



Bezprzewodowy Router Szerokopasmowy 11N
– Podręcznik Użytkownika

Wireless-N Broadband Router 11N
– User Guide

Spis treści

ROZDZIAŁ 1: WPROWADZENIE	5
Zawartość opakowania	5
ROZDZIAŁ 2: PODSTAWOWE INFORMACJE DOTYCZĄCE ROUTERA.....	5
Panel tylny	5
Połączenia:	6
Panel górny	6
Instalacja urządzenia	7
ROZDZIAŁ 3: PODŁĄCZANIE SZEROKOPASMOWEGO ROUTERA BEZPRZEWODOWEGO N	8
Sprawdzanie połączenia sieciowego	9
ROZDZIAŁ 4 PODSTAWOWA KONFIGURACJA	10
Dostęp do narzędzia konfiguracyjnego opartego na technologii Web	10
Kreator konfiguracji	10
ROZDZIAŁ 5: USTAWIENIA ZAAWANSOWANE	12
Ustawienia sieci LAN	12
Ustawienia sieci WAN – PPPoE	13
Ustawienia sieci WAN – Static IP	14
Ustawienia sieci WAN – L2TP	14
Ustawienia sieci WAN – PPTP	14
Klonowanie adresów MAC	15
Ustawienia DNS	15
ROZDZIAŁ 6: USTAWIENIA SIECI BEZPRZEWODOWEJ	16
Ustawienia podstawowe	16
1. Mixed WEP	16
2. WPA-Personal	17
3. WPA2-Personal	17
4. WPA-Enterprise	18
5. WPA2-Enterprise	18
Ustawienia WPS	19
Ustawienia WDS	20
Zaawansowane ustawienia bezprzewodowe	21
Status połączenia bezprzewodowego	21
ROZDZIAŁ 7: SERWER DHCP	22
Lista serwerów DHCP	22
ROZDZIAŁ 8: SERWER WIRTUALNY	23
Przekazywanie pojedynczego portu	23
Przekazywanie zakresu portów	24
Ustawienia DMZ	25
Ustawienia UPnP	25
ROZDZIAŁ 9: KONTROLA RUCHU	26
Kontrola ruchu	26

ROZDZIAŁ 10: USTAWIENIA ZABEZPIECZEŃ	27
Ustawienia filtra klienta	27
Ustawienia adresów MAC	28
Zdalne zarządzanie Web	28
Lokalne zarządzanie Web	28
Ping WAN	29
ROZDZIAŁ 11: USTAWIENIA ROUTINGU	29
Tabela routingu	29
ROZDZIAŁ 12: NARZĘDZIA SYSTEMOWE	29
Czas	29
DDNS	30
Kopia zapasowa/przywracanie	30
Aktualizacja oprogramowania	30
Przywracanie domyślnych ustawień fabrycznych	31
Uruchamianie ponowne	31
Zmiana hasła	31
Dziennik systemowy	31
ZAŁĄCZNIK A: WŁAŚCIWOŚCI PRODUKTU	32

Rozdział 1: Wprowadzenie

Dziękujemy za zakup bezprzewodowego routera szerokopasmowego W306R N. Wykorzystuje on zaawansowaną technologię MIMO (Multi Input, Multi Output) i pełni funkcję routera, bezprzewodowego punktu dostępu, przełącznika 4-portowego i zapory ogniowej, umożliwiając współdzielenie dostępu do Internetu za pośrednictwem czterech gniazd lub dostępu bezprzewodowego. Dzięki zgodności ze standardem IEEE 802.11n (Draft 2.0) istnieje możliwość nawiązania połączenia z istniejącymi adapterami PCI, USB i kart 802.11b/g w komputerach przenośnych. Prędkość transmisji 300 Mbps zapewnia doskonałe wrażenia podczas oglądania filmów wideo, grania online i innych czynności.

Ponadto router obsługuje wszystkie najnowsze funkcje bezpieczeństwa sieci bezprzewodowych, takie jak 64-/128-bitowe szyfrowanie WEP, szyfrowanie WPS (PBC i PIN), filtrowanie pakietów i przekazywanie portów, zapobiegające nieautoryzowanemu dostępowi i chroniące sieć przed atakami z zewnątrz.

Przyjazny dla użytkownika kreator instalacji na płycie CD pomaga w konfiguracji bezprzewodowego routera szerokopasmowego. Urządzeniem można również zarządzać za pośrednictwem lokalnego/zdalnego, prostego w użyciu narzędzia opartego na technologii sieci Web. Jest to idealne rozwiązanie dla niewielkich biur i małych przedsiębiorstw.

Zawartość opakowania

- ◆ Bezprzewodowy router szerokopasmowy W306R N
- ◆ Przewód sieciowy Ethernet
- ◆ Skrócony podręcznik instalacji
- ◆ Zasilacz
- ◆ Płyta CD-ROM

W razie braku lub uszkodzenia jednego z powyższych elementów, prosimy o kontakt ze sprzedawcą, u którego nabyto urządzenie, w celu wymiany.

Rozdział 2: Podstawowe informacje dotyczące routera

Panel tylny

Oto opis tylnego panelu urządzenia. Jak widać na poniższym rysunku, znajdują się na nim porty RJ-45 do połączeń kablowych oraz przycisk Reset.



Połączenia:

Interfejs na panelu tylnym	Opis
1-4 (porty LAN)	Podłączanie urządzeń sieciowych Ethernet (komputery, przełączniki, koncentratory).
RESET/WPS	Uwaga: Po naciśnięciu przycisku RESET przez 7 sekund następuje skasowanie skonfigurowanych ustawień i przywrócenie urządzenia do domyślnych ustawień fabrycznych. Naciśnięcie tego przycisku przez 1 sekundę powoduje włączenie funkcji WPS (PBC).
WAN	Podłączanie modemu DSL, modemu kablowego lub dostępnego połączenia szerokopasmowego.
POWER	Gniazdo zasilacza.

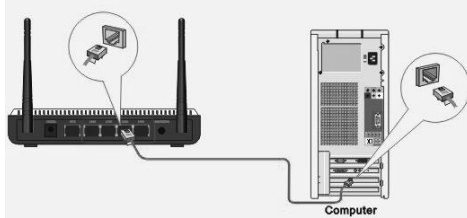
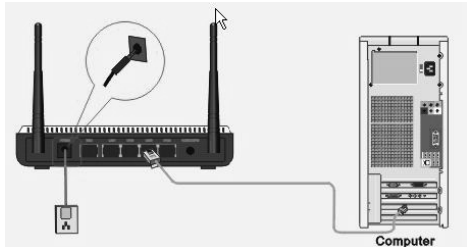
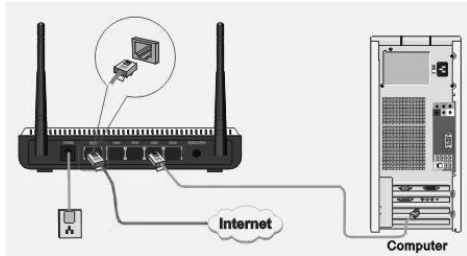
Panel górny

Na panelu górnym znajdują się przedstawione poniżej wskaźniki LED routera.

Diody LED:

Wskaźnik LED	Status	Opis
POWER	Zawsze Wł.	Wskaźnik POWER jest zawsze Wł., gdy urządzenie jest włączone i działa prawidłowo.
SYS	Miganie	Wskaźnik SYS miga, gdy system działa prawidłowo.
WAN	Zawsze Wł.	Wskazuje prawidłowe połączenie portów WAN.
	Miganie	Wskazuje przesyłanie/ odbiór pakietów danych.
WLAN	Miganie	Wskazuje prawidłowy stan sygnału bezprzewodowego.
LAN(1/2/3/4)	Zawsze Wł.	Wskazuje prawidłowe połączenie portów LAN.
	Miganie	Wskazuje przesyłanie/ odbiór pakietów danych.
WPS	Miganie	Wskazuje negocjowanie routera z klientami WPS w trybie WPS (PBC lub kod PIN).

Instalacja urządzenia

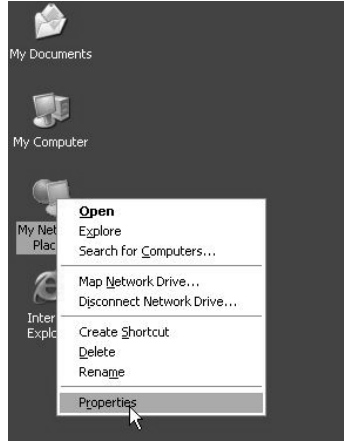
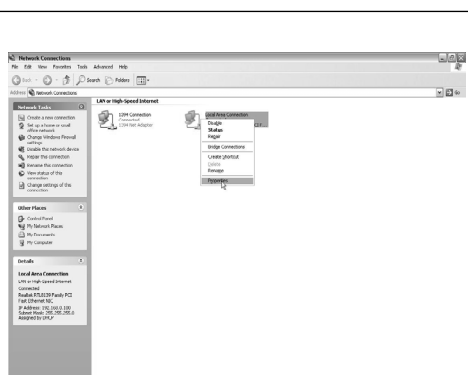
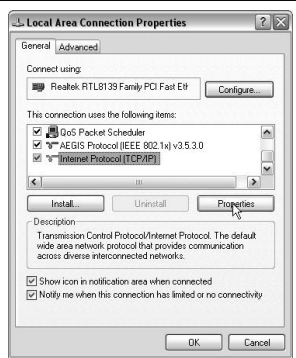
<p>1. Połącz port LAN routera z adapterem sieciowym komputera za pomocą jednego kabla.</p>	 <p>Computer</p>
<p>2. Podłącz zasilacz do routera, korzystając z dołączonego przewodu.</p>	 <p>Computer</p>
<p>3. Podłącz linię połączenia szerokopasmowego do portu WAN routera.</p>	 <p>Internet</p> <p>Computer</p>

WAŻNE: Użyć dołączonego zasilacza sieciowego. Inne zasilacze mogą spowodować uszkodzenie i unieważnienie gwarancji produktu.

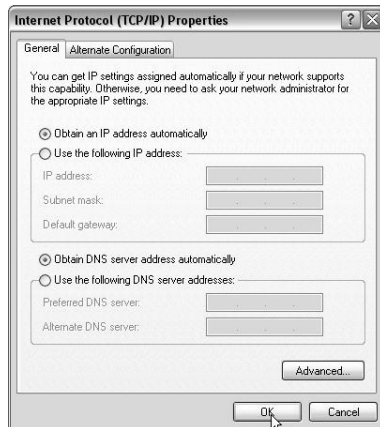
Rozdział 3: Podłączanie szerokopasmowego routera bezprzewodowego N

W celu przeprowadzenia prostej i szybkiej konfiguracji sieci wymagane są następujące kroki.

Ustawianie konfiguracji sieci w Moim komputerze

<p>Kliknij prawym przyciskiem myszy „My Network Places” (Moje miejsca sieciowe) i wybierz „Properties” (Właściwości).</p>	
<p>Kliknij prawym przyciskiem myszy „Local Area Network Connection” (Połączenie lokalne) i wybierz „Properties” (Właściwości).</p>	
<p>Wybierz „Internet Protocol (TCP/IP)” (Protokół internetowy (TCP/IP)) i kliknij „Properties” (Właściwości).</p>	

Zaznacz opcję „Obtain an IP address automatically” (Uzyskaj adres IP automatycznie) oraz „Obtain DNS server address automatically” (Uzyskaj adres serwera DNS automatycznie). Kliknij „OK”, aby zapisać konfigurację.



Lub wybierz opcję „Use the following IP address” (Użyj następującego adresu IP) i wpisz adres IP, maskę podsięci, bramę domyślną zgodnie z rysunkiem po prawej stronie. Należy oczywiście wpisać adres serwera DNS dostarczony przez dostawcę usług. Można również użyć domyślnej bramy routera jako serwera proxy DNS. Kliknij „OK”, aby zapisać konfigurację.

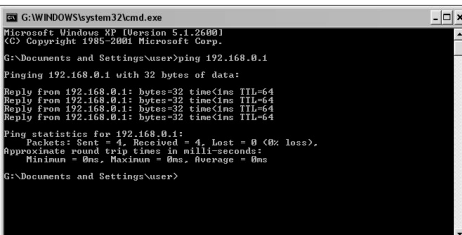


Sprawdzanie połączenia sieciowego

Wybierz „Start”— „Programs” (Programy) — „Accessories” (Akcesoria) — „Command Prompt” (Wiersz polecenia).

Wprowadź polecenie „ping 192.168.0.1” i naciśnij klawisz „Enter”. Jeżeli wskazanie na ekranie jest podobne do przedstawionego na rysunku po prawej stronie, oznacza to, że połączenie komputera z routerem jest prawidłowe.



Jeśli nie, upewnij się, że router i adapter sieciowy zostały podłączone prawidłowo. Po zakończeniu wszystkich przygotowań przejdź do rozdziału 4, aby poznać więcej opcji.



