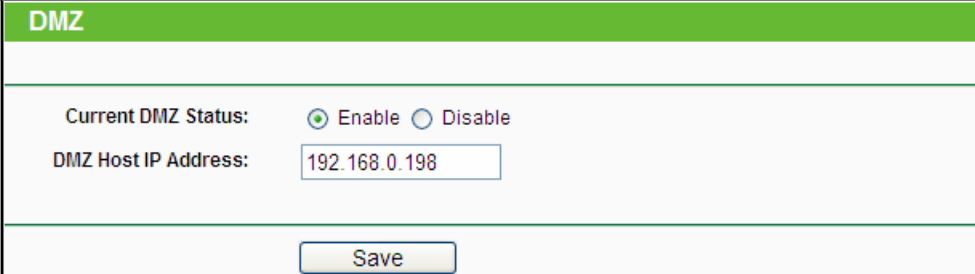
Common Service Port:

Фигура А-5 Добавяне и промяна на запис за виртуален сървър

→ Забележка:

Обратната страна трябва да писка вашия WAN IP, който се показва в страницата "Status".

- 4) Как се активира DMZ хост: Влезте с регистрацията си в рутера, изберете меню "Forwarding" отляво на браузера и натиснете подменю "DMZ". На страницата "DMZ" натиснете радио бутон Enable и напишете своя IP адрес в поле "DMZ Host IP Address", като ползвате 192.168.0.198 като пример, не забравяйте да натиснете бутон **Save**.



DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Фигура А-6 DMZ

- 5) Как се активира H323 ALG: Влезте с регистрацията си в рутера, изберете меню "Security" отляво на браузера и натиснете подменю "Basic Security". На страницата "Basic Security" натиснете радио бутон Enable, който се намира до H323 ALG. Не забравяйте да натиснете бутон Save.

Basic Security

Firewall

SPI Firewall: Enable Disable

VPN

PPTP Passthrough: Enable Disable

L2TP Passthrough: Enable Disable

IPSec Passthrough: Enable Disable

ALG

FTP ALG: Enable Disable

TFTP ALG: Enable Disable

H323 ALG: Enable Disable

Save

Фигура А-7 Basic Security

4. Искам да създам WEB сървър в локалната мрежа, какво трябва да направя?

- 1) Тъй като WEB Server port 80 ще си пречи с WEB management port 80 на рутера, трябва да смените номера на WEB management port, за да избегнете това.
- 2) Как се сменя номера на WEB management port: Влезте с регистрацията си в рутера, изберете меню "Security" отляво на браузера и натиснете подменю "Remote Management". На страница "Remote Management" напишете номер на порт, различен от 80, например 88, в поле "Web Management Port". Натиснете Save и рестартирайте рутера.

Remote Management

Web Management Port:

Remote Management IP Address: (Enter 255.255.255.255 for all)

Save

Фигура А-8 Дистанционно управление

→ Забележка:

Ако горната конфигурация се активира, конфигурирайте рутера като напишете 192.168.0.1:88 (LAN IP адреса на рутера: Web Management Port) в полето за адрес на уеб-браузера.

- 3) Влезте с регистрацията си в рутера, изберете меню "Forwarding" отляво на браузера и натиснете подменю "Virtual Servers". На страница "Virtual Servers" натиснете Add New..., след това на страница "Add or Modify a Virtual Server" въведете "80" в празното място до "Service Port" и вашия IP адрес в "IP Address", като вземаме 192.168.0.188 за пример, не забравяйте да натиснете **Enable** и **Save**.

| Virtual Servers | | | | | | |
|-----------------|--------------|---------------|---------------|----------|---------|---|
| ID | Service Port | Internal Port | IP Address | Protocol | Status | Modify |
| 1 | 80 | 21 | 192.168.0.188 | ALL | Enabled | Modify Delete |

Фигура А-9 Виртуални сървъри

| Add or Modify a Virtual Server Entry | |
|--------------------------------------|--|
| Service Port: | <input type="text" value="80"/> (XX-XX or XX) |
| Internal Port: | <input type="text" value="21"/> (XX, Only valid for single Service Port or leave it blank) |
| IP Address: | <input type="text" value="192.168.0.188"/> |
| Protocol: | <input type="text" value="ALL"/> |
| Status: | <input type="text" value="Enabled"/> |
| Common Service Port: | <input type="text" value="--Select One--"/> |

Фигура А-10 Добавяне или промяна на запис за виртуален сървър

5. Безжичните станции не могат да се свържат с рутера.

