



NAVODILA ZA UPORABO

TP LINK WLAN-usmerjevalnik TL-WR841N

Kataloška št.: 39 97 34

KAZALO

VSEBINA PAKETA	3
1. UVOD	3
1.1 PREGLED LASTNOSTI NAPRAVE	3
1.2 POJMOVANJE	4
1.3 GLAVNE ZNAČILNOSTI NAPRAVE	4
1.4 SESTAVNI DELI NAPRAVE.....	5
2. PRIKLOP USMERJEVALNIKA.....	7
2.1 SISTEMSKE ZAHTEVE	7
2.2 ZAHTEVE ZA NAMESTITEV V PROSTORU.....	7
2.3 POVEZAVA USMERJEVALNIKA	7
3. VODNIK ZA HITRO NAMESTITEV.....	8
3.1 KONFIGURACIJA TCP/IP.....	8
3.2 VODNIK ZA HITRO NAMESTITEV	10
4. KONFIGURACIJA USMERJEVALNIKA	15
4.1 PRIJAVA.....	15
4.2 STATUS.....	16
4.3 HITRA NASTAVITEV	17
4.4 WPS.....	17
4.5 OMREŽJE	19
4.6 BREŽIČNE NASTAVITVE	29
4.7 DHCP	37
4.8 POSREDOVANJE	40
4.9 ZAŠČITA.....	45
4.10 STARŠEVSKI NADZOR.....	49
4.11 NADZOR DOSTOPA	52
4.12 NAPREDNO USMERJANJE	61
4.13 NADZOR PASOVNE ŠIRINE	63
4.14 IP & MAC ZAVEZJOČE NASTAVITVE.....	65
4.15 DINAMIČNI DNS	67
4.16 SISTEMSKA ORODJA	69
DODATEK A: POGOSTO ZASTAVLJENA VPRAŠANJA.....	78
DODATEK B: KONFIGURACIJA RAČUNALNIKA	82
DODATEK C: TEHNIČNI PODATKI	85
DODATEK D: SLOVAR	86
GARANCIJSKI LIST	88

VSEBINA PAKETA

V vašem paketu se mora nahajati naslednje:

- Brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps
- Napajalnik za brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps
- Hiter vodnik za namestitvev
- CD za brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps, na katerem so:
 - ta navodila za uporabo
 - ostale koristne informacije



Opomba:

Prepričajte se, da se v paketu nahaja vse naštetu. Če je katerikoli od navedenih predmetov poškodovan ali manjka, se obrnite na vašega distributerja.

1. UVOD

Zahvaljujemo se vam za nakup brezžičnega N usmerjevalnika TL-WR841N/TL-WR841ND 300 Mbps.

1.1 PREGLED LASTNOSTI NAPRAVE

Brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps ima vgrajeno 4 portno stikalo, požarni zid, NAT usmerjevalnik in brezžično dostopno točko (AP). Napaja ga 2x2 MIMO tehnologija, zato 300 Mbps brezžični N usmerjevalnik omogoča izjemen doomet in hitrost, ki v celoti zadovoljuje potrebe omrežja manjše pisarne / domače pisarne (SOHO) in vseh uporabnikov, ki zahtevajo visoko zmogljivost omrežja.

Neverjetna hitrost

Brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps zagotavlja hitrost brezžične povezave do 300 Mbps z drugimi 802.11n brezžičnimi klienti. Neverjetna hitrost je idealna za ravnanje z velikim številom podatkovnih tokov hkrati, kar zagotavlja stabilnost in gladko delovanje vašega omrežja. Delovanje tega 802.11n brezžičnega usmerjevalnika vam bo dala nepričakovane omrežne izkušnje pri hitrostih, ki so veliko višje od 802.11g. Kompatibilen je tudi z izdelki IEEE 802.11g in IEEE 802.11b.

Večkratna varnostna zaščita

Brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps z ukrepi večkratne varnostne zaščite, vključno s SSID nadzorom oddajanja in brezžičnim LAN 64/128/152-bitnim WEP šifriranjem, WiFi zaščitenim dostopom (WPA2- PSK, WPA- PSK), kakor tudi z napredno zaščito požarnega zidu, zagotavlja popolno zasebnost podatkov.

Fleksibilen nadzor dostopa

Brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps zagotavlja fleksibilen nadzor dostopa, tako da lahko starši ali omrežni administratorji vzpostavijo omejen dostop za otroke ali zaposlene. Podpira tudi Virtualni strežnik in DMZ gostitelja za

sprožanje porta, tako da lahko omrežni administratorji s funkcijo upravljanja na daljavo upravljajo in nadzorujejo omrežje v realnem času.

Enostavna namestitvev

Ker je usmerjevalnik kompatibilen s skoraj vsemi glavnimi operacijskimi sistemi, ga je zelo lahko upravljati. Podpira čarovnika za hitro nastavitvev, podrobna navodila pa so po korakih opisana v teh navodilih za uporabo. Pred namestitvijo usmerjevalnika ta navodila preberite in se seznanite z vsemi funkcijami naprave.

1.2 POJMOVANJE

Usmerjevalnik ali TL-WR841N/TL-WR841ND, ki je naveden v teh navodilih, se brez dodatne razlage nanaša na brezžični N usmerjevalnik TL-WR841N/TL-WR841ND 300 Mbps.



Opomba:

Ta navodila za uporabo se nanašajo na dve napravi: TL-WR841N in TL-WR841ND. Zaradi poenostavitve se v navodilih omenja TL-WR841ND.

Razlika med njima pa je:

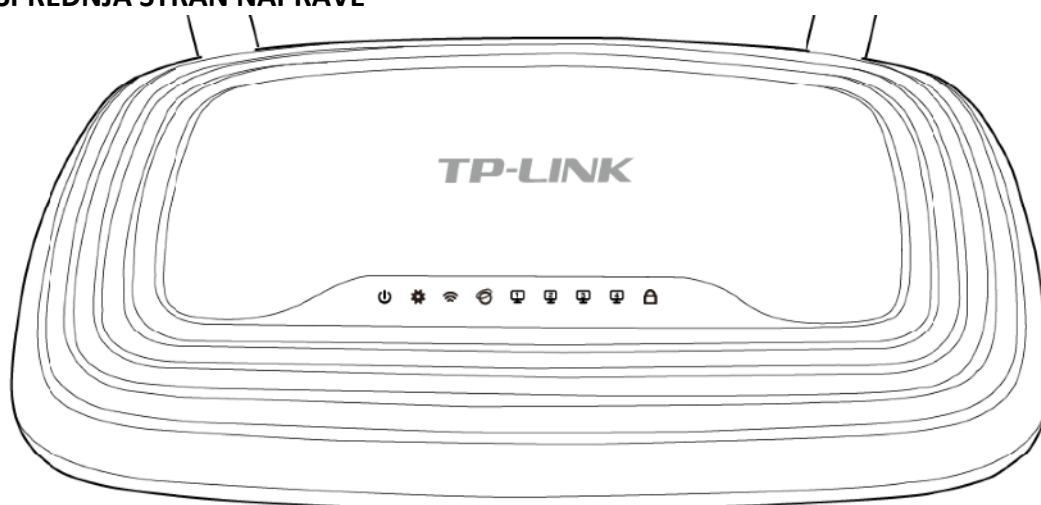
- TL-WR841N je usmerjevalnik z dvema fiksnima antenama.
- TL-WR841ND je usmerjevalnik z dvema snemljivima antenama.

1.3 GLAVNE ZNAČILNOSTI NAPRAVE

- Naprava je skladna z IEEE 802.11n da zagotavlja brezžično stopnjo prenosa podatkov do 300 Mbps.
- En 10/100M Auto-Negotiation RJ45WAN port, štiri 10/100M Auto-Negotiation RJ45 LAN port, podpira Auto MDI/MDIX.
- Zagotavlja preverjanje pristnosti WPA/WPA2, WPA-PSK/WPA2-PSK, TKIP/AES šifrirno zaščito.
- Izmenjuje podatkovni in internetni dostop za uporabnike, podpira dinamičen IP/ statičen IP/ PPPoE internetni dostop.
- Podpira virtualni strežnik, posebno aplikacijo in DMZ gostitelja.
- Podpira UPnP, dinamičen DNS, statično usmerjanje.
- Zagotavlja samodejno povezavo na internet in načrtovano povezavo na internet v določenem času.
- Vgrajen ima NAT in DHCP strežnik in podpira distribucijo statičnega IP naslova.
- Omogoča starševski nadzor in nadzor dostopa.
- Na internet se poveže na zahtevo, z njega pa pri PPPoE odklopi, če miruje.
- Zagotavlja 64/128/152-bitno WEP šifrirno zaščito in brezžičen LAN ACL (seznam nadzora dostopa).
- Omogoča pretočno statistiko.
- Omogoča posodobitev programske opreme in spletno upravljanje.

1.4 SESTAVNI DELI NAPRAVE

SPREDNJA STRAN NAPRAVE



Slika 1 – 1: Sprednja stran naprave

Na sprednji strani usmerjevalnika se nahajajo LED indikatorji (gledano z leve proti desni).

Ime	Status	Pomen
⏻ (Vklop)	Izklopljen	Naprava je izklopljena.
	Sveti	Naprava je vklopljena.
⚙️ (Sistem)	Utripa	Usmerjevalnik deluje pravilno.
	Sveti/izklopljen	Usmerjevalnik ima sistemsko napako.
📶 (WLAN)	Izklopljen	Brezžična funkcija ni omogočena.
	Utripa	Brezžična funkcija je omogočena.
🌐 (WAN), 🖥️ (LAN 1-4)	Izklopljen	Na ustrezen port ni povezana nobena naprava.
	Sveti	Na ustrezen port je povezana naprava, vendar ni aktivnosti.
	Utripa	Aktivna naprava je povezana na ustrezni port.
🔒 (WPS)	Počasi utripa	Brezžična naprava se povezuje v omrežje z WPS funkcijo. Ta postopek bo trajal prvi 2 minuti.
	Sveti	Brezžična naprava je uspešno dodana v omrežje z WPS funkcijo.
	Hitro utripa	Dodajanje brezžične naprave v omrežje z WPS funkcije ni bilo uspešno.

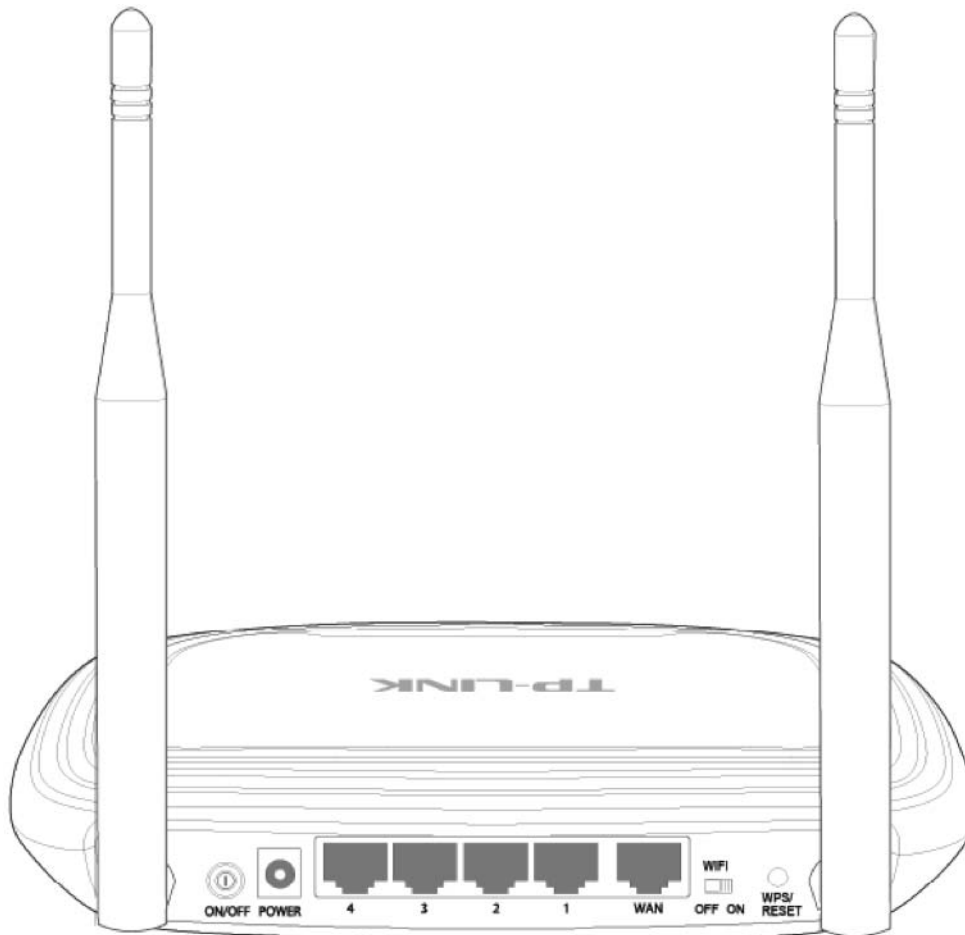
Tabela 1 – 1: Opis LED indikatorjev



Opomba:

Ko je naprava uspešno dodana v omrežje z WPS funkcijo, WPS LED indikator sveti še približno 5 minut, nato pa se izklopi.

ZADNJA STRAN NAPRAVE



Slika 1 – 2: Zadnja stran naprave

Na zadnji strani naprave se nahajajo naslednji njeni deli (gledano z leve proti desni):

- **“ON/OFF“**: stikalo za vklop naprave.
- **“POWER“**: Vtičnica za napajanje kamor vstavite napajalnik. Prosimo uporabite priloženi napajalnik.
- **“4,3,2,1 (LAN)“**: ti porti (4,3,2,1) usmerjevalnik povezujejo z lokalnim(i) računalnikom(i).
- **“WAN“**: v WAN port vstavite DSL / kabelski modem ali Ethernet.
- **“WIFI ON/OFF“**: s tem stikalom omogočite/onemogočite brezžično funkcijo.
- **“WPS/RESET“**: ta gumb se uporablja tako za WPS funkcijo, kot tudi za ponastavitev naprave. ZA WPS funkcijo gumb držite manj kot 5 sekund; za ponastavitev pa gumb držite dlje kot 5 sekund.

- **Če se uporablja kot gumb za ponastavitev:**

Obstajata dva načina za ponastavitev usmerjevalnika na tovarniške nastavitve:

- 1) Uporaba funkcije **“Factory Defaults“** (tovarniške privzete nastavitve) v **“System Tools -> Factory Defaults“** (sistemska orodja -> tovarniške privzete nastavitve) v spletnem orodju usmerjevalnika.
- 2) Uporaba gumba **WPS/RESET**: ko je usmerjevalnik vklopljen, gumb **WPS/RESET** pritisnite in držite (več kot 5 sekund), dokler ne začne LED indikator **“SYS“** hitro utripati (prej utripa počasi). Nato gumb spustite in počakajte da se usmerjevalnik ponovno zažene s privzetimi tovarniškimi nastavitvami.

- **Če se uporablja kot WPS gumb:**
 - Če uporabljate naprave – kliente, kot so na primer brezžični adapterji, ki podpirajo nastavitve Wi-Fi zaščite, lahko s pritiskom na ta gumb na hitro vzpostavite povezavo med usmerjevalnikom in napravo – klientom in samodejno konfigurirate brezžično zaščito za vaše brezžično omrežje.
- **Brezžična antena:** za sprejemanje in pošiljanje brezžičnih podatkov.

2. PRIKLOP USMERJEVALNIKA

2.1 SISTEMSKE ZAHTEVE

- Širokopasovni dostop do internetnih storitev (DSL / kabel/ Ethernet).
- En DSL/kabelski modem, ki ima RJ45 konektor (ki pa ni potreben, če je usmerjevalnik direktno povezan na Ethernet).
- Računalniki z delujočim Ethernet adapterjem in Ethernet kabel z RJ45 konektorji.
- TCP/IP protokol na vsakem računalniku.
- Spletni brskalnik kot je na primer Microsoft Internet Explorer, Mozilla Firefox ali Apple Safari.

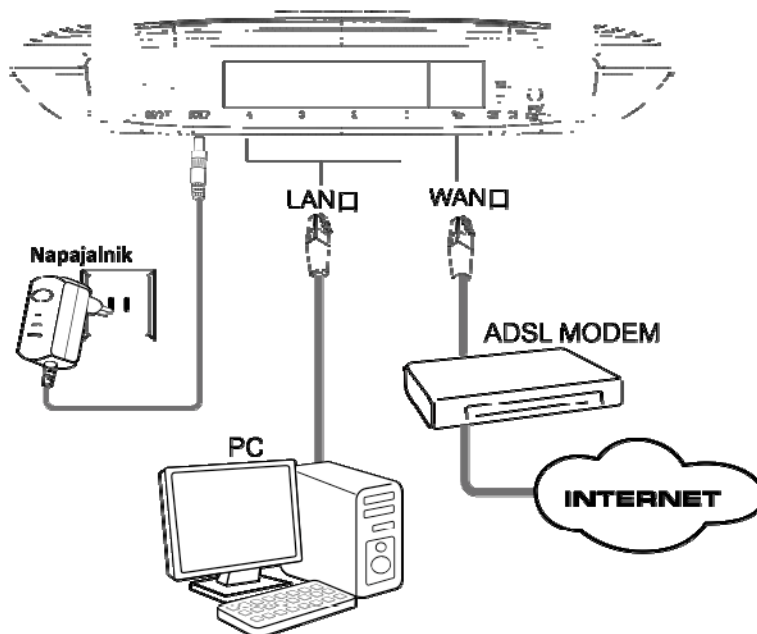
2.2 ZAHTEVE ZA NAMESTITEV V PROSTORU

- Usmerjevalnik postavite na dobro zračno mesto, ki je umaknjeno od grelnih naprav ali ventilacije.
- Izogibajte se neposrednemu sevanju kakršnekoli močne svetlobe (kot je na primer sončna svetloba).
- Okoli usmerjevalnika naj bo vsaj 5 cm prostega prostora.
- Temperaturno območje delovanja: 0°C – 40°C (32°F - 104°F).
- Delovanje v območju vlažnosti: 10% - 90% relativna vlažnost, nekondenzirajoča.

2.3 POVEZAVA USMERJEVALNIKA

Pred namestitvijo usmerjevalnika se prepričajte, da je vaš računalnik preko širokopasovnega dostopa uspešno povezan na internet. Če imate s tem težave, se obrnite na vašega ponudnika internetnih storitev. Potem pa usmerjevalnik namestite skladno s spodaj navedenimi koraki. Ne pozabite izvleči omrežnega vtiča in imejte pri tem vseskozi suhe roke.

1. Izklopite računalnik, kabelski/DSL modem in usmerjevalnik.
2. Poiščite optimalno mesto za postavitve usmerjevalnika. Najboljše mesto je ponavadi v sredini vašega brezžičnega omrežja.
3. Prilagodite položaj anten. Ponavadi ustreza navpičen položaj.
4. Kakor je prikazano na sliki 2 – 1, v LAN na LAN porte usmerjevalnika priklopite vaš računalnik (PC) in vsak switch (če imate brezžični NIC in želite uporabljati brezžično funkcijo, lahko ta korak preskočite).
5. Kakor je prikazano na sliki 2 – 1, v WAN port na usmerjevalniku vstavite DSL/kabelski modem.
6. Napajalnik vstavite v napajalno vtičnico usmerjevalnika, drugi konec pa v električno vtičnico. Usmerjevalnik se samodejno zažene.
7. Vključite računalnik in kabelski/DSL modem.



Slika 2 – 1: Namestitev strojne opreme brezžičnega N usmerjevalnika TL-WR841ND 300Mbps

3. VODNIK ZA HITRO NAMESTITEV

V tem poglavju je opisano, kako z uporabo **vodnika za hitro namestitev** v nekaj minutah konfigurirate osnovne funkcije brezžičnega N usmerjevalnika TL-WR841ND 300Mbps.

3.1 KONFIGURACIJA TCP/IP

Privzeto ime domene brezžičnega N usmerjevalnika TL-WR841ND 300Mbps je <http://tplinklogin.net>, privzet IP naslov je 192.168.0.1 in privzet Subnet Mask je 255.255.255.0. Te vrednosti lahko poljubno spreminjate. V teh navodilih so za opis uporabljene privzete vrednosti.

Lokalni računalni priklopite v LAN porte na usmerjevalniku. Nato lahko na spodnja dva načina konfigurirate IP naslov vašega računalnika.

- Ročna konfiguracija IP naslova
 - 1) Za vaš računalnik nastavite TCP/IP protokol. Če za to potrebujete navodila, glejte “Dodatek B: Konfiguracija računalnika”.
 - 2) Konfigurirajte parametre omrežja. IP naslov je 192.168.0.xxx (“xxx” je katerokoli število od 2 do 254), Subnet Mask je 255.255.255.0 in Gateway je 192.168.0.1 (privzet IP naslov usmerjevalnika).
- Avtomatično pridobivanje IP naslova
 - 1) TCP/IP protokol na vašem računalniku nastavite na način “**Obtain an IP address automatically**” (samodejno pridobivanje IP naslova). Če za to potrebujete navodila, glejte “Dodatek B: Konfiguracija računalnika”.
 - 2) Nato bo vgrajeni DHCP strežnik računalniku določil IP naslov.

Sedaj lahko v ukazno vrstico vpišete “Ping” ukaz in preverite omrežno povezavo med vašim računalnikom in usmerjevalnikom. Naslednji opisan primer je za operacijski sistem Windows 2000.

Odprite ukazno vrstico in vtipkajte *ping 192.168.0.1*. in nato pritisnite “Enter”.

- Če je prikazani rezultat podoben prikazu na sliki 3 – 1, to pomeni, da je povezava med vašim računalnikom in usmerjevalnikom dobro vzpostavljena.

```

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>
  
```

Slika 3 – 1: Uspešen rezultat Ping ukaza

- Če je prikazani rezultat podoben prikazu na sliki 3 – 2, to pomeni, da povezava med vašim računalnikom in usmerjevalnikom ni uspela.

```

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>
  
```

Povezavo preverite po naslednjih korakih:

1. Ali je povezava med vašim računalnikom in usmerjevalnikom pravilna?



Opomba:

LED indikatorji 1/2/3/4 LAN portov ki ste jih uporabili na usmerjevalniku in LED indikatorji na adapterju vašega računalnika morajo svetiti.

2. Ali je TCP/IP konfiguracija za vaš računalnik pravilna?



Opomba:

Če je IP naslov vašega usmerjevalnika 192.168.0.1, mora biti IP naslov vašega računalnika znotraj območja 192.168.0.2 – 192.168.0.254.

3. Ali je privzet LAN IP usmerjevalnika pravilen?



Opomba:

Če je LAN IP modema, ki je povezan z vašim usmerjevalnikom 192.168.0.x, se privzet LAN IP usmerjevalnika samodejno preklopi z 192.168.0.1 na 192.168.1.1 in se tako izogne IP konfliktu. Zato lahko za preverjanje omrežne povezave med vašim računalnikom in usmerjevalnikom odprete ukazno vrstico, vtipkate *ping 192.168.1.1* in pritisnete **“Enter“**.

3.2 VODNIK ZA HITRO NAMESTITEV

S spletnim orodjem lahko brezžični N usmerjevalnik TL-WR841ND 300 Mbps enostavno konfigurirate in upravljate. Spletno orodje lahko uporabljate na katerihkoli operacijskih sistemih Windows, Macintosh ali UNIX s spletnim brskalnikom kot je na primer Microsoft Internet Explorer, Mozilla Firefox ali Apple Safari.

1. Za dostop do konfiguracijskega orodja odprite spletni brskalnik, vanj vtipkajte privzeto ime domene <http://tplinklogin.net>.



Slika 3 – 3: Prijava na usmerjevalnik

Po nekaj trenutkih se odpre podobno okno kot je prikazano na sliki 3 – 4. V polje uporabniško ime in geslo vtipkajte **admin** – oboje z majhnimi črkami. Nato kliknite gumb **OK** ali pritisnite gumb **“Enter“**.



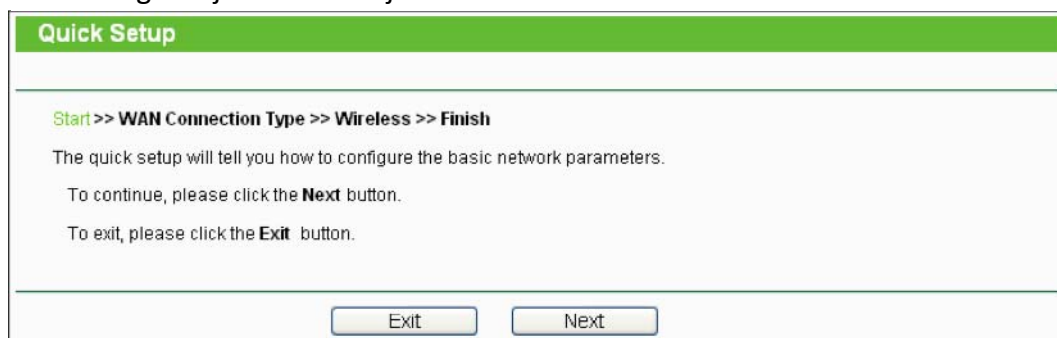
Slika 3 – 4: Prijava v Windows



Opomba:

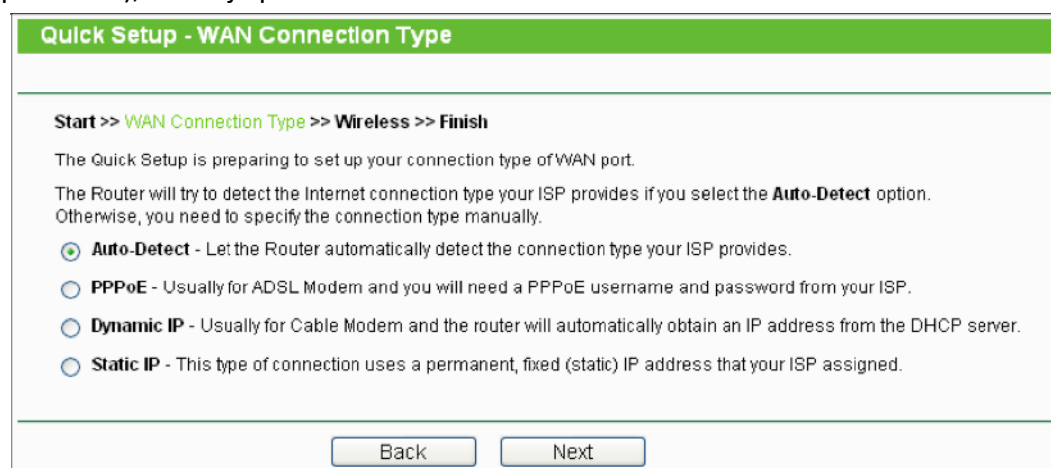
Če se zgornje okno ne pokaže, to pomeni, da je vaš spletni brskalnik nastavljen na proxy. Pojdite na meni "Tools > Internet Options > Connections > LAN Settings" in na zaslonu ki se pokaže, odstranite kljukico v kvadratku "Using Proxy" ter za dokončanje kliknite OK.