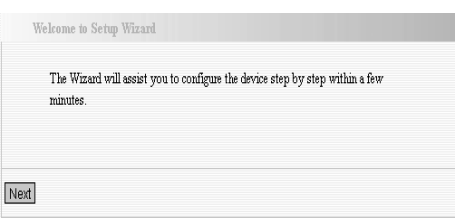
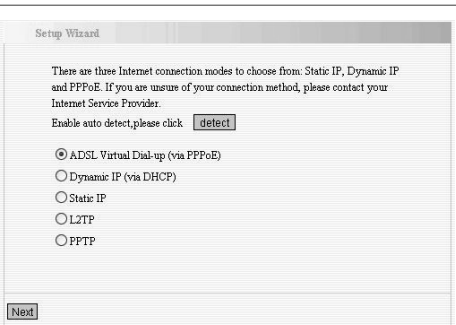
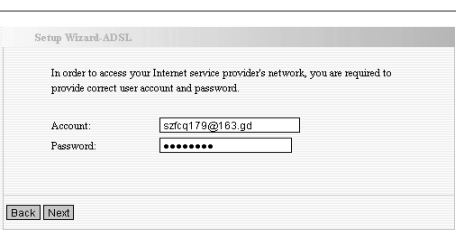
Rozdział 4 Podstawowa konfiguracja

W tym rozdziale przedstawiono konfigurację szerokopasmowego routera bezprzewodowego N za pomocą narzędzia konfiguracyjnego opartego na technologii sieci Web.

Dostęp do narzędzi konfiguracyjnych opartych na technologii Web

<p>Aby uzyskać dostęp do narzędzi konfiguracyjnych routera, włącz przeglądarkę internetową, np. Internet Explorer lub Firefox, a następnie wpisz domyślny adres IP routera: <code>http://192.168.0.1</code>. Naciśnij „Enter”.</p>	
<p>W polu nazwy użytkownika i hasła wpisz „admin”. Kliknij „OK”.</p>	

Kreator konfiguracji

<p>Tak wygląda okno powitania kreatora, umożliwiającego szybką konfigurację routera. Kliknij „Next” (Dalej).</p>	
<p>Na następnym ekranie należy wybrać jeden z trybów połączenia internetowego. Jeżeli nie masz pewności, kliknij przycisk „Detect” lub skontaktuj się z dostawcą usług internetowych, a następnie kliknij „Next”.</p>	
<p>Tryb połączenia 1: ADSL Virtual Dial-up (Via PPPoE)</p> <p>Podaj nazwę konta (Account) i hasło (Password) dostarczone przez dostawcę i kliknij „Next” (Dalej).</p>	

Tryb połączenia 2: Dynamic IP (Via DHCP)

Jeżeli tryb używanego połączenia to Dynamic IP, oznacza to, że adres IP zmienia się przy każdym nawiązywaniu połączenia. Nie trzeba wprowadzać takich informacji, jak w przypadku trybu 3.

Tryb połączenia 3: Static IP

Na tym ekranie należy uzupełnić pola IP Address (Adres IP), Subnet Mask (Maska podsieci), Gateway (Brama) oraz Primary DNS server (Główny serwer DNS) na podstawie informacji uzyskanych od dostawcy usług internetowych, a następnie kliknąć „**Next**” (Dalej).

Setup Wizard-Static IP

This Internet connection mode requires network address information from your Internet service provider.

IP Address:
Subnet Mask:
Gateway:
Primary DNS Server:
Secondary DNS Server: (optional)

[Back](#) [Next](#)

Tryb połączenia 4: L2TP

Wybierz protokół L2TP (Layer 2 Tunneling Protocol), jeżeli dostawca usług wykorzystuje połączenie L2TP; dostawca udostępni nazwę użytkownika i hasło – należy tu wpisać te parametry.

Protokół L2TP zapewnia dwa tryby dostępu.

Jeżeli L2TP dostarczany przez dostawcę to **Dynamic IP**: Wybierz opcję Dynamic IP.

Jeżeli L2TP dostarczany przez dostawcę to **Static IP**: Wprowadź parametry dostarczone przez dostawcę.

Po zakończeniu konfiguracji kliknij „Next” (Dalej).

Setup Wizard-L2TP

L2TP Server IP Address:
User Name:
Password:
IP Address:
Address Mode:
Subnet Mask:
Default Gateway:

[back](#) [next](#)

Tryb połączenia 5: PPTP

Jeżeli typ używanego połączenia to „PPP Tunneling Protocol”, wprowadź następujące parametry, dostarczone przez dostawcę usług: Server IP Address (Adres IP serwera), User Name (Nazwa użytkownika) oraz Password (Hasło).

Protokół PPTP zapewnia dwa tryby dostępu.

Jeżeli PPTP dostarczany przez dostawcę to **Dynamic IP**: Wybierz opcję Dynamic IP.

Jeżeli PPTP dostarczany przez dostawcę to **Static IP**: Wprowadź parametry dostarczone przez dostawcę.

Po zakończeniu konfiguracji kliknij „Next” (Dalej).

Setup Wizard-PPTP

PPTP Server IP Address:
User Name:
Password:
Address Mode:
IP Address:
Subnet Mask:
Default Gateway:

[back](#) [next](#)

Kliknij „**Apply**” (**Zastosuj**), w sekcji **System Tools (Narzędzia systemowe)** wybierz „**Reboot**” (**Uruchom ponownie**) i naciśnij przycisk „**Reboot the router**” (Uruchom router ponownie).

Setup Wizard

The basic configuration is completed.
Please apply and reboot the device, or press "Reboot the router" button in System Tools of the left menu.

Następuje ponowne uruchomienie; poczekaj kilka minut i **NIE** wyłączaj urządzenia.

Reboot

Click here to reboot the router.

12%

W menu po lewej stronie kliknij pozycję „System Status” (Status systemu), aby wyświetlić bieżące informacje dotyczące sieci i systemu. Jeżeli status połączenia (Connection Status) jest aktywny (Connected), podstawowe ustawienia routera zostały skonfigurowane pomyślnie. Twój komputer jest połączony z Internetem. Aby skonfigurować więcej opcji, postępuj zgodnie z objaśnieniami w rozdziale *Ustawienia zaawansowane*.

Network Status

Connection Status	Connected
WAN IP	218.18.40.67
Subnet Mask	255.255.255.255
Gateway	218.17.71.1
Primary DNS Server	202.96.128.166
Secondary DNS Server	202.96.134.133
Connection Mode	PPPoE
Connection Timer	00:03:10

Rozdział 5: Ustawienia zaawansowane

W tym rozdziale przedstawione są zaawansowane opcje konfiguracji routera, obejmujące ustawienia sieci LAN, ustawienia sieci WAN, klonowanie adresów MAC oraz ustawienia DNS.

Ustawienia sieci LAN

MAC Address (Adres MAC): Fizyczny adres MAC routera, widziany w sieci lokalnej. Nie można go zmienić.

IP Address (Adres IP): Adres IP routera w sieci LAN (nie adres IP komputera). Po zmodyfikowaniu adresu IP, należy go pamiętać w celu uzyskania dostępu do narzędzia konfiguracyjnego podczas następnego logowania. Wartością domyślną jest 192.168.0.1.

Subnet Mask (Maska podsieci): Wyświetlana jest maska podsieci routera w celu oszacowania wielkości sieci. Wartością domyślną jest 255.255.255.0.

LAN Settings

This is to configure the basic parameters for LAN ports.

MAC Address	00:0C:41:86:0A:B2
IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Ustawienia sieci WAN – PPPoE

Connection Mode (Tryb połączenia): Wyświetlany jest bieżący tryb połączenia.

Account (Konto): Wpisz nazwę podaną przez usługodawcę.

Password (Hasło): Wpisz hasło podane przez usługodawcę.

MTU: Maximum Transmission Unit – Maksymalna jednostka transmisji. Rozmiar największego datagramu, który można wysłać w sieci. Wartość domyślna to 1492. **NIE** zmieniaj jej, jeśli nie jest to konieczne.

Service Name (Nazwa usługi): Zdefiniowana jako zespół charakterystyk stosowanych przy połączeniu PPPoE. Wpisz, jeśli została podana. **NIE** zmieniaj jej, jeśli nie jest to konieczne.

AC Name (Nazwa AC): Wpisz, jeśli została podana. **NIE** zmieniaj jej, jeśli nie jest to konieczne.

Connect Automatically (Łącz automatycznie): Automatyczne łączenie z Internetem po ponownym uruchomieniu systemu lub awarii połączenia.

Connect Manually (Łącz ręcznie): Ręczne łączenie z Internetem przez użytkownika.

Connect on Demand (Łącz na żądanie): Ponowne nawiązywanie połączenia z Internetem po określonym czasie (maks. czas bezczynności). Zero oznacza, że połączenie jest aktywne cały czas. Można podać liczbę minut, po upływie których połączenie z Internetem zostanie zerwane.

Connect on Fixed Time (Łącz w ustalonym czasie): Łączenie z Internetem w czasie ustalonym przez użytkownika.

WAN Settings

WAN connection mode: PPPoE

Account

Password

MTU (Default by 1492. Do NOT Modify Unless Necessary)

Service Name (Do NOT Modify Unless Necessary)

AC Name (Do NOT Modify Unless Necessary)

Internet Connection Option

☒ Connect Automatically.

☐ Connect Manually.

☐ Connect on Demand

Max Idle Time: (60—3600 seconds)

☐ Connect on Fixed Time

IMPORTANT: Please set the time in "System Tools" before you select this Internet connection.

Time From h m T h m

Ustawienia sieci WAN – Static IP

Jeżeli tryb używanego połączenia to statyczny IP, należy wprowadzić następujące informacje adresowe.

IP Address (Adres IP):

Wpisz adres IP sieci WAN, podany przez usługodawcę.

Subnet Mask (Maska podsieci): Wpisz maskę podsieci WAN.

Gateway (Brama): Wpisz bramę sieci WAN.

Primary DNS Server (Główny serwer DNS): Podaj podstawowy serwer DNS dostarczony przez usługodawcę.

Secondary DNS Server (Drugorzędny serwer DNS): Podaj drugorzędny serwer DNS

WAN Settings

WAN connection mode: Static IP

IP Address: 192.168.1.2

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS Server: 192.168.0.1

Secondary DNS Server: (option)

Apply Cancel

Ustawienia sieci WAN – L2TP

L2TP Server IP (Adres IP serwera L2TP): Podaj adres IP serwera dostarczony przez usługodawcę.

User Name (Nazwa użytkownika): Wpisz nazwę użytkownika L2TP.

Password (Hasło): Wpisz hasło L2TP.

MTU: Maksymalna jednostka transmisji. Może zająć konieczność zmiany w celu zapewnienia maksymalnej wydajności dla określonego dostawcy. Domyślną wartością MTU jest 1400.

Address Mode (Tryb adresowania): Wybierz „Static”, jeżeli usługodawca dostarczył adres IP, maskę podsieci i bramę. W większości przypadków wybierz opcję „Dynamic”.

IP Address (Adres IP): Podaj adres IP serwera L2TP dostarczony przez usługodawcę.

Subnet Mask (Maska podsieci): Wpisz maskę podsieci dostarczoną przez usługodawcę.

Default Gateway (Brama domyślna): Wpisz domyślną maskę podsieci dostarczoną przez usługodawcę.

WAN Settings

WAN connection mode: L2TP

L2TP Server IP: 0.0.0.0

User Name: tenda

Password: *****

MTU: 1400

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

Ustawienia sieci WAN – PPTP

PPTP Server IP (Adres IP serwera PPTP): Podaj adres IP serwera dostarczony przez usługodawcę.

User Name (Nazwa użytkownika): Wpisz nazwę użytkownika PPTP podaną przez usługodawcę.

Password (Hasło): Wpisz hasło PPTP podane przez usługodawcę.

Address Mode (Tryb adresowania): Wybierz „Static”, jeżeli usługodawca dostarczył adres IP, maskę podsieci i bramę. W większości przypadków wybierz opcję „Dynamic”.

IP Address (Adres IP): Podaj adres IP serwera PPTP dostarczony przez usługodawcę.

Subnet Mask (Maska podsieci): Wpisz maskę podsieci dostarczoną przez usługodawcę.

Default Gateway (Brama domyślna): Wpisz domyślną maskę podsieci dostarczoną przez usługodawcę.

Setup Wizard: PPTP

PPTP Server IP Address: 0.0.0.0

User Name: tenda

Password: *****

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

back next

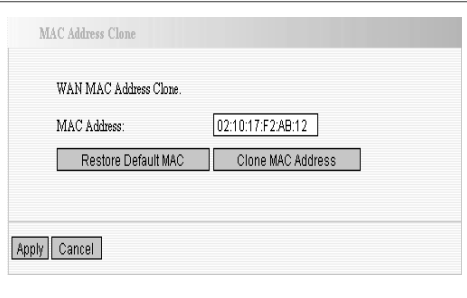
Klonowanie adresów MAC

W celu uzyskania dostępu do sieci, niektórzy usługodawcy wymagają od użytkowników końcowych adresów MAC. Ta funkcja kopiuje adres MAC urządzenia sieciowego do routera.