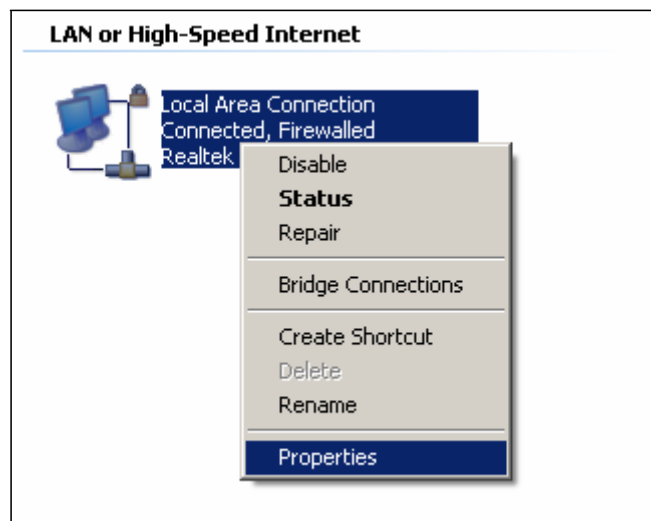
- 1) Уверете се, че "Wireless Router Radio" е активиран.
- 2) Уверете се, че SSID на безжичните станции съответства на SSID на рутера.
- 3) Уверете се, че безжичните станции има правилния ключ за кодиране, когато рутерът е кодиран
- 4) Ако безжичната връзка е готова, но нямате достъп до рутера, проверете IP адреса на вашите безжични станции.

Приложение В: Конфигуриране на компютъра.

В тази част ще ви покажем как да инсталирате и конфигурирате правилно TCP/IP в Windows XP. Първо се уверете, че вашият Ethernet адаптер в работи, вижте ръководството на адаптера, ако е необходимо.