1. Po uspešni prijavi lahko kliknete na meni "**Quick Setup**" (hitra nastavitve) in na hitro konfigurirate vaš usmerjevalnik.



Slika 3 – 5: Hitra namestitve

2. Kliknite "**Next**" (naprej) in pokaže se okno "**WAN Connection Type**" (tip WAN povezave), kakor je prikazano na sliki 3 – 6.



Slika 3 – 6: Tip WAN povezave

Usmerjevalnik omogoča funkcijo "**Auto-Detect**" (samozaznave) in podpira tri najbolj priljubljene načine povezave na internet: **PPPoE**, **Dinamičen IP** in **Statičen IP**.

3. Če izberete "**Auto-Detect**", usmerjevalnik samodejno zazna tip povezave, ki jo omogoča vaš internetni ponudnik. Prepričajte se da je pred zaznavo kabel varno nameščen v WAN port. Ustrezna konfiguracijska stran se pokaže takrat, ko usmerjevalnik uspešno zazna aktivno internetno storitev.
 - 1) Če je zaznan tip povezave **PPPoE**, se pojavi prikaz kot kaže slika 3 – 7.

Slika 3 -7: Hitra namestitev – PPPoE

- **“User Name/Password”** – vnesite uporabniško ime in geslo, ki ste ga dobili od vašega ponudnika internetnih storitev. Ta polja so občutljiva na male in velike črke. Če imate pri tem postopku težave, se obrnite na vašega ponudnika internetnih storitev.
- **“Confirm Password”** – ponovno vnesite geslo, ki ste ga dobili od vašega ponudnika internetnih storitev in potrdite, da je vnešeno geslo pravilno. Če se geslo in potrditev gesla razlikujeta, se pojavi spodnje okno. Kliknite **OK** in še enkrat vnesite geslo v polje “Password” in “Confirm Password”.



- 2) Če je zaznan tip povezave **Dinamičen IP**, se pojavi prikaz kot kaže slika 3 – 8.
- Če se na usmerjevalnik povezujete z glavnega računalnika, izberite **“Yes”** in nato kliknite na **“Clone MAC address”** (kloniraj MAC naslov).

Slika 3 – 8: Hitra namestitev – MAC klon

- Če se na usmerjevalnik povezujete z drugega računalnika, ki ni glavni računalnik, izberite **No** in nato v polje **“WAN MAC Address”** vnesite MAC naslov glavnega računalnika.

Slika 3 – 9: Hitra namestitev – MAC klon

3) Če je zaznan tip povezave **Statičen IP**, se pojavi prikaz kot kaže slika 3 – 10.

Slika 3 – 10: Hitra namestitev – Statičen IP

- **“IP Address”** – to je WAN IP naslov kot ga vidijo zunanji uporabniki na internetu (vključno z vašim ponudnikom internetnih storitev). V polje vnesite IP naslov.
 - **“Subnet Mask”** – Subnet Mask se uporablja za WAN IP naslov in ponavadi je 255.255.255.0.
 - **“Default Gateway”** (privzet “gateway”) – po potrebi v polje vnesite IP naslov za gateway.
 - **“Primary DNS”** – po potrebi v polje vnesite primarni IP naslov DNS strežnika.
 - **“Secondary DNS”** – če vaš ponudnik internetnih storitev zagotovi še en DNS strežnik (sekundarni), ga vnesite v to polje.
4. Za nadaljevanje kliknite **“Next”** (naprej) in pokaže se okno za brezžične nastavitve kot ga prikazuje slika 3 – 11.

Quick Setup - Wireless

Start >> WAN Connection Type >> **Wireless** >> Finish

Please use the WIFI switch on the device to enable/disable radio

Wireless Radio:

Wireless Network Name: (Also called the SSID)

Region:

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode:

Channel Width:

Channel:

Max Tx Rate:

Wireless Security:

Disable Security

WPA-PSK/WPA2-PSK

PSK Password:

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

No Change

Slika 3 – 11: Hitra namestitev – Brezžične nastavitve

- **“Wireless Radio”** (brezžični radio) – brezžični radio lahko omogočite/ onemogočite samo z uporabo stikala “WIFI ON/OFF”, ki se nahaja na napravi.
- **“Wireless Network Name”** (ime brezžičnega omrežja) – vnesite vrednost do največ 32 znakov. Isto SSID ime mora biti dodeljeno vsem brezžičnim napravam v vašem omrežju. Upoštevajoč vašo zaščito brezžičnega omrežja, je privzet SSID nastavljen na TP-LINK_XXXXXX (pri tem XXXXXX označuje zadnjih edinstvenih 6 števil vsakega MAC naslova usmerjevalnika). Te vrednosti so občutljive na male in velike črke. Na primer: *TEST* in *test* nista enaka.
- **Regija** – iz spustnega seznama izberite vašo regijo. To polje določa regijo, kjer se lahko uporabi brezžična funkcija usmerjevalnika. Uporaba brezžične funkcije v regiji, ki je različna od tiste, ki je označena na seznamu, je lahko nezakonita. Če vaše države ni na seznamu, se za pomoč obrnite na vašo vladno agencijo.



Opomba:

Zaradi lokalnih zakonskih omejitev, verzija za Severno Ameriko nima možnosti izbire regije.

- **“Mode”** (način) – to polje določa brezžični način v katerem deluje usmerjevalnik.
- **“Channel Width”** (širina kanala) – iz spustnega seznama izberite katerokoli širino kanala. Privzeta nastavitvev je samodejna, torej lahko samodejno prilagodi širino kanala za vaše kliente.

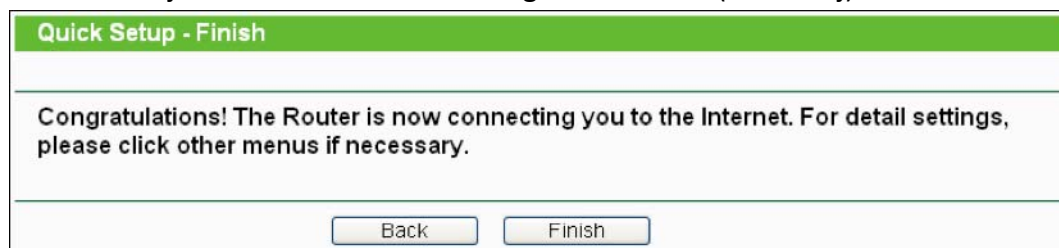
- **“Channel”** (kanal) – to polje določa katera frekvenca bo v uporabi. Privzet kanal je nastavljen na **“Auto”**, tako da dostopne točke avtomatično izberejo najboljši kanal. Brezžičnega kanala ni potrebno menjati, razen če zaznate motnje z drugo dostopno točko v bližini.
- **“Max Tx Rate”** – v tem polju lahko omejite največjo stopnjo prenosa usmerjevalnika.
- **“Disable Security”** (onemogoči zaščito) – funkcija brezžične zaščite je lahko omogočena ali onemogočena. Če je onemogočena, se brezžične postaje lahko na usmerjevalnik povežejo brez šifriranja. Zelo je priporočljivo, da za omogočanje zaščite izberete eno od spodnjih možnosti.
- **WPA-PSK/WPA2-PSK** – Izberite WPA, ki temelji na pred-izmenjanim geslom.
 - **PSK geslo** – vnesete lahko **ASCII** ali **hexadecimalne** znake.
 Pri **ASCII** lahko ključ sestavljajo katerakoli števila 0 do 9 in črke A do Z, dolžina pa naj bo med 8 in 63 znakov.
 Pri **hexadecimalnem** lahko ključ sestavljajo katerakoli števila od 0 do 9 in črke A do F, dolžina pa naj bo med 8 in 64 znakov.
 Upoštevajte tudi, da je ključ občutljiv na male in velike črke, kar pomeni da na kočni rezultat vplivajo male in velike črke. Priporočljivo je tudi, da si ključ in vse povezane nastavitve brezžične zaščite zapišete.

- **“No Change”** (ni sprememb) – če izberete to možnost, se konfiguracija brezžične zaščite ne spremeni!

To so nastavitve le za osnovne brezžične parametre. Za naprednejše nastavitve glejte poglavje “4.6 Brezžične nastavitve”.

5. Kliknite gumb **“Next”** (naprej). Pokaže se okno **“Finish”** (dokončaj), kot ga prikazuje slika 3 – 12.

Za dokončanje hitre namestitve kliknite gumb **“Finish”** (dokončaj).



Slika 3 – 12: Hitra namestitve - Dokončanje

4. KONFIGURACIJA USMERJEVALNIKA

V tem poglavju so prikazane ključne funkcije in načini konfiguracije vsake strani menija.

4.1 PRIJAVA

Po uspešni prijavi, se v spletnem orodju na levi pokaže petnajst glavnih menijev. Na desni pa so njihove pripadajoče razlage in napotki.

Podrobne razlage za vsako ključno funkcijo spletne strani so razložene v naslednjih poglavjih.

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

4.2 STATUS

Statusna stran prikazuje trenutne informacije statusa usmerjevalnika. Vse informacije so na voljo le za branje.

Status		
Firmware Version:	3.13.16 Build 120405 Rel.65615n	
Hardware Version:	WR941N v8 00000000	
LAN		
MAC Address:	00-0A-EB-13-09-13	
IP Address:	192.168.0.1	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_130919	
Mode:	11bgn mixed	
Channel Width:	Automatic	
Channel:	Auto (Current channel 1)	
Max Tx Rate:	300Mbps	
MAC Address:	00-0A-EB-13-09-13	
WDS Status:	Disable	
WAN		
MAC Address:	00-0A-EB-13-09-1A	
IP Address:	0.0.0.0	PPPoE(Connect on Demand)
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	
DNS Serve:	0.0.0.0, 0.0.0.0	
Online Time:	0 day(s) 00:00:00	Connecting...
Traffic Statistics		
	Received	Sent
Bytes:	0	4,527
Packets:	0	60
System Up Time:	0 days 00:06:25 <input type="button" value="Refresh"/>	

Slika 4 – 1: Status usmerjevalnika

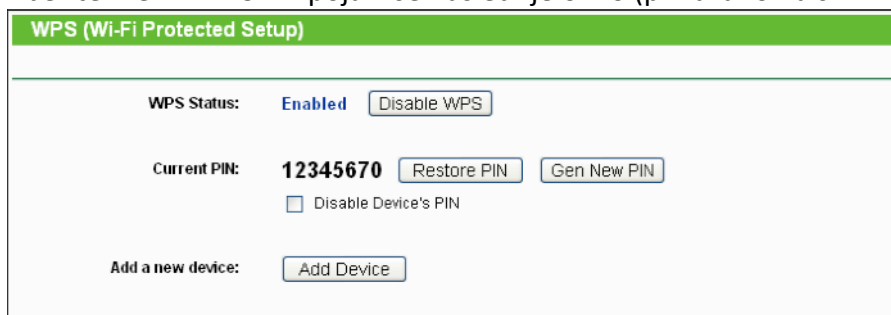
4.3 HITRA NASTAVITEV

Prosimo glejte navodila v poglavju "3.2. Vodnik hitre namestitve".

4.4 WPS

V tem poglavju je prikazan postopek kako na hiter način z WPS funkcijo (nastavitev Wi-Fi zaščite) dodati novo brezžično napravo na obstoječe omrežje.

- a) Izberite meni "WPS" in pojavi se naslednje okno (prikazano na sliki 4 – 2).



Slika 4 -2: WPS

- "WPS Status" – tukaj lahko funkcijo WPS omogočite ali onemogočite.
 - "Current PIN" – tukaj je prikazana trenutna vrednost PINa usmerjevalnika. Privzet PIN usmerjevalnika lahko najdete na nalepki, ki je nameščena na usmerjevalniku.
 - "Restore PIN" – obnovitev PINa usmerjevalnika na privzeto vrednost.
 - "Gen New PIN" – kliknite ta gumb in dobili boste novo naključno vrednost za PIN usmerjevalnika. Z generiranjem novega PINa lahko zagotovite zaščito omrežja.
 - "Disable Device's PIN" – tukaj lahko ročno onemogočite PIN usmerjevalnika. Če usmerjevalnik sprejme več zgrešenih poskusov za preverjanje pristnosti registriranja od zunaj, se funkcija samodejno onemogoči.
 - "Add Device" – s klikom na ta gumb lahko v obstoječe omrežje ročno dodate novo napravo.
- b) Dodajanje nove naprave:

Če brezžični adapter podpira nastavitev Wi-Fi zaščite (WPS), lahko brezžično povezavo med brezžičnim adapterjem in usmerjevalnikom vzpostavite ali z uporabo metode PBC (pritisni gumb konfiguracije) ali z uporabo PIN metode.



Opomba:

Za vzpostavitev uspešne povezave z WPS, je medtem potrebno narediti tudi ustrezno konfiguracijo nove naprave za WPS funkcijo.

I. Uporaba gumba WPS

Če ima vaša naprava klienta WPS gumb, ga uporabite.

Korak 1: Za eno sekundo pritisnite gumb "WPS/RESET", ki se nahaja na zadnji strani naprave. Privzet WPS status lahko ostane omogočen ("Enabled") in kliknite gumb "Add Device" kot na sliki 4 – 2, nato izberite "Press the button of the new device in two minutes" (gumb nove naprave pritisnite v dveh minutah) in kliknite "Connect" (poveži) – kot je prikazano na spodnji sliki.

Slika 4 – 3: Dodaj novo napravo

Korak 2: Neposredno pritisnite in držite WPS gumb naprave klienta.

Korak 3: WPS LED indikator utripa dve minuti med postopkom nastavitve Wi-Fi zaščite.

Korak 4: Ko WPS LED indikator sveti, se je naprava klienta uspešno povezala na usmerjevalnik.

Korak 5: Za nadaljnje napotke glejte vašo napravo klienta ali njena navodila za uporabo.

II. V usmerjevalnik vnesite PIN naprave klienta

To metodo uporabite takrat, ko ima naprava klienta nastavitve Wi-Fi zaščite s PIN številko.

Korak 1: Obdržite privzet WPS status omogočen (“**Enabled**”), kliknite gumb “**Add Device**” (dodaj napravo) kot na sliki 4 – 2, nato se pojavi spodnje okno.

Slika 4 – 4: Dodaj novo napravo

Korak 2: PIN številko klienta vnesite v polje ki je prikazano na zgornji sliki WPS. Nato kliknite gumb “**Connect**” (poveži).

Korak 3: Na zaslonu slike 4 – 4 se pokaže “**Connected successfully**” (uspešno povezan), kar pomeni da se je naprava klienta uspešno povezala na usmerjevalnik.

III. V napravo klienta vnesite PIN usmerjevalnika

To metodo uporabite, če vas naprava klienta sprašuje po PIN številki usmerjevalnika.

Korak 1: V napravo klienta vnesite PIN številko, ki je navedena na zaslonu pri nastavitvi Wi-Fi zaščite. (PIN številka pa je navedena tudi na nalepki na spodnji strani usmerjevalnika.)

Korak 2: Med procesom nastavitve Wi-Fi zaščite LED indikator WPS dve minuti utripa.

Korak 3: Ko WPS LED indikator sveti, se je naprava klienta uspešno povezala na usmerjevalnik.

Korak 4: Za nadaljnje napotke glejte vašo napravo klienta ali njena navodila za uporabo.

 **Opomba:**

- 1) Če je naprava uspešno dodana v omrežje, WPS LED indikator na usmerjevalniku pet minut sveti zeleno.
- 2) Če je brezžična funkcija usmerjevalnika onemogočena, WPS funkcije ni mogoče konfigurirati. Pred konfiguracijo WPS se zato prepričajte, da je brezžična funkcija omogočena.

4.5 OMREŽJE



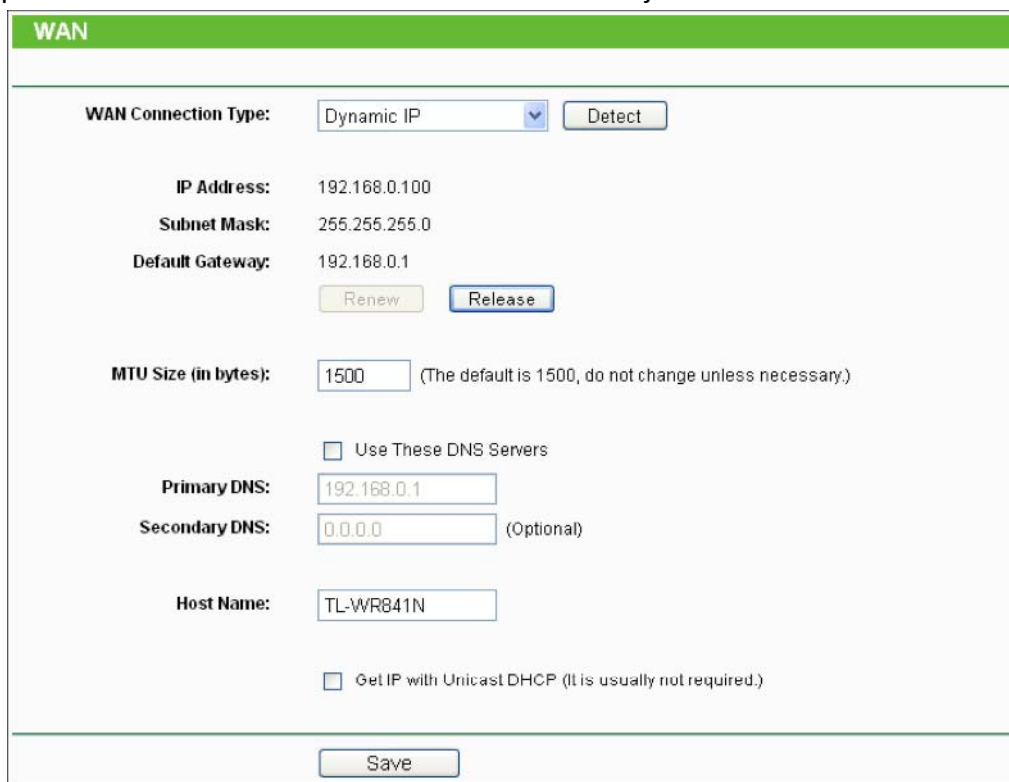
Slika 4 – 5: Meni omrežja

V meniju omrežja se nahajajo trije podmeniji (kot prikazuje slika 4 – 5): **LAN**, **WAN** in **MAC klon**. S klikom nanje lahko konfigurirate pripadajočo funkcijo.

WAN

Izberite meni "**Network → WAN**" (omrežje → WAN) in na spodnjem zaslonu lahko konfigurirate IP parametre za WAN.

1. Če vaš ponudnik internetnih storitev omogoča DHCP storitev, prosimo izberite tip **dinamičnega IP** in usmerjevalnik bo IP parametre samodejno pridobil od vašega ponudnika internetnih storitev. Prikaz na zaslonu je tak kot na sliki 4 – 6.

A screenshot of the WAN configuration page. The title bar is green with "WAN" in white. The page has a white background with a green border. It contains several fields and buttons:

- WAN Connection Type:** A dropdown menu set to "Dynamic IP" with a "Detect" button next to it.
- IP Address:** 192.168.0.100
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 192.168.0.1
- Buttons for "Renew" and "Release".
- MTU Size (in bytes):** 1500 (The default is 1500, do not change unless necessary.)
- Use These DNS Servers
- Primary DNS:** 192.168.0.1
- Secondary DNS:** 0.0.0.0 (Optional)
- Host Name:** TL-WR841N
- Get IP with Unicast DHCP (It is usually not required.)
- A "Save" button at the bottom.

Slika 4 – 6: WAN – dinamični IP

Ta stran prikazuje WAN IP parametre, ki jih dinamično določi vaš ponudnik internetnih storitev. Parametri vključujejo IP naslov, Subnet Mask, privzet

Gateway in ostalo. S klikom na gumb **“Renew”** (obnovi) obnovite parametre vašega ponudnika internetnih storitev. S klikom na gumb **“Release”** (opusti) IP parametre opustite.

- **“MTU Size”** – vrednost normalnega **MTU** (največja enota hitrosti) za večino Ethernet omrežij je 1500 bytov. Privzete vrednosti **“MTU Size”** ni priporočljivo menjati, razen če to zahteva vaš ponudnik internetnih storitev.
- **“Use These DNS Servers”** – če vam vaš ponudnik internetnih storitev dodeli enega ali dva DNS naslova, izberite **“Use These DNS Servers”** (uporabi te DNS strežnike) in v ustrezna polja vpišite primarni in sekundarni naslov. V nasprotnem primeru bo DNS strežnike dinamično določil vaš ponudnik internetnih storitev.



Opomba:

Če po vnosu DNS naslovov in povezavi na spletno stran dobite nazaj sporočilo o napaki, po vsej verjetnosti vaši DNS serverji niso pravilno nastavljeni. Obrnite se na vašega ponudnika internetnih storitev in pridobite naslove DNS strežnikov.

- **“Host Name”** – pri tej možnosti določite ime gostitelja usmerjevalnika.
- **“Get IP with Unicast DHCP”** – nekaj DHCP strežnikov ponudnikov internetnih storitev ne podpira uporabe oddajanja. Če IP naslova ne morete normalno dobiti, lahko uporabite to možnost (potrebna je zelo redkokdaj).

Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.

2. Če vaš ponudnik internetnih storitev zagotavlja statičen ali fiksni IP naslov, Subnet Mask, Gateway in DNS nastavitve, izberite **statičen IP**. Pokaže se stran za nastavitve statičnega IP, kakor je prikazano na sliki 4 – 7.

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 'Static IP' in a dropdown menu, with a 'Detect' button next to it. 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.

Slika 4 – 7: WAN – statični IP

- **IP naslov** – v decimalni zapis s pikami vnesite IP naslov ki ste ga dobili od vašega ponudnika internetnih storitev.
- **“Subnet Mask”** – v decimalni zapis s pikami vnesite Subnet Mask ki ste ga dobili od vašega ponudnika internetnih storitev, ponavadi je to 255.255.255.0.
- **Privzet Gateway** – (opcijsko) v decimalni zapis s pikami vnesite IP naslov za gateway, ki ste ga dobili od vašega ponudnika internetnih storitev.

- **MTU velikost** – vrednost normalnega **MTU** (največja enota hitrosti) za večino Ethernet omrežij je 1500 bytov. Privzete vrednosti **“MTU Size”** ni priporočljivo menjati, razen če to zahteva vaš ponudnik internetnih storitev.
- **Primarni / sekundarni DNS** – (opcijsko) v decimalni zapis s pikami vnesite enega ali dva DNS naslova, ki ste ga dobili od vašega ponudnika internetnih storitev.

Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.

3. Če vaš ponudnik internetnih storitev zagotavlja PPPoE povezavo, izberite možnost **PPPoE/Russia PPPoE**. Nato je potrebno vnesti naslednje parametre (kot prikazuje slika 4 – 8):

Slika 4 – 8: WAN – PPPoE

- **“User Name/Password”** – vnesite uporabniško ime in geslo, ki ste ga dobili od vašega ponudnika internetnih storitev. Ta polja so občutljiva na male in velike črke.
- **“Secondary Connection”** – ta je na voljo samo za PPPoE povezavo. Če vaš ponudnik internetnih storitev za povezavo v lokalno omrežje zagotovi dodaten tip povezave, kot je dinamičen/statičen IP, lahko za aktiviranje te sekundarne povezave preverite gumb dinamičen/statičen IP.
 - **“Disabled”** (onemogočen) – sekundarna povezava je po privzeti nastavitvi onemogočena, tako da je na voljo le PPPoE povezava. Takšna nastavitvev je priporočljiva.
 - **Dinamičen IP** - preverite lahko ta gumb in dinamičen IP uporabite kot sekundarno povezavo za povezovanje v lokalno omrežje vašega ponudnika internetnih storitev.

- **Statičen IP** - preverite lahko ta gumb in statičen IP uporabite kot sekundarno povezavo za povezovanje v lokalno omrežje vašega ponudnika internetnih storitev.
- **“Connect on Demand”** (povezava na zahtevo) – v tem načinu delovanja lahko internetno povezavo samodejno prekinete po določenem času neaktivnosti (**“Max Idle Time”** – najdaljši čas mirovanja) in ponovno vzpostavite ko se poskusite ponovno povezati na internet. Če želite, da vaša internetna povezava vseskozi deluje, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kolikor naj jih preteče pred prekinitvijo internetne povezave.
- **“Connect Automatically”** (avtomatična povezava) – povezava se po prekinitvi samodejno vzpostavi.
- **“Time-based Connecting”** (povezava glede na čas) – povezava je vzpostavljena le v nastavljenem časovnem obdobju (začetni in končni čas sta nastavljena v HH:MM formatu).



Opomba:

Šele ko na strani nastavitve sistemskega časa **“System Time → Time”** (sistemska orodja → čas) čas konfigurirate, bo funkcija **“Time-based Connecting”** začela veljati.

- **“Connect Manually”** – s klikom na gumb **“Connect/Disconnect”** se takoj povežete/prekinete povezavo. Ta način delovanja funkcijo **“Max Idle Time”** podpira na enak način kot način delovanja **“Connect on Demand”**. Internetna povezava se samodejno prekine po določenem časovnem obdobju neaktivnosti in ponovno vzpostavi ko se želite zopet povezati na internet. Za takojšnjo povezavo kliknite na gumb **“Connect”** (poveži). Za takojšnjo prekinitvev povezave kliknite na gumb **“Disconnect”**.

Previdnost: Včasih povezave ni mogoče prekiniti kljub temu, da je določen najdaljši čas mirovanja, ker se nekatere aplikacije v ozadju vseskozi povezujejo na internet.

Če želite narediti še kakšne naprednejše konfiguracije, kliknite na gumb **“Advanced”** (napredno) in pokaže se stran kot jo prikazuje slika 4 – 9:

Slika 4 – 9: Napredne nastavitve PPPoE

- **“MTU Size”** – privzeta MTU vrednost je 1480 bytov, kar ponavadi zadostuje. Vrednosti privzete MTU velikosti ni prporočljivo spreminjati, razen če tako zahteva vaš ponudnik internetnih storitev.
- **“Service Name/AC Name”** – Imena storitve in imena AC (dostopa do koncentratorja) ne konfigurirajte, razen če ste prepričani, da je to potrebno za vašega ponudnika internetnih storitev. V večini primerov vse deluje tudi če so ta polja prazna.
- **“ISP Specified IP Address”** – če vaš ponudnik internetnih storitev med prijavo ne določi IP naslova samodejno, prosimo obkljukajte kvadratek **“Use IP address specified by ISP”** (uporabite IP naslov vašega ponudnika internetnih storitev) in v decimalni zapis s pikami vnesite IP naslov, ki ste ga dobili od vašega ponudnika internetnih storitev.
- **“Detect Online Interval”** – usmerjevalnik bo zaznal dostop do koncentratorja na spletu na vsak interval. Privzeta vrednost je “0”. Vnesete lahko vrednost med “0” in “120”. Vrednost “0” pomeni da ni zaznave.
- **“Primary DNS/Secondary DNS”** – če vaš ponudnik internetnih storitev med prijavo ne določi DNS naslovov usmerjevalnika samodejno, prosimo obkljukajte kvadrataek **“Use the following DNS servers”** (uporabite naslednje DNS strežnike) in v decimalni zapis s pikami vnesite IP naslov primarnega strežnika vašega ponudnika internetnih storitev. Če je na voljo tdi sekundarni DNS naslov, vnesite še tega.

Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.

4. Če vaš ponudnik internetnih storitev zagotavlja povezavo **“BigPond Cable”** (ali **“Heart Beat Signal”**), prosimo izberite **“BigPond Cable”**. Vnesti je potrebno naslednje parametre (slika 4 – 10).

The screenshot shows a configuration window titled "WAN" with a green header. The "WAN Connection Type" is set to "BigPond Cable". Below this, there are input fields for "User Name" (containing "username"), "Password" (masked with dots), "Auth Server" (containing "sm-server"), and "Auth Domain" (empty). The "MTU Size (in bytes)" is set to "1500" with a note: "(The default is 1500, do not change unless necessary.)". Under "Connection Mode", "Connect on Demand" is selected, with a "Max Idle Time" of "15" minutes. Other options are "Connect Automatically" and "Connect Manually", both with "Max Idle Time" of "15" minutes. At the bottom, there are buttons for "Connect", "Disconnect", and "Disconnected!". A "Save" button is located at the very bottom of the window.

Slika 4 – 10

- **“User Name/Password”** – vnesite uporabniško ime in geslo, ki ste ga dobili od vašega ponudnika spletnih storitev. Ta polja so občutljiva na male in velike črke.
 - **“Auth Server”** – vnesite IP naslov strežnika za preverjanje pristnosti ali ime gostitelja.
 - **“Auth Domain”** – vtipkajte pripono imena domenskega strežnika glede na vašo lokacijo.
na primer:
NSW / ACT – **nsw.bigpond.net.au**
VIC / TAS / WA / SA / NT – **vic.bigpond.net.au**
QLD – **qld.bigpond.net.au**
 - **MTU velikost** – vrednost normalnega **MTU** (največja enota hitrosti) za večino Ethernet omrežij je 1500 bytov. Privzete vrednosti **“MTU Size”** ni priporočljivo spreminjati, razen če to zahteva vaš ponudnik internetnih storitev.
 - **“Connect on Demand”** (povezava na zahtevo) – v tem načinu delovanja lahko internetno povezavo samodejno prekinete po določenem času neaktivnosti (**“Max Idle Time”** – najdaljši čas mirovanja) in ponovno vzpostavite ko se poskusite ponovno povezati na internet. Če želite, da vaša internetna povezava vseskozi deluje, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kolikor naj jih preteče pred prekinitvijo internetne povezave.
 - **“Connect Automatically”** (avtomatična povezava) – povezava se po prekinitvi samodejno vzpostavi.
 - **“Connect Manually”** – s klikom na gumb **“Connect/Disconnect”** se takoj povežete/prekinete povezavo. Ta način delovanja funkcijo **“Max Idle Time”** podpira na enak način kot način delovanja **“Connect on Demand”**. Internetna povezava se samodejno prekine po določenem časovnem obdobju neaktivnosti in ponovno vzpostavi ko se želite zopet povezati na internet. Za takojšno povezavo kliknite na gumb **“Connect”** (poveži). Za takojšnjo prekinitve povezave kliknite na gumb **“Disconnect”**.
Previdnost: Včasih povezave ni mogoče prekiniti kljub temu, da je določen najdaljši čas mirovanja, ker se nekatere aplikacije v ozadju vseskozi povezujejo na internet.
Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.
5. Če vaš ponudnik internetnih storitev zagotavlja povezavo **“L2TP”**, prosimo izberite možnost **“L2TP/Russia L2TP”**. Vnesti pa je potrebno naslednje parametre (slika 4 – 11):

The screenshot shows a WAN configuration window with a green header. The settings are as follows:

- WAN Connection Type:** L2TP/Russia L2TP (dropdown menu)
- User Name:** username (text input)
- Password:** [masked with dots] (password input)
- Buttons:** Connect (blue), Disconnect (yellow), Disconnected! (text)
- IP Configuration:**
 - Dynamic IP
 - Static IP
 - Server IP Address/Name:** [empty text input]
 - 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.)
- Connection Mode:**
 - Connect on Demand
 - Connect Automatically
 - Connect Manually
- Save** button at the bottom.

Slika 4 – 11

- **“User Name/Password”** – vnesite uporabniško ime in geslo, ki ste ga dobili od vašega ponudnika spletnih storitev. Ta polja so občutljiva na male in velike črke.
- **Dinamičen IP / Statičen IP** – izberite eno ali drugo možnost, ki vam jo je posredoval vaš ponudnik internetnih storitev. Za takojšnjo povezavo kliknite gumb **“Connect”** (poveži), za takojšnjo prekinitev povezave pa gumb **“Disconnect”** (prekini).
- **“Connect on Demand”** (povezava na zahtevo) – usmerjevalnik lahko konfigurirate tako, da prekine internetno povezavo po določenem času neaktivnosti (**“Max Idle Time”** – najdaljši čas mirovanja). Če je bila vaša internetna povezava prekinjena zaradi neaktivnosti, **“Connect on Demand”** omogoča, da usmerjevalnik samodejno ponovno poskuša vzpostaviti povezavo takoj, ko poskušate ponovno dostopati do interneta. Če želite funkcijo **“Connect on Demand”** kliknite na gumb. Če želite, da vaša internetna povezava vseskozi deluje, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kolikor naj jih preteče pred prekinitvijo internetne povezave.
- **“Connect Automatically”** (avtomatična povezava) – povezava se po prekinitvi usmerjevalnika samodejno vzpostavi. Za uporabo te možnosti kliknite na gumb.
- **“Connect Manually”** – usmerjevalnik lahko konfigurirate tako da se povezava ali prekinitev izvede ročno. Po določenem času neaktivnosti (**“Max Idle Time”**),

usmerjevalnik prekine spletno povezavo, ki je samodejno ne bo mogoče ponovno vzpostaviti takoj, ko boste poskušali ponovno dostopati do interneta. Za uporabo te možnosti kliknite na gumb. Če želite, da je vaša internetna povezava vseskozi aktivna, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kot želite da traja internetna povezava, razen če vnesete novo spletno stran.

Previdnost: Včasih povezave ni mogoče prekiniti kljub temu, da je določen najdaljši čas mirovanja, ker se nekatere aplikacije v ozadju vseskozi povezujejo na internet.

Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.

6. Če vaš ponudnik internetnih storitev zagotavlja povezavo **“PPTP”**, prosimo izberite možnost **“PPTP/Russia PPTP”**. Vnesti pa je potrebno naslednje parametre (slika 4 – 12):

The screenshot shows the WAN configuration interface. At the top, there is a green header with the text 'WAN'. Below it, the 'WAN Connection Type' is set to 'PPTP/Russia PPTP'. The 'User Name' field contains 'username' and the 'Password' field is filled with dots. There are 'Connect' and 'Disconnect' buttons, with a 'Disconnected!' status indicator. The 'Dynamic IP' radio button is selected. The 'Server IP Address/Name' field is empty. Below this, there are fields for 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS', all containing '0.0.0.0'. The 'Internet IP Address' and 'Internet DNS' fields also contain '0.0.0.0'. The 'MTU Size (in bytes)' is set to '1420' with a note '(The default is 1420, do not change unless necessary.)'. The 'Max Idle Time' is set to '15' minutes. The 'Connection Mode' has three options: 'Connect on Demand' (selected), 'Connect Automatically', and 'Connect Manually'. A 'Save' button is at the bottom.

Slika 4 – 12: PPTP nastavitve

- **“User Name/Password”** – vnesite uporabniško ime in geslo, ki ste ga dobili od vašega ponudnika spletnih storitev. Ta polja so občutljiva na male in velike črke.
- **Dinamičen IP / Statičen IP** – izberite eno ali drugo možnost, ki vam jo je posredoval vaš ponudnik internetnih storitev in vnesite njegov IP naslov ali ime domene.
Če izberete statični IP in vnesete ime domene, je potrebno vnesti tudi DNS, ki ga določi ponudnik internetnih storitev. Nato kliknite gumb **“Save”** (shrani).

Za takojšnjo povezavo kliknite gumb **“Connect”** (poveži), za takojšnjo prekinitvev povezave pa gumb **“Disconnect”** (prekini).

- **“Connect on Demand”** (povezava na zahtevo) – usmerjevalnik lahko konfigurirate tako, da prekine internetno povezavo po določenem času neaktivnosti (**“Max Idle Time”** – najdaljši čas mirovanja). Če je bila vaša internetna povezava prekinjena zaradi neaktivnosti, **“Connect on Demand”** omogoča, da usmerjevalnik samodejno ponovno poskuša vzpostaviti povezavo takoj, ko poskušate ponovno dostopati do interneta. Če želite funkcijo **“Connect on Demand”** kliknite na gumb. Če želite, da vaša internetna povezava vseskozi deluje, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kolikor naj jih preteče pred prekinitvijo internetne povezave.
- **“Connect Automatically”** (avtomatična povezava) – povezava se po prekinitvi usmerjevalnika samodejno vzpostavi. Za uporabo te možnosti kliknite na gumb.
- **“Connect Manually”** – usmerjevalnik lahko konfigurirate tako da se povezava ali prekinitvev izvede ročno. Po določenem času neaktivnosti (**“Max Idle Time”**), usmerjevalnik prekine spletno povezavo, ki je samodejno ne bo mogoče ponovno vzpostaviti takoj, ko boste poskušali ponovno dostopati do interneta. Za uporabo te možnosti kliknite na gumb. Če želite, da je vaša internetna povezava vseskozi aktivna, v polje **“Max Idle Time”** vnesite **“0”**. Sicer pa vnesite število minut, kot želite da traja internetna povezava, razen če vnesete novo spletno stran.

Previdnost: Včasih povezave ni mogoče prekiniti kljub temu, da je določen najdaljši čas mirovanja, ker se nekatere aplikacije v ozadju vseskozi povezujejo na internet.

Kliknite gumb **“Save”** (shrani) in shranite vaše spremembe.



Opomba:

Če niste prepričani kako izbrati ustrezen tip povezave, kliknite na gumb **“Detect”** (zaznaj) in usmerjevalniku omogočite, da avtomatsko razišče strežnike in protokole vaše internetne povezave. Tip povezave se sporoči takrat, ko usmerjevalnik uspešno zazna aktivno spletno storitev. To sporočilo je le za vašo referenco. Za večjo sigurnost tip povezave preverite pri vašem ponudniku internetnih storitev. Različni tipi internetnih povezav, ki jih usmerjevalnik lahko prepozna so:

- **PPPoE** – so povezave ki uporabljajo PPPoE, ki zahtevajo uporabniško ime in geslo.
- **Dinamični IP** – so povezave ki uporabljajo dinamično določanje IP naslova.
- **Statični IP** – so povezave ki uporabljajo statično določanje IP naslova.

Usmerjevalnik ne more prepoznati povezav PPTP/ L2TO / BigPond. Če ponudnik internetnih storitev uporablja enega od teh protokolov, je potrebno povezavo konfigurirati ročno.

MAC KLON

Izberite meni **“Network → MAC Clone”** (omrežje → MAC klon) in na spodnjem zaslonu lahko konfigurirate MAC naslov za WAN, kot je prikazano na sliki 4 – 13:

Slika 4 – 13: Klon MAC naslova

Nekateri ponudniki internetnih storitev zahtevajo, da MAC naslov vašega adapterja registrirate. Pri tem so redko potrebne spremembe.

- **WAN MAC naslov** – to polje prikazuje trenutni MAC naslov WAN porta. Če vaš ponudnik internetnih storitev zahteva, da registrirate MAC naslov, v to polje vnesite pravi MAC naslov v XX-XX-XX-XX-XX-XX (XX je katerakoli hexadecimalna oblika).
- **MAC naslov vašega računalnika** – to polje prikazuje MAC naslov računalnika, ki upravlja usmerjevalnik. Če se zahteva MAC naslov, lahko kliknete na gumb **“Clone MAC Address To“** (MAC naslov kloniraj v) in ta MAC naslov popolni polje **“WAN MAC Address“** (WAN MAC naslov).

Za obnovitev MAC nalova WAN porta v privzete tovarniške nastavitve kliknite gumb **“Restore Factory MAC“** (obnovi MAC tovarniško nastavitve).

Kliknite gumb **“Save“** (shrani) in shranite vaše spremembe.



Opomba:

Funkcijo kloniranja MAC naslova lahko uporablja le računalnik v LAN (lokalnem omrežju).

LAN

Izberite meni **“Network → LAN“** (omrežje → LAN) in na spodnjem zaslonu lahko konfigurirate LAN parametre, kot je prikazano na sliki 4 – 14:

Slika 4 – 14: LAN

- **MAC naslov** – fizični naslov usmerjevalnika, kot ga vidi LAN. Vrednosti ni mogoče spremeniti.
- **IP naslov** – vnesite IP naslov vašega usmerjevalnika ali pa ga ponastavite v decimalni zapis s pikami (privzeta tovarniška nastavitve: 192.168.0.1).
- **Subnet Mask** – naslov kode, ki določa velikost omrežja. Ponavadi se uporablja 255.255.255.0.



Opomba:

- 1) Če spremenite LAN IP naslov, morate za prijavo v usmerjevalnik uporabiti novi naslov.

- 2) Če novo nastavljeni LAN IP naslov ni v istem subnet-u, se temu ustrezno hkrati spremeni bazen IP naslovov DHCP strežnika. Virtualni strežnik in DMZ gostitelj pa začneta veljati šele ko sta ponovno konfigurirana.

4.6 BREŽIČNE NASTAVITVE

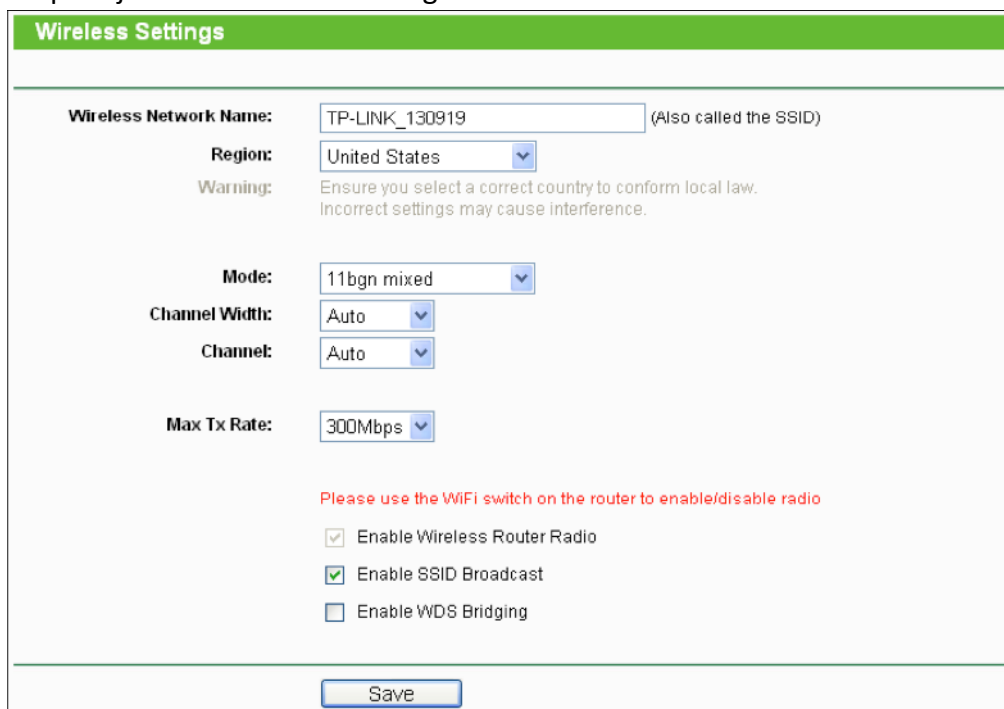


Slika 4 – 15: Brežični meni

V brezžičnem meniju je pet podmenijev (kot prikazuje slika 4 – 15): **brežične nastavitve**, **brežična zaščita**, **brežično MAC filtriranje**, **napredne brezžične nastavitve** in **statistika brezžičnega omrežja**.

BREŽIČNE NASTAVITVE

Izberite meni **“Wireless → Wireless Settings“** (brežično → brezžične nastavitve) in na spodnjem zaslону lahko konfigurirate osnovne nastavitve.



Slika 4 – 16: Brežične nastavitve

- **“Wireless Network Name“** (ime brezžičnega omrežja) – vnesite vrednost do 32 znakov. Isto ime SSID je potrebno določiti tudi vsem drugim brezžičnim napravam v vašem omrežju. Upoštevajoč zaščito brezžičnega omrežja, je privzet SSID nastavljen na TP-LINK_XXXXXX (XXXXXX ponazarja zadnjih šest števil vsakega MAC naslova usmerjevalnika). Vrednost je občutljiva na male in velike črke (*TEST* in *test* na primer nista enaka).

- **“Region“** (regija) – iz spustnega seznama izberite vašo regijo. V tem polju je določena regija, kjer se lahko uporablja brezžična funkcija usmerjevalnika. Uporaba brezžične funkcije v regiji, ki je različna od tiste, ki je označena na seznamu, je lahko nezakonita. Če vaše države ni na seznamu, se za pomoč obrnite na vašo vladno agencijo.

Ko iz spustnega seznama izberete vašo regijo, kliknite na gumb **“Save“** (shrani). Nato se pojavi pogovorno okno, v katerem kliknete **OK**.



Pogovorno okno



Opomba:

Zaradi lokalnih zakonskih omejitev, verzija za Severno Ameriko nima možnosti izbire regije.

- **“Mode“** (način) – izberite zeleni način. Privzeta tovarniška nastavitvev je mešan 11bgn.

“11b only“ (samo 11b) – to nastavitvev izberite, če so vsi brezžični klienti 802.11b.

“11g only“ (samo 11g) – to nastavitvev izberite, če so vsi brezžični klienti 802.11g.

“11n only“ (samo 11n) – to nastavitvev izberite le, če so vsi brezžični klienti 802.11n.

“11bg mixed“ (mešano 11bg) – to nastavitvev izberite, če uporabljate brezžične kliente 802.11b in 802.11g.

“11bgn mixed“ (mešano 11bgn) – to nastavitvev izberite, če uporabljate brezžične kliente 802.11b, 11g in 11n.

Izberite zeleni brezžični način. Ko je izbran način 802.11g, se lahko na usmerjevalnik povežejo le brezžične postaje 802.11g. Ko je izbran način 802.11n, se lahko na dostopne točke povežejo le brezžične postaje 802.11n. Zelo je priporočljivo, da način nastavitvev na **802.11b&g&n**, da se na usmerjevalnik lahko povežejo vse 802.11b, 802.11g in 802.11n brezžične postaje.

- **“Channel Width“** (širina kanala) – iz spustnega seznama izberite širino kanala. Privzeta nastavitvev je avtomatično, kar pomeni da se širina kanala za kliente prilagaja avtomatično.



Opomba:

Če v polju **“Mode“** izberete **“11b only“**, **“11g only“** ali **“11n only“**, se polje za izbiro širine kanala obarva sivo, vrednost postane 20M in tega ni mogoče spremeniti.

- **“Channel“** (kanal) – to polje določa katera frekvenca bo v uporabi. Privzet kanal je nastavljen na **Auto**, tako da dostopne točke avtomatično izberejo najboljši kanal. Brezžičnega kanala ni potrebno menjati, razen če zaznate motnje z drugo dostopno točko v bližini.
- **“Max Tx Rate“** – v tem polju lahko omejite največjo stopnjo prenosa usmerjevalnika.

- **“Enable Wireless Router Radio”** – brezžični radio usmerjevalnika je lahko za dostop brezžičnim postajam omogočen ali neomogočen. To lahko storite le z uporabo WIFI ON/OFF stikala na napravi.
- **“Enable SSID Broadcast”** (omogoči prikaz SSID) – ko brezžični klienti pregledujejo lokalno področje in iščejo brezžično omrežje za povezavo, zaznajo SSID, ki ga oddaja usmerjevalnik. Če obkljukate kvadrateg **“Enable SSID Broadcast”**, usmerjevalnik prikazuje ime (SSID).
- **“Enable WDS Bridging”** (omogoči WDS most) – obkljukajte ta kvadrateg in omogočite WDS. S to funkcijo lahko usmerjevalnik premosti dva ali več WLAN-ov. Če je ta možnost izbrana, je potrebno nastaviti še parametre, ki so prikazani na sliki 4 –17. Prepričajte se, da so spodnje nastavitve pravilne.

Slika 4 – 17

- **“SSID to be bridged** (za premostitev) – to je SSID dostopne točke (AP), na katero se vaš usmerjevalnik poveže kot klient. Uporabite lahko tudi funkcijo iskanja in na tak način izberete SSID za povezavo.
- **“BSSID to be bridged** (za premostitev) – to je BSSID dostopne točke (AP), na katero se vaš usmerjevalnik poveže kot klient. Uporabite lahko tudi funkcijo iskanja in na tak način izberete BSSID za povezavo.
- **“Survey”** (poizvedba) – s klikom na ta gumb lahko iščete dostopne točke, ki delujejo na trenutnem kanalu.
- **“Key Type”** (tip ključa) – to možnost je potrebno izbrati skladno s konfiguracijo zaščite dostopne točke. Priporočljivo je, da je tip varnosti enak kot tip varnosti vaše dostopne točke.
- **“WEP Index”** – to možnost je potrebno izbrati kadar je tip ključa WEP (ASCII) ali WEP (HEX). Označuje indeks WEP ključa.
- **“Auth Type”** – to možnost je potrebno izbrati kadar je tip ključa WEP (ASCII) ali WEP (HEX). Označuje tip avtorizacije korena dostopne točke.
- **“Password”** – če dostopna točka, na katero se bo povezal usmerjevalnik potrebuje geslo, morate v to prazno polje vnesti geslo.

BREŽIČNA ZAŠČITA

Izberite meni **“Wireless → Wireless Security ”** (brezžično → brezžična zaščita) kjer lahko konfigurirate nastavitve zaščite vašega brezžičnega omrežja.

Usmerjevalnik podpira pet načinov brezžične zaščite: WEP (kابلu enakovredna zasebnost), WPA (zaščiten Wi-Fi dostop), WPA2 (zaščiten Wi-Fi dostop 2), WPA-PSK (pred-izmenjan ključ), WPA2-PSK (pred-izmenjan ključ).

Slika 4 – 18: Brezžična zaščita

- **“Disable Security”** (onemogoči zaščito) – če brezžične zaščite ne želite uporabljati, označite ta gumb. Vendar pa je zelo priporočljivo, da izberete eno od naslednjih metod za omogočanje zaščite.
- **“WEP”** – temelji na standardu IEEE 802.11. Če označite ta gumb, se pokaže rdeče obvestilo kot ga prikazuje slika 4 – 19.

Slika 4 – 19

- **“Type”** – na spustnem seznamu lahko izberete tip WEP zaščite. Privzeta nastavitve je **“Automatic”** (samodejno), ki tako samodejno izbira med tipom preverjanja pristnosti **“Shared Key”** (skupni ključ) ali **“Open System”** (odprt sistem), ki temelji na zmožnostih in zahtevah brezžičnih postaj.
- **“WEP Key Format”** (oblika WEP ključa) – tukaj sta omogočeni obliki **“Hexadecimal”** (hexadecimalna/šestnajstična) in **“ASCII”**. Hexadecimalna oblika je kakršnakoli kombinacija šestnajstičnih znakov (0-9, a-f, A-F) v določeni dolžini. **“ASCII”** oblika je kakršnakoli kombinacija znakov na tipkovnici v določeni dolžini.

- **“WEP Key“** (WEP ključ) – izberite kateri od štirih ključev se bo uporabil pri vnosu ujemajočega WEP ključa, ki ga ustvarite. Prepričajte se, da so te vrednosti enake na vseh brezžičnih postajah v vašem omrežju.
- **“Key Type“** (tip ključa) – za šifriranje lahko izberete dolžino WEP ključa (64-bitni, ali 128-bitni, ali 152-bitni). “Disabled“ (onemogočen) pomeni, da je ta vnos WEP ključa nepravilen.

64-bitni – vnesete lahko 10 hexadecimalnih znakov (katerakoli kombinacija 0-9, a-f, A-F) ali 5 ASCII znakov.

128-bitni - vnesete lahko 26 hexadecimalnih znakov (katerakoli kombinacija 0-9, a-f, A-F) ali 13 ASCII znakov.

152-bitni - vnesete lahko 32 hexadecimalnih znakov (katerakoli kombinacija 0-9, a-f, A-F) ali 16 ASCII znakov.



Opomba:

Če ključa ne nastavite, je funkcija brezžične zaščite še vedno onemogočena, kljub temu da ste izbrali tip preverjanja pristnosti “Shared Key“ (skupni ključ).

➤ **“WPA / WPA2 – Enterprise“** – temelji na Radius strežniku.

- **“Version“** (verzija) – verzijo WPA zaščite lahko izberete v spustnem seznamu. Privzeta nastavitvev je **“Automatic“**, kar pomeni da avtomatsko izbira med **“WPA“** ali **“WPA2“** ter temelji na zmožnostih in zahtevah brezžične postaje.
- **“Encryption“** (šifriranje) – izbirate lahko med **“Automatic“**, **“TKIP“** ali **“AES“**.



Opomba:

Če označite gumb **“WPA / WPA2 – Enterprise“** in izberete šifriranje **“TKIP“**, se v oknu pokaže rdeče obvestilo, kot je prikazano na sliki 4 – 20.

Slika 4 – 20

- **“Radius Server IP“** – vnesite IP naslov Radius strežnika.
 - **“Radius Port“** – vnesite številko porta Radius strežnika.
 - **“Radius Password“** – vnesite geslo za Radius strežnik.
 - **“Group Key Update Period“** (čas za posodobitev skupinskega ključa) – določite sekundni interval za posodobitev skupinskega ključa. Vrednost naj bo 30 ali več. Če želite posodobitev onemogočiti, vnesite 0.
- **“WPA-PSK / WPA2-PSK – Personal (Recommended)”** (osebno, priporočljivo) – je WPA/WPA2 način preverjanja pristnosti, ki temelji na pred-izmenjanemu geslu.
- **“Version“** (verzija) – verzijo WPA-PSK zaščite lahko izberete v spustnem seznamu. Privzeta nastavitvev je **“Automatic“**, kar pomeni da avtomatsko izbira med **“WPA-PSK“** ali **“WPA2-PSK“** ter temelji na zmožnostih in zahtevah brezžične postaje.
 - **“Encryption“** (šifriranje) – kadar je način preverjanja pristnosti nastavljen na **“WPA-PSK“** ali **“WPA“**, lahko za šifriranje izbirate med **“Automatic“**, **“TKIP“** ali **“AES“**.



Opomba:

Če označite gumb **“WPA-PSK / WPA2-PSK – Personal (Recommended)”** in izberete šifriranje **“TKIP”**, se v oknu pokaže rdeče obvestilo, kot je prikazano na sliki 4 – 21.

Slika 4 – 21

- **“PSK Passphrase”** – vnesete lahko ASCII znake z dolžino med 8 in 63 znakov ali 8 do 64 hexadecimalnih znakov.
- **“Group Key Update Period”** (čas za posodobitev skupinskega ključa) – določite sekundni interval za posodobitev skupinskega ključa. Vrednost naj bo 30 ali več. Če želite posodobitev onemogočiti, vnesite 0.