MAC Address (Adres MAC): Adres MAC używany do rejestracji w sieci usługodawcy.

Clone MAC address (Klonuj adres MAC): Rejestracja adresu MAC komputera.

Restore default MAC address (Przywróć domyślny adres MAC): Przywracanie domyślnego adresu MAC urządzenia.



Ustawienia DNS

DNS to skrót od Domain Name System (lub Service) – System nazw domenowych. Jest to usługa internetowa konwertująca nazwy domen na adresy IP dostarczana przez usługodawców. Jeśli nie posiadasz takiego systemu, skontaktuj się z usługodawcą.

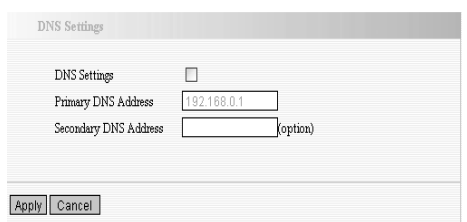
DNS: Zaznacz pole wyboru, aby włączyć serwer DNS.

Primary DNS Address (Główny adres DNS):

Wpisz wymagany adres dostarczony przez usługodawcę.

Secondary DNS Address (Drugorzędny adres DNS):

Wpisz drugi adres dostarczony przez dostawcę, pole opcjonalne.



Rozdział 6: Ustawienia sieci bezprzewodowej

W tym rozdziale znajdują się głównie informacje dotyczące ustawień bezprzewodowych, obejmujące ustawienia podstawowe, ustawienia zabezpieczeń, kontrolę dostępu i ustawienia zaawansowane.

Tryb bezprzewodowy

Ustawienia podstawowe

Network Mode (Tryb sieci): Obsługa trybów 802.11b/g połączony, 802.11b, 802.11g oraz 802.11b/g/n połączony.

Main SSID (Główny SSID): Główny identyfikator zestawu usług. „Nazwa” sieci bezprzewodowej.

Minor SSID (Podrzędny SSID): Podrzędny identyfikator zestawu usług. Parametr opcjonalny.

Broadcast (SSID) (Emisja (SSID)): Wybierz opcję „enabled” (włączona), aby SSID urządzenia był widoczny dla klientów bezprzewodowych.

BSSID: 48-bitowa metoda identyfikacji wykorzystywana do identyfikacji określonego podstawowego zestawu usług (BSS) w ramach jednego obszaru. W sieciach BSS z infrastrukturą BSSID to adres MAC punktu dostępowego.

Channel (Kanał): Menu rozwijane, służące do wyboru kanału roboczego sieci bezprzewodowej. Wybierz jedną z wartości 1 do 13 lub opcję AutoSelect (Wybór automatyczny), aby wybrać różne kanały.

Channel Bandwidth (Szerokość pasma kanału): Wybierz roboczą częstotliwość bezprzewodową 20M lub 20/40M.

HT TxStream: Strumień przesyłu częstotliwości radiowej.

HT RxStream: Strumień odbioru częstotliwości radiowej.



Ustawienia zabezpieczeń sieci bezprzewodowej

Ta strona służy do konfiguracji zabezpieczeń bezprzewodowych routera. Obsługiwanych jest sześć trybów zabezpieczeń: WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise oraz RADIUS. Jeżeli zabezpieczenia sieci bezprzewodowej mają być wyłączone, wybierz opcję „Disable” z menu rozwijanego.

1. Mixed WEP

WEP (Wired Equivalent Privacy – Odpowiednik przewodowej prywatności) to podstawowa metoda szyfrowania, wykorzystująca ciągi kluczy cyfrowych (o długości 64 lub 128 bitów) do szyfrowania

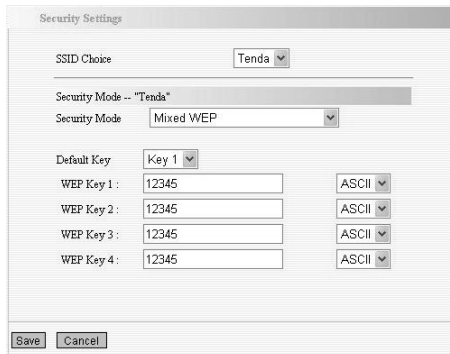
danych bezprzewodowych. Używając tego samego klucza we wszystkich urządzeniach sieciowych, można uniemożliwić nieautoryzowanym urządzeniom bezprzewodowym monitorowanie transmisji lub zasobów sieciowych.

SSID Choice (Wybór SSID): Wybierz SSID, dla którego mają być skonfigurowane zabezpieczenia. Urządzenie umożliwia konfigurację różnych poziomów zabezpieczeń dla głównego SSID i podrzędnego.

Security Mode (Tryb zabezpieczeń): Dostępne są różne tryby zabezpieczeń; można wybrać mixed WEP, WPA-Personal, WPA-Enterprise itd.

Default Key (Klucz domyślny): Wybierz ważny klucz szyfrowania:

WEP Key1, 2, 3, 4 (Klucz WEP1, 2, 3, 4): Wpisz klucz WEP. Klucz musi być zgodny z formatem i musi być ważny. Klucz powinien się składać ze znaków ASCII lub znaków heksadecymalnych



2. WPA-Personal

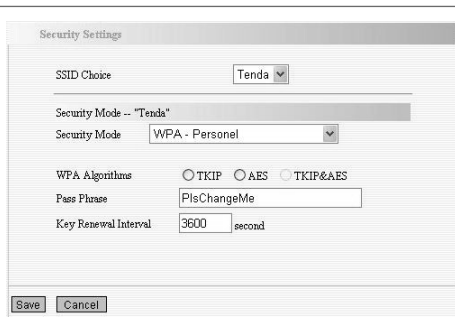
WPA (Wi-Fi Protected Access – Technologia chronionego dostępu Wi-Fi), standard Wi-Fi, jedna z najnowszych metod szyfrowania, zwiększająca bezpieczeństwo WEP. Wykorzystuje ona bardziej rozbudowane typy szyfrowania (np. TKIP lub AES) i może dynamicznie zmieniać klucze przy każdym autoryzowanym

urządzeniu bezprzewodowym.

WPA Algorithms (Algorytmy WPA): Wybierz jeden z typów szyfrowania, AES lub TKIP. (AES jest skuteczniejszy niż TKIP).

Pass Phrase (Fraza szyfrująca): Wpisz klucz, składający się z 8 – 63 znaków ASCII.

Key Renewal Interval (Okres odnawiania klucza): Podaj okres odnawiania klucza. Jest to informacja dla routera, jak często ma on zmieniać klucze.



The screenshot shows the 'Security Settings' window. At the top, 'SSID Choice' is set to 'Tenda'. Below it, 'Security Mode -- "Tenda"' is selected. The 'Security Mode' dropdown is set to 'WPA - Personal'. Under 'WPA Algorithms', the radio buttons for 'TKIP', 'AES', and 'TKIP&AES' are visible, with 'AES' being the selected option. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Save' and 'Cancel' buttons.

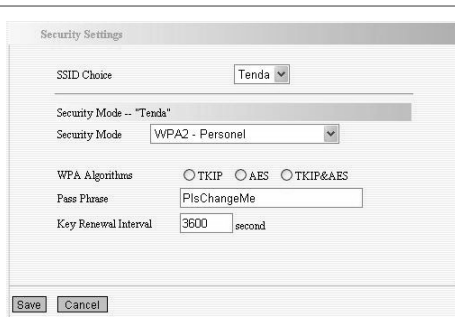
3. WPA2-Personal

WPA2 (Wi-Fi Protected Access version 2 – Technologia chronionego dostępu Wi-Fi, wersja 2), metoda łatwa w konfiguracji i bezpieczniejsza niż odpowiednik przewodowej prywatności (WEP).

WPA Algorithms (Algorytmy WPA): Wybierz algorytmy kluczy, takie jak TKIP, AES i TKIP&AES.

Pass Phrase (Fraza szyfrująca): Wpisz klucz, składający się z 8 – 63 znaków ASCII.

Key Renewal Interval (Okres odnawiania klucza): Podaj okres odnawiania klucza. Jest to informacja dla routera, jak często ma on zmieniać klucze.



The screenshot shows the 'Security Settings' window. At the top, 'SSID Choice' is set to 'Tenda'. Below it, 'Security Mode -- "Tenda"' is selected. The 'Security Mode' dropdown is set to 'WPA2 - Personal'. Under 'WPA Algorithms', the radio buttons for 'TKIP', 'AES', and 'TKIP&AES' are visible, with 'AES' being the selected option. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Save' and 'Cancel' buttons.

4. WPA-Enterprise

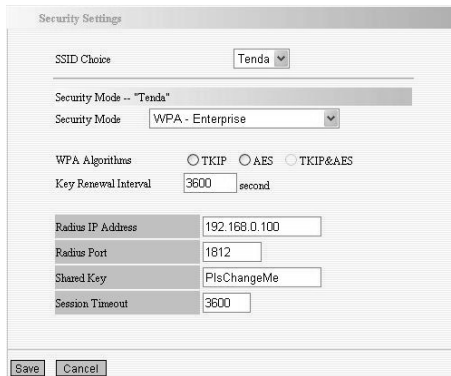
Ten protokół uwierzytelniania jest oparty na serwerze RADIUS. Ten tryb zabezpieczeń jest używany wówczas, gdy do routera jest podłączony serwer RADIUS.

Radius IP Address (Adres IP serwera RADIUS): Podaj adres IP serwera RADIUS.

Radius Port (Port serwera Radius): Podaj numer portu serwera RADIUS.

Shared key (Współdzielony klucz): Klucz szyfrowania, używany do uwierzytelniania routera przez serwer RADIUS.

Session Timeout (Przeterminowanie sesji): Okres czasu ponownego uwierzytelniania między routerem a serwerem. Domyślna wartość to 3600s.



The screenshot shows the 'Security Settings' window with the following configuration:

- SSID Choice: Tenda
- Security Mode -- "Tenda": WPA - Enterprise
- WPA Algorithms: TKIP, AES, TKIP&AES (all unselected)
- Key Renewal Interval: 3600 second
- Radius IP Address: 192.168.0.100
- Radius Port: 1812
- Shared Key: PlsChangeMe
- Session Timeout: 3600
- Buttons: Save, Cancel

5. WPA2-Enterprise

Ten tryb zabezpieczeń jest również używany wówczas, gdy do routera jest podłączony serwer RADIUS.

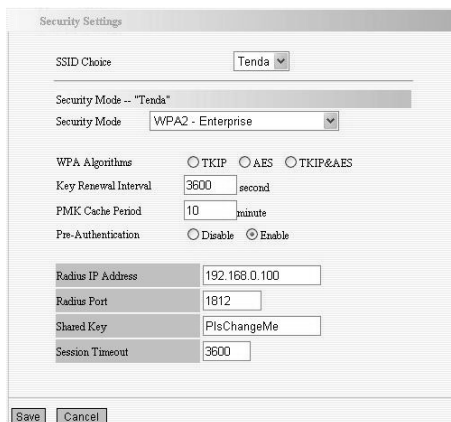
WPA Algorithms (Algorytmy WPA): Wybierz algorytmy kluczy, takie jak TKIP i AES.

Radius IP Address (Adres IP serwera RADIUS): Podaj adres IP serwera RADIUS.

Radius Port (Port serwera Radius): Podaj numer portu serwera RADIUS.

Shared key (Współdzielony klucz): Klucz szyfrowania, używany do uwierzytelniania routera przez serwer RADIUS.

Session Timeout (Przeterminowanie sesji): Okres czasu ponownego uwierzytelniania między routerem a serwerem. Domyślna wartość to 3600s.



The screenshot shows the 'Security Settings' window with the following configuration:

- SSID Choice: Tenda
- Security Mode -- "Tenda": WPA2 - Enterprise
- WPA Algorithms: TKIP, AES, TKIP&AES (all unselected)
- Key Renewal Interval: 3600 second
- PMK Cache Period: 10 minute
- Pre-Authentication: Disable, Enable (Enable is selected)
- Radius IP Address: 192.168.0.100
- Radius Port: 1812
- Shared Key: PlsChangeMe
- Session Timeout: 3600
- Buttons: Save, Cancel

Ten tryb zabezpieczeń jest używany wówczas, gdy do routera jest podłączony serwer RADIUS. 802.1x, rodzaj protokołu uwierzytelniania opartego na portach, to typ uwierzytelniania i strategia dla użytkowników. Port może być portem fizycznym lub logicznym (np. VLAN). Dla bezprzewodowych użytkowników sieci, port jest po prostu kanałem. Ostatecznym przeznaczeniem uwierzytelniania 802.1x jest kontrola, czy port może zostać użyty. Jeżeli port zostanie uwierzytelniony pomyślnie, można go otworzyć, co pozwala na przesyłanie wszystkich komunikatów. Jeżeli port nie zostanie uwierzytelniony, można utrzymać go w stanie „zamkniętym”, przez co będą mogły być przesyłane przez niego tylko komunikaty protokołu uwierzytelniania 802.1x.