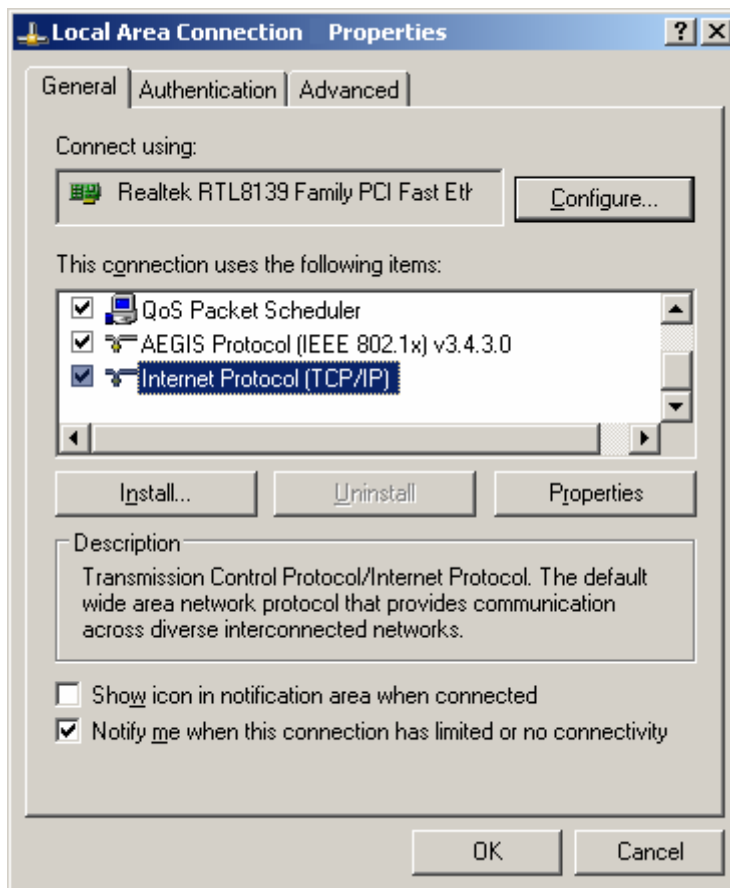
1. Конфигуриране на TCP/IP компонент

- 1) В Windows лентата със задачи натиснете бутон Start, изберете Settings, и след това натиснете Control Panel.
- 2) Натиснете икона Network and Internet Connections и след това Network Connections в появилия се прозорец.
- 3) Натиснете с десен бутон на мишката иконата, показано долу, изберете Properties.



Фигура В-1

- 4) В появилия се прозорец, показано по-долу, натиснете два пъти върху Internet Protocol (TCP/IP).



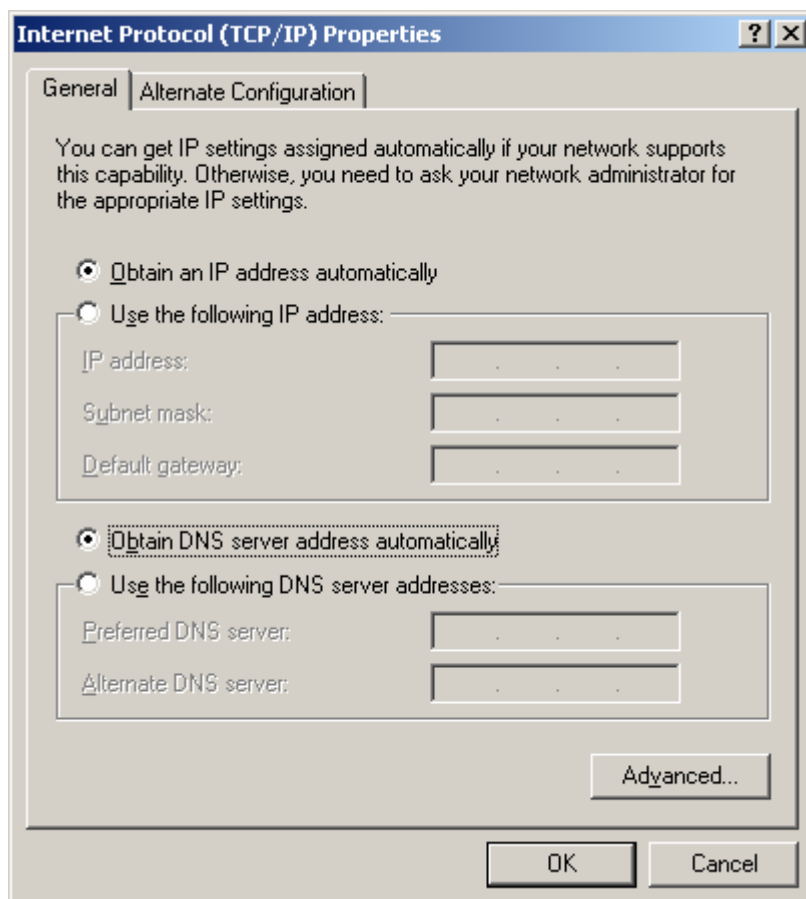
Фигура В-2

- 5) Ще се покаже прозорец TCP/IP Properties и позиция IP Address на този прозорец е отворена по подразбиране.

Сега имате два начина за конфигуриране на **TCP/IP** протокол:

- Автоматично задаване на IP адрес**

Изберете Obtain an IP address automatically и Obtain DNS server automatically, както е показано на долната фигура:



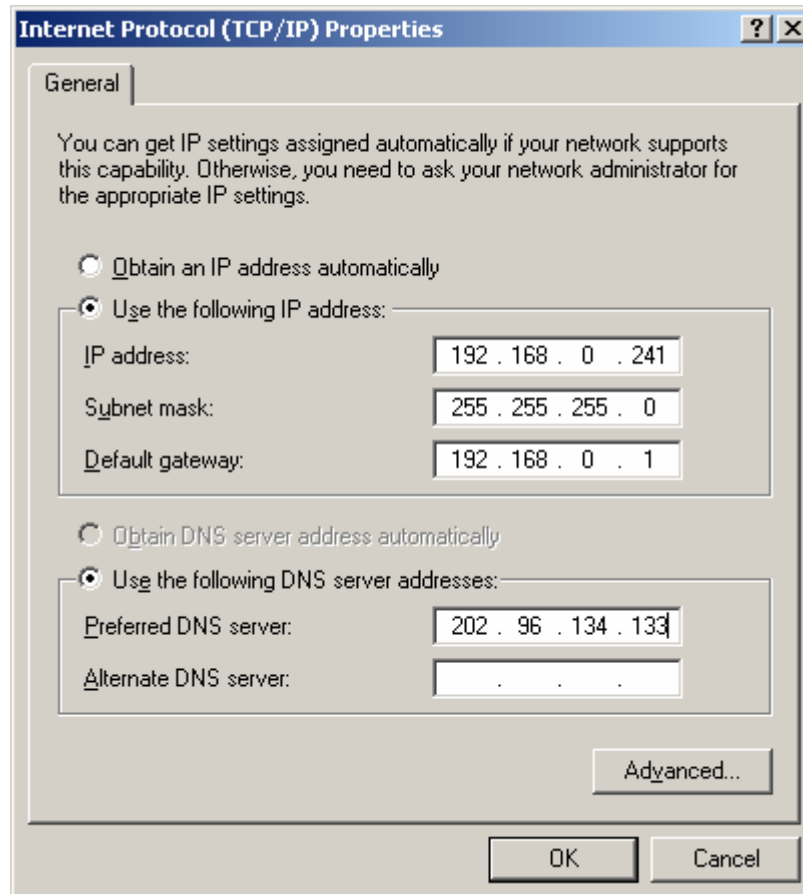
Фигура В-3

→ **Забележка:**

За операционна система Windows 98 или по-ранна, компютърът и рутерът може да трябва да бъдат рестартирани.

Ръчно задаване на IP адрес

- 1 Изберете радио бутон **Use the following IP address.**
- 2 Ако LAN IP адресът на рутера е 192.168.0.1, посочете за **IP address** - 192.168.0.x (x е число от 2 до 254) и **Subnet mask** като 255.255.255.0.
- 3 Напишете LAN IP адреса на рутера (IP по подразбиране е 192.168.0.1) в **Default gateway** поле.
- 4 Изберете **Use the following DNS server addresses.** В поле **Preferred DNS Server** можете да въведете същата стойност като **Default gateway** или да напишете IP адреса на локалния DNS сървър.



Натиснете **OK** за запазване на настройките.

Приложение С: Спецификации

| Обща информация | |
|---------------------------------|---|
| Стандарти | IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g и IEEE 802.11n |
| Протоколи | TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP |
| Портове | Един 10/100M Auto-Negotiation WAN RJ45 порт, четири 10/100M Auto-Negotiation LAN RJ45 порта, поддържащи Auto MDI/MDIX |
| Тип кабели | 10BASE-T: UTP категория 3, 4, 5 кабел (максимум 100 м) EIA/TIA-568 100Ω STP (максимум 100 м) |
| | 100BASE-TX: UTP категория 5, 5е кабел (максимум 100 м) EIA/TIA-568 100Ω STP (максимум 100 м) |
| Светлинни диоди | Power, System, WLAN, WAN, LAN (1-4), QSS |
| Безопасност и излъчване | FCC, CE |
| Безжична връзка | |
| Честотна лента | 2.4~2.4835GHz |
| Скорост радио данни | 11n : до 300Mbps (Automatic) 11g : 54/48/36/24/18/12/9/6Mbps (Automatic) 11b : 11/5.5/2/1Mbps (Automatic) |
| Честотно разширение | DSSS(Direct Sequence Spread Spectrum) |
| Модулация | DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM |
| Сигурност | WEP/WPA/WPA2/WPA2-PSK/WPA-PSK |
| Чувствителност @PER | 270M: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER |
| Работна среда и физически данни | |
| Температура | работна: 0C~40°C (32°F~104°F) |
| | на съхранение: -40C~70°C(-40°F~158°F) |
| Влажност | работна: 10% - 90% RH, без конденз |
| | на съхранение: 5% - 90% RH, без конденз |