Za shranjevanje nastavitvev na tej strani obvezno kliknite na gumb **“Save”** (shrani).

BREŽIČNI MAC FILTER

Izberite meni **“Wireless → MAC Filtering”** (brežično → MAC filtriranje) kjer lahko s konfiguriracijo funkcije **“Wireless MAC Filtering”** kontrolirate brezžični dostop. Pokaže se slika 4 – 22.

Slika 4 – 22: Brežično MAC filtriranje

Za filtriranje brezžičnih uporabnikov po MAC naslovih, kliknite na **“Enable”** (omogoči). Privzeta nastavev je **“Disabled”** (onemogoči).

- **“MAC Address”** (MAC naslov) – MAC naslov brezžične postaje, ki jo želite filtrirati.
- **“Status”** – status vnosa – lahko je **“Enabled”** (omogočen) ali **“Disabled”** (onemogočen).
- **“Description”** (opis) – enostaven opis brezžične postaje.

Za dodajanje novih MAC naslovov za filtriranje, kliknite gumb **“Add New...”** (dodaj nov...). Pokaže se okno **“Add or Modify Wireless MAC Address Filtering entry”** (dodaj ali spremeni vnos filtriranja MAC naslova), kakor prikazuje slika 4 – 23:

Slika 4 – 23: Dodaj ali spremeni vnos filtriranja brezžičnega MAC naslova

Za dodajanje ali spreminjanje vnosov MAC naslova, sledite spodnjim napotkom:

1. V polje **“MAC Address“** vnesite ustrezen MAC naslov. Oblika zapisa MAC naslova je XX-XX-XX-XX-XX-XX (X je katerokoli hexadecimalno število). Na primer: 00-0A-EB-B0-00-0B.
2. V polje **“Description“** vpišite enostaven opis brezžične postaje. Na primer: Brezžična postaja A.
3. Za **“Status“** tega vnosa iz spustnega seznama izberite **“Enabled“** (omogoči) ali **“Disabled“** (onemogoči).
4. Za shranjevanje vnosa kliknite gumb **“Save“** (shrani).

Za spreminjanje ali izbris obstoječega vnosa:

1. V vnosu, ki ga želite spremeniti kliknite **“Modify“** (spremeni). Če želite vnos izbrisati, kliknite **“Delete“** (izbriši).
2. Spremenite informacijo.
3. Za shranjevanje vnosa kliknite gumb **“Save“** (shrani).

Kliknite gumb **“Enable All“**, če želite omogočiti vse vnose.

Kliknite gumb **“Disable All“**, če želite onemogočiti vse vnose.

Kliknite gumb **“Delete All“**, če želite vse vnose izbrisati.

Kliknite gumb **“Next“**, če se želite premakniti na naslednjo stran.

Kliknite gumb **“Previous“**, če se želite vrniti na prejšnjo stran.

Na primer: če želite, da lahko brezžična postaja A z MAC naslovom 00-0A-EB-B0-00-0B in brezžična postaja B z MAC naslovom 00-0A-EB-00-07-5F dostopata do usmerjevalnika, vse ostale brezžične postaje pa do usmerjevalnika ne smejo dostopati, lahko seznam **“Wireless MAC Address Filtering“** konfigurirate po spodaj navedenih korakih:

1. Za omogočanje funkcije kliknite gumb **“Enable“**.
2. Za pravila filtriranja (**“Filtering Rules“**) označite gumb **“Allow the stations specified by any enabled entries in the list to access“** (vsem omogočenim vnosom s seznama dovoli dostop).
3. Če že obstajajo vnosi, kliknite izbriši vse ali onemogoči vse.
4. Kliknite gumb **“Add new...“** (dodaj nov...).
 - 1) V polje **“MAC Address“** vnesite MAC naslova 00-0A-EB-B0-00-0B/ 00-0A-EB-00-07-5F.
 - 2) V polje **“Description“** vpišite Brezžična postaja A/B.
 - 3) V spustnem seznamu **Statusa** izberite **“Enabled“** (omogoči).
 - 4) Kliknite gumb **“Save“** (shrani).
 - 5) Kliknite gumb **“Back“** (nazaj).

Konfigurirana pravila filtriranja morajo biti prikazana podobno kot na spodnjem seznamu:

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 B	Modify Delete

NAPREDNE BREZŽIČNE NASTAVITVE

Izberite meni **“Wireless → Wireless Advanced”** (brezžično → napredne brezžične nastavitve) in konfigurirajte napredne nastavitve brezžičnega omrežja.

Slika 4 – 24: Napredne brezžične nastavitve

- **“Transmit Power”** (moč prenosa) – tukaj določite moč prenosa usmerjevalnika. Izbirate lahko med **“High”** (visok), **“Middle”** (srednji) in **“Low”** (nizek). Privzeta in priporočljiva nastavitev je **“High”**.
- **“Beacon Interval”** – tukaj vnesite vrednost za **“Beacon”** interval: med 40-1000 milisekundami. **“Beacons”** so paketi, ki jih usmerjevalnik pošlje za sinhronizacijo brezžičnega omrežja. Vrednost intervala določa časovni interval teh paketov. Privzeta vrednost je 100.
- **“RTS Threshold”** (prag zahtevka za pošiljanje) – tukaj določite prag RTS (zahtevke za pošiljanje). Če je paket večji od velikosti praga RTS, usmerjevalnik na posebno sprejemno postajo pošlje RTS okvire in se pogodi za pošiljanje okvira podatkov. Privzeta vrednost je 2346.
- **“Fragmentation Threshold”** (prag razdrobljenosti) – ta vrednost je največja velikost, ki določa ali se bodo paketi razdrobili. Nastavitev prenizkega praga razdrobljenosti lahko povzroči počasno delovanje omrežja, saj bo paketov preveč. 2346 je privzeta in priporočena nastavitev.
- **“DTIM Interval”** – ta vrednost določi interval DTIM (sporočilo o navedbi dostavljenega prenosa). Polje DTIM je polje ki odšteva in kliente informira o naslednji možnosti za prisluh oddajanju in **“multicast”** sporočilom. Ko usmerjevalnik zavaruje sporočila o oddajanju ali **“multicast”** sporočila za povezane kliente, pošlje naslednji DTIM z DTIM vrednostjo intervala. Določite lahko vrednost med 1 – 255 **“beacon”** intervalov. Privzeta nastavitev je 1, kar pomeni, da je DTIM interval enak **“beacon”** intervalu.
- **“Enable WMM”** (omogoči WMM) – WMM funkcija zagotavlja, da se paketi z visoko pomembnostjo prenašajo prednostno. Je zelo priporočljiva nastavitev.
- **“Enable Short GI”** – ta funkcija je priporočljiva zato, ker z zmanjšanjem zaščitnega časovnega intervala poveča zmogljivost podatkov.

- **“Enabled AP Isolation”** – ta funkcija lahko brezžične postaje na vašem omrežju med seboj izolira. Brezžične naprave bodo lahko komunicirale z usmerjevalnikom, med seboj pa ne. Obkljukajte kvadratik, če želite uporabljati to funkcijo. Privzeta nastavitve izolacije ne omogoča.



Opomba:

Če nastavitve na tej strani ne poznate dobro, je priporočljivo, da obdržite privzete nastavitve; sicer lahko pride do zmanjšane uspešnosti delovanja brezžičnega omrežja.

BREŽIČNA STATISTIKA

Izberite meni **“Wireless → Wireless Statistics”** (brezžično → statistika brezžičnega omrežja) kjer lahko za vsako brezžično postajo vidite MAC naslov, trenutni status, sprejete in poslane pakete.

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"/>			

Slika 4 – 25: Statistika brezžičnega omrežja

- **“MAC Address”** – MAC naslov povezane brezžične postaje.
- **“Current Status”** – delujoči status povezane brezžične postaje: eden od **“STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected** (ni povezan).
- **“Received Packets”**– paketi, ki jih postaja sprejme.
- **“Sent Packets”** – paketi, ki jih postaja pošlje.

Vrednosti na tej strani ne morete spreminjati. Za posodobitev strani in prikaz trenutno povezanih brezžičnih postaj, kliknite na gumb **“Refresh”** (osveži).

Če so številke povezanih brezžičnih postaj prikazane na več kot eni strani, za premik na naslednjo stran kliknite gumb **“Next”** (naprej), za povratek na prejšnjo stran pa gumb **“Previous”** (prejšnji).



Opomba:

Ta stran se samodejno posodablja vsakih 5 sekund.

4.7 DHCP

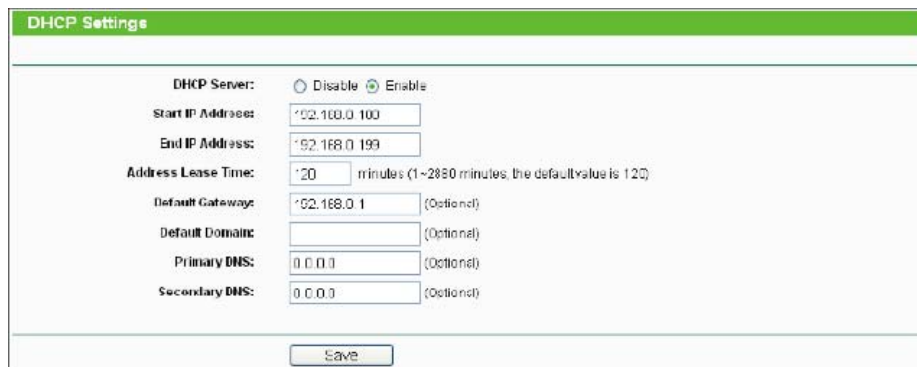
DHCP
- DHCP Settings
- DHCP Client List
- Address Reservation

Slika 4 – 26: Meni DHCP

V DHCP meniju se nahajajo trije podmeniji (kot prikazuje slika 4 – 26): **DHCP nastavitve**, **DHCP seznam klientov** in **rezervacija naslovov**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije.

DHCP NASTAVITVE

Izberite meni **“DHCP → DHCP Settings“** (DHCP → DHCP nastavitve) in na strani konfigurirajte DHCP strežnik, kakor prikazuje slika 4 – 27. Privzeto je usmerjevalnik nastavljen na DHCP (dinamičen konfiguracijski protokol gostitelja) strežnik, ki zagotavlja TCP/IP konfiguracijo za vse računalnike, ki so povezani na LAN usmerjevalnika.



Slika 4 – 27: DHCP nastavitve

- **“DHCP Server – Enable ali Disable“** – omogoči ali onemogoči DHCP strežnik. Če strežnik onemogočite, potem mora biti znotraj vašega omrežja drug DHCP strežnik, sicer je potrebno računalnik ročno konfigurirati.
- **“Start IP Address“** (začetni IP naslov) – pri dodeljevanju IP naslova, DHCP strežniku določite začetni IP naslov. Privzet začetni naslov je 192.168.0.100.
- **“End IP Address“** (končni IP naslov) – pri dodeljevanju IP naslova, DHCP strežniku določite končni IP naslov. Privzet končni naslov je 192.168.0.199.
- **“Address Lease Time“** (zakupni čas naslova) – to je količina časa, ko ima omrežni uporabnik s trenutnim dinamičnim IP naslovom dovoljenje za povezavo na usmerjevalnik. Čas vnesite v minutah, uporabnik pa bo imel “zakupljen” dinamični IP naslov za to časovno obdobje. Ko se čas izteče, bo uporabniku samodejno dodeljen nov dinamični IP naslov. Časovno obdobje je 1 – 2880 minut. Privzeta vrednost je 120 minut.
- **“Default Gateway“** (privzet Gateway) / opcijsko – priporočljivo je vnesti IP naslov LAN porta usmerjevalnika. Privzeta vrednost je 192.168.0.1.
- **“Default Domain“** (privzeta domena) / opcijsko – vnesite ime domene vašega omrežja.
- **“Primary DNS“** (primarni DNS) / opcijsko – vnesite DNS IP naslov, ki ste ga prejeli od vašega ponudnika internetnih storitev, ali pa se obrnite na ponudnika.
- **“Secondary DNS“** (sekundarni DNS) / opcijsko – vnesite IP naslov drugega DNS strežnika, če vaš ponudnik internetnih storitev omogoča dva strežnika.

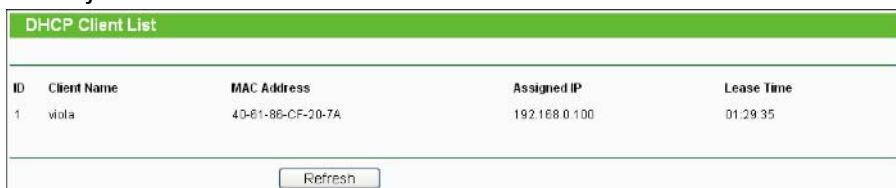


Opomba:

Če želite uporabljati usmerjevalnikovo funkcijo DHCP strežnika, je potrebno vse računalnike na LAN konfigurirati na **“Obtain an IP Address automatically“** (IP naslov pridobite samodejno).

SEZNAM KLIENTOV DHCP

Izberite meni **“DHCP → DHCP Client List“** (DHCP → seznam klientov DHCP) in na strani lahko vidite informacije o klientih, ki so povezani z usmerjevalnikom, kakor prikazuje slika 4 – 28.



ID	Client Name	MAC Address	Assigned IP	Lease Time
1	viola	40-61-86-CF-20-7A	192.168.0.100	01:29:35

Slika 4 – 28: Seznam klientov DHCP

- **“Client Name“** – ime DHCP klienta.
- **“MAC Address“** – MAC naslov DHCP klienta.
- **“Assigned IP“** – IP naslov, ki ga je usmerjevalnik dodelil DHCP klientu.
- **“Lease Time“** – čas zakupa DHCP klienta. Po pretečenem času dinamičnega IP naslova, je uporabniku samodejno dodeljen nov dinamični IP naslov.

Vrednosti na tej strani ni mogoče spreminjati. Za posodobitev te strani in prikaz trenutno povezanih naprav, kliknite gumb **“Refresh“** (osveži).

REZERVACIJA NASLOVA

Izberite meni **“DHCP → Address Reservation“** (DHCP → rezervacija naslova) in preko naslednjega zaslona (na sliki 4 – 29) lahko vidite in dodajate rezervirane naslove za kliente. Ko za računalnik na LANu določite rezerviran IP naslov, bo ob dostopanju na DHCP strežnik ta računalnik, vsakokrat prejel isti IP naslov. Najbolje je, da se IP naslovi določijo za strežnike, ki zahtevajo stalne IP nastavitve.



ID	MAC Address	Reserved IP Address	Status	Modify
----	-------------	---------------------	--------	--------

Slika 4 – 29: Rezervacija naslova

- **“Mac Address“** – MAC naslov računalnika, za katerega želite rezervirati IP naslov.
- **“Reserved IP Address“** – IP naslov, ki ga usmerjevalnik rezervira za računalnik.
- **“Status“** – status tega vnosa – lahko je **“Enabled“** (omogočen) ali **“Disabled“** (onemogočen).

Rezervacija IP naslova:

1. Kliknite gumb **“Add New...“** (dodaj nov...). Pojavi se prikaz kot na sliki 4 – 30.
2. Vnesite MAC naslov (v obliki XX-XX-XX-XX-XX-XX) in IP naslov (v decimalni obliki s pikami) računalnika, za katerega želite rezervirati IP naslov.
3. Kliknite gumb **“Save“** (shrani).

Slika 4 – 30: Dodaj ali spremeni vnos rezervacije naslova

Spreminjanje ali izbris obstoječega vnosa:

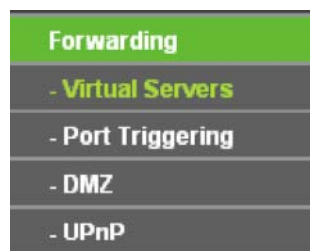
1. Na vnosu, ki ga želite spremeniti, kliknite gumb **“Modify”**. Če želite vnos izbrisati, kliknite **“Delete”** (izbriši).
2. Spremenite informacije.
3. Kliknite gumb **“Save”** (shrani).

Kliknite gumb **“Enable/Disable All”**, če želite vse vnose omogočiti/onemogočiti.

Kliknite gumb **“Delete All”**, če želite vse vnose izbrisati.

Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

4.8 POSREDOVANJE



Slika 4 – 31: Meni za posredovanje

V meniju posredovanje se nahajajo štirje podmeniji (kot prikazuje slika 4 – 31): **virtualni strežniki, sprožanje portov, DMZ in UPnP**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije.

VIRTUALNI STREŽNIKI

Izberite meni **“Forwarding → Virtual Servers”** (posredovanje → virtualni strežniki) in na zaslonu lahko vidite in dodate virtualne strežnike (kot prikazuje slika 4 – 32). Virtualni strežniki se lahko uporabijo za nastavitve javnih storitev na vašem LAN-u, kot je na primer DNS, spletna pošta in FTP. Virtualni strežnik je definiran kot storitveni port in vse internetne zahteve na ta port bodo preusmerjene na računalnik, ki ga določa IP strežnika. Računalnik, ki je uporabljen za virtualni strežnik, mora imeti statični ali rezervirani IP naslov, ker se lahko sicer pri uporabi DHCP funkcije njegov IP naslov spremeni.

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

Slika 4 – 32: Virtualni strežniki

- **“Service Port”** (port storitev) – število zunanjih portov. Vnesete lahko en port storitev ali območje storitvenih portov (v obliki XXX-YYY, kjer je XXX začetna številka porta, YYY pa končna številka porta).
- **“Internal Port”** (notranji port) – številka notranjega porta storitev na računalniku, kjer delujejo aplikacije storitev. Če je **notranji port** enak **portu storitev**, lahko polje pustite prazno, če pa imate le **port storitev**, vnesite specifično številko porta.
- **“IP Address”** – IP naslov računalnika, ki omogoča aplikacijo storitev.
- **“Protocol”** – protokol, ki se uporablja pri tej aplikaciji – lahko je **TCP**, **UDP** ali **All** (vsi protokoli, ki jih usmerjevalnik podpira).
- **“Status”** – status tega vnosa – lahko je **“Enabled”** (omogočen) ali **“Disabled”** (onemogočen).

Vnos virtualnega strežnika:

1. Kliknite gumb **“Add New...”** (dodaj nov...). Pojavi se prikaz kot na sliki 4 – 33.
2. S seznama **“Common Service Port”** (pogosti porti storitev) izberite port storitev, ki ga želite uporabljati. Če ta seznam nima storitev, ki jih želite uporabljati, v polje **“Service Box”** vnesite številko ali območje porta storitev.
3. V polje **“IP Address”** vnesite IP naslov računalnika.
4. Izberite protokol za to aplikacijo – lahko je **TCP**, **UDP** ali **All**.
5. Virtualni strežnik omogočite z izbiro **“Enable”**.
6. Kliknite gumb **“Save”** (shrani).

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text"/> (000-XXX or XXX)
Internal Port:	<input type="text"/> (000, Only valid for single Service Port or leave it blank)
IP Address:	<input type="text"/>
Protocol:	All
Status:	Enabled
Common Service Port:	--Select One--
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Slika 4 – 33: Dodaj ali spremeni vnos virtualnega strežnika



Opomba:

Če ima vaš računalnik ali strežnik več kot le eno razpoložljivo storitev, izberite drugo storitev in za ta računalnik ali strežnik vnesite enak IP naslov.

Spreminjanje ali izbris obstoječega vnosa:

1. Na vnosu, ki ga želite spremeniti, kliknite gumb **“Modify”**. Če želite vnos izbrisati, kliknite **“Delete”** (izbriši).
2. Spremenite informacije.
3. Kliknite gumb **“Save”** (shrani).

Kliknite gumb **“Enable/Disable All”**, če želite vse vnose omogočiti/onemogočiti.

Kliknite gumb **“Delete All”**, če želite vse vnose izbrisati.

Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.



Opomba:

Če storitveni port virtualnega strežnika nastavite na 80, je potrebno na strani **“Security → Remote Management”** (varnost → upravljanje na daljavo), port za spletno upravljanje spremeniti na katerokoli drugo vrednost razen 80 – na primer 8080. Drugače bo prišlo do konflikta za onemogočanje virtualnega strežnika.

SPROŽANJE PORTA

Izberite meni **“Forwarding → Port Triggering”** (posredovanje → sprožanje porta) in na zaslonu lahko vidite in dodate sprožanje porta (kot prikazuje slika 4 – 34). Nekatere aplikacije zahtevajo več povezav – to so na primer spletne igre, video konferenca, klicanje preko interneta in tako dalje. Te aplikacije ne morejo delovati s čistim NAT usmerjevalnikom. Sprožanje porta se zato uporablja za nekatere od teh aplikacij, ki lahko delujejo z NAT usmerjevalnikom.

ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
Add New... Enable All Disable All Delete All						
Previous Next						

Slika 4 – 34: Sprožanje porta

Ko enkrat konfigurirate usmerjevalnik, je delovanje sledeče:

1. Lokalni gostitelj s številko destinacijskega porta, ki je naveden v polju **“Trigger Port”** (sproži port) naredi izhodno povezavo.
2. Usmerjevalnik to povezavo zabeleži, odpre vhodni port ali porte, ki so v tabeli sprožanja portov povezani s tem vnosom in jih poveže z lokalnim gostiteljem.
3. Kadar je potrebno, lahko zunanji gostitelj z enim od portov, ki so določeni v polju **“Incoming Ports”**, poveže lokalnega gostitelja.
 - **“Trigger Port”** – port za izhodni promet. Izhodna povezava, ki uporablja ta port, bo sprožila to pravilo.
 - **“Trigger Protocol”** – protokol ki se uporablja za sprožanje portov je **TCP, UDP** ali **All** (vsi protokoli, ki jih podpira usmerjevalnik).
 - **“Incoming Ports”** – port ali območje portov, ki jih uporablja daljinski sistem, ko se odzove na izhodni zahtevek. Odgovor z uporabo enega od teh portov bo posredovan na računalnik, ki je pravilo sprožil. Vnesete lahko do največ 5 skupin portov (ali delov portov). Vsaka skupina portov mora biti med seboj ločena z **“,”**. Na primer: 2000-2038, 2050-2051, 2085, 3010-3030.

- **“Incoming Protocol”** – protokol, ki se uporablja za območje vhodnih portov, lahko je **TCP** ali **UDP** ali **ALL** (vsi protokoli, ki jih podpira usmerjevalnik).
- **“Status”** – status tega vnosa – lahko je **“Enabled”** (omogočen) ali **“Disabled”** (onemogočen).

Za dodajanje novega pravila, sledite spodnjim korakom:

1. Kliknite gumb **“Add New...”** (dodaj nov...). Pojavi se prikaz kot na sliki 4 – 35.
2. S seznama **“Common Application”** (pogoste aplikacije) izberite pogosto aplikacijo in nato se v polju **“Incoming Ports”** samodejno izpolni polje **“Trigger Port”**. Če na seznamu ni aplikacije, ki jo potrebujete, **“Trigger Port”** in **“Incoming Ports”** vnesite ročno.
3. Iz spustnega seznama **“Trigger Protocol”** izberite protokol, ki se uporabi za port za sprožanje – **TCP, UDP** ali **ALL**.
4. Iz spustnega seznama **“Incoming Protocol”** izberite protokol, ki se uporabi za vhodni port – **TCP, UDP** ali **ALL**.
5. V polju **“Status”** izberite **“Enable”** (omogoči).
6. Za shranjevanje novega pravila kliknite gumb **“Save”** (shrani).

Slika 4 – 35: Dodaj ali spremeni vnos za sprožanje porta

Spreminjanje ali izbris obstoječega vnosa:

1. Na vnosu, ki ga želite spremeniti, kliknite gumb **“Modify”**. Če želite vnos izbrisati, kliknite **“Delete”** (izbriši).
2. Spremenite informacije.
3. Kliknite gumb **“Save”** (shrani).

Kliknite gumb **“Enable All”**, če želite vse vnose omogočiti.

Kliknite gumb **“Disable All”**, če želite vse vnose onemogočiti.

Kliknite gumb **“Delete All”**, če želite vse vnose izbrisati.



Opomba:

1. Ko je sprožanje povezave sproščeno, se ustrezajoči odprti porti zaprejo.
2. Vsako pravilo lahko na LAN-u sinhrono uporabi le en gostitelj. Sprožilna povezava drugih gostiteljev na LAN-u bo zavrnjena.
3. Vhodni porti se ne morejo prekrivati.

DMZ

Izberite meni **“Forwarding → DMZ”** (posredovanje → DMZ) in na zaslonu lahko vidite in konfigurirate DMZ gostitelja (kot prikazuje slika 4 – 36). Funkcija DMZ gostitelja dovoljuje, da se en lokalni gostitelj internetu izpostavi za storitev s posebnim namenom, ko je na primer spletna igra ali video konferenca. DMZ gostitelj posreduje vse porte hkrati. Računalnik, katerega port je posredovan, mora imeti onemogočeno funkcijo DHCP klienta in dodeljen mu mora biti nov statični IP naslov, ker se lahko med uporabo DHCP funkcije njegov IP naslov spremeni.



Slika 4 – 36: DMZ

Določanje računalnika ali strežnika za DMZ strežnik::

1. Označite gumb **“Enable”** (omogoči).
2. V polje **“DMZ Host IP Address”** vnesite IP naslov lokalnega gostitelja.
3. Kliknite gumb **“Save”** (shrani).

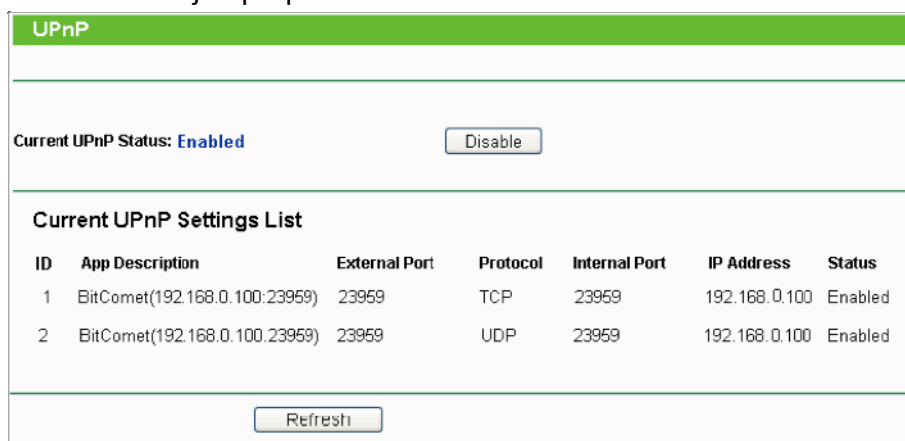


Opomba:

Ko nastavite DMZ gostitelja, požarni zid povezan s tem gostiteljem ne bo deloval.

UPnP

Izberite meni **“Forwarding → UPnP”** (posredovanje → UPnP) in na zaslonu lahko vidite informacije o **“UPnP”** (univerzalni “vstavi in igray”) – kot prikazuje slika 4 – 37. Ta funkcija napravam, kot so na primer spletni računalniki omogoča, da po potrebi dostopajo do virov lokalnega gostitelja. UPnP naprave lahko storitvena aplikacija na LAN-u samodejno prepozna.



ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	BitComet(192.168.0.100:23959)	23959	TCP	23959	192.168.0.100	Enabled
2	BitComet(192.168.0.100:23959)	23959	UDP	23959	192.168.0.100	Enabled

Slika 4 – 37: UPnP

- **“Current UPnP Status”** (trenutni UPnP status) – UPnP lahko s klikom na gumb omogočite **“Enabled”** ali onemogočite **“Disabled”**.
- **“Current UPnP Setting List”** (trenutni seznam nastavitvev UPnP) – ta tabela prikazuje trenutne informacije o UPnP.

- “App Description” – opis, ki ga v zahtevi UPnP omogoča aplikacija.
- “External Port” – zunanji port, ki ga za aplikacijo odpre usmerjevalnik.
- “Protocol” – tip protokola, ki ga za aplikacijo odpre usmerjevalnik.
- “Internal Port” – notranji port, ki ga usmerjevalnik odpre za lokalnega gostitelja.
- “IP Address” – IP naslov UPnP naprave, ki trenutno dostopa na usmerjevalnik.
- “Status” – tukaj je prikazan status porta. “Enabled” pomeni, da je port še vedno aktiven. Sicer je port neaktiven.

Za posodobitev trenutnega seznama UPnP nastavitev kliknite gumb “Refresh” (osveži).

4.9 ZAŠČITA

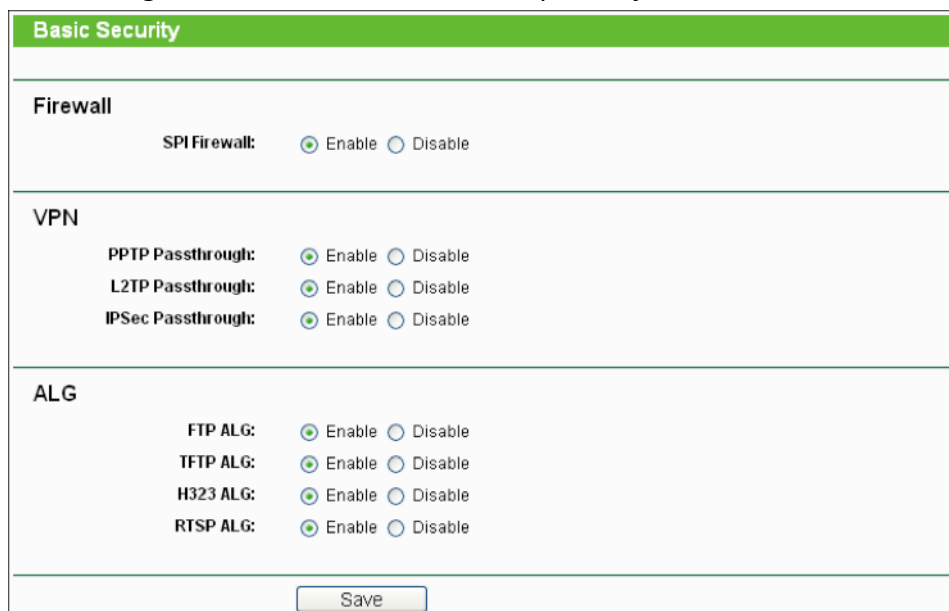


Slika 4 – 38: Meni zaščite

V meniju zaščite se nahajajo štiri podmeniji (kot prikazuje slika 4 – 31): **osnovna zaščita**, **napredna zaščita**, **lokalno upravljanje** in **upravljanje na daljavo**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije.

OSNOVNA ZAŠČITA

Izberite meni “Security → Basic Security” (zaščita → osnovna zaščita) in na zaslonu lahko konfigurirate osnovno zaščito – kot prikazuje slika 4 – 39.



Slika 4 – 39: Osnovna zaščita

- “Firewall” (požarni zid) – požarni zid vaše omrežje ščiti pred zunanjim svetom. Požarni zid umerjevalnika lahko tukaj omogočite ali onemogočite.

- **“SPI Firewall”** – SPI (napredni pregled paketa, znan tudi kot dinamično filtriranje paketa) s sledenjem stanja na sejo pomaga preprečiti kibernetični napad. To potrjuje, da je promet, ki gre skozi sejo, v skladu s protokolom. Po privzeti nastavitvi je SPI požarni zid omogočen. Če želite vse računalnike v LAN-u izpostaviti zunanjemu svetu, ga lahko izklopite.
- **“VPN”** – če želite, da se VPN tunelom, ki uporabljajo IPSec, PPTP ali L2PT protokole, omogoči prehod skozi požarni zid, mora biti VPN “Passthrough” omogočen.
 - **“PPTP Passthrough”** – tunelski protokol od točke do točke (PPTP) omogoča, da je protokol od točke do točke (PPP) speljan skozi IP omrežje. Za omogočanje, da so PPTP tuneli speljani skozi usmerjevalnik, obdržite privzeto nastavitvev **“Enabled”**.
 - **“L2TP Passthrough”** – 2.plast tunelskega protokola (L2TP) je metoda, ki se uporablja za omogočanje sej od točke do točke preko interneta na stopnji 2.plasti. Za omogočanje, da so L2TP tuneli speljani skozi usmerjevalnik, obdržite privzeto nastavitvev **“Enabled”**.
 - **“IPSec Passthrough”** – internetni protokol zaščite (IPSec) je niz protokolov za zagotovitev zasebne, varne komunikacije preko omrežij internetnih protokolov (IP). To poteka skozi uporabo kriptografskih varnostnih storitev. Za omogočanje, da so IPSec tuneli speljani skozi usmerjevalnik, obdržite privzeto nastavitvev **“Enabled”**.
- **“ALG”** – priporočljivo je, da se omogoča “Application Layer Gateway” (ALG), ker ALG omogoča da so filtri naslovov prevodov omrežja (NAT) priključeni na gateway. Na ta način podpirajo naslov in prevod porta nekaterih aplikacij plasti “nadzora/podatkov” protokolov, kot so na primer FTP, TFTP, H323 in podobni.
 - **“FTP ALG”** – obdržite privzeto nastavitvev **“Enabled”** in omogočite FTP klientom in strežnikom prenos podatkov preko NAT.
 - **“TFTP ALG”** – obdržite privzeto nastavitvev **“Enabled”** in omogočite TFTP klientom in strežnikom prenos podatkov preko NAT.
 - **“H323 ALG”** - obdržite privzeto nastavitvev **“Enabled”** in omogočite Microsoft NetMeeting klientom in strežnikom komunikacijo preko NAT.
 - **“RTSP ALG”** – kliknite **“Enable”** in omogočite nekatere klientom media predvajalnikov, da preko NAT komunicirajo z nekaterimi media strežniki.

Kliknite gumb **“Save”** in shranite vaše nastavitve.

NAPREDNA ZAŠČITA

Izberite meni **“Security → Advanced Security”** (zaščita → napredna zaščita) in na zaslonu lahko zaščitite usmerjevalnik pred napadi **“TCP-SYN Flood, UDP Flood”** in **“ICMP-Flood”** – kot prikazuje slika 4 – 40.

Slika 4 – 40: Napredne nastavitve

- **“Packets Statistics Interval (5-60)”** – privzeta vrednost je 10. Na spustnem seznamu izberite vrednost med 5 in 60 sekundami. Vrednost intervala statistike paketov ponazarja časovni del statistike paketov. “TCP-SYN Flood, UDP Flood” in “ICMP-Flood” uporabljajo rezultat statistike za analizo.
- **“DoS Protection”** – zaščita zanikanja storitev. Označite gumb **“Enable”** ali **“Disable”** in tako omogočite ali onemogočite funkcijo DoS zaščite. Šele ko je omogočena, so omogočeni “flood” filtri.



Opomba:

DoS zaščita deluje šele takrat, ko je omogočen **“Traffic Statistics”** v sistemskih orodjih.

- **“Enable ICMP-FLOOD Attack Filtering”** – omogočite ali onemogočite filter napada ICMP-FLOOD.
- **“ICMP-FLOOD Packets Threshold (5-3600)”** – privzeta nastavitev je 50. Vnesite vrednost med 5 in 3600. Ko je trenutno število paketov ICMP-FLOOD nad nastavljeno vrednostjo, usmerjevalnik takoj zažene funkcijo blokiranja.
- **“Enable UDP-FLOOD Filtering”** – omogoči ali onemogoči UDP-FLOOD filtriranje.
- **“UDP-FLOOD Packets Threshold (5-3600)”** – privzeta nastavitev je 500. Vnesite vrednost med 5 in 3600. Ko je trenutno število paketov UPD-FLOOD nad nastavljeno vrednostjo, usmerjevalnik takoj zažene funkcijo blokiranja.
- **“Enable TCP-SYN-FLOOD Attack Filtering”** – omogoči ali onemogoči TCP-SYN-FLOOD filtriranje napada.
- **“TCP-SYN-FLOOD Packets Threshold (5-3600)”** – privzeta nastavitev je 50. Vnesite vrednost med 5 in 3600. Ko je trenutno število paketov TCP-SYN-FLOOD nad nastavljeno vrednostjo, usmerjevalnik takoj zažene funkcijo blokiranja.
- **“Ignore Ping Packet From WAN Port to Router”** – omogoči ali onemogoči “neupoštevanje Ping paketov od WAN porta na usmerjevalnik”. Privzeta nastavitev je onemogočeno. Če je nastavitev omogočena, ping paket z interneta ne more dostopati do usmerjevalnika.

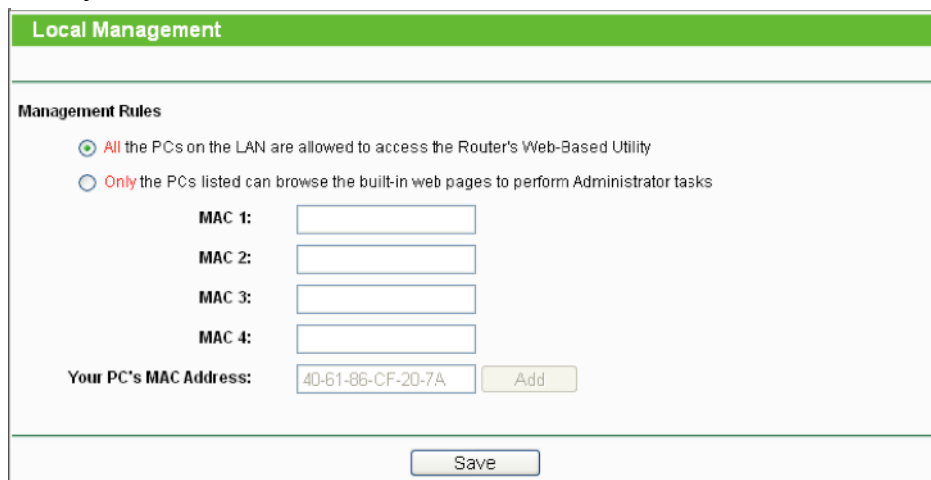
- **“Forbid Ping Packet From WAN Port to Router”** – omogoči ali onemogoči “prepoved Ping paketov od WAN porta na usmerjevalnik”. Privzeta nastavitve je onemogočena. Če je nastavitve omogočena, ping paket z LANa ne more dostopati do usmerjevalnika. To funkcijo lahko uporabite za zaščito pred nekaterimi virusi.

Kliknite gumb **“Save”** in shranite vaše nastavitve.

Za prikaz DoS tabele gostitelja z blokiranjem, kliknite gumb **“Blocked DoS Host List”**.

LOKALNO UPRAVLJANJE

Izberite meni **“Security → Local Management”** (zaščita → lokalno upravljanje) in na zaslonu lahko konfigurirate pravilo upravljanja, kot prikazuje slika 4 – 41. Funkcija upravljanja vam omogoča, da računalnikom na LAN zavrnete dostop do usmerjevalnika.



Slika 4 – 41: Lokalno upravljanje

Po privzeti nastavitvi je označen gumb **“All the PCs on the LAN are allowed to access the Router's Web-Based Utility”** (vsi računalniki na LANu lahko dostopajo do spletnega orodja usmerjevalnika). Če želite, da le računalniki znotraj omrežja z določenimi MAC naslovi lokalno dostopajo do strani nastavitve usmerjevalnika, označite gumb **“Only the PCs listed can browse the built-in web pages to perform Administrator tasks”** (le navedeni računalniki lahko pregledujejo vgrajene spletne strani za izvajanje nalog administratorja) in nato v ločena polja vnesite vsak MAC naslov. Oblika MAC naslova je XX-XX-XX-XX-XX-XX (X je hexadecimalno število). Le z MAC naslovi navedeni računalniki lahko pregledujejo vgrajene spletne strani za izvajanje nalog administratorja, medtem ko so vsi drugi blokirani.

Po kliku na gumb **“Add”** (dodaj), so MAC naslovi vaših računalnikov dodani na zgornji seznam.

Kliknite gumb **“Save”** in shranite vaše nastavitve.

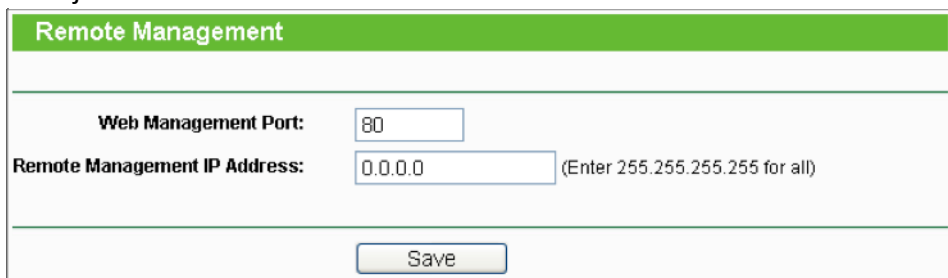


Opomba:

Če je vaš računalnik blokirani, vi pa želite ponovno dostopati do računalnika, uporabite koničast predmet, ki ga vstavite v odprtino **“Reset”** na zadnji strani naprave, držite približno 5 sekund in ponastavite privzete računalniške nastavitve na spletnem orodju usmerjevalnika.

UPRAVLJANJE NA DALJAVO

Izberite meni **“Security → Remote Management“** (zaščita → upravljanje na daljavo) in na zaslonu lahko konfigurirate funkcijo upravljanja, kot prikazuje slika 4 – 42. Ta funkcija vam omogoča, da usmerjevalnik preko interneta upravljate z oddaljene lokacije.



Slika 4 – 42: Upravljanje na daljavo

- **“Web Management Port“** – Dostop spletnega brskalnika ponavadi uporablja HTTP storitveni port 80. Privzeta številka spletnega porta tega usmerjevalnika za upravljanje na daljavo je 80. Za še večjo varnost lahko z vnosom številke v polje, spremenite spletni port upravljanja na daljavo na port po meri. Izberite številko med 1 in 65534, vendar pa ne uporabljajte številke kateregakoli pogostega storitvenega porta.
- **“Remote Management IP Address“** – to je trenutni naslov, ki ga uporabite pri dostopanju do usmerjevalnika z interneta. Ta funkcija je onemogočena, ko je IP naslov nastavljen na privzeto vrednost 0.0.0.0. Za omogočanje te funkcije 0.0.0.0. spremenite na veljaven IP naslov. Če ga nastavite na 255.255.255.255, lahko preko interneta na usmerjevalnik dostopajo vsi gostitelji.



Opomba:

- 1) Za dostop do usmerjevalnika, je v naslovno vrstico vašega brskalnika (v Internet Explorerju) ali lokacijsko polje (v Navigatorju) potrebno vnesti WAN IP vašega usmerjevalnika, ki mu sledi dvopičje in številka porta po meri. Na primer: če je WAN naslov vašega usmerjevalnika 202.96.12.8 in uporabljena številka porta 8080, v vaš brskalnik vnesite <http://202.96.12.8:8080>. Kasneje je morda potrebno vnesti geslo usmerjevalnika. Po uspešno vnešenem uporabniškem imenu in geslu, lahko dostopate do spletnega orodja brskalnika.
- 2) Bodite pozorni, da spremenite privzeto geslo usmerjevalnika na veliko bolj varno geslo.

4.10 STARŠEVSKI NADZOR

Izberite meni **“Parental Control“** (starševski nadzor) in na zaslonu lahko konfigurirate starševski nadzor, kot prikazuje slika 4 – 43. To funkcijo lahko uporabite za nadzor otrok pri internetnih aktivnostih, za omejitev dostopa otrokom do določenih spletnih naslovov in za omejitev časa brskanja po internetu.

Slika 4 – 43: Nastavitve starševskega nadzora

- **“Parental Control”** – če želite omogočiti delovanje te funkcije, označite **“Enable”**, sicer označite **“Disable”**.
- **“MAC Address of Parental PC”** – v to polje vnesite MAC naslov računalnika ki upravlja ali pa lahko uporabite spodnji gumb **“Copy To Above”** (kopiraj zgoraj).
- **“MAC Address of Your PC”** – to polje prikazuje MAC naslov računalnika ki upravlja usmerjevalnik. Če je MAC naslov vašega adapterja registriran, lahko kliknete na gumb **“Copy To Above”** in ta naslov prenesete v zgornje polje MAC naslova starševskega računalnika.
- **“Website Description”** – opis dovoljenih spletnih strani za nadzorovani računalnik.
- **“Schedule”** – dovoljeno časovno obdobje dostopa na internet za nadzorovani računalnik. Za podrobnejše informacije pojdite na **“Access Control → Schedule”** (nadzor dostopa → razpored).
- **“Modify”** – na tem mestu lahko obstoječ vnos popravljate ali izbrišete.

Za dodajanje novega vnosa sledite spodnjim korakom:

1. Kliknite gumb **“Add New...”** (dodaj nov...) in pojavi se okno, ki je prikazano na sliki 4 – 44.
2. Vnesite MAC naslov računalnika (na primer 00-11-22-33-44-AA) ki ga želite nadzorovati, v polje MAC naslov otrokovega računalnika (**“MAC Address of Child PC”**). Ali pa MAC naslov izberete s spustnega seznama seznama vseh naslovov v trenutnem LANu (**“All Address in Current LAN”**).
3. V polje **“Website Description”** (opis strani) navedite opis (na primer dovoli Google) spletne strani, do katere dovolite dostop.
4. V polje **“Allowed Domain Named”** vnesite ime dovoljene domene spletne strani (polno ime ali ključne besede – na primer google). Dovoljene bodo vse domene, ki vključujejo ključno besedo (www.google.com, www.google.com.hk).
5. Iz spustnega seznama **“Effective Time”** izberite časovni razpored (na primer Schedule_1), ki naj velja za ta vnos. Če na seznamu ni za vas primernih razporedov, kliknite na spodnji rdeče obarvan **“Schedule”** (razpored). Na ta način boste prišli na stran naprednejših nastavitvev razporeda, kjer boste lahko ustvarili razpored ki ga potrebujete.

6. V polju **“Status”** lahko izbirate med **“Enabled”** ali **“Disabled”** in tako ta vnos omogočite ali onemogočite.
 7. Kliknite gumb **“Save”** in shranite vaše nastavitve.
- Kliknite na gumb **“Enable All”** in omogočite delovanje vseh pravil na seznamu.
 Kliknite na gumb **“Disable All”** in onemogočite delovanje vseh pravil na seznamu.
 Kliknite na gumb **“Delete All”** in izbrišite vse vnose v tabeli.
 Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

The screenshot shows a web form titled "Add or Modify Parental Control Entry". At the top, there is a green header bar with the title. Below the header, a note states: "The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time settings](#)"."

The form contains the following fields and controls:

- MAC Address of Children's PC:** A text input field.
- All MAC Address In Current LAN:** A dropdown menu with "--Please Select--" as the selected option.
- Website Description:** A text input field.
- Allowed Website Name:** A series of seven stacked text input fields.
- Effective Time:** A dropdown menu with "Anytime" selected. Below it, a note says: "The time schedule can be set in "Access Control -> [Schedule](#)"."
- Status:** A dropdown menu with "Enabled" selected.

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

Slika 4 – 44: Dodaj ali spremeni vnos za starševski nadzor.

Na primer: če želite, da ima računalnik vaših otrok z MAC naslovom 00-11-22-33-44-AA dostop do spletne strani www.google.com le ob nedeljah in le takrat, ko je računalnik staršev z MAC naslovom 00-11-22-33-44-BB brez omejitev, sledite spodnjim nastavitvam:

1. Kliknite meni **“Parental Control”** na levi, da se odpre stran z nastavitvami za starševski nadzor. Označite **“Enable”** (omogoči) in v polje **“MAC Address of Parental PC”** (računalnik staršev) vnesite MAC naslov 00-11-22-33-44-BB.
2. Na levi strani kliknite **“Access Control → Schedule”** (nadzor dostopa → nastavitve) in na strani nastavitvev razporeda kliknite **“Add New...”** (dodaj nov...). Tako ustvarite nov razpored z opisom razporeda: Schedule_1, dan je nedelja, čas je cel dan – 24 ur.
3. Na levi ponovno kliknite **“Parental Control”**, da se vrnete na stran kjer dodate ali spremenite vnos starševskega nadzora:
 - Kliknite gumb **“Add New...”** (dodaj nov...).
 - V polje **“MAC Address of Childrens PC”** (MAC naslov računalnika otrok) vnesite 00-11-22-33-44-AA.
 - V polje **“Website Description”** (opis strani) vpišite **“dovoli Google”**.

- V polje “**Allowed Website Name**” (dovoljena imena spletnih strani) vnesite www.google.com.
- Iz spustnega seznama “**Effective Time**” (čas veljavnosti) izberite “Schedule_1”, ki ste ga pravkar ustvarili.
- V polju “**Status**” izberite “Enable” (omogoči).

4. Za dokončanje nastavitvev kliknite gumb “**Save**” (shrani).

Nato pojdite nazaj na stran nastavitvev starševskega nadzora, kjer lahko vidite seznam, kot je prikazan na sliki 4 – 45.

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

Slika 4 – 45: Nastavitve starševskega nadzora

4.11 NADZOR DOSTOPA



Slika 4 – 46: Nadzor dostopa

V meniju nadzora dostopa se nahajajo štiri podmeniji (kot prikazuje slika 4 – 46): **pravilo, gostitelj, cilj in razpored**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije.

“RULE”

Izberite meni “**Access Control → Rule**” (nadzor dostopa → pravilo) in na zaslonu lahko vidite in nastavite pravila za nadzor dostopa, kot prikazuje slika 4 – 47.

Access Control Rule Management

Enable Internet Access Control

Default Filter Policy

Allow the packets specified by any enabled access control policy to pass through the Router

Deny the packets specified by any enabled access control policy to pass through the Router

ID	Rule Name	Host	Target	Schedule	Enable	Modify
	<input type="button" value="Setup Wizard"/>					
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>						
<input type="button" value="Move"/> ID <input type="text"/> To ID <input type="text"/>						

Current No. Page

Slika 4 – 47: Upravljanje pravil nadzora dostopa

- **“Enable Internet Access Control”** – obkljukajte kvadratega in omogočite funkcijo nadzora dostopa do interneta in začnejo veljati privzeta merila filtra.
- **“Rule Name”** – tukaj je prikazano ime pravila, ki je unikatno.
- **“Host”** – tukaj je prikazan v pripadajočem pravilu izbran gostitelj.
- **“Target”** – tukaj je prikazan v pripadajočem pravilu izbran cilj.
- **“Schedule”** – tukaj je prikazan v pripadajočem pravilu izbran raspored.
- **“Action”** – tukaj je prikazano dejanje, ki ga izvede usmerjevalnik za ukvarjanje s paketi. Lahko je **“Allow”** (dovoli) ali **“Deny”** (zavrni). Dovoljenje pomeni, da usmerjevalnik dovoli, da gredo paketi skozi usmerjevalnik. Zavrnitev pa pomeni, da usmerjevalnik zavrne prehod paketov skozi usmerjevalnik.
- **“Status”** – V tem polju je prikazan status pravila. **“Enabled”** pomeni, da pravilo velja, **“Disabled”** pa pomeni, da pravilo ne velja.
- **“Modify”** – tukaj lahko obstoječe pravilo spremenite ali izbrišete.

Za dodajanje pravil obstajata dva načina.

Način 1:

1. Kliknite gumb **“Setup Wizard”** (čarovnik za nastavitve) in pokaže se okno, kot ga prikazuje slika 4 – 48.

Slika 4 – 48: Nitra nastavitve – kreiranje vnosa gostitelja

- **“Mode”** (način) – tukaj sta dve možnosti: **IP naslov** ali **MAC naslov**. Iz spustnega seznama lahko izberete kateregakoli.
 - **“Host Description”** – v tem polju ustvarite unikatni opis gostitelja (na primer Host_1).
Če ste izbrali **IP naslov**, lahko izbirate naslednje:
 - **“LAN IP Address”** – vnesite IP naslov ali območje naslovov gostitelja v obliki decimalnega zapisa s pikami (na primer 192.168.0.23).
Če ste izbrali **MAC naslov**, lahko izbirate naslednje:
 - **“MAC Address”** – vnesite MAC naslov gostitelja v obliki XX-XX-XX-XX-XX-XX (na primer 00-11-22-33-44-AA).
2. Ko zaključite s kreiranjem vnosa gostitelja kliknite **“Next”** (naprej) in pokaže se okno kot na sliki 4 – 49.

Quick Setup - Create an Access Target Entry

Mode:

Target Description:

IP Address: -

Target Port: -

Protocol:

Common Service Port:

Slika 4 – 49: Hitra nastavitvev – kreiranje vnosa ciljnega dostopa

- **“Mode”** (način) – tukaj sta dve možnosti: **IP naslov** ali **ime domene**. Iz spustnega seznama lahko izberete kateregakoli.
 - **“Host Description”** – v tem polju ustvarite opis cilja. Upoštevajte, da mora biti opis unikaten (na primer Target_1).
Če ste izbrali **IP naslov**, lahko izbirate naslednje:
 - **“IP Address”** – vnesite IP naslov (ali območje naslovov) cilja v obliki decimalnega zapisa s pikami (na primer 192.168.0.23).
 - **“Target Port”** – določite port ali območje portov cilja. Za nekatere pogoste storitvene porte lahko uporabite spodnji element “Common Service Port”.
 - **“Protocol”** – tukaj lahko izbirate med štirimi možnostmi – All, TCP, UDP ali ICMP. Za cilj iz spustnega seznama izberite enega izmed njih.
 - **“Common Service Port”** – tukaj naštejite nekatere pogoste storitvene porte. Če port izberete iz spustnega seznama, se v polju “Target Port” samodejno izpiše njegova pripadajoča številka. Če na primer izberete FTP, se v polju “Target Port” samodejno izpiše “21”.
 - Če ste izbrali **ime domene**, lahko izbirate naslednje:
 - **“Domain Name”** – tukaj lahko vnesete štiri imena domen – ali s celim imenom ali pa v ključnih besedah (na primer google). Vse domene, ki vključujejo ključne besede bodo blokirane ali dovoljene.
3. Ko zaključite s kreiranjem vnosa ciljnega dostopa kliknite **“Next”** (naprej) in pokaže se okno kot na sliki 4 – 50.

Quick Setup - Create an Advanced Schedule Entry

Note: The Schedule is based on the time of the Router.