WEP: Wybierz opcję „włącz/wyłącz” dla szyfrowania WEP, wskazującego proces uwierzytelniania między adapterem bezprzewodowym a routerem bezprzewodowym.

Radius IP Address (Adres IP serwera RADIUS): Podaj adres IP serwera RADIUS.

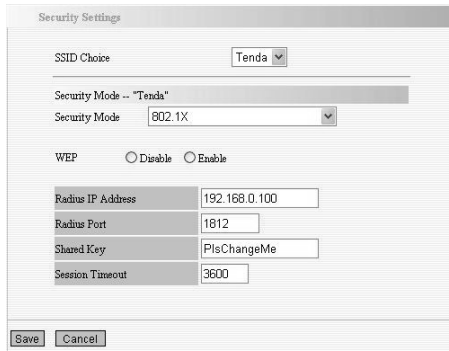
Radius Port (Port serwera Radius): Podaj numer portu serwera RADIUS.

Shared key (Współdzielony klucz):

Klucz szyfrowania, używany do uwierzytelniania routera przez serwer RADIUS.

Session Timeout (Przeterminowanie sesji): Okres czasu ponownego uwierzytelniania między routerem a serwerem. Domyślna wartość to 3600s.

UWAGA: Aby zwiększyć poziom bezpieczeństwa, nie używaj słów, które są dostępne w słowniku lub są łatwe do zapamiętania! Klienci bezprzewodowi zapamiętują klucz WEP, dzięki czemu należy wprowadzić klucz WEP tylko raz; zaleca się używanie skomplikowanych kluczy WEP, aby zwiększyć poziom bezpieczeństwa.



Security Settings

SSID Choice: Tenda

Security Mode -- "Tenda"

Security Mode: 802.1X

WEP: ☐ Disable ☒ Enable

Radius IP Address: 192.168.0.100

Radius Port: 1812

Shared Key: PlsChangeMe

Session Timeout: 3600

Save Cancel

Ustawienia WPS

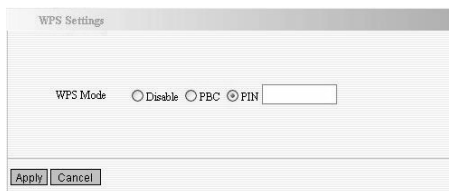
WPS (Wi-Fi Protected Setup) to prosta i szybka metoda nawiązywania połączenia między klientami sieci bezprzewodowej a routerem przez zaszyfrowane dane. Użytkownicy tylko podają kod PIN do konfiguracji, nie wybierając metody szyfrowania i nie wprowadzając ręcznie tajnych kluczy.

WPS Mode (Tryb WPS): Obsługa dwóch metod konfiguracji ustawień WPS:

PBC (Push-Button Configuration) – Konfiguracja przez naciśnięcie przycisku i kod PIN.

PBC: Wybierz PBC lub naciśnij przycisk WPS na panelu routera (Naciśnij przycisk przez jedną sekundę, wskaźnik WPS będzie migać przez 2 minuty, co oznacza, że funkcja WPS jest włączona. Podczas migania można włączyć inny router, aby zaimplementować negocjację WPS/PBC między nimi. Obecnie metoda WPS obsługuje tylko dostęp dla jednego klienta. Po upływie dwóch minut wskaźnik WPS gaśnie).

PIN: Po włączeniu tej opcji należy wprowadzić kod PIN klienta **bezprzewodowego i zachować ten sam kod w kliencie.**



WPS Settings

WPS Mode: ☐ Disable ☐ PBC ☒ PIN

Apply Cancel

Ustawienia WDS

W tym trybie można rozszerzyć zasięg sieci, łącząc ze sobą nawet cztery inne punkty dostępowe, przy czym każdy z punktów może wciąż przyjmować klientów bezprzewodowych.

Lazy Mode (Tryb wolny): Należy skonfigurować BSSID routera w innym urządzeniu bez konieczności wprowadzania w nim BSSID innego routera, po czym zostają one automatycznie połączone.


Bridge Mode (Tryb mostu): Za pomocą tego trybu można połączyć bezprzewodowo dwie lub więcej sieci przewodowych. W tym trybie należy dodać bezprzewodowy adres MAC urządzenia łączącego do tabeli adresów MAC punktu dostępowego routera lub wybrać adres z tabeli skanowania. Urządzenie łączące musi jednocześnie działać w trybie Lazy, Repeatre lub Bridge.

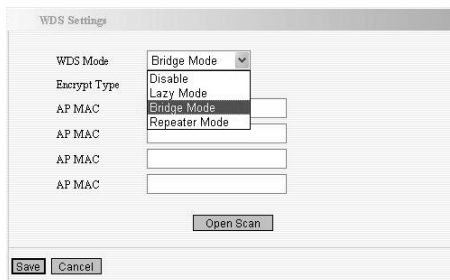
Repeater Mode (Tryb wzmacniaka): Można wybrać ten tryb w celu zwiększenia odległości między dwoma urządzeniami sieci WLAN. Działając jako wzmacniak WDS, router W306R łączy się z kartą klienta jako punktem dostępowym i innym punktem dostępowym. W typowych zastosowaniach wzmacniaka, punkty dostępowe łączące się z innymi punktami wyposażonymi w funkcję WDS, muszą również obsługiwać WDS. W tym trybie należy dodać bezprzewodowy adres MAC urządzenia łączącego do tabeli adresów MAC punktu dostępowego routera, a łączący się klient musi działać w trybie Lazy, Repeatre lub w trybie klienta.

Encrypt Type (Typ szyfrowania): Możesz wybrać tryb WEP, tryb TKIP lub tryb AES.

Pass Phrase (Fraza szyfrująca): Podaj klucz w formacie zgodnym z wybraną metodą szyfrowania.

AP MAC: Wpisz adres MAC innego routera bezprzewodowego.

 **UWAGA:** Oba routery bezprzewodowe muszą używać tego samego zakresu, numeru kanału i ustawień zabezpieczeń!



WDS Settings

WDS Mode: Bridge Mode

Encrypt Type: Disable

AP MAC:

AP MAC:

AP MAC:

AP MAC:

Open Scan

Save Cancel

Zaawansowane ustawienia bezprzewodowe

Ta sekcja służy do konfigurowania zaawansowanych ustawień bezprzewodowych routera, takich jak preambula radiowa, częstotliwość 802.11g/n, próg fragmentacji, próg RTS, okres rozgłaszania i interwał DTIM.

BG protection Mode (Tryb ochrony BG): Domyślnie Auto (automatyczny). Można wybrać ustawienie On (Wł.) lub Off (Wyt.).

Basic Data Rates (Podstawowa przepływność danych): Odnosnie różnych wymogów, możesz wybrać jedną z pasujących wartości podstawowej przepływności danych. Domyślnie wartość ta wynosi (1-2-5.5-11Mbps...).

Beacon Interval (Okres rozgłaszania): Ustaw okres rozgłaszania bezprzewodowego sygnału radiowego. Nie zmieniaj domyślnej wartości, jeśli nie wiesz, jaka ona jest; domyślnie: 100.

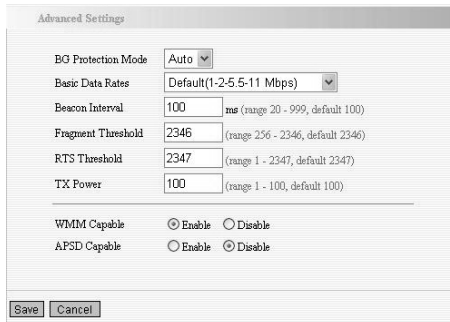
Fragment Threshold (Próg fragmentacji): Nie zmieniaj domyślnej wartości, jeśli nie wiesz, jaka ona jest; domyślnie: 2346.

RTS Threshold (Próg RTS): Ustaw próg RTS bezprzewodowego sygnału radiowego. Nie zmieniaj domyślnej wartości, jeśli nie wiesz, jaka ona jest; domyślnie: 2347.

TX Power (Moc TX): Możesz ustawić wyjściową moc bezprzewodowego sygnału radiowego. Jeżeli router nie jest używany w naprawdę dużej przestrzeni, ustawienie mocy wyjściowej na 100% może nie być konieczne. Zwiększy to poziom bezpieczeństwa (złotliwi / nieznanzi użytkownicy z określonej odległości nie będą w stanie uzyskać dostępu do routera).

WMM Capable (Zgodność z WMM): Zwiększenie wydajności transferu danych treści multimedialnych podczas przesyłania ich przez sieć bezprzewodową. Jeśli nie wiesz, co to za funkcja / nie jesteś pewien, czy jest wymagana, zaleca się ustawienie „Enable” (Włącz) – jest to również wartość domyślna.

APSD Capable (Zgodność z APSD): Opcja służy do automatycznego wyłączania zasilania. Domyślnie wyłączona.




Kontrola dostępu bezprzewodowego

Aby chronić sieć bezprzewodową, kontrola dostępu bezprzewodowego opiera się na zarządzaniu adresami MAC.

MAC Address Filter (Filtr adresów MAC): Aby wszystkie zewnętrzne adresy IP mogły uzyskiwać dostęp do routera, wybierz opcję „Disable” (Wyłącz).

MAC Address (Adres MAC): Aby określić zewnętrzny adres IP, wpisz ręcznie adres MAC i kliknij „Add” (Dodaj).

MAC Address List (Lista adresów MAC): Tutaj wyświetlane są wszystkie dodane adresy MAC. Kliknij „Delete” (Usuń), aby usunąć filtr dla tego adresu MAC.



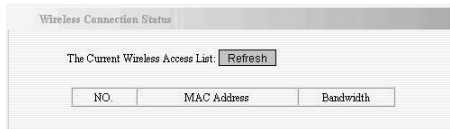
Status połączenia bezprzewodowego

Na tej stronie wyświetlany jest aktualny status dostępu bezprzewodowego. Kliknij „Refresh” (Odśwież), aby zaktualizować informacje dotyczące połączenia bezprzewodowego.

MAC Address (Adres MAC):

Wyświetla adres MAC połączonego komputera.

Bandwidth (Szerokość pasma): Wyświetla pasmo kanału hosta do nawiązania połączenia.



Wireless Connection Status

The Current Wireless Access List:

NO.	MAC Address	Bandwidth

Rozdział 7: Serwer DHCP

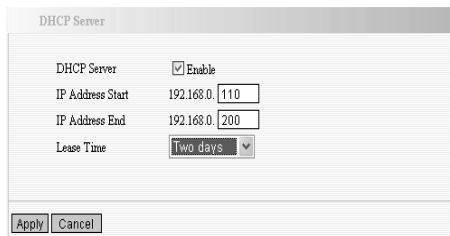
DHCP (Dynamic Host Control Protocol) służy do automatycznego przypisywania adresów IP do komputerów w sieci. Po aktywacji serwera DHCP, będzie on automatycznie alokować nieużywane adresy IP z puli adresów do komputera wysyłającego żądanie połączenia, przy włączonej opcji „Obtain an IP Address Automatically” (Uzyskaj adres IP automatycznie). Wymagane jest zatem określenie początkowego i końcowego adresu puli adresów IP.

DHCP Server (Serwer DHCP):

Zaznacz pole wyboru, aby włączyć serwer DHCP.

IP Address Start/End (Początkowy/końcowy adres IP): Podaj zakres adresów IP do rozdzielania przez serwer DHCP.

Lease Time (Czas dzierżawy): Okres dzierżawienia adresu IP.



DHCP Server

DHCP Server ☒ Enable

IP Address Start 192.168.0.110

IP Address End 192.168.0.200

Lease Time

Lista serwerów DHCP

Przypisywanie statycznych adresów IP dodaje określony, statyczny adres IP do przypisanego adresu MAC. Powiązane informacje można wyświetlić na liście serwerów DHCP.

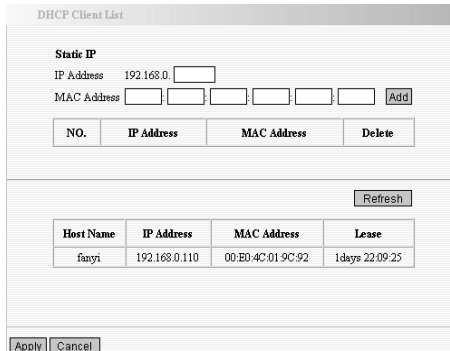
IP Address (Adres IP): Wpisz jeden adres IP dla komputera w sieci LAN.

MAC Address (Adres MAC):

Wpisz adres MAC komputera, do którego chcesz przypisać powyższy adres IP. Kliknij „Add” (Dodaj), aby dodać pozycję na listę.

Hostname (Nazwa hosta): Nazwa komputera dodana jako nowy adres IP.

Lease Time (Czas dzierżawy): Okres dzierżawienia danego adresu IP.



DHCP Client List

Static IP

IP Address 192.168.0.