Приложение D: Речник

- **802.11n - 802.11n** се създава върху предходни 802.11 стандарти чрез добавяне на MIMO (много входи и изходи). MIMO използва много приемо-предавателни антени, за да се осъществи завишено преминаване на данни чрез пространствено мултиплексиране и завишен обхват чрез използване на пространствено разнообразие, вероятно чрез схеми за кодиране като Alamouti кодиране. Enhanced Wireless Consortium (EWC) [3] е създаден за усилване на IEEE 802.11n процеса на развитие и спомагане за технологична спецификация за взаимодействие на продукти от следваща генерация безжична локална мрежова свързаност (WLAN).
- **802.11b** - Стандарт 802.11b определя безжична свързаност при 11 Mbps с използване на технология за разширение на спектъра в директна последователност (DSSS) и работа в нелицензиран радио спектър при 2.4GHz и WEP криптиране за сигурност. 802.11b мрежите се наричат още Wi-Fi мрежи.
- **802.11g** - спецификация за безжична мрежова свързаност при 54 Mbps с използване на технология за разширение на спектъра в директна последователност (DSSS), с използване на OFDM модулация и работа в нелицензиран радио спектър при 2.4GHz, и обратна съвместимост с IEEE 802.11b устройства, и WEP криптиране за сигурност.
- **DDNS (Dynamic Domain Name System)** - Способността за задаване на фиксиран хост или име на домейн на динамичен Интернет IP адрес.
- **DHCP (Dynamic Host Configuration Protocol)** - Протокол, който автоматично конфигурира TCP/IP параметрите за всички компютри, които са свързани към DHCP сървър.
- **DMZ (Demilitarized Zone)** - Демилитаризирана зона позволява един локален хост да бъде отворен за Интернет за услуга със специална цел, като например Интернет игри или видеоконференция.
- **DNS (Domain Name System)** – Интернет услуга, която преобразува имената на уебсайтове в IP адреси.
- **Domain Name** - Описателно име за адрес или група адреси в Интернет.
- **DSL (Digital Subscriber Line)** - технология, която позволява изпращането или получаването на данни през съществуващи, традиционни телефонни линии.
- **ISP (Internet Service Provider)** - Компания, която осигурява достъп до Интернет - Интернет доставчик.
- **MTU (Maximum Transmission Unit)** - Размерът байтове на най-големия пакет, който може да бъде предаден.
- **NAT (Network Address Translation)** - NAT технологията превръща IP адресите на локалната мрежа в друг IP адрес за Интернет.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE е протокол за свързване на отдалечени

хостове към Интернет през постоянно налична връзка чрез симулация на дайъл-ъп връзка.

- **SSID - Service Set Identification** представлява тридесет и две символен (максимум) числово-буквен ключ за идентифициране на безжична локална мрежа. За да могат безжични устройства в мрежа да комуникират едно с друго, всички устройства трябва да са конфигурирани с еднаква SSID. Това е обикновено параметър за конфигурация за безжична PC карта. Съответства на ESSID в безжична точка за достъп и на името на безжичната мрежа.
- **WEP (Wired Equivalent Privacy)** - Механизъм за неприкосновеност на данни, базиран на 64-bit или 128-bit или 152-bit алгоритъм за споделен ключ, както в описано в стандарт IEEE 802.11.
- **Wi-Fi** - Търговско име за 802.11b стандарт за безжична мрежа, дадено от Wireless Ethernet Compatibility Alliance (WECA, вижте <http://www.wi-fi.net>), група за индустриални стандарти, спомагаща функционалната съвместимост между 802.11b устройства.
- **WLAN (Wireless Local Area Network)** - Група компютри или свързани устройства, които комуникират едно с друго безжично, като потребителите са ограничени в една локална зона.