Schedule Description:

Day: Everyday Select Days

Mon Tue Wed Thu Fri Sat Sun

Time: all day-24 hours:

Start Time: (HHMM)

Stop Time: (HHMM)

Slika 4 – 50: Hitra nastavitvev – kreiranje vnosa naprednejšega razporeda

- **“Schedule Description”** – v tem polju ustvarite opis razporeda. Upoštevajte, da mora biti opis unikaten (na primer Schedule_1).

- **“Day”** – če označite **“Everyday”** izberete vse dneve v tednu, če pa označite **“Select Days”**, je potrebno še določiti dan (dneve).
 - **“Time”** – obkljukajte **“24 ur”** ali pa določite začetni in končni čas.
 - **“Start Time”** – vnesite začetni čas v formatu HHMM (HHMM so 4 številke). Na primer 0800 pomeni 8:00.
 - **“Stop Time”** – vnesite končni čas v formatu HHMM (HHMM so 4 številke). Na primer 2000 pomeni 20:00.
4. Ko zaključite s kreiranjem vnosa naprednejšega razporeda kliknite **“Next”** (naprej) in pokaže se okno kot na sliki 4 – 51.

Slika 4 – 51: kreiranje vnosa nadzora dostopa

- **“Rule”** – v tem polju ustvarite ime pravila. Upoštevajte, da mora biti ime unikatno (na primer Rule_1).
 - **“Host”** – v tem polju iz spustnega seznama izberite gostitelja za to pravilo. Privzeta vrednost je **“Host Description”**, opis gostitelja ki ste ga pravkar kreirali.
 - **“Target”** – v tem polju iz spustnega seznama izberite cilj za to pravilo. Privzeta vrednost je **“Target Description”**, opis cilja ki ste ga pravkar kreirali.
 - **“Schedule”** – v tem polju iz spustnega seznama izberite razpored za to pravilo. Privzeta vrednost je **“Schedule Description”**, opis razporeda ki ste ga pravkar kreirali.
 - **“Status”** – v tem polju imate dve možnosti – **“Enabled”** ali **“Disabled”**. Z omogočanjem pravilo začne veljati. Če pa izberete onemogoči, pravilo ne začne veljati.
5. S klikom na **“Finish”** zaključite z dodajanjem novega pravila.

Način 2:

1. Kliknite gumb **“Add New...”** in pokaže se okno kot ga prikazuje slika 4 – 52.
2. V polje **“Rule Name”** vnesite ime pravila (na primer Rule_1).
3. Iz spustnega seznama izberite gostitelja (**“Host”**) ali izberite **“Click Here To Add New Host List”** (za dodajanje novega seznama gostiteljev kliknite tukaj).
4. Iz spustnega seznama izberite cilj (**“Target”**) ali izberite **“Click Here To Add New Target List”** (za dodajanje novega seznama ciljev kliknite tukaj).
5. Iz spustnega seznama izberite razpored (**“Schedule”**) ali izberite **“Click Here To Add New Schedule List”** (za dodajanje novega seznama razporedov kliknite tukaj).
6. V polju **“Status”** izberite **“Enabled”** ali **“Disabled”** in tako vnos omogočite ali onemogočite.
7. Kliknite gumb **“Save”** (shrani).

Slika 4 – 52: Vnos dodajanja internetnega nadzora dostopa

Na primer: če želite omogočiti gostitelju z MAC naslovom 00-11-22-33-44-AA dostop do www.google.com le v času med 18:00 in 20:00 ob sobotah in nedeljah, ostalim gostiteljem v LANu pa prepovedati dostop do interneta, sledite spodnjim navodilom:

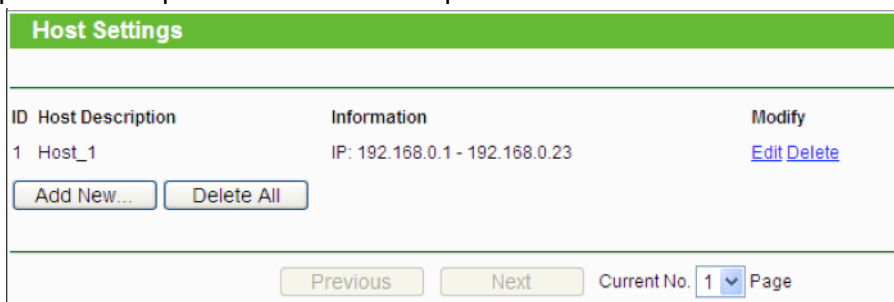
1. Kliknite na podmeni na levi **“Rule of Access Control”** (pravilo nadzora dostopa) in se vrnite na stran seznama pravil. Izberite **“Enable Internet Access Control”** (omogoči nadzor dostopa do interneta) in izberite **“Allow the packets specified by any enabled access control policy to pass through the Router”** (dopusti paketom, ki so navedeni v kateremkoli merilu nadzora dostopa, prehod skozi usmerjevalnik).
2. Priporočamo vam, da kliknete na čarovnika za namestitvev (**“Setup Wizard”**) in tako dokončate vse naslednje nastavitve.
3. Kliknite na podmeni na levi **“Host of Access Control”** (gostitelj nadzora dostopa) in pojdite na stran seznama gostiteljev. Dodajte nov vnos, kjer je opis gostitelja Host_1, MAC naslov pa 00-11-22-33-44-AA.
4. Kliknite na podmeni na levi **“Target of Access Control”** (cilj nadzora dostopa) in pojdite na stran seznama ciljev. Dodajte nov vnos, kjer je opis cilja Target_1, ime domene pa www.google.com.
5. Kliknite na podmeni na levi **“Schedule of Access Control”** (razpored nadzora dostopa) in pojdite na stran seznama razporedov. Dodajte nov vnos, kjer je opis razporeda Schedule_1, dan je Sat in Sun, začetni čas je 1800, končni čas pa 2000.
6. Kliknite na podmeni na levi **“Rule of Access Control”**, kliknite na gumb **“Add New...”** in kot sledi dodajte novo pravilo:
 - V polju **“Rule Name”** ustvarite ime pravila. Upoštevajte, da mora biti ime unikatno, na primer Rule_1.
 - V polju **“Host”** izberite Host_1.
 - V polju **“Target”** izberite Target_1.
 - V polju **“Schedule”** izberite Schedule_1.
 - V polju **“Status”** izberite Enable.
 - Za dokončanje nastavitvev kliknite gumb **“Save”** (shrani).

Nato pojdite nazaj na stran upravljanja pravil nadzora dostopa in videli boste spodnji seznam.

ID	Rule Name	Host	Target	Schedule	Enable	Modify
1	Rule_1	Host_1	Target_1	Schedule_1	<input checked="" type="checkbox"/>	Edit Delete

“HOST“

Izberite meni **“Access Control → Host“** (nadzor dostopa → gostitelj) in na zaslonu lahko vidite seznam gostiteljev, kot prikazuje slika 4 – 53. Seznam gostiteljev je potreben za pravilo nadzora dostopa.



ID	Host Description	Information	Modify
1	Host_1	IP: 192.168.0.1 - 192.168.0.23	Edit Delete

Current No.

Slika 4 – 53: Nastavitve gostitelja

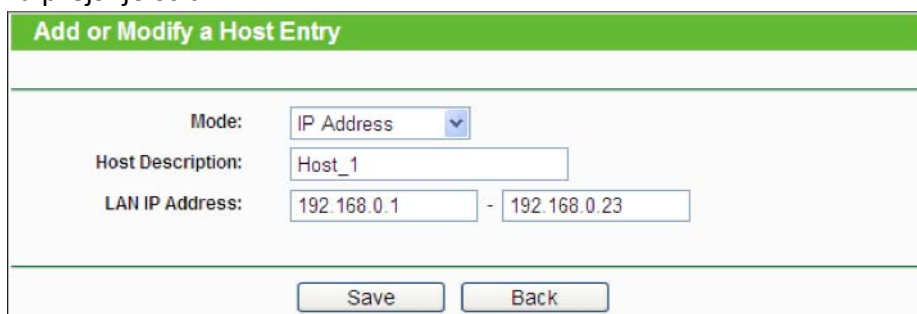
- **“Host Description“** – tukaj je prikazan opis gostitelja in ta opis je unikatni.
- **“Information“** – tukaj je prikazana informacija o gostitelju. Lahko je IP ali MAC naslov.
- **“Modify“** – tukaj lahko spremenite ali izbrišete obstoječi vnos.

Za dodajanje novega vnosa sledite spodnjim korakom:

1. Kliknite gumb **“Add New...“** (dodaj nov...).
2. V polju **“Mode“** izberite IP naslov ali MAC naslov.
 - Če izberete IP naslov, se pokaže okno kot na sliki 4 – 54.
 - 1) V polje **“Host Description“** zapišite unikatni opis gostitelja (na primer Host_1).
 - 2) V polje **“LAN IP Address“** vnesite IP naslov.
 - Če izberete MAC naslov, se pokaže okno kot na sliki 4 – 55.
 - 1) V polje **“Host Description“** zapišite unikatni opis gostitelja (na primer Host_1).
 - 2) V polje **“MAC Address“** vnesite MAC naslov.
3. Za dokončanje nastavitvev kliknite gumb **“Save“** (shrani).

Kliknite gumb **“Delete All“** in izbrišite vse vnose v tabeli.

Kliknite gumb **“Next“**, če želite iti na naslednjo stran in gumb **“Previous“**, če želite iti na prejšnjo stran.



Add or Modify a Host Entry

Mode:

Host Description:

LAN IP Address: -

Slika 4 – 54: Dodaj ali spremeni vnos gostitelja.

Slika 4 – 55: Dodaj ali spremeni vnos gostitelja

Na primer: če želite omejiti internetne aktivnosti gostitelja z MAC naslovom 00-11-22-33-44-AA, najprej sledite spodnjim nastavitvam:

1. V oknu s slike 4 – 53 kliknite gumb **“Add New...”** in vstopite na stran za dodajanje ali spreminjanje vnosa gostitelja.
2. V polju **“Mode”** (način) iz spustnega seznama izberite MAC naslov.
3. V polje **“Host Description”** vpišite **unikaten** opis gostitelja (na primer Host_1).
4. V polje **“MAC Address”** vnesite 00-11-22-33-44-AA.
5. Za dokončanje nastavitvev kliknite gumb **“Save”** (shrani).

Nato pojdite nazaj na stran nastavitvev gostitelja in videli boste spodnji seznam.

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

“TARGET”

Izberite meni **“Access Control → Target”** (nadzor dostopa → cilj) in na zaslonu lahko vidite in nastavite seznam ciljev, kot prikazuje slika 4 – 56. Seznam ciljev je potreben za pravilo nadzora dostopa.

Slika 4 – 56: Nastavitve cilja

- **“Target Description”** – tukaj je prikazan opis cilja in ta opis je unikatni.
- **“Information”** – cilj je lahko IP naslov, port ali ime domene.
- **“Modify”** – tukaj lahko spremenite ali izbrišete obstoječi vnos.

Za dodajanje novega vnosa sledite spodnjim korakom:

1. Kliknite gumb **“Add New...”** (dodaj nov...).
2. V polju **“Mode”** izberite IP naslov ali ime domene.
 - Če izberete **IP naslov**, se pokaže okno kot na sliki 4 – 74.
 - 1) V polje **“Target Description”** zapišite unikatni opis cilja (na primer Target_1).

- 2) V polje **“IP Address”** vnesite IP naslov cilja.
 - 3) Iz spustnega seznama **“Common Service Port”** izberite pogosto storitev, zato da se polje **Target Port** izpiše samodejno. Če na spustnem seznamu ni storitve, ki jo želite izbrati, **“Target Port”** ročno določite.
 - 4) V polju **“Protocol”** izberite TCP, UDP, ICMP ali All.
- Če izberete ime domene, se pokaže okno kot na sliki 4 – 58.
 - 1) V polje **“Target Description”** zapišite unikaten opis cilja (na primer Target_1).
 - 2) V polje **“Domain Name”** vnesite ime domene v celoti ali ključne besede (na primer google). Vsako ime domene, ki vsebuje ključne besede (www.google.com, www.google.com.hk) bo blokirano ali dovoljeno. Vnesete lahko 4 imena domen.
3. Kliknite gumb **“Save”** (shrani).
 Kliknite gumb **“Delete All”** in izbrišite vse vnose v tabeli.
 Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

Slika 4 – 57: Dodaj ali spremeni vnos cilja dostopa

Slika 4 – 58: Dodaj ali spremeni vnos cilja dostopa

Na primer: če želite omejiti internetne aktivnosti gostitelja z MAC naslovom 00-11-22-33-44-AA v LANu da dostopa le do www.google.com, najprej sledite spodnjim nastavitvam:

1. V oknu s slike 4 – 56 kliknite gumb **“Add New...”** in vstopite na stran za dodajanje ali spreminjanje vnosa cilja dostopa.
2. V polju **“Mode”** (način) iz spustnega seznama izberite ime domene.
3. V polje **“Target Description”** vpišite **unikaten** opis cilja (na primer Target_1).
4. V polje **“Domain Name”** vnesite www.google.com.
5. Za dokončanje nastavitvev kliknite gumb **“Save”** (shrani).

Nato pojdite nazaj na stran nastavitvev cilja in videli boste spodnji seznam.

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

“SCHEDULE”

Izberite meni **“Access Control → Schedule”** (nadzor dostopa → razpored) in na zaslonu lahko vidite in nastavite seznam razporedov, kot prikazuje slika 4 – 59. Seznam razporedov je potreben za pravilo nadzora dostopa.



ID	Schedule Description	Day	Time	Modify
Add New... Delete All				
Previous Next Current No. 1 Page				

Slika 4 – 59: Nastavitve razporeda

- **“Schedule Description”** – tukaj je prikazan opis razporeda in ta opis je unikatni.
- **“Day”** – tukaj je (so) naveden(i) dan v tednu (dnevi).
- **“Time”** – tukaj je navedeno časovno obdobje v dnevu.
- **“Modify”** – tukaj lahko spremenite ali izbrišete obstoječi vnos.

Za dodajanje novega razporeda sledite spodnjim korakom:

1. Kliknite gumb **“Add New...”** (dodaj nov...) v oknu s slike 4 – 59 in pojavi se novo okno, kot ga prikazuje slika 4 – 60.
2. V polje **“Schedule Description”** zapišite unikatni opis razporeda (na primer Schedule_1).
3. V polju **“Day”** izberite dan ali dneve, ki jih potrebujete.
4. V polju **“Time”** lahko izberete cel dan 24 ur ali pa lahko v ustrezna polja vnesete začetni in končni čas.
5. Za dokončanje nastavitvev kliknite gumb **“Save”** (shrani).

Kliknite gumb **“Delete All”** in izbrišite vse vnose v tabeli.

Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

Slika 4 – 60: Napredne nastavitve razporeda

Na primer: če želite omejiti internetne aktivnosti gostitelja z MAC naslovom 00-11-22-33-44-AA da dostopa do www.google.com le med **18:00 do 20:00** ob **sobotah** in **nedeljah**, najprej sledite spodnjim nastavitvam:

1. V oknu s slike 4 – 59 kliknite gumb **“Add New...”** in vstopite na stran naprednih nastavitvev razporeda.
2. V polje **“Schedule Description”** vpišite **unikaten** opis razporeda (na primer Schedule_1).
3. V polju **“Day”** označite **“Select Days”** (izberi dneve) in nato izberite **“Sat”** in **“Sun”**.
4. V polje **“Time”** vnesite **“Start Time”** (začetni čas) 1800 in **“Stop Time”** (končni čas) 2000.
5. Za dokončanje nastavitvev kliknite gumb **“Save”** (shrani).

Nato pojdite nazaj na stran nastavitvev razporeda in videli boste spodnji seznam.

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

4.12 NAPREDNO USMERJANJE

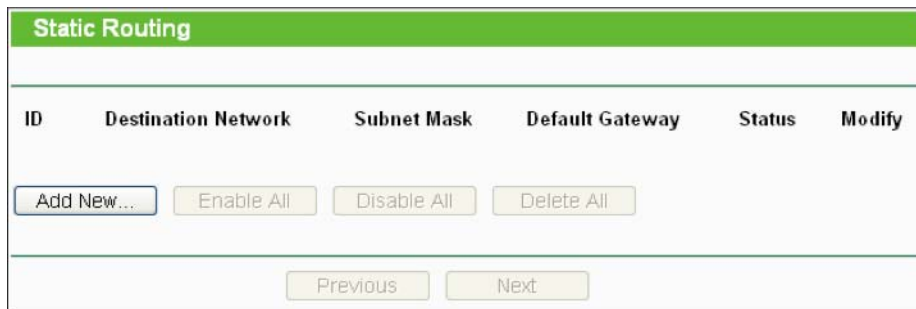


Slika 4 – 61: Meni naprednega usmerjanja

V meniju naprednega usmerjanja se nahajata dva podmenija (kot prikazuje slika 4 – 61): **statični seznam usmerjanja** in **tabela sistemskega usmerjanja**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije.

STATIČNO USMERJANJE

Izberite meni **“Advanced Routing → Static Routing”** (napredno usmerjanje → statično usmerjanje) in na naslednjem zaslону (kot ga prikazuje slika 4 – 62) lahko konfigurirate statično usmerjanje. Statična pot je predhodno določena pot, kamor mora potovati informacija omrežja da doseže specifičnega gostitelja ali omrežje.



Slika 4 – 62: Statično usmerjanje

Za dodajanje vnosov statičnega usmerjanja sledite spodnjim korakom:

1. Kliknite na gumb **“Add New...”** ki ga vidite na sliki 4 – 62 in pokaže se naslednje okno, kot ga prikazuje slika 4 – 63.



Slika 4 – 63: Dodaj ali spremeni vnos statičnega usmerjanja

2. Vnesite naslednje podatke:
 - **“Destination Network”** - destinacijsko omrežje je naslov omrežja ali gostitelja, ki ga želite določiti za statično usmerjanje.
 - **“Subnet Mask”** – Subnet Mask določa kateri del IP naslova je del omrežja in kateri je del gostitelja.
 - **“Default Gateway”** – to je IP naslov privzetega Gateway-a naprave, ki dopušča kontakt med usmerjevalnikom in omrežjem ali gostiteljem.
3. V spustnem seznamu **“Status”** za ta vnos izberite **“Enabled”** (omogoči) ali **“Disabled”** (onemogoči).
4. Za začetek veljavnosti vnosa kliknite gumb **“Save”** (shrani).

Kliknite gumb **“Delete”** in izbrišite ta vnos.

Kliknite gumb **“Enable All”** in omogočite delovanje vseh vnosov.

Kliknite gumb **“Disable All”** in onemogočite delovanje vseh vnosov.

Kliknite gumb **“Delete All”** in izbrišite vse vnose.

Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

TABELA SISTEMSKEGA USMERJANJA

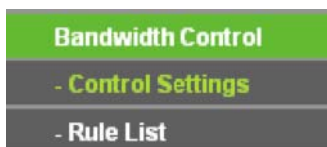
Izberite meni **“Advanced Routing → System Routing Table”** (napredno usmerjanje → tabela systemskega usmerjanja) in vidite lahko vse veljavne vnose smeri, ki so v uporabi. Za vsak vnos so prikazani destinacijski IP naslov, **“Subnet Mask”**, **“Gateway”** in vmesnik.

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	0.0.0.0	0.0.0.0	192.168.1.1	WAN

- **“Destination Network”** – destinacijsko omrežje je naslov omrežja ali gostitelja, kamor je dodeljena statična usmeritev.
- **“Subnet Mask”** – Subnet Mask določa kateri del IP naslova je del omrežja in kateri je del gostitelja.
- **“Gateway”** – to je IP naslov privzetega Gateway-a naprave, ki dopušča kontakt med usmerjevalnikom in omrežjem ali gostiteljem.
- **“Interface”** – ta vmesnik vam pove ali je destinacijski IP naslov na **LAN & WLAN**-u (notranje kabelsko in brezžično omrežje) ali na **WAN**-u (internet).

Za posodobitev prikazanih podatkov kliknite gumb **“Refresh”** (osveži).

4.13 NADZOR PASOVNE ŠIRINE



Slika 4 – 64

V meniju nadzora pasovne širine se nahajata dva podmenija (kot prikazuje slika 4 – 64). Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije. Podrobne informacije za vsak podmeni so navedene spodaj.

NASTAVITVE NADZORA

Izberite meni **“Bandwidth Control → Control Settings”** (nadzor pasovne širine → nastavitve nadzora) in na naslednji strani lahko konfigurirate **“egress”** pasovne širine in **“ingress”** pasovne širine. Njune vrednosti morajo biti nižje od 100000Kbps. Za optimalen nadzor pasovne širine izberite pravi tip linije in vašega ponudnika internetnih storitev povprašajte za skupno pasovno širino **“egress”** in **“ingress”**.

The image shows the 'Bandwidth Control Settings' configuration page. It has a green header. Below the header, there is a checkbox for 'Enable Bandwidth Control:'. Underneath, there is a 'Line Type:' section with two radio buttons: 'ADSL' (which is selected) and 'Other'. Below that, there are two input fields: 'Egress Bandwidth:' with the value '512' and 'Kbps' next to it, and 'Ingress Bandwidth:' with the value '2048' and 'Kbps' next to it. At the bottom of the form is a 'Save' button.

Slika 4 – 64: Nastavitve pasovne širine

- **“Enable Bandwidth Control”** – ta kvadrataček obkrožite, če želite, da začnejo veljati nastavitve pasovne širine.

- **“Line Type”** – izberite pravi tip vaše omrežne povezave. Če ne veste kaj izbrati, povprašajte vašega ponudnika internetnih storitev.
- **“Egress Bandwidth”** – hitrost nalaganja (“upload”) preko WAN porta.
- **“Ingress Bandwidth”** – hitrost prenosa (“download”) preko WAN porta.

SEZNAM PRAVIL

Izberite meni **“Bandwidth Control → Rules List”** (nadzor pasovne širine → seznam pravil) in na spodnjem prikazu lahko vidite in konfigurirate pravila pasovne širine.

ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							

Current No. 1 Page

Slika 4 – 66: Seznam pravil pasovne širine

- **“Description”** – to je informacija o pravilih kot je območje naslovov.
- **“Egress Bandwidth”** – v tem polju je prikazana največja in najmanjša pasovna širina nalaganja (“upload”) preko WAN porta. Privzeta vrednost je 0.
- **“Ingress Bandwidth”** – v tem polju je prikazana največja in najmanjša pasovna širina prenosa (“download”) preko WAN porta. Privzeta vrednost je 0.
- **“Enable”** – prikazuje status pravila (ali velja).
- **“Modify”** – za spreminjanje pravila kliknite ta gumb. S klikom na **“Delete”** pravilo izbrišete.

Za dodajanje/spreminjanje pravila nadzora pasovne širine, sledite spodnjim korakom:

Korak 1: Kliknite gumb **“Add New...”** kot prikazuje slika 4 – 66 in pokaže se okno kot na sliki 4 – 67.

Korak 2: Vnesite informacije kot na spodnji sliki.

Enable:

IP Range: -

Port Range: -

Protocol: All

Min Bandwidth(Kbps) **Max Bandwidth(Kbps)**

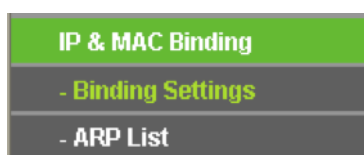
Egress Bandwidth:

Ingress Bandwidth:

Slika 4 – 67: Nastavitve pravila pasovne širine

Korak 3: Kliknite gumb **“Save”** (shrani).

4.14 IP & MAC ZAVEZJOČE NASTAVITVE



Slika 4 – 68: Meni IP&MAC zavezujočih nastavitvev

V meniju IP&MAC zavezujočih nastavitvev se nahajata dva podmenija (kot prikazuje slika 4 – 68): **zavezujoče nastavitve** in **ARP seznam**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije. Podrobne informacije za vsak podmeni so navedene spodaj.

ZAVEZUJOČE NASTAVITVE

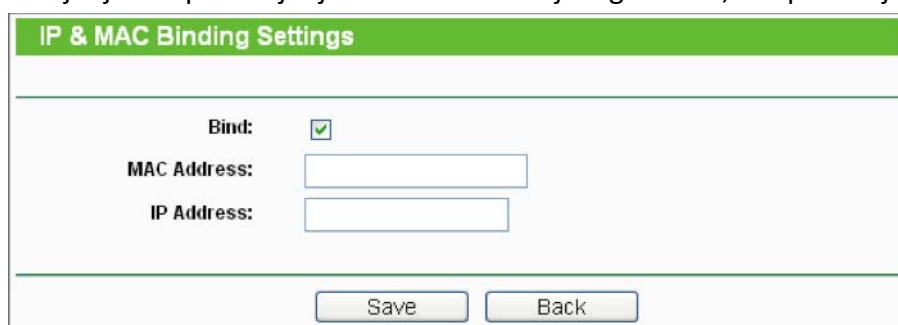
Ta stran prikazuje tabelo IP&MAC zavezujočih nastavitvev. Upravljate jo lahko skladno z vašimi željami kot prikazuje slika 4 – 69.



Slika 4 – 69: Zavezujoče nastavitve

- **“MAC Address”** – MAC naslov računalnika pod nadzorom v LAN.
- **“IP Address”** – Dodeljen IP naslov računalnika pod nadzorom v LAN.
- **“Bind”** – Obkljukajte to možnost in omogočite ARP zavezo za določeno napravo.
- **“Modify”** – spreminjanje ali izbris obstoječega vnosa.

Kadar želite dodati ali spremeniti IP&MAC zavezujoč vnos, lahko kliknete na gumb **“Add New...”** ali gumb **“Modify”** in odpre se naslednja stran. Ta je namenjena dodajanju ali spreminjanju IP&MAC zavezujočega vnosa, kot prikazuje slika 4 – 70.



Slika 4 – 70: IP&MAC zavezujoče nastavitve

Za dodajanje IP&MAC zavezujočih vnosov sledite spodnjim korakom:

1. Kliknite gumb **“Add New...”** kot prikazuje slika 4 – 69.
2. Vnesite MAC naslov in IP naslov.

3. Obkljukajte kvadrata "Bind".
4. Za shranjevanje kliknite na gumb "Save".

Za spreminjanje ali izbris obstoječega vnosa sledite spodnjim korakom:

1. V tabeli poiščite želeni vnos.
2. Po želji v stolpcu "Modify" kliknite na "Modify" (spremeni) ali "Delete" (izbriši).

Za iskanje obstoječega vnosa sledite spodnjim korakom:

1. Kliknite na gumb "Find" (poišči), kot prikazuje slika 4 – 69.
2. Vnesite MAC naslov ali IP naslov.
3. Kliknite na gumb "Find" kot prikazuje slika 4 – 71.

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

Slika 4 – 71: Poišči IP&MAC zavezujoč vnos

Kliknite gumb "Enable All" in omogočite delovanje vseh vnosov.
Kliknite gumb "Delete All" in izbrišite vse vnose.

ARP SEZNAM

Za upravljanje računalnika lahko opazujete računalnike v LAN tako, da preverjate povezavo MAC naslova in IP naslova na ARP seznamu. Lahko pa na ARP seznamu tudi konfigurirate elemente. Na tej strani je prikazan ARP seznam; prikazuje vse obstoječe IP&MAC zavezujoče vnose, kot je prikazano tudi na sliki 4 – 72.