MAC Address

NO.	IP Address	MAC Address	Delete

Host Name	IP Address	MAC Address	Lease
flanyi	192.168.0.110	00:E0:4C:01:9C:92	1days 22:09:25

Rozdział 8: Serwer wirtualny

Przekazywanie pojedynczego portu

Router W306R można skonfigurować jako serwer wirtualny w zastępstwie usług lokalnych za portem LAN. Żądania zdalne będą przekierowywane do serwerów lokalnych przez serwer wirtualny. Ten rozdział dotyczy przekazywania pojedynczego portu. Przekazywanie pojedynczego portu umożliwia skonfigurowanie w sieci usług publicznych, takich jak serwery Web, FTP, e-mail i innych wyspecjalizowanych aplikacji internetowych.

UWAGA: Serwer wirtualny wykorzystuje znaną nazwę hosta i publiczny adres IP.

External Port (Port zewnętrzny): Numer zewnętrznego portu dla serwera lub aplikacji internetowej, na przykład, port 21 dla usługi FTP.

Internal Port (Port wewnętrzny):

Numer portu komputera LAN ustawiony przez router. Ruch internetowy z portu zewnętrznego będzie przekazywany do portu wewnętrznego.

Na przykład, wewnętrzny port NR 66 może pełnić funkcję zewnętrznego portu NR 21 dla usługi FTP.

IP Address (Adres IP): Wpisz adres IP komputera, na którym chcesz skonfigurować aplikację.

Protocol (Protokół): Wybierz protokół (TCP/UDP/Oba) dla aplikacji.

Well-Known Service Port (Port publicznej usługi): Wybierz publiczne usługi jak DNS, FTP z menu rozwijanego, aby dodać do skonfigurowanych powyżej.

Delete/Enable (Usuń/włącz): Kliknij, aby zaznaczyć dla danej operacji.

UWAGA: Po ustawieniu serwera wirtualnego portu usług jako 80, port zarządzania Web na stronie zdalnego zarządzania Web należy ustawić na dowolną wartość z wyjątkiem 80, np. 8080. W przeciwnym razie wystąpi konflikt powodujący dezaktywację serwera wirtualnego.

Single Port Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port	To IP Address	Protocol	Enable	Delete
1.	66 21	192.168.0.10	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) Add ID 1

Apply Cancel

Single Port Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port	To IP Address	Protocol	Enable	Delete
1.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
2.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) Add ID 1

Apply Cancel

Przekazywanie zakresu portów

Ten rozdział dotyczy przekazywania zakresu portów. Przekazywanie zakresu portów umożliwia skonfigurowanie w sieci zakresu usług publicznych, takich jak serwery Web, FTP, e-mail i innych wyspecjalizowanych aplikacji internetowych do przypisanego adresu IP w sieci LAN.

Start/End Port (Port początkowy/końcowy): Podaj początkowy/końcowy numer portu, określający zakres portów zewnętrznych używanych do konfiguracji serwera lub aplikacji internetowych.

IP Address (Adres IP):

Wpisz adres IP komputera, na którym chcesz skonfigurować aplikację.

Protocol (Protokół):

Wybierz protokół (TCP/UDP/Oba) dla aplikacji.

Well-Known Service Port (Port publicznej usługi): Wybierz publiczne usługi jak DNS, FTP z menu rozwijanego, aby dodać do skonfigurowanych powyżej.

Delete/Enable (Usuń/włącz): Kliknij, aby zaznaczyć dla danej operacji.

Port Range Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/> - <input type="text"/>	192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) ID 1

Ustawienia wyzwalania portu

Jeżeli klienci wewnętrzni mają dostęp do serwera zewnętrznego w Internecie dla wybranej aplikacji, klienci żądają połączenia z serwerami, a serwer żąda również połączenia z klientem. Jednak przy ustawieniu domyślnym, router odmawia przyjęcia żądań z sieci WAN, co powoduje zatrzymanie komunikacji. **Wyzwalanie portów** służy do definiowania zasad wyzwalania. Jeżeli klienci mają dostęp do serwera, urządzenie otwiera port przez który serwer wysłał żądania do klienta.

IP Range (Zakres IP): Wewnętrzny zakres adresów IP dla żądań zewnętrznych aplikacji serwerowych.

Trigger Port (Port wyzwalania): Zakres portów, przez które klienci wewnętrzni wysyłają ruch żądań do serwera zewnętrznego; zakres 1 – 65535. Uwaga – niski pierwszy numer i dwa puste mogą w razie potrzeby utrzymywać ten sam numer.

External Port (Port zewnętrzny): Zakres portów, przez które serwer zewnętrzny wysyła ruch żądań do klientów wewnętrznych; zakres 1 – 65535. Uwaga – niski pierwszy numer i dwa puste mogą w razie potrzeby utrzymywać ten sam numer.

Apply (Zastosuj): Włączenie lub wyłączenie zasady.

Add (Dodaj): Po zakończeniu edycji zasady kliknij przycisk „Add”, aby dodać bieżący wpis do listy wyzwalania portów.

Apply (Zastosuj): Kliknij „Apply”, aby aktywować bieżącą zasadę.

Cancel (Anuluj): Kliknij „Cancel” (Anuluj), aby porzucić wszystkie zmiany.

Można usuwać lub modyfikować wcześniejsze zasady na liście.

Uwaga: Aplikacja specjalna może być używana tylko na jednym komputerze. Jeżeli więcej niż jeden komputer będzie chciało otworzyć ten sam port wyzwalania, port zewnętrzny zostanie połączony z ostatnim komputerem.

Port Trigger Settings

Port Trigger ☒

IP Range	Trigger Port	External Port
192.168.0. - .	0 - 0	0 - 0

Protocol: TCP&UDP ☐

Num	IP	Trigger Port	External Port	Protocol	Apply	Edit	Del
-----	----	--------------	---------------	----------	-------	------	-----

Ustawienia usługi ALG

ALG (Application Layer Gateway – Brama warstwy aplikacji)

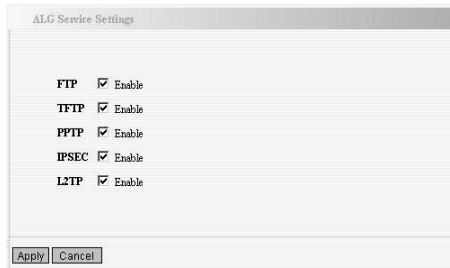
W kontekście sieci komputerowych, ALG lub brama warstwy aplikacji to element zabezpieczeń rozszerzający zapórę ogniową lub NAT wykorzystywany w sieci komputerowej. Umożliwia ona podłączanie spersonalizowanych filtrów NAT do bramy w celu obsługi tłumaczenia adresów oraz portów dla określonych protokołów „control/data” warstwy aplikacji, takich jak FTP, BitTorrent, SIP, RTSP, aplikacji do przesyłania plików itd.

Aby protokoły te mogły pracować przez NAT lub zapórę ogniową, aplikacja musi znać kombinację adresu/numeru portu umożliwiającą przesyłanie pakietów przychodzących lub NAT musi monitorować ruch i dynamicznie otwierać mapowanie portów (otwory w zaporze) na żądanie. Uprawnione dane aplikacji mogą wówczas przechodzić przez kontrole bezpieczeństwa zapory ogniowej i NAT, które w przeciwnym razie ograniczałyby ruch niespełniający kryteriów filtrowania.

Zazwyczaj aplikacje klientów mogą używać dynamicznych portów TCP/UDP do komunikacji z publicznymi portami wykorzystywanymi przez aplikacje serwera, chociaż konfiguracja zapory ogniowej może dopuszczać tylko określoną liczbę portów publicznych. W razie braku usługi ALG, porty byłyby blokowane lub administrator sieci musiałby jawnie otwierać dużą liczbę portów w zaporze, osłabiając bezpieczeństwo sieci i zwiększając ryzyko ataków na te porty.

Przy domyślnych ustawieniach ALG, następujące protokoły są włączone. **Zaleca się pozostawienie tych ustawień bez zmian.**

1. FTP
2. TFTP
3. PPTP
4. IPSec
5. L2TP

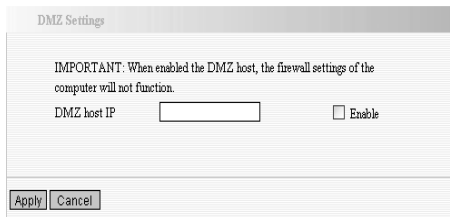


Ustawienia DMZ

Funkcja DMZ umożliwia ujawnienie w Internecie komputera w sieci na potrzeby usług specjalnych, takich jak gry internetowe lub wideokonferencje.

DMZ Host IP Address (Adres IP hosta DMZ): Adres IP komputera, który ma być ujawniony.


Enable (Włącz): Zaznacz pole wyboru, aby włączyć hosta DMZ. **WAŻNE:** Po włączeniu hosta DMZ, ustawienia zapory ogniowej dotyczące DMZ nie będą działać.



Ustawienia UPnP

Urządzenie obsługuje najnowszą technologię Universal Plug and Play. Funkcja ta działa w systemie Windows XP lub Windows ME oraz w systemach, w których zainstalowano oprogramowanie obsługujące UPnP. Dzięki funkcji UPnP, host w sieci LAN może wymagać od routera przetworzenia specjalnego przełączenia portów w celu umożliwienia hostowi zewnętrznemu przeglądanie zasobów hosta wewnętrznego.

Enable UPnP (Włącz UPnP): Zaznacz pole wyboru, aby włączyć UPnP.



Rozdział 9: Kontrola ruchu

Kontrola ruchu

Kontrola ruchu służy do ograniczania szybkości komunikacji w sieci LAN i WAN. Obsługiwanych jest do 20 pozycji ze zdolnością maks. szybkości 254 komputerów, obejmując konfigurację zakresu adresów IP.

Enable Traffic Control (Włącz kontrolę ruchu):

Włączanie lub wyłączanie kontroli szerokości pasma dla wewnętrznych adresów IP.

Interface (Interfejs): Ograniczanie szerokości pasma wysyłania i pobierania na porcie WAN.

Service (Serwis): Wybór typu kontrolowanej usługi, jak np. usługa HTTP.

IP Starting Address (Początkowy adres IP): Pierwszy adres IP do kontroli ruchu.

IP Ending Address (Końcowy adres IP): Ostatni adres IP do kontroli ruchu.

Uploading/Downloading (Wysyłanie/pobieranie): Określenie szybkości ruchu dla wybranego adresu IP: wysyłanie lub pobieranie.

Bandwidth (Szerokość pasma): Określenie min./maks. szybkości wysyłania/pobierania (KB/s), która nie może przekraczać prędkości WAN.

Apply (Zastosuj): Włączenie bieżącej zasady. W przeciwnym razie zasada będzie wyłączona.

Add (Dodaj): Po zakończeniu edycji zasady kliknij przycisk „Add”, aby dodać bieżącą zasadę do listy zasad.

Apply (Zastosuj): Kliknij „Save” (Zapisz), aby aktywować bieżącą zasadę.

Cancel (Anuluj): Kliknij „Cancel” (Anuluj), aby porzucić wszystkie zmiany.

Można usuwać lub modyfikować wcześniejsze zasady na liście.

Traffic Control Settings

Traffic Control ☒

Interface **Upload BW** **Download BW**

WAN: 512 2048 (KB/s, The bandwidth can not be zero)

Protocol Port Service

Services: TCP&UDP 0 All

IP: 192.168.0. ~

Up/Down: Up

BW Range: ~ (KB/s, The bandwidth can not be zero)

Apply: ☐

Add

Num	Port	IP	Up/Down	BW Range	Apply	Edit	Del
-----	------	----	---------	----------	-------	------	-----

Apply Cancel

Rozdział 10: Ustawienia zabezpieczeń

Ustawienia filtra klienta

Korzystając z dalszego zarządzania komputerami w sieci LAN, można kontrolować dostęp niektórych portów do Internetu za pomocą funkcji filtrowania pakietów danych.

Client Filter (Filtr klienta):

Zaznacz, aby włączyć filtrowanie klientów.

Access Policy (Polityka dostępu): Wybierz jedną z wartości z menu rozwijanego.

Enable (Włącz): Zaznacz, aby włączyć politykę dostępu.

Clear the Policy (Wyczyść politykę):

Kliknij „Clear”, aby skasować wszystkie ustawienia polityki.

Filter Mode (Tryb filtrowania):

Kliknij jeden z przycisków, aby włączyć lub wyłączyć dostęp do Internetu.

Policy Name (Nazwa polityki):

Wpisz nazwę wybranej polityki dostępu.

IP Start/End (Początkowy/końcowy IP):

Wpisz

początkowy/końcowy adres IP.

Port No. (Nr portu): Podaj zakres portów w oparciu o protokół dla polityki dostępu.

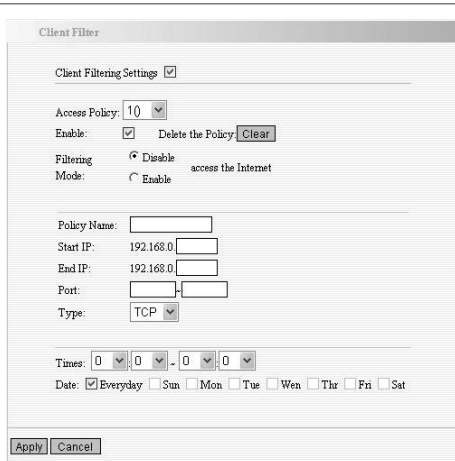
Protocol (Protokół):

Wybierz protokół (TCP/UDP/Oba) z menu rozwijanego.

Times (Czas):

Wybierz zakres czasu filtrowania klientów.

Days (Dni): Wybierz ilość dni, przez które polityka dostępu będzie aktywna.



Ustawienia filtrowania URL

Ustawienia służące do kontrolowania komputerów mających dostęp do stron internetowych. Można użyć filtrowania URL, aby komputer miał dostęp do określonych stron internetowych w określonym czasie i w celu blokowania dostępu do określonych stron internetowych w określonym czasie.

URL Filter (Filtr URL): Zaznacz, aby włączyć filtrowanie adresów URL.

Access Policy (Polityka dostępu): Wybierz jedną z wartości z menu rozwijanego.

Enable (Włącz):

Zaznacz, aby włączyć politykę dostępu.

Clear the Policy (Wyczyść politykę): Kliknij „Clear”, aby skasować wszystkie ustawienia polityki.

Filter Mode (Tryb filtrowania): Kliknij jeden z przycisków, aby włączyć lub wyłączyć dostęp do Internetu.

Policy Name (Nazwa polityki): Wpisz nazwę wybranej polityki dostępu.

Start/End IP (Początkowy/końcowy IP): Wpisz początkowy/końcowy adres IP.

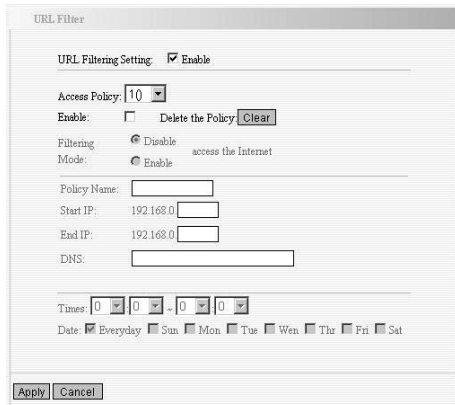
DNS:

Określ ciągi tekstu lub słowa kluczowe w DNS. Jeżeli część adresu URL zawiera te ciągi lub słowa, strona będzie niedostępna i nie będzie wyświetlana.

Times (Czas): Wybierz zakres czasu filtrowania klientów.

Days (Dni):

Wybierz ilość dni, przez które polityka dostępu będzie aktywna.



Ustawienia adresów MAC

W celu usprawnienia zarządzania komputerami w sieci LAN, można kontrolować dostęp komputerów do Internetu za pomocą filtrowania adresów MAC.

MAC Address Filter (Filtr adresów MAC):
Zaznacz, aby włączyć filtrowanie adresów MAC.

Access Policy (Polityka dostępu):
Wybierz jedną z wartości z menu rozwijanego.

Enable (Włącz): Zaznacz, aby włączyć politykę dostępu.

Clear the Policy (Wyczyść politykę):
Kliknij „Clear”, aby skasować wszystkie ustawienia polityki.

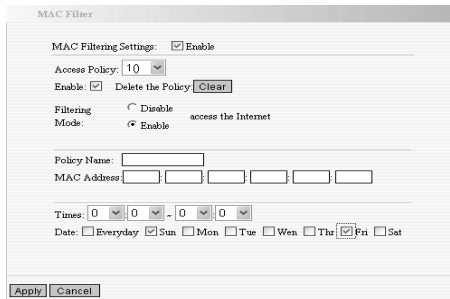
Filter Mode (Tryb filtrowania): Kliknij jeden z przycisków, aby włączyć lub wyłączyć dostęp do Internetu.

Policy Name (Nazwa polityki): Wpisz nazwę wybranej polityki dostępu.

MAC Address (Adres MAC): Wpisz adres MAC, dla którego ma być aktywna polityka dostępu.

Times (Czas): Wybierz zakres czasu filtrowania klientów.

Days (Dni): Wybierz ilość dni, przez które polityka dostępu będzie aktywna.



Zapobieganie atakom sieciowym

W tej części zawarte są ustawienia ochrony sieci wewnętrznej przed atakami zewnętrznymi, takimi jak SYN Flooding, Smurf, LAND itd. Po wykryciu nieznanego ataku, router automatycznie ogranicza szerokość pasma.

Adres IP urządzenia atakującego można znaleźć w dzienniku systemowym („System Log”).

Prevent Network Attack (Zapobiegaj atakom sieciowym):
Zaznacz, aby włączyć ochronę przed atakami.

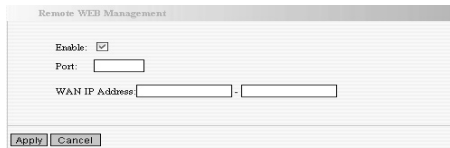


Zdalne zarządzanie Web

Ta sekcja umożliwia administratorowi sieci zdalne zarządzanie routerem. Aby uzyskać dostęp do routera spoza sieci lokalnej, wybierz opcję „Enable” (Włącz).

Enable (Włącz): Zaznacz, aby włączyć zdalne zarządzanie Web.
Port (Port): Port zarządzania otwarty dla dostępu zewnętrznego. Wartość domyślna to 80.

WAN IP Address (Adres IP sieci WAN): Określ zakres adresów IP sieci WAN do zarządzania zdalnego.

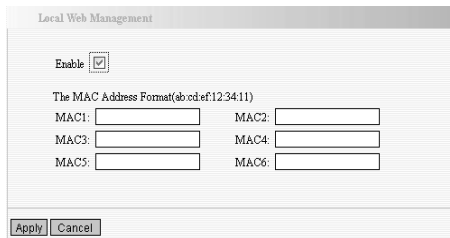


Lokalne zarządzanie Web

Lokalne zarządzanie Web, alternatywa dla zdalnego zarządzania Web, umożliwiająca administratorowi sieci zarządzanie routerem w sieci LAN. Domyślnie wszystkie komputery w sieci LAN mogą uzyskać dostęp do narzędzia zarządzającego Web. Można wpisać określony adres MAC komputera w sieci LAN.

Enable (Włącz):
Zaznacz, aby włączyć lokalne zarządzanie Web.

MAC1/2/3...:
Wpisz adresy MAC komputerów w sieci LAN.



Ping WAN

Test polecenia ping, sprawdzający stan połączenia internetowego. Po wyłączeniu testu system będzie ignorować test polecenia ping z sieci WAN.

Disable the Ping for WAN (Wyłącz Ping dla sieci WAN): Zaznacz, aby włączyć opcję.

WAN Ping

Disable the Ping for WAN ☒

Apply Cancel

Rozdział 11: Ustawienia routingu

Tabela routingu

Głównym obowiązkiem routera jest wyszukiwanie najlepszej ścieżki dla każdej ramki danych oraz przesyłanie tej ramki do miejsca docelowego. Dlatego też dla routera ważne jest wybranie najlepszej ścieżki, tzn. arytmetyka routingu. Na potrzeby tej funkcji, w routerze zapisywanych jest wiele ścieżek transferowych (tabela routingu), wybieranych w razie potrzeby.

Routing Table

Destination IP	Subnet Mask	Gateway	Metric	Interface
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.100	0	eth2.2

Refresh

Trasa statyczna

Trasa statyczna jest ustawiana z góry przez administratora. Zazwyczaj jest ona zapisywana w konfiguracji sieciowej podczas instalacji systemu operacyjnego. Nie trzeba jej zmieniać w przypadku zmiany struktury sieci.

Destination LAN IP (Docelowy IP w sieci LAN): Adres zdalnego hosta, który ma tworzyć trasę statyczną.

Subnet Mask (Maska podsieci):

Udział sieciowy docelowego IP w sieci LAN.

Gateway (Brama): Brama następnego odcinka.

Static Routing

Destination LAN IP	Subnet Mask	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add

Rozdział 12: Narzędzia systemowe

Czas

W tej sekcji można wybrać strefę czasową danej lokalizacji. Po wyłączeniu routera, ustawienia czasu znikają. Router pobierze jednak czas GMT automatycznie po uzyskaniu dostępu do Internetu.

Time Zone (Strefa czasowa): Wybierz strefę czasową z menu rozwijanego.

Customized time (Czas użytkownika): Wpisz czas spersonalizowany.

Time Settings

Time Zone:
(GMT+08:00)Beijing,China,Hong Kong,Singapore,Taipei

(Notice: GMT time can be obtained only after accessing to the Internet.)

Customized time: ☐

: : : : :

Apply Cancel

DDNS


Router obsługuje funkcję **DDNS (Dynamic Domain Name System – Dynamiczny system nazw domenowych)**. Służy ona do przypisywania stałego hosta i nazwy domeny do dynamicznego adresu IP, używanego do monitorowania hostingu stron internetowych, serwerów FTP i in. za routerem. Aby aktywować tę funkcję, wybierz „Enable” (Włącz) i usługodawcę DDNS do zarejestrowania.

DDNS: Naciśnij przycisk, aby włączyć lub wyłączyć usługę DDNS.
Service Provider (Usługodawca): Wybierz pozycję z listy rozwijanej i naciśnij „Sign up”, aby zarejestrować usługę.

User Name (Nazwa użytkownika): Wpisz nazwę użytkownika, zgodną z nazwą rejestracji.

Password (Hasło): Wpisz ustawione hasło.

Domain Name (Nazwa domeny): Wpisz nazwę domeny (opcjonalne).



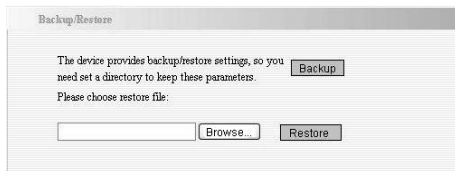
Kopia zapasowa/przywracanie

Urządzenie jest wyposażone w funkcję tworzenia kopii zapasowej/przywracania ustawień. Należy ustawić folder, aby zachować parametry.

Backup (Kopia zapasowa): Kliknij ten przycisk, aby wykonać kopię zapasową konfiguracji routera.

Browse (Przeglądaj): Kliknij ten przycisk, aby wyszukać folder, w którym ma być utworzona kopia.

Restore (Przywróć): Kliknij ten przycisk, aby przywrócić konfigurację routera.



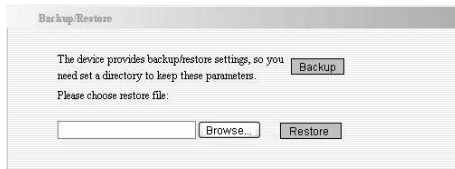
Aktualizacja oprogramowania

Router jest wyposażony w funkcję aktualizacji oprogramowania sprzętowego. Należy najpierw wyszukać pakiet aktualizacji, a następnie kliknąć przycisk „Upgrade” (Aktualizuj). Pakiety można pobrać ze strony internetowej www.tenda.cn. Po zakończeniu aktualizacji następuje automatyczne uruchomienie ponowne routera.

Browse (Przeglądaj): Kliknij ten przycisk, aby wyszukać folder, w którym zapisano pliki aktualizacji.

Upgrade (Aktualizuj): Kliknij ten przycisk, aby rozpocząć aktualizację.

WAŻNE: Nie wyłączaj systemu podczas aktualizacji oprogramowania, aby uniknąć uszkodzenia urządzenia. Router uruchomi się ponownie po zakończeniu aktualizacji.



Przywracanie domyślnych ustawień fabrycznych

Ten przycisk służy do resetowania wszystkich ustawień konfiguracji do wartości domyślnych. Oznacza to, że zostaną utracone wszystkie ustawione opcje. W razie potrzeby zaleca się zapisanie odpowiednich ustawień.

Restore to Factory Default Settings (Przywróć domyślne ustawienia fabryczne): Kliknij ten przycisk, aby przywrócić domyślne ustawienia fabryczne.


Ustawienia fabryczne:

User Name (Nazwa użytkownika): **admin**

Password (Hasło): **admin**

IP Address (Adres IP): **192.168.0.1**

Subnet Mask (Maska podsieci): **255.255.255.0**

 **UWAGA:** Po przywróceniu domyślnych ustawień należy ponownie uruchomić urządzenie, aby ustawienia te zostały zastosowane.

Restore to Factory Default Settings

Restore to Factory Default Settings.

Uruchamianie ponowne

Ponowne ustawienie routera powoduje aktywację skonfigurowanych ustawień lub ponowne ustawienie routera w razie awarii routera.

Reboot the router (Uruchom router ponownie): Kliknij ten przycisk, aby zresetować urządzenie.

Reboot

Click here to reboot the router.

Zmiana hasła


W tej sekcji można ustawić nową nazwę użytkownika i hasło w celu lepszego zabezpieczenia routera i sieci. Nowe hasło musi się składać z mniej niż 14 znaków.

User Name (Nazwa użytkownika): Wpisz nową nazwę użytkownika urządzenia.

Old Password (Stare hasło): Wpisz stare hasło.

New Password (Nowe hasło): Wpisz nowe hasło.