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

Slika 4 – 72: ARP seznam

- "MAC Address" – MAC naslov računalnika pod nadzorom v LAN.
- "IP Address" – Dodeljen IP naslov računalnika pod nadzorom v LAN.
- "Status" – navaja ali sta MAC in IP naslov vezana.
- "Configure" – naloži ali izbriši element.
 - "Load" – naloži element na IP&MAC zavezujoč seznam.
 - "Delete" – izbriši element.

Kliknite gumb "Bind All" in vežite vse trenutne elemente, ki so na voljo po omogočanju delovanja.

Kliknite gumb "Load All" in naložite vse elemente na IP&MAC zavezujoč seznam.

Kliknite gumb "Refresh" in osvežite vse elemente.

Opomba:

Elementa na IP&MAC zavezujoč seznam ni mogoče dodati, če je bil IP naslov elementa prej že naložen. Pojavi se tudi sporočilo o napaki. prav tako ukaz "Load All" naloži le elemente brez vmešavanja v IP&MAC zavezujoč seznam.

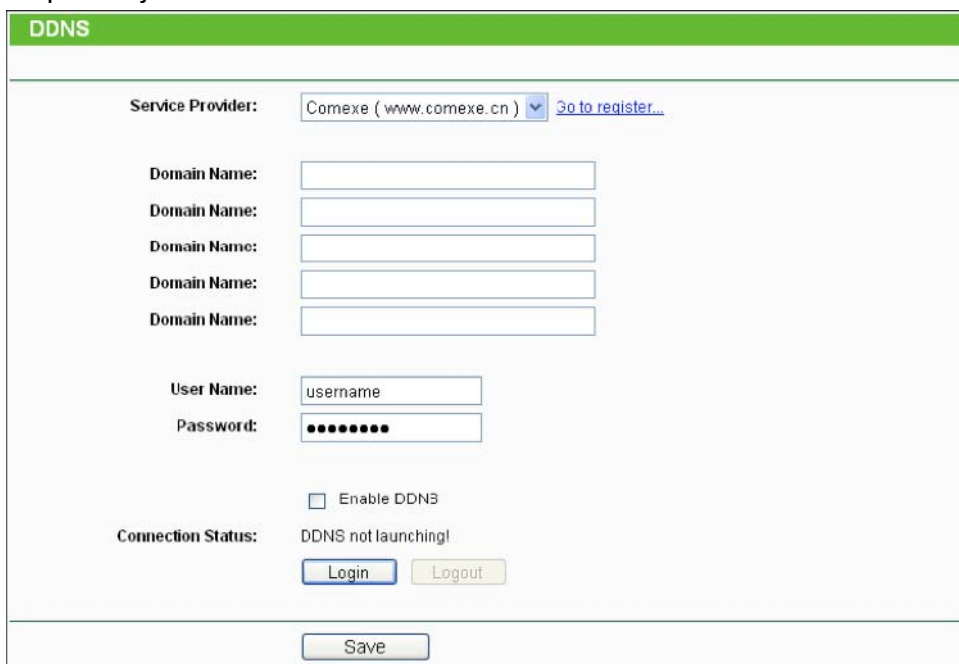
4.15 DINAMIČNI DNS

Izberite meni "**Dynamic DNS**", kjer lahko konfigurirate dinamično DNS funkcijo.

Usmerjevalnik omogoča delovanje **DDNS** (dinamičnega systemskega imena domene), ki omogoča gostovanje spletne strani, FTP strežnika ali strežnika s spletno pošto, ki ima določeno ime domene (imenovano po sebi) in dinamični IP naslov. Nato se lahko vaši prijatelji z vnosom imena vaše domene povežejo na vaš strežnik, ne glede na to kakšen je vaš IP naslov. Pred uporabo te funkcije se morate prijaviti za DDNS ponudnika storitev, kot je www.comexe.cn, www.dyndns.org ali www.no-ip.com. Ponudnik storitev dinamičnega DNS klienta vam bo posredoval geslo ali ključ.

Comexe.cn DDNS

Če je vaš izbrani **ponudnik storitev** dinamičnega DNS www.comexe.cn, se stran odpre kot prikazuje slika 4 – 73.



Slika 4 – 73: Nastavitve Comexe.cn DDNS

Za nastavitve DDNS sledite tem navodilom:

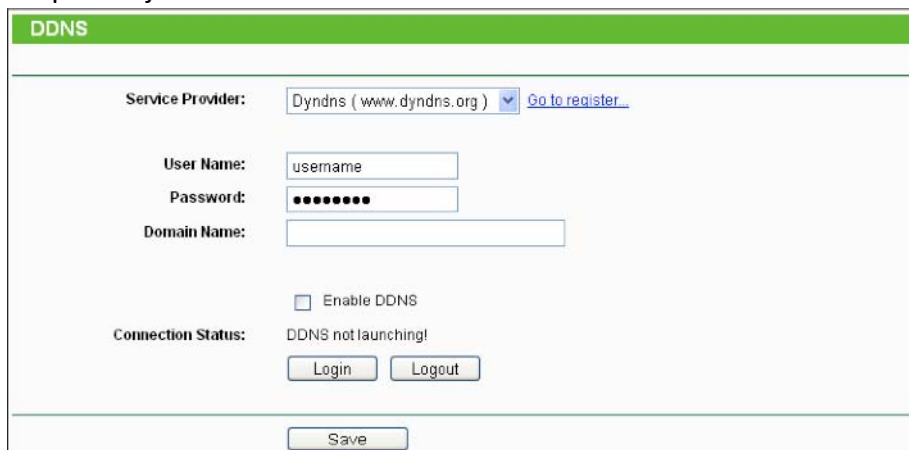
1. V polje pišite "**Domain Name**" vpišite ime domene, ki ste jo prejeli od ponudnika storitev dinamičnega DNS.
2. V polje "**User Name**" vpišite uporabniško ime za vaš DDNS račun.
3. V polje "**Password**" vpišite geslo za vaš DDNS račun.
4. Za prijavo v DDNS storitev kliknite gumb "**Login**".

"**Connection Status**" – tukaj je prikazan status povezave DDNS storitve.

Za odjavo iz DDNS storitve kliknite gumb "**Logout**".

Dyndns.org DDNS

Če je vaš izbrani **ponudnik storitev** dinamičnega DNS www.dyndns.org, se stran odpre kot prikazuje slika 4 – 74.



Slika 4 – 74: Nastavitve dyndns.org DDNS

Za nastavitve DDNS sledite tem navodilom:

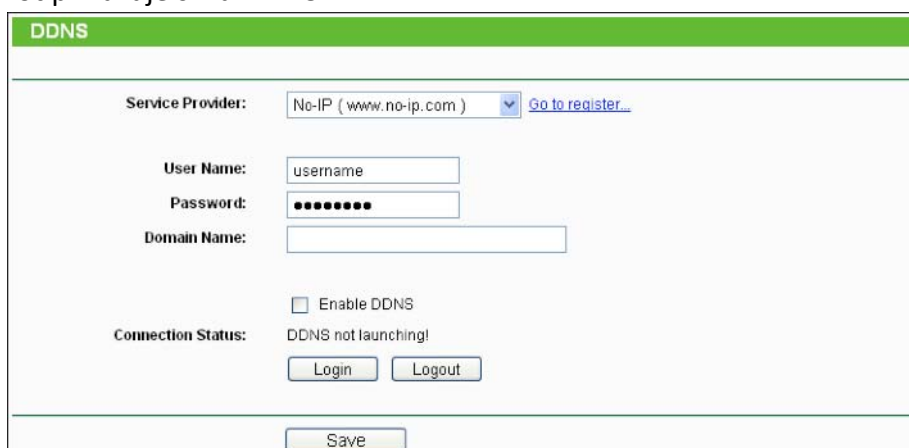
1. V polje “**User Name**” vpišite uporabniško ime za vaš DDNS račun.
2. V polje “**Password**” vpišite geslo za vaš DDNS račun.
3. V polje pišite “**Domain Name**” vpišite ime domene, ki ste jo prejeli od ponudnika storitev dinamičnega DNS.
4. Za prijavo v DDNS storitev kliknite gumb “**Login**”.

“**Connection Status**” – tukaj je prikazan status povezave DDNS storitve.

Za odjavo iz DDNS storitve kliknite gumb “**Logout**”.

No-ip.com DDNS

Če je vaš izbrani **ponudnik storitev** dinamičnega DNS www.no-ip.com, se stran odpre kot prikazuje slika 4 – 75.



Slika 4 – 75: Nastavitve no-ip.com DDNS

Za nastavitve DDNS sledite tem navodilom:

1. V polje “**User Name**” vpišite uporabniško ime za vaš DDNS račun.
2. V polje “**Password**” vpišite geslo za vaš DDNS račun.

3. V polje pišite **“Domain Name”** vpišite ime domene, ki ste jo prejeli od ponudnika storitev dinamičnega DNS.
 4. Za prijavo v DDNS storitev kliknite gumb **“Login”**.
- “Connection Status”** – tukaj je prikazan status povezave DDNS storitve.
Za odjavo iz DDNS storitve kliknite gumb **“Logout”**.

4.16 SISTEMSKA ORODJA



Slika 4 – 76: Meni sistemskih orodij

Izberite meni **“System Tools”** (sistemska orodja) in med podmeniji lahko vidite: **časovne nastavitve, diagnostiko, posodobitev programske opreme, privzete tovarniške nastavitve, varnostno kopijo & obnovitev, ponovni zagon naprave, geslo, sistemske prijave in statistiko**. Kliknite na kateregakoli in lahko boste konfigurirali njegove funkcije. Podrobne informacije za vsak podmeni so navedene spodaj.

ČASOVNE NASTAVITVE

Izberite meni **“System Tools → Time Settings”** (sistemska orodja → časovne nastavitve), kjer lahko v naslednjem oknu konfigurirate čas.

Slika 4 – 77: Časovne nastavitve

- **“Time Zone”** – Iz spustnega seznama izberite vaš lokalni časovni pas.
- **“Date”** – v ustrezna prazna polja vnesite lokalni datum v obliki MM/DD/LL.
- **“Time”** – v ustrezna prazna polja vnesite vaš lokalni čas v obliki HH/MM/SS.
- **“NTP Server 1 / NTP Server 2”** – vnesite naslov ali domeno **NTP strežnika 1** ali **NTP strežnika 2** in usmerjevalnik bo prednostno dobil čas z NTP strežnika. Dodatno ima usmerjevalnik vgrajen nekakšen pogost NTP strežnik, da lahko ob povezavi na internet samodejno pridobi podatke o času.
- **“Enable Daylight Saving”** – označite kvadratik in omogočite delovanje funkcije poletnega časa.
- **“Start”** – začetek poletnega časa. V prvem kvadratu izberite mesec, v drugem kvadratu izberite teden, v tretjem kvadratu izberite dan in v zadnjem kvadratu izberite čas.
- **“End”** – konec poletnega časa. V prvem kvadratu izberite mesec, v drugem kvadratu izberite teden, v tretjem kvadratu izberite dan in v zadnjem kvadratu izberite čas.
- **“Daylight Saving Status”** – prikazuje ali je v uporabi poletni čas.

Ročna nastavitve časa:

1. Izberite lokalni časovni pas.
2. V obliki mesec/dan/leto vnesite **datum**.
3. V obliki ura/minuta/sekunda vnesite **čas**.
4. Kliknite gumb **“Save”** (shrani).

Avtomatska nastavitve časa:

1. Izberite lokalni časovni pas.
2. Vnesite ime domene ali **NTP strežnika 1** ali **NTP strežnika 2**.
3. Kliknite na gumb **“Get GMT”** in sistemski čas pridobite z interneta, če ste nanj povezani.

Nastavitve poletnega časa:

1. Označite kvadratik in omogočite poletni čas.
2. V polju **“Start”** iz spustnega seznama izberite čas začetka.
3. V polju **“End”** iz spustnega seznama izberite čas konca.
4. Za shranjevanje nastavitve kliknite gumb **“Save”**.

	<input checked="" type="checkbox"/> Enable Daylight Saving
Start:	Mar ▾ 3rd ▾ Sun ▾ 2am ▾
End:	Nov ▾ 2nd ▾ Sun ▾ 3am ▾
Daylight Saving Status:	daylight saving is down.
<p style="font-size: small;">Ncte: 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.</p>	



Opomba:

1. Nastavitve se uporabljajo za nekatere funkcije, ki temeljijo na času – na primer požarni zid. Pri uspešni prijavi na usmerjevalnik morate določiti vaš časovni pas, sicer te funkcije ne začnejo veljati.

2. Če usmerjevalnik izklopite, se nastavitev časa izbriše.
3. Če je tako nastavljen, usmerjevalnik GMT samodejno pridobi na internetu.
4. Poletni čas začne delovati eno minuto po zaključeni konfiguraciji.

DIAGNOSTIKA

Izberite meni **“System Tools → Diagnostics”** (sistemska orodja → diagnostika), kjer lahko v naslednjem oknu označite funkcijo **“Ping”** ali **“Traceroute”** in tako preverite povezljivost vašega omrežja.

Slika 4 – 78: Orodja diagnostike

- **“Diagnostic Tool”** – označite gumb in tako izberite eno diagnostično orodje.
 - **“Ping”** – to orodje diagnostike odpravlja težave s povezljivostjo, dosegljivostjo in ločljivostjo imena za danega gostitelja ali **“gateway”**.
 - **“Traceroute”** – to orodje diagnostike preverja delovanje povezave.



Opomba:

“Ping/traceroute” lahko uporabite za testiranje tako IP naslova kot imena domene. Če je “pinganje/traceroutanje” IP naslova uspešno, imena domene pa neuspešno, imate verjetno težavo z ločljivostjo imena. V takem primeru zagotovite, da je ime domene ki jo navajate lahko rešeno z uporabo poizvedb DNS (sistemskega imena domen).

- **“IP Address/Domain Name”** – vnesite destinacijski IP naslov (kot na primer 192.168.0.1) ali ime domene (na primer <http://www-tp-link.com>).
- **“Pings Count”** – število “Ping” paketov za “Ping” povezavo.
- **“Ping Packet Size”** – velikost “Ping” paketa.
- **“Ping Timeout”** – nastavite časa čakanja na odgovor vsakega “Ping” paketa. Če odgovora ni v določenem času, je povezava pretečena.
- **“Traceroute Max TTL”** – največje število obročev za “Traceroute” povezavo.

Kliknite gumb **“Start”** in preverite povezljivost interneta.

Stran **“Diagnostic Results”** prikazuje rezultate diagnostike.

Če so rezultati podobni prikazom na spodnji sliki, je povezljivost interneta dobra.

```
Diagnostic Results
-----
Pinging 192.168.0.1 with 64 bytes of data:

Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4

Ping statistics for 192.168.0.1
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
  Minimum = 1, Maximum = 1, Average = 1
```

Slika 4 – 79: Rezultati diagnostike

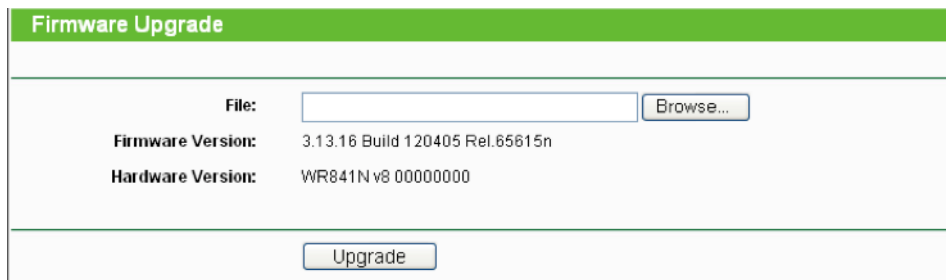


Opomba:

Le en uporabnik naenkrat lahko uporablja to orodje. Možnosti “Number of Pings”, “Ping Size” in “Ping Timeout” se uporabljajo za funkcijo “Ping”. Možnost “Tracert Hops” pa se uporablja za funkcijo “Traceroute”.

POSODOBITEV PROGRAMSKE OPREME

Izberite meni “System Tools → Firmware Upgrade” (sistemska orodja → posodobitev programske opreme), kjer lahko v spodnjem oknu posodobite programsko opremo usmerjevalnika na zadnjo verzijo.



Slika 4 – 80: Posodobitev programske opreme

- “Firmware Version” – tukaj je prikazana trenutna verzija programske opreme.
- “Hardware Version” – tukaj je prikazana trenutna verzija strojne opreme. Verzija posodobitve strojne opreme mora biti skladna s trenutno verzijo strojne opreme usmerjevalnika.

Za posodobitev programske opreme usmerjevalnika sledite spodnjim navodilom:

1. S spletne strani TP-LINK prenesite najnovejšo datoteko posodobitve (<http://www.tp-link.com>).
2. V polje “Field” vnesite pot in ime datoteke posodobitve. Ali pa kliknite na gumb “Browse” (prebrskaj) in poiščite datoteko posodobitve.
3. Kliknite gumb “Upgrade” (posodobi).



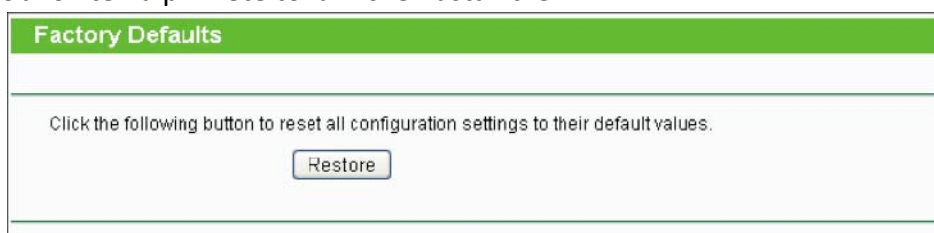
Opomba:

- 1) Nove verzije programske opreme se nahajajo na <http://www.tp-link.com> od kjer jih lahko prenesete brezplačno. Posodobitev programske opreme ni potrebna, razen če je v novi verziji funkcija, ki jo želite uporabljati. Kadar pa naletite na težave, ki jih povzroča usmerjevalnik in ne njegova konfiguracij, lahko poizkusite s posodobitvijo programske opreme.

- 2) Kadar posodabljate programsko opremo usmerjevalnika, lahko pride do izgube trenutnih konfiguracij, zato si pred posodobitvijo izpišite vaše nastavitve po meri in se tako izognite izgubi pomembnih nastavitvev.
- 3) Med samim postopkom posodobitve programske opreme usmerjevalnika ne izklopite in tudi ne pritisnite gumba "Reset", ker lahko pride do okvare usmerjevalnika.
- 4) Po zaključeni posodobitvi se usmerjevalnik samodejno ponovno zažene.

PRIVZETE TOVARNIŠKE NASTAVITVE

Izberite meni "**System Tools → Factory Defaults**" (sistemska orodja → privzete tovarniške nastavitve), kjer lahko v spodnjem oknu konfiguracije usmerjevalnika obnovite na privzete tovarniške nastavitve.



Slika 4 – 81: Obnovitev privzetih tovarniških nastavitvev

Kliknite gumb "**Restore**" in vse nastavitve konfiguracij povrnite na privzete tovarniške vrednosti.

- Privzeta nastavitvev "**User Name**" (uporabniško ime): admin
- Privzeta nastavitvev "**Password**" (geslo): admin
- Privzeta nastavitvev "**IP Address**" (IP naslov): 192.168.0.1
- Privzeta nastavitvev "**Subnet Mask**": 255.255.255.0



Opomba:

Ko se ponastavijo privzete tovarniške nastavitve, izgubite vse do tedaj shranjene nastavitve.

VARNOSTNA KOPIJA & OBNOVITEV

Izberite meni "**System Tools → Backup & Restore**" (sistemska orodja → varnostna kopija & obnovitev), kjer lahko kot varnostno kopijo shranite trenutno konfiguracijo usmerjevalnika in s pomočjo datoteke varnostne kopije obnovite konfiguracijo, kot je prikazano na sliki 4 – 82.



Slika 4 – 82: Konfiguracija varnostne kopije in obnovitve

- Za shranjevanje vseh nastavitvev konfiguracije v obliki varnostne kopije na lokalnem računalniku, kliknite gumb "**Backup**".
- Za posodobitev konfiguracij usmerjevalnika sledite tem navodilom:
 - Kliknite gumb "**Browse**" in poiščite datoteko posodobitve za usmerjevalnik ali pa v prazno polje vneste točno pot do datoteke nastavitvev.
 - Kliknite gumb "**Restore**".

Opomba:

Trenutno konfiguracijo pokriva prenešana datoteka konfiguracije. Postopek posodobitve traja 20 sekund in usmerjevalnik se nato samodejno ponovno zažene. V izogib poškodbam mora biti usmerjevalnik med postopkom posodobitve vklopljen.

PONOVNI ZAGON NAPRAVE

Izberite meni **“System Tools → Reboot”** (sistemska orodja → ponovni zagon naprave), kjer lahko v naslednjem oknu kliknete na gumb **“Reboot”** in ponovno zaženete usmerjevalnik.



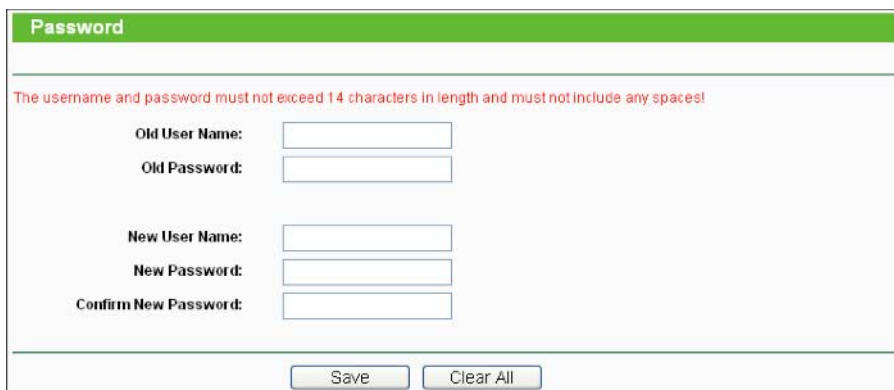
Slika 4 – 83: Ponovni zagon usmerjevalnika

Nekatere nastavitve usmerjevalnika začnejo veljati šele po ponovnem zagonu. To so:

- Sprememba LAN IP naslova (sistem se samodejno ponovno zažene).
- Sprememba DHCP nastavitvev.
- Sprememba brezžične konfiguracije.
- Sprememba porta za spletno upravljanje.
- Posodobitev programske opreme usmerjevalnika (sistem se samodejno ponovno zažene).
- Obnovitev nastavitvev usmerjevalnika na privzete tovarniške nastavitve (sistem se samodejno ponovno zažene).
- Posodobitev konfiguracije z datoteko (sistem se samodejno ponovno zažene).

GESLO

Izberite meni **“System Tools → Password”** (sistemska orodja → geslo), kjer lahko v naslednjem oknu spremenite privzeto uporabniško ime in geslo usmerjevalnika (kot prikazuje slika 4 – 84).



Slika 4 – 84: Geslo

Zelo je priporočljivo zamenjati privzeto uporabniško ime in geslo usmerjevalnika, ker bodo vsi uporabniki, ki bodo želeli dostopati do spletnih orodij usmerjevalnika ali hitre nastavitve pozvani, da vnesejo privzeto uporabniško ime in geslo.

 **Opomba:**

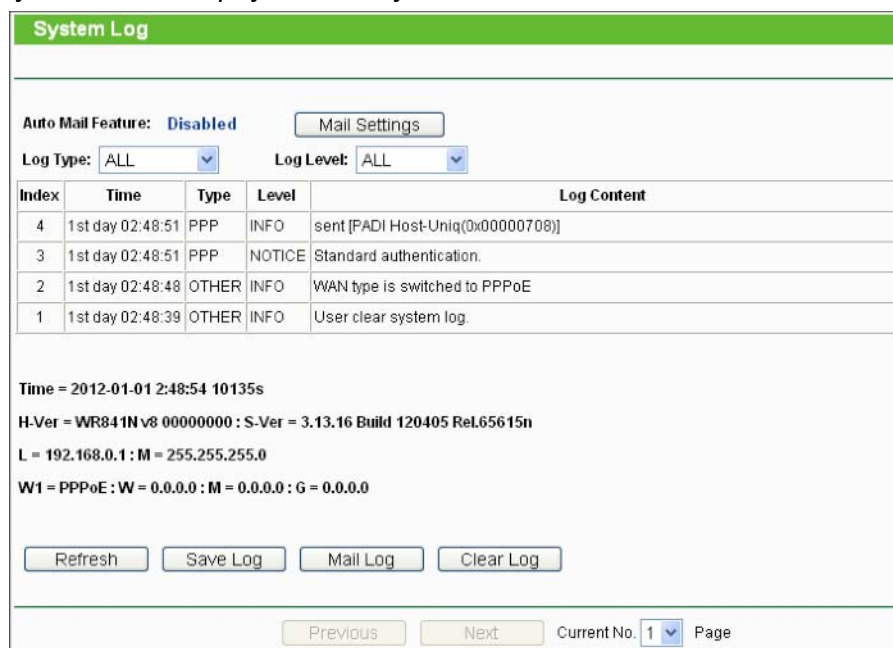
Novo uporabniško ime in geslo ne smeta biti daljša od 14 znakov in ne smeta imeti presledkov. Za potrditev geslo vnesite dvakrat.

Ko končate kliknite gumb **“Save”** (shrani).

Za izbris vsega kliknite gumb **“Clear All”**.

SISTEMSKE PRIJAVE

Izberite meni **“System Tools → System Log”** (sistemska orodja → sistemske prijave), kjer lahko vidite prijave usmerjevalnika.



Index	Time	Type	Level	Log Content
4	1st day 02:48:51	PPP	INFO	sent [FADI Host-Uniq(0x00000708)]
3	1st day 02:48:51	PPP	NOTICE	Standard authentication.
2	1st day 02:48:48	OTHER	INFO	WAN type is switched to PPPoE
1	1st day 02:48:39	OTHER	INFO	User clear system log.

Time = 2012-01-01 2:48:54 10135s
H-Ver = WR841N v8 00000000 : S-Ver = 3.13.16 Build 120405 Rel.65615n
L = 192.168.0.1 : 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

Slika 4 – 85: Sistemske prijave

- **“Auto Mail Feature”** – označuje ali je funkcija samodejne pošte omogočena ali ne.
- **“Mail Settings”** – nastavite naslov poštnega predala za sprejemanje in pošiljanje pošte, naslov strežnika, informacijo potrditve in tudi urnik za funkcijo samodejne pošte, kot prikazuje slika 4 – 86.

Slika 4 – 86: Nastavitve poštnega računa

- **“From”** – naslov vašega poštnega predala. Usmerjevalnik se vanj poveže za pošiljanje prijav.
- **“To”** – naslov prejemnika. Destinacijski poštni predal, kjer se sprejemajo prijave.
- **“SMTP Server”** – vaš SMTP strežnik. Ustreza poštnemu predalu vpisanem v polju “From”. Če niste prepričani v naslov se lahko prijavite na spletno stran pomoči.
- **“Authentication”** – Večina SMTP strežnikov zahteva preverjanje pristnosti. Potrebno je pri večini poštnih predalov, ki za prijavo potrebujejo uporabniško ime in geslo.



Opomba:

Šele ko izberete **“Authentication”**, morat v naslednja polja vnesti uporabniško ime in geslo.