Re-enter to Confirm (Wpisz ponownie, aby zatwierdzić): Wpisz ponownie, aby potwierdzić nowe hasło.

 **UWAGA:** Zaleca się zmianę hasła w celu zabezpieczenia sieci i routera.

Change Password

Note: User Name and Password makeup only by number or land letter.

User Name

Old Password

New Password

Re-enter to Confirm

Dziennik systemowy

W tej części można obejrzeć dziennik systemowy. Kliknij „Refresh” (Odśwież), aby zaktualizować dziennik. Kliknij „Clear” (Wyczyść), aby kasować wszystkie informacje. Jeżeli dziennik zawiera powyżej 150 rekordów, są one kasowane automatycznie.

Refresh (Odśwież): Kliknij ten przycisk, aby zaktualizować dziennik.

Clear (Wyczyść): Kliknij ten przycisk, aby kasować wyświetlany dziennik.

System Log

Page 1 content

1	2000-01-01 00:00:09	DHCP	Send discover
2	2000-01-01 00:00:12	DHCP	Send discover
3	2000-01-01 00:00:15	DHCP	Send discover
4	2000-01-01 00:00:21	System	system start.
5	2000-01-01 00:01:18	DHCP	Send discover
6	2000-01-01 00:01:21	DHCP	Send discover
7	2000-01-01 00:01:24	DHCP	Send discover
8	2000-01-01 00:00:09	DHCP	Send discover
9	2000-01-01 00:00:12	DHCP	Send discover
10	2000-01-01 00:00:15	DHCP	Send discover

[1] [2] [3]

Załącznik A: Właściwości produktu

- Połączenie routera, bezprzewodowego punktu dostępowego, przełącznika 4-portowego i zapory ogniowej w jednym urządzeniu
- Zgodność ze standardami IEEE802.11n, IEEE802.11b i IEEE802.11g
- Technologia MIMO wykorzystuje sygnał odbity, ośmiokrotnie zwiększając zasięg transmisji standard 802.11g i redukując liczbę martwych punktów w obszarze zasięgu łączności bezprzewodowej
- Szybkość odbioru 300 Mbps, szybkość wysyłania 300 Mbps
- Obsługa formatu WMM, generującego płynny dźwięk i obraz wideo
- Obsługa metod szyfrowania WEP 64/128-bitowy, WPA, WPA2 i uwierzytelniania 802.1x
- Obsługa szyfrowania WPS (PBC i PIN), umożliwiające korzystanie z krótkich haseł
- Zdalne/lokalne zarządzanie oparte na technologii sieci Web
- Obsługa technologii roamingu bezprzewodowego, zapewniającej tworzenie bardzo wydajnych połączeń bezprzewodowych
- Obsługa trybu ukrycia SSID i kontroli dostępu adresów
- Obsługa Auto MDI/MDIX
- Dziennik systemowy, śledzący status routera
- Obsługa filtrowania adresów MAC, NAT, NAPT
- Obsługa UPnP i DDNS
- Obsługa kontroli dostępu dla 30 adresów MAC
- Obsługa funkcji serwera/klienta DHCP
- Obsługa SNTP
- Obsługa funkcji serwera wirtualnego i hosta DMZ
- Automatyczny wybór kanału sieci bezprzewodowej
- Obsługa funkcji WDS (bezprzewodowy system dystrybucji)

Contents

CHAPTER 1: INTRODUCTION	35
Package Contents.....	35
CHAPTER 2: GETTING TO KNOW THE WIRELESS-N BROADBAND ROUTER	35
The Rear Panel.....	35
The Front Panel	36
Hardware Installation	37
CHAPTER 3: GETTING TO CONNECT THE WIRELESS-N BROADBAND ROUTER.....	38
How to Set the Network Configurations for My Computer	38
How to Check the Network Connection	39
CHAPTER 4: BASIC CONFIGURATIONS	39
How to Access the Web-based Configuration Utility	39
Setup Wizard	40
CHAPTER 5: ADVANCED SETTINGS	42
LAN Settings	42
WAN Settings—PPPoE	43
WAN Settings—Static IP	43
WAN Settings—L2TP	43
WAN Settings—PPTP	44
MAC Address Clone.....	44
DNS Settings	44
CHAPTER 6: WIRELESS SETTINGS	45
Wireless Mode	45
Basic Settings.....	46
Wireless Security Settings	46
WEP	46
WPA-Personal	47
WPA2-Personal	47
WPA-Enterprise	48
WPA2-Enterprise	48
WPS	49
WDS	50
Advanced Wireless Settings	51
Wireless Access Control	51
Wireless Connection Status.....	52
CHAPTER 7: DHCP SERVER	52
DHCP Server List.....	52
CHAPTER 8: VIRTUAL SERVER.....	53
Single Port Forwarding	53
Port Range Forwarding.....	54
Port Trigger	54
ALG Service.....	55
DMZ Settings	55
UPnP Settings.....	55

CHAPTER 9: TRAFFIC CONTROL.....	56
Traffic Control	56
CHAPTER 10: SECURITY SETTINGS.....	57
Client Filter Settings.....	57
URL Filter Settings.....	57
MAC Address Settings.....	58
Prevent Network Attack.....	58
Remote Web Management.....	58
Local Web Management.....	58
Wan Ping	59
CHAPTER 11: ROUTING SETTINGS.....	59
Routing Table	59
Static Route	59
CHAPTER 12: SYSTEM TOOLS.....	59
Time	59
DDNS.....	60
Backup/Restore	60
Firmware Upgrade	60
Restore to Factory Default Settings	61
Reboot	61
Change Password.....	61
System Log	61
APPENDIX A: PRODUCT FEATURES.....	62

Chapter 1: Introduction

Thank you for choosing the W306R Wireless-N Broadband Router. It employs the advanced MIMO (Multi Input, Multi Output) technology and integrates router, wireless access point, four-port switch and firewall in one, which will allow you to share Internet access over the four switched ports or via the wireless broadcast. Compatible with IEEE 802.11n (Draft 2.0) standard, it can connect with existing 802.11b/g PCI, USB and Notebook adapters. Up to 300Mbps transmission rate allows you to enjoy real-time activities such as video streaming, online gaming and so on.

Besides, the Wireless-N Broadband Router supports all of the latest wireless security features, such as 64/128-bit WEP encryption, WPS (PBC and PIN) encryption method, packet filtering and port forwarding, to prevent unauthorized access and protect your network against malicious attack.

Moreover, the user-friendly Setup Wizard on the CD-ROM can assist you to set up the Wireless-N Broadband Router easily. It also can be managed or configured through Local/Remote easy-to-use Web-based utility. So it is the best choice for SOHOs and small-sized enterprises.

Package Contents

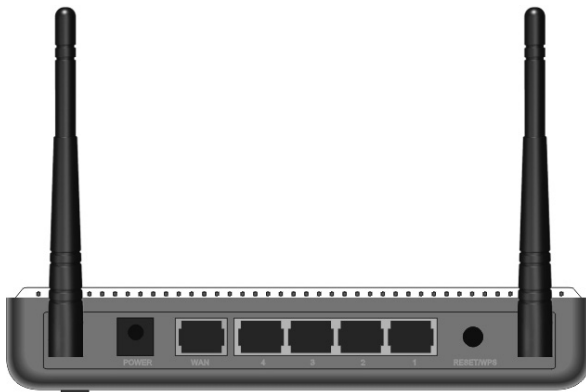
- One W306R Wireless-N Broadband Router
- One Ethernet Network Cable
- One Quick Installation Guide
- One Power Adapter
- One CD-ROM

If any of listed items are missing or damaged, please contact the Tenda reseller from whom you purchased for replacement immediately.

Chapter 2: Getting to Know the Wireless-N Broadband Router

The Rear Panel

Here is the description of the back panel. The RJ-45 ports for cable connection and Reset button are located on the back panel as shown below.



Połączenia:

Rear Panel Interface	Description
1-4 (LAN Ports)	Connect to Ethernet devices (such as computers, switches, hubs).
RESET/WPS	Note: After pressing the RESET button for 7 seconds, the configurations you have set will be deleted and the device will restore to the factory default settings. If you press this button for 1 second, the WPS (PBC) function is enabled.
WAN	Connect to DSL Modem, Cable Modem or community broadband
POWER	Receptor for the supplied power adapter.

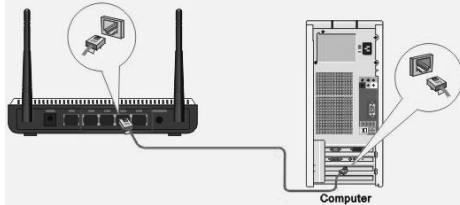
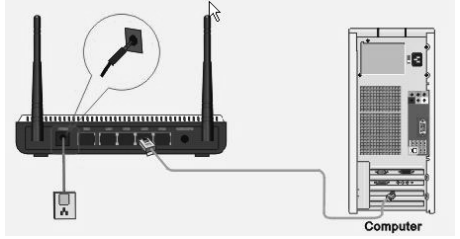
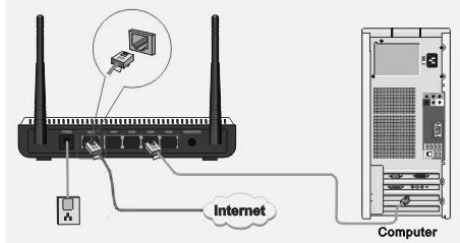
The Top Panel

There are the Router's LED indicators on the top panel as shown below.

Diody LED:

LED Indicator	Status	Description
POWER	Always ON	The POWER indicator is Always ON when it is powered on and works properly.
SYS	Blinking	The SYS is blinking regularly when the system works normally.
WAN	Always ON	Indicates the correct connection of the WAN ports.
	Blinking	Indicates the Router is transmitting/receiving data packets.
WLAN	Blinking	Indicates the wireless signal is OK.
LAN(1/2/3/4)	Always ON	Indicates the correct connection of the LAN ports.
	Blinking	Indicates the Router is transmitting/receiving data packets.
WPS	Blinking	Indicates the Router is negotiating with WPS clients in WPS Mode (PBC or PIN Code).

Hardware Installation

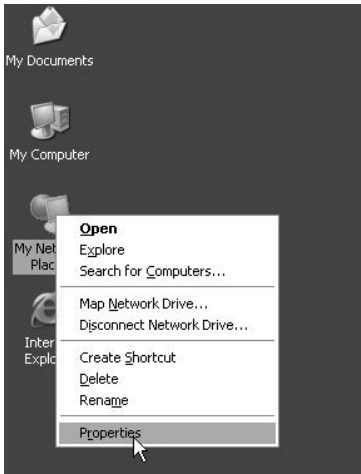
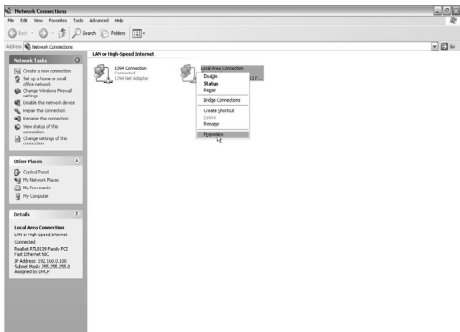
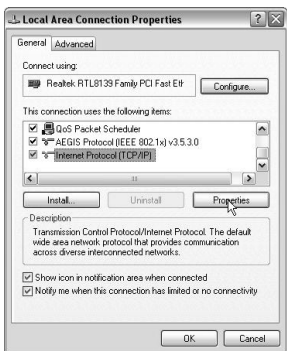
<p>1. Please connect the LAN port of the router to the network adapter of your computer with one cable.</p>	
<p>2. Please use the delivery-attached power adapter to power the router.</p>	
<p>3. Please connect your broadband line provided by your ISP to the WAN port of your router.</p>	

IMPORTANT: Please use the included power adapter. Use of a different power adapter could cause damage and void the warranty for this product.


Chapter 3: Getting to Connect the Wireless-N Broadband Router

For easy and fast configuration, the following steps for network configuration are required.

How to Set the Network Configurations for My Computer

<p>Right click "My Network Places" and select "Properties".</p>	
<p>Right click "Local Area Network Connection" and select "Properties".</p>	
<p>Select "Internet Protocol (TCP/IP)" and click "Properties".</p>	

Or select **“Use the following IP address”** and enter the IP address, Subnet mask, Default gateway as shown right. Of course, you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click **“OK”** to save the configurations.



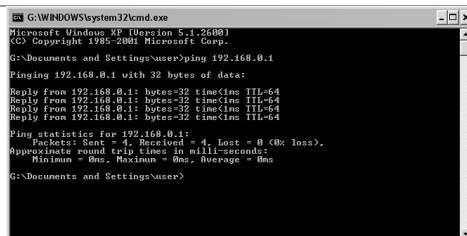
The dialog box shows the 'General' tab for Internet Protocol (TCP/IP) Properties. It has two main sections. The first section is for IP address settings, with 'Obtain an IP address automatically' unselected and 'Use the following IP address:' selected. The IP address is 192.168.0.2, Subnet mask is 255.255.255.0, and Default gateway is 192.168.0.1. The second section is for DNS server settings, with 'Obtain DNS server address automatically' unselected and 'Use the following DNS server addresses:' selected. The Preferred DNS server is 192.168.0.1, and the Alternate DNS server is blank. There are 'Advanced...', 'OK', and 'Cancel' buttons at the bottom.