- **“User Name”** – ime vašega poštnega računa, ki je naveden v polju “From”. Del za @ je izključen.
- **“Password”** – geslo vašega poštnega računa.
- **“Confirm the Password”** – za potrditev še enkrat vnesite geslo.
- **“Enable Auto Mail Feature”** – izberite za samodejno pošiljanje prijav. Trenutne prijave lahko pošiljate vsak dan ob določenem času ali v intervalih, vendar velja le eno pravilo od obeh. Vnesite želeni čas ali intervale v pripadajoče polje, kot prikazuje slika 4 – 86.

Kliknite gumb **“Save”** in shranite nastavitve.

Kliknite gumb **“Back”** za povratek na prejšnjo stran.

- **“Log Type”** – z izbiro tipa prijave, bodo prikazane le prijave tega tipa.
- **“Log Level”** – z izbiro stopnje prijave, bodo prikazane le prijave te stopnje.
- **“Refresh”** – osvežite stran, da se prikaže zadnji seznam prijav.
- **“Save Log”** – kliknite in vse prijave shranite v obliki txt datoteke.
- **“Mail Log”** – kliknite če želite ročno poslati elektronsko sporočilo trenutnih prijav skladno z naslovom in potrditvenimi informacijami v nastavitvah pošte.
- **“Clear Log”** – vse prijave bodo za vedno izbrisane iz usmerjevalnika, ne le s strani.

Kliknite gumb **“Next”**, če želite iti na naslednjo stran in gumb **“Previous”**, če želite iti na prejšnjo stran.

STATISTIKA

Izberite meni **“System Tools → Statistics”** (sistemska orodja → statistika), kjer lahko vidite statistiko usmerjevalnika, vključno s celotnim prometom in vrednostjo zadnjega intervala statistike paketov v sekundah.

Slika 4 – 87: Statistika

- **“Current Statistics Status”** – omogoči ali onemogoči status trenutne statistike. Privzeta nastavitev je onemogoči. Za omogočanje kliknite gumb **“Enable”**. Če je onemogočena, je onemogočena tudi funkcija DoS zaščite v varnostnih nastavitvah.
- **“Packet Statistics Interval (5-60)”** – privzeta nastavitev je 10. Iz spustnega seznama izberite vrednost med 5 in 60 sekundami. Interval statistike paketov označuje časovni del statistike paketov.
- **“Sorted Rules”** – izberite kako so sortirane prikazane statistike.

Za samodejno osveževanje označite kvadratke **“Auto-refresh”**.

Za takojšnje osveževanje kliknite gumb **“Refresh”**.

Kliknite gumb **“Reset All”** in vrednosti vseh vnosov ponastavite na nič.

Kliknite gumb **“Delete All”** in izbrišite vse vnose v tabeli.

Tabela statistik:

IP/MAC naslov		S povezano statistiko sta prikazana IP in MAC naslov.
Skupaj	Paketi	Skupno število paketov, ki jih prejme in posreduje usmerjevalnik.
	Byti	Skupno število Bytov, ki jih prejme in posreduje usmerjevalnik.
Trenutno	Paketi	Skupno število prejetih in posredovanih paketov v zadnjem sekundnem intervalu statistike paketov.
	Byti	Skupno število prejetih in posredovanih Bytov zadnjem sekundnem intervalu statistike paketov.
	ICMP Tx	Število ICMP paketov posredovanih na Wan na sekundo pri določenem intervalu statistike paketov. Prikazan je kot “curent transmitting rate/Max transmitting rate” (trenutna

		stopnja posredovanja/največja stopnja posredovanja).
	UDP Tx	Število UDP paketov posredovanih na Wan na sekundo pri določenem intervalu statistike paketov. Prikazan je kot "curent transmitting rate/Max transmitting rate" (trenutna stopnja posredovanja/največja stopnja posredovanja).
	TCP SYN Tx	Število TCP SYN paketov posredovanih na Wan na sekundo pri določenem intervalu statistike paketov. Prikazan je kot "curent transmitting rate/Max transmitting rate" (trenutna stopnja posredovanja/največja stopnja posredovanja).
Spremeni	Ponastavi	Ponastavi vrednost vnosa na nič.
	Izbriši	Izbriši obstoječ vnos iz tabele.

Na vsaki strani je 5 vnosov. Kliknite gumb **"Previous"** in se vrnite na prejšnjo stran ali **"Next"** in pojdite na naslednjo stran.

DODATEK A: POGOSTO ZASTAVLJENA VPRAŠANJA

1. Kako konfiguriram usmerjevalnik za dostop ADSL uporabnikov do interneta?

- 1) Najprej konfigurirajte ADSL modem konfiguriran v RFC1483 premostitvenem modelu.
- 2) Ethernet kabel z vašega ADSL modema povežite na WAN port usmerjevalnika. Telefonski kabel vstavite v Line port ADSL modema.
- 3) Prijavite se v usmerjevalnik, kliknite meni **"Network"** na levi strani brskalnika in kliknite podmeni **"WAN"**. V oknu **"WAN"** izberite **"PPPoE"** za WAN tip povezave. V polje **"User Name"** vnesite uporabniško ime, v polje **"Password"** pa geslo in zaključite s klikom na gumb **"Connect"** (poveži).

The screenshot shows a configuration window for WAN Connection Type. The 'WAN Connection Type' dropdown is set to 'PPPoE/Russia PPPoE' with a 'Detect' button next to it. Below this, the 'PPPoE Connection' section contains a 'User Name' field with the text 'username' and a 'Password' field with masked characters (dots).

Slika A – 1: Tip povezave PPPoE

- 4) Če imate ADSL zakup glede na količino porabljenih minut, za način povezave na internet izberite **"Connect on Demand"** ali **"Connect Manually"** (povezava na zahtevo ali ročna povezava). V izogib zapravljanju plačanega časa v **"Max Idle Time"** (najdaljši čas mirovanja) vnesite ustrezno količino minut. Sicer pa lahko za način povezave na internet izberete **"Auto-Connecting"** (samodejno povezovanje).

Slika A – 2: Način povezave PPPoE



Opomba:

- 1) Včasih povezave ni mogoče prekiniti kljub temu, da je določen najdaljši čas mirovanja, ker se nekatere aplikacije v ozadju vseskozi povezujejo na internet.
- 2) Če ste kabelski uporabnik, usmerjevalnik konfigurirajte skladno z zgornjimi koraki.

2. Kako konfiguriram usmerjevalnik za dostop Ethernet uporabnikov do interneta?

- 1) Prijavite se v usmerjevalnik, kliknite meni **“Network”** na levi strani brskalnika in kliknite podmeni **“WAN”**. V oknu **“WAN”** izberite **“Dynamic IP”** za WAN tip povezave. Zaključite s klikom na gumb **“Save”**.
- 2) Nekateri ponudniki internetnih storitev zahtevajo, da registrirate MAC naslov vašega adapterja, ki je med namestitvijo povezan na vaš kabelski/DSL modem. Če vaš ponudnik internetnih storitev zahteva, da registrirate MAC naslov, se prijavite v usmerjevalnik in v meniju na levi kliknite na **“Network”** in nato v podmeni **“MAC Clone”**. Če je MAC naslov vašega računalnika pravi, na strani **“MAC Clone”** kliknite na gumb **“Clone MAC Address”** in MAC naslov vašega računalnika se prenese v polje **“WAN MAC Address”**. Drugače pa v to isto polje MAC naslov vnesite ročno. Oblika MAC naslova je XX-XX-XX-XX-XX-XX. Nato kliknite gumb **“Save”** (shrani). Nastavitve začne veljati po ponovnem zagonu usmerjevalnika.

Slika A – 3: MAC klon

3. Želim uporabljati “NetMeeting”, kaj moram narediti?

- 1) Če **“NetMeeting”** začnete kot sponzor, z usmerjevalnikom ni potrebno narediti ničesar.
- 2) Če pa začnete z odgovorom, pa je potrebno konfigurirati virtualni strežnik ali DMZ gostitelja ter poskrbeti, da je H323 ALG omogočen.
- 3) Kako konfigurirati virtualni strežnik: prijavite se na usmerjevalnik, kliknite na meni **“Forwarding”** na levi strani in na podmeni **“Virtual Servers”**. Na strani **“Virtual Servers”** kliknite **“Add New...”**, na naslednji strani **“Add or Modify a Virtual Server Entry”** v prazno polje **“Service Port”** vnesite **“11130”** in v prazno polje **“IP Address”** vnesite vaš IP naslov (na primer 192.168.0.198) in ne pozabite klikniti na **“Enable”** (omogoči) in **“Save”**(shrani).

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

Slika A – 4: Virtualni strežniki

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text" value="11130"/> (XX-XX or XX)
Internal Port:	<input type="text" value="11120"/> (XX, Only valid for single Service Port or leave it blank)
IP Address:	<input type="text" value="192.168.0.198"/>
Protocol:	<input type="text" value="ALL"/>
Status:	<input type="text" value="Enabled"/>
Common Service Port:	<input type="text" value="--Select One--"/>

Slika A – 5: Dodaj ali spremeni vnos virtualnega strežnika



Opomba:

Vaša nasprotna stran mora klicati vaš WAN IP, ki je prikazan na "Statusni" strani.

- 4) Kako omogočiti DMZ gostitelja: prijavite se na usmerjevalnik, kliknite na meni "Forwarding" na levi strani in na podmeni "DMZ". Na "DMZ" strani označite "Enable" in v polje "DMZ Host IP Address" vnesite vaš IP naslov (na primer 192.168.0.198) in ne pozabite klikniti na gumb "Save" (shrani).

DMZ	
Current DMZ Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DMZ Host IP Address:	<input type="text" value="192.168.0.198"/>

Slika A – 6: DMZ

- 5) Kako omogočiti H323 ALG: prijavite se na usmerjevalnik, kliknite na meni "Security" na levi strani in na podmeni "Basic Security". Na strani osnovne zaščite poleg H323ALG označite gumb "Enable". Ne pozabite klikniti na gumb "Save" (shrani).

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
RTSP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

Slika A – 7: Osnovna zaščita

4. Na LAN želim postaviti spletni strežnik, kaj moram narediti?

- 1) Ker port 80 WEB strežnika moti port 80 WEB upravljanja na usmerjevalniku, je v izogib motnjam potrebno spremeniti številko porta za WEB upravljanje.
- 2) Spreminjanje številke porta za WEB upravljanje: prijavite se na usmerjevalnik, kliknite na meni **“Security“** na levi strani in na podmeni **“Remote Management“**. Na strani upravljanja na daljavo, v polje **“Web Management Port“** vnesite številko porta različno od 80, na primer 88. Kliknite gumb **“Save“** in ponovno zaženite usmerjevalnik.

Remote Management	
Web Management Port:	<input type="text" value="88"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all)
<input type="button" value="Save"/>	

Slika A – 8: Upravljanje na daljavo



Opomba:

Če začne veljati zgornja konfiguracija, za konfiguracijo usmerjevalnika v naslovno polje spletnega brskalnika vnesite 192.168.0.1:88 (LAN IP naslov usmerjevalnika: Web port upravljanja).

- 3) Prijavite se na usmerjevalnik, kliknite na meni **“Forwarding“** na levi strani in na podmeni **“Virtual Servers“**. Na strani **“Virtual Servers“** kliknite **“Add New...“**, na naslednji strani **“Add or Modify a Virtual Server“** v prazno polje **“Service Port“** vnesite **“80“** in v prazno polje **“IP Address“** vnesite vaš IP naslov (na primer 192.168.0.188) in ne pozabite klikniti na **“Enable“** (omogoči) in **“Save“** (shrani).

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

Slika A – 9: Virtualni strežniki

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:	--Select One--

Slika A – 10: Dodaj ali spremeni vnos virtualnega strežnika

5. Brezžične postaje se ne morejo povezati na usmerjevalnik.

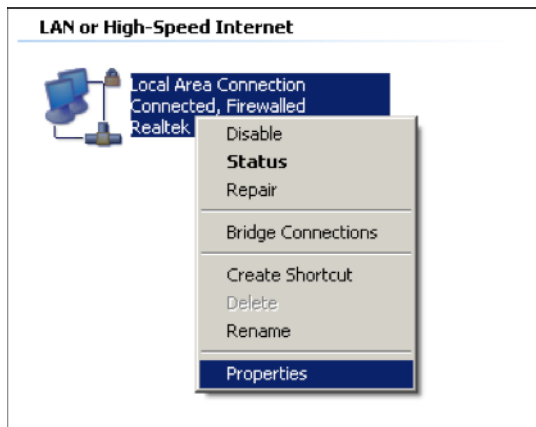
- 1) Prepričajte se, da je označen kvadrček **“Enable Wireless Router Radio”**.
- 2) Prepričajte se, da je SSID brezžičnih postaj skladen s SSID usmerjevalnika.
- 3) Prepričajte se, da imajo brezžične postaje pravi **“KEY”** (ključ) za šifriranje, ko je usmerjevalnik šifriran.
- 4) Če je brezžična povezava pripravljena, vendar pa ne morete dostopati do usmerjevalnika, preverite IP naslov vaših brezžičnih postaj.

DODATEK B: KONFIGURACIJA RAČUNALNIKA

V tem poglavju je navedeno, kako namestiti in pravilno konfigurirati TCP/IP v Windows XP. Najprej preverite ali deluje vaš Ethernet adapter in se po potrebi obrnite na navodila za uporabo adapterja.

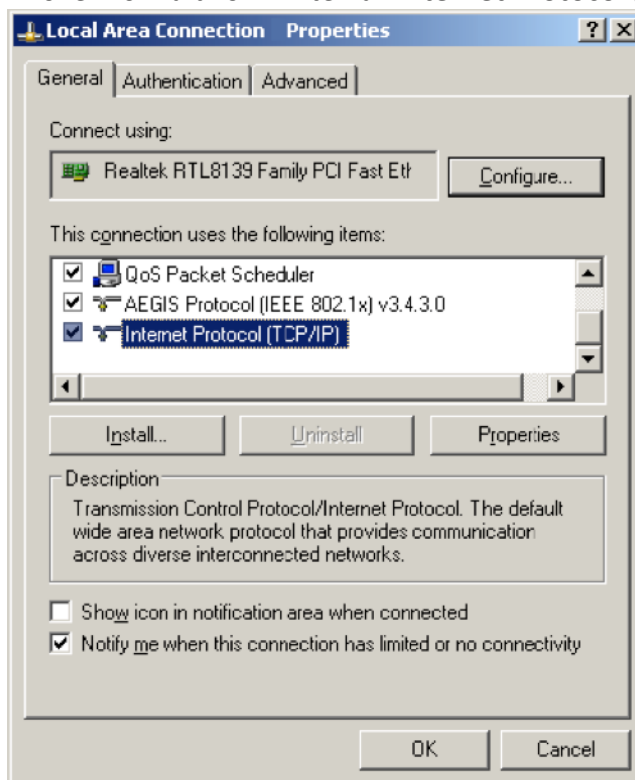
1. Konfiguracija komponente TCP/IP

- 1) V opravilni vrstici Windows, kliknite **“Start”** in nato **“Control Panel”** (nadzorna plošča).
- 2) Kliknite ikono **“Network and Internet Connections”** (omrežne in internetne povezave) in nato v pojavnem oknu kliknite zavihek **“Connections”** (povezave).
- 3) Z desno miškino tipko kliknite na ikono kot je prikazano na sliki in izberite **“Properties”** (lastnosti).



Slika B – 1

- 4) V novem oknu dvokliknite na **“Internet Protocol (TCP/IP)”** (inernetni protokol).



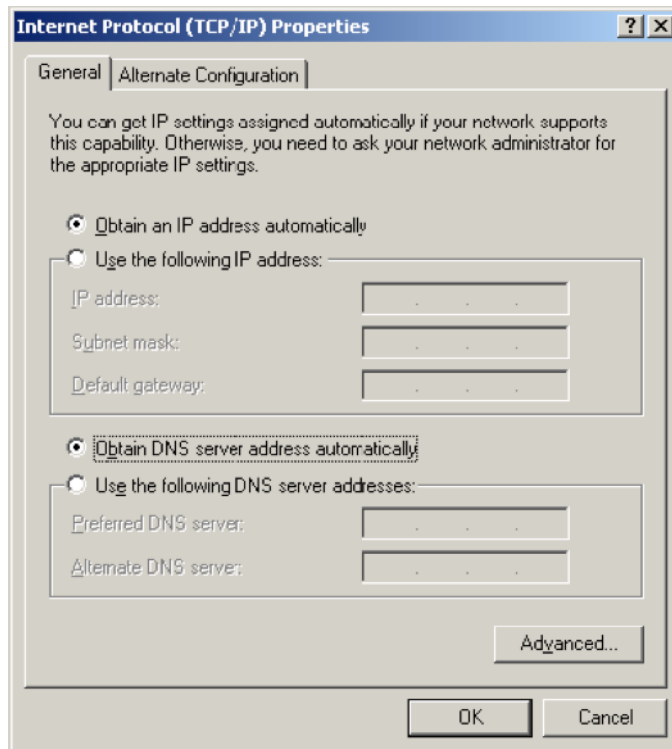
Slika B – 2

- 5) Odpre se naslednje okno za **“TCP/IP Properties”** (TCP/IP lastnosti) in tukaj je po privzeti nastavitvi odprt zavihek **“IP Address”**.

Sedaj imate za konfiguracijo **TCP/IP** protokola dve možnosti:

➤ **Samodejna nastavitvev IP naslova**

Kot je prikazano na spodnji sliki izberite **“Select an IP address automatically”** in **“Obtain DNS server automatically”**:



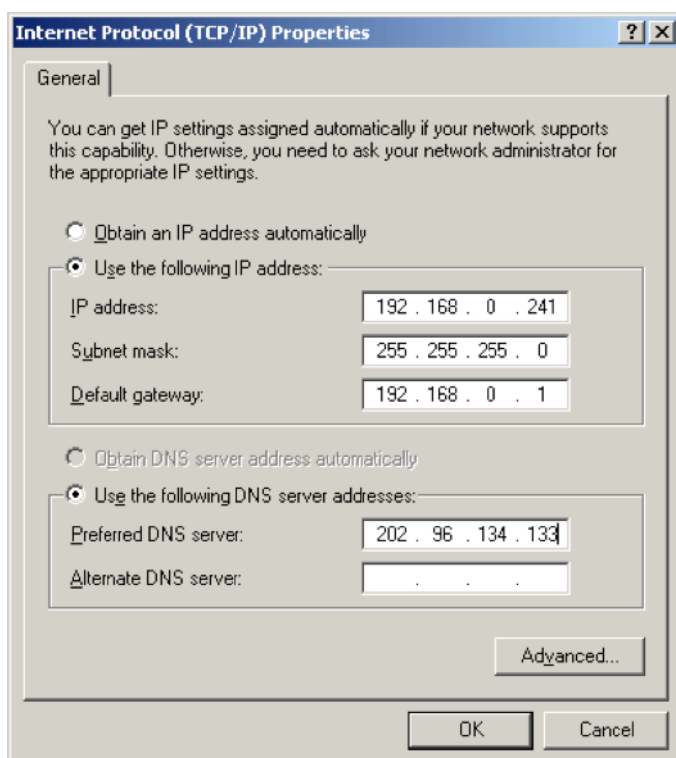
Slika B – 3

 **Opomba:**

Pri operacijskih sistemih Windows 98 ali starejših, je morda potrebno sedaj računalnik in usmerjevalnik ponovno zagnati.

➤ **Ročna nastavitve IP naslova**

- 1 Označite gumb **“Use the following IP address”**. Na voljo so naslednji elementi.
- 2 Če je LAN IP naslov usmerjevalnika 192.168.0.1, **IP address** določite kot 192.168.0.x (x je vrednost med 2 in 254), **“Subnet Mask”** pa je 255.255.255.0.
- 3 V polje **“Default gateway”** vnesite LAN IP naslov usmerjevalnika (privzet je 192.168.0.1).
- 4 Izberite **“Use the following DNS server addresses**. V polje **“Preferred DNS Server”** lahko vnesete enako vrednost kot za **“Default gateway”** ali pa vnesite IP naslov lokalnega DNS strežnika.



Sedaj za shranjevanje vaših nastavitvev kliknite gumb **OK**.

DODATEK C: TEHNIČNI PODATKI

Splošno	
Standardi	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n
Protokoli	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNMP
Porti	En 10/100M Auto-Negotiation WAN RJ45 port, štiri 10/100M Auto-Negotiation LAN RJ45 ports ki podpirajo Auto MDI/MDIX
Tip kableske povezave	10BASE-T: UTP kategorija 3, 4, 5 cable (največ 100m) EIA/TIA-568 100Ω STP (največ 100m)
	100BASE-TX: UTP kategorija 5, 5e cable (največ 100m) EIA/TIA-568 100Ω STP (največ 100m)
LED indikatorji	Vklop, sistem, WLAN, WAN, LAN (1-4), WPS
Varnost in emisije	FCC, CE
Brezžičnost	
Frekvenčni pas	2.4~2.4835GHz
Stopnja radijskih podatkov	11n: do največ 300Mbps (avtomatsko) 11g: 54/48/36/24/18/12/9/6Mbps (avtomatsko) 11b: 11/5.5/2/1Mbps (avtomatsko)
Frekvenčna širitev	DSSS (Direct Sequence Spread Spectrum)
Modulacija	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Varnost	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK

Občutljivost @ 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;
Delovanje v okolju	
Temperaturno okolje	Delovanje: 0° - 40°C (32°F - 104°F) Shranjevanje: -40°C - 70°C (-40°F - 158°F)
Vlažnost	Delovanje: 10% - 90% RH, nekondenzirajoča Shranjevanje: 5% - 90% RH, nekondenzirajoča

DODATEK D: SLOVAR

- **802.11n** – 802.11n z dodajanjem MIMO (večkratni vhod-večkratni izhod) nadgrajuje predhodne 802.11 standarde. MIMO uporablja večje število oddajnikov in sprejemnih anten ki omogočajo večjo prepustnost podatkov prek prostorskega multipleksiranja in z izkoriščanjem prostorske raznolikosti povečano območje, morda prek kodiranja programov, kot je "Alamouti" kodiranje. Okrepljen brezžični konzorcij (EWC) [3] je bil ustanovljen za pospešitev procesa razvoja IEEE 802.11n in spodbujanja tehnoloških specifikacij za interoperabilnost naslednje generacije izdelkov brezžičnega lokalnega omrežja (WLAN).
- **802.11b** – Standard 802.11b določa brezžično omrežno povezovanje pri 11 Mbps z direktnim zaporedjem tehnologije širjenja spektra (DSSS) in ki deluje na radijskem spektru brez licence na 2.4GHz in WEP šifriranja za varnost. 802.11b omrežje se imenuje tudi Wi-Fi omrežje.
- **802.11g** – Specifikacija za brezžično omrežno povezovanje pri 54 Mbps, ki uporablja tehnologijo direktnega zaporedja širjenja spektra (DSSS), z uporabo OFDM modulacije in deluje na radijskem spektru brez licence na 2.4GHz in je združljiv z 802.11b napravami in WEP šifriranjem za varnost.
- **DDNS** – zmožnost dodeljevanja fiksnega gostitelja in imena domene dinamičnemu internetnemu IP naslovu.
- **DHCP** – protokol, ki samodejno konfigurira TSP/IP parametre za vse računalnike ki so povezani na DHCP strežnik.
- **DMZ** – demilitarizirano območje omogoča da je en lokalni gostitelj izpostavljen internetu za storitev s posebnim namenom, kot so internetne igre ali videokonferenca.
- **DNS** – internetna storitev, ki imena spletnih strani prevaja v IP naslove.
- **Domain Name** – (ime domene) opisno ime naslova ali skupine naslovov na internetu.
- **DSL** – tehnologija, ki omogoča pošiljanje ali sprejemanje podatkov preko navadne telefonske linije.
- **MTU** – velikost v bytih največjega paketa ki ga je mogoče prenesti.
- **NAT** – NAT tehnologija prevaja IP naslove lokalnih omrežij (LAN) v drugačne IP naslove za splet.

- **PPPoE** – PPPoE je protokol za povezovanje gostiteljev na internet preko vseskozi vzpostavljene povezave s simulacijo klicne povezave.
- **SSID** – je alfanumerični ključ z največ 32 znaki, ki identificira brezžično lokalno omrežje. Da lahko brezžične naprave v omrežju komunicirajo med seboj, morajo biti vse naprave konfigurirane na isti SSID. To je tipični parameter konfiguracije za brezžično kartico PC. Ustreza ESSID v brezžični dostopni točki in imenu brezžičnega omrežja.
- **WEP** – Mehanizem zasebnosti podatkov, ki temelji na 64-bitnem ali 128-bitnem ali 152-bitnem deljenem ključnem algoritmu, kot je opisano v standardu IEEE 802.11.
- **Wi-Fi** - Trgovsko ime za 802.11b brezžični standard povezovanja, ki jo dodeli Wireless Ethernet Compatibility Alliance (WECA, glej <http://www.wi-fi.net>), skupina industrijskih standardov, ki spodbuja interoperabilnost med napravami 802.11b.
- **WLAN** – skupina računalnikov in povezanih naprav komunicirajo med seboj brezžično, njihovi omrežni uporabniki pa so omejeni v lokalnem omrežju.



GARANCIJSKI LIST

Conrad Electronic d.o.o. k.d.
Ljubljanska c. 66, 1290 Grosuplje
Fax: 01/78 11 250, Tel: 01/78 11 248
www.conrad.si, info@conrad.si

Izdelek: **TP LINK WLAN-usmerjevalnik TL-WR841N**
Kat. št.: **39 97 34**

Garancijska Izjava:

Proizvajalec jamči za kakovost oziroma brezhibno delovanje v garancijskem roku, ki začne teči z izročitvijo blaga potrošniku. **Garancija velja na območju Republike Slovenije. Garancija za izdelek je 1 leto.**

Izdelek, ki bo poslan v reklamacijo, vam bomo najkasneje v skupnem roku 45 dni vrnil popravljene ali ga zamenjali z enakim novim in brezhibnim izdelkom. Okvare zaradi neupoštevanja priloženih navodil, nepravilne uporabe, malomarnega ravnanja z izdelkom in mehanske poškodbe so izvzete iz garancijskih pogojev. **Garancija ne izključuje pravic potrošnika, ki izhajajo iz odgovornosti prodajalca za napake na blagu.**

Vzdrževanje, nadomestne dele in priklopne aparate proizvajalec zagotavlja še 3 leta po preteku garancije.

Servisiranje izvaja proizvajalec sam na sedežu firme CONRAD ELECTRONIC SE, Klaus-Conrad-Strasse 1, Nemčija.

Pokvarjen izdelek pošljete na naslov: Conrad Electronic d.o.o. k.d., Ljubljanska cesta 66, 1290 Grosuplje, skupaj z izpolnjenim garancijskim listom.

Prodajalec: _____

Datum izročitve blaga in žig prodajalca:

Garancija velja od dneva nakupa izdelka, kar kupec dokaže s priloženim, pravilno izpolnjenim garancijskim listom.

- Garancija velja na območju Republike Slovenije.
- Garancija ne izključuje pravic potrošnika, ki izhajajo iz odgovornosti prodajalca za napake na blagu.