How to Check the Network Connection

Select **“Start” — “Programs” — “Accessories” — “Command Prompt”**.

Input the **“ping 192.168.0.1”** and press **“Enter”**. If the screen displays as the right figure, it means your PC is connected to your router successfully.

If not, please make sure the hardware installation and network adapter are OK. After all preparations are made, please proceed to Chapter 4 for more and advanced configuration.



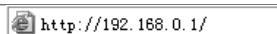
```
G:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2004 Microsoft Corp.
G:\Documents and Settings\User>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
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
G:\Documents and Settings\User>
```

Chapter 4 Basic Configurations

This section is to show you how to configure your new Wireless-N Broadband Router through the Web-based Configuration Utility.

How to Access the Web-based Configuration Utility

To access the Router’s Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter the Router’s default IP address, <http://192.168.0.1>. Press **“Enter”**.

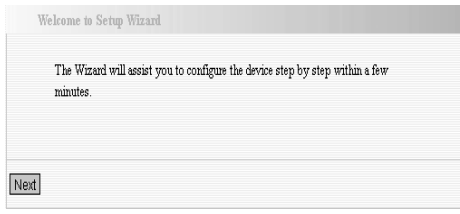
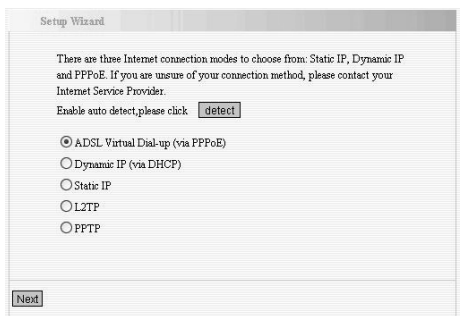
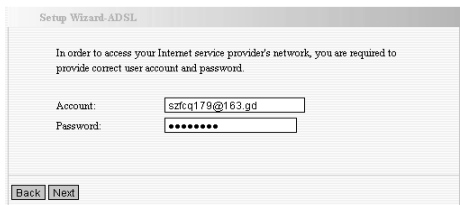
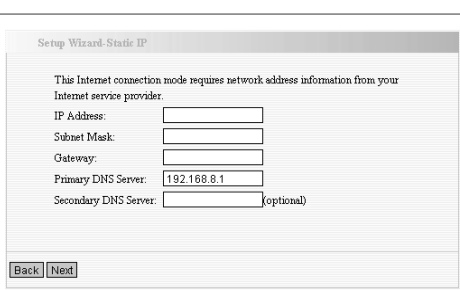


Please input the **“admin”** in both User Name and Password. Click **“OK”**.



The dialog box is titled 'Connect to 192.168.0.1'. It shows a key icon and the text '300M Wireless-N Broadband Router'. There are two input fields: 'User name:' with 'admin' entered and 'Password:' with '*****' entered. There is a checkbox labeled 'Remember my password' which is checked. There are 'OK' and 'Cancel' buttons at the bottom.

Setup Wizard

<p>Here is the “Welcome to Setup Wizard” for configuring your Router quickly. Click “Next”.</p>	
<p>In this screen, select one mode of your Internet connection you use. If you are not clear, press the “Detect” button or contact your Internet Service Provider, and click “Next”.</p>	
<p>Connection Mode 1: ADSL Virtual Dial-up (Via PPPoE)</p> <p>Enter the Account and Password provided by your ISP, and click “Next”.</p> <p>Connection Mode 2: Dynamic IP (Via DHCP)</p> <p>If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like Mode 2 or Mode 3.</p>	
<p>Connection Mode 3: Static IP</p> <p>In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click “Next”.</p>	

Connection Mode 4: L2TP

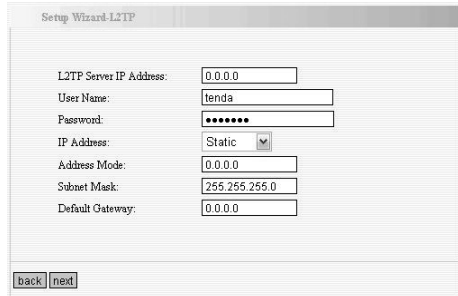
Select L2TP (Layer 2 Tunneling Protocol) if your ISP use a L2TP connection, your ISP will provide you with a username and password, please fill in the parameters.

L2TP provides two access modes.

If the L2TP offered by your ISP is Dynamic IP: Please select Dynamic IP.

If the L2TP offered by your ISP is Static IP: Please fill in the parameters provided by your ISP.

After configuration, please click **"Next"**.



Connection Mode 5: PPTP

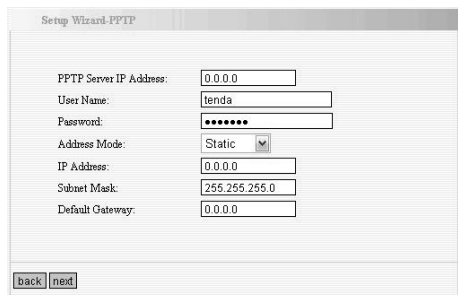
If the connection is **"PPP Tunneling Protocol"**, please input the following parameters provided by your ISP: Server IP Address, User Name, and Password.

PPTP provides two access modes.

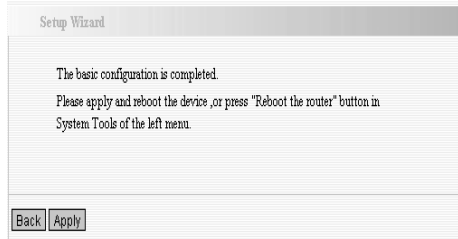
If the PPTP offered by your ISP is Dynamic IP: Please select Dynamic IP.

If the PPTP offered by your ISP is Static IP: Please fill in the parameters provided by your ISP.

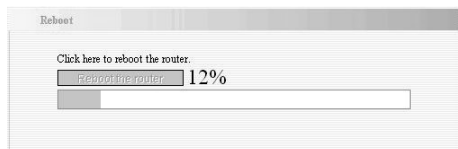
After configuration, please click **"Next"**.



Click **"Apply"**, select **"Reboot"** in System Tools of the left menu and press the **"Reboot the router"** button.



It is rebooting now, please wait for a few minutes and DO NOT power off it.



Click the **"System Status"** in the left menu of the Web-based Utility to find out the current network and system information. If the **"Connection Status"** is **"Connected"**, Congratulations you on completing the Router's basic settings. You are on the Internet now. If you want to configure more, please proceed to the following explanations for Advanced Settings.

Network Status	
Connection Status	Connected
WAN IP	218.18.40.67
Subnet Mask	255.255.255.255
Gateway	218.17.71.1
Primary DNS Server	202.96.128.166
Secondary DNS Server	202.96.134.133
Connection Mode	PPPoE
Connection Timer	00:03:10
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	

Chapter 5: Advanced Settings

This section is to conduct the advanced configurations for the Router, including LAN Settings, WAN settings, MAC Address Clone and DNS Settings.

LAN Settings

MAC Address: The Router's physical MAC address as seen on your local network, which is unchangeable.

IP Address: The Router's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.0.1 is the default value.

Subnet Mask: It's shown the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value.

LAN Settings	
This is to configure the basic parameters for LAN ports.	
MAC Address	00:0C:41:86:0A:B2
IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WAN Settings—PPPoE

Connection Mode: Show your current connection mode.

Account: Enter them provided by your ISP.

Password: Enter them provided by your ISP.

MTU: Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1492. Do NOT modify it unless necessary.

Service Name: It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.

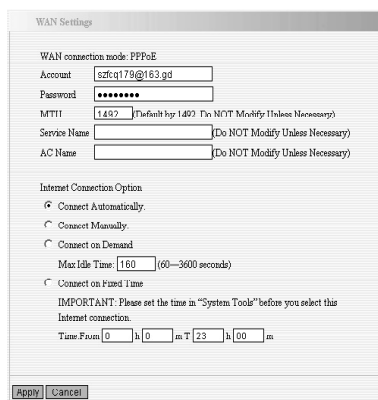
AC Name: Enter it if provided. Do NOT modify it unless necessary.

Connect Automatically: Connect automatically to the Internet after reboot

Connect Manually: Connect to the Internet by the user manually.

Connect on Demand: Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.

Connect on Fixed Time: Connect to the Internet during the time you fix.



WAN Settings

WAN connection mode: PPPoE

Account: szf:q179@163.gd

Password: *****

MTU: 1492 (Default by 1492 (Do NOT Modify Unless Necessary))

Service Name: (Do NOT Modify Unless Necessary)

AC Name: (Do NOT Modify Unless Necessary)

Internet Connection Option:

☒ Connect Automatically.

☐ Connect Manually.

☐ Connect on Demand

Max Idle Time: 160 (60—3600 seconds)

☐ Connect on Fixed Time

IMPORTANT: Please set the time in "System Tools" before you select this Internet connection.

Time From: 0 h 0 m T 23 h 00 m

Apply Cancel

WAN Settings—Static IP

If your connection mode, static IP is chosen, please enter the following addressing information.

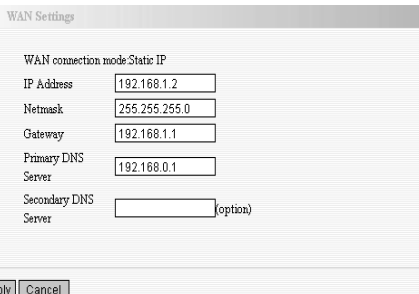
IP Address: Here enter the WAN IP address provided by your ISP.

Subnet Mask: Enter the WAN Subnet Mask here.

Gateway: Enter the WAN Gateway here.

Primary DNS Server: Enter the Primary DNS server provided by your ISP.

Secondary DNS Server: Enter the secondary DNS



WAN Settings

WAN connection mode: Static IP

IP Address: 192.168.1.2

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS Server: 192.168.0.1

Secondary DNS Server: (option)

Apply Cancel

WAN Settings—L2TP

L2TP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter L2TP username.

Password: Enter L2TP password.

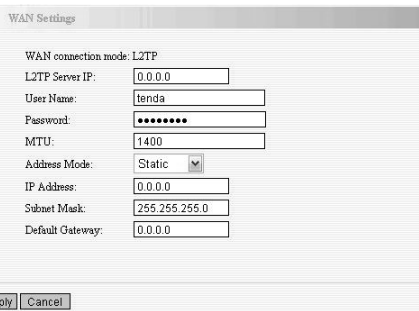
MTU: Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1400 is the default MTU.

Address Mode: Select "Static" if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the L2TP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.



WAN Settings

WAN connection mode: L2TP

L2TP Server IP: 0.0.0.0

User Name: tenda

Password: *****

MTU: 1400

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

WAN Settings—PPTP

PPTP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter PPTP username provided by your ISP.

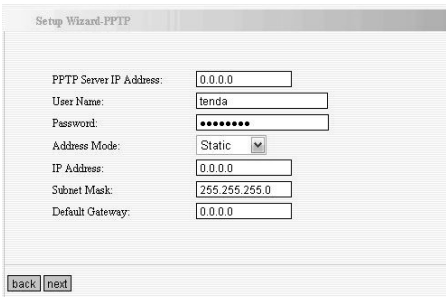
Password: Enter PPTP password provided by your ISP.

Address Mode: Select "Static" if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the PPTP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.



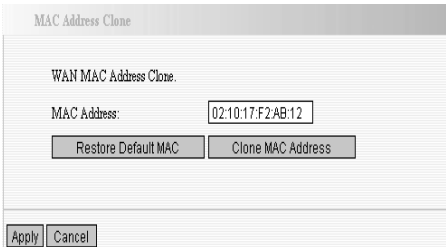
MAC Address Clone

Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

MAC Address: The MAC address to be registered with your Internet service provider.

Clone MAC address: Register your PC's MAC address.

Restore default MAC address: Restore the default hardware MAC address.



DNS Settings

DNS is short for Domain Name System(or Service), an Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.

DNS:

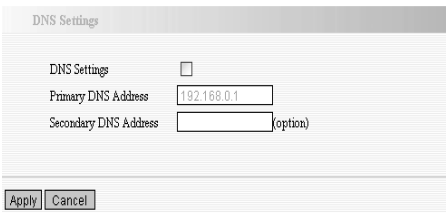
Click the checkbox to enable the DNS server.

Primary DNS Address:

Enter the necessary address provided by your ISP.

Secondary DNS Address:

Enter the second address if your ISP provides, which is optional.



Chapter 6: Wireless Settings

This section mainly deals with the wireless settings, including Basic Settings, Security Setting, Access Control and Advanced Settings.

Wireless Mode

AP Mode: router serves as an access point in this mode to be connected. The work stations around will be connected with router by SSID to share the Internet resources. To configure the AP mode, open the Basic Setting and Security Setting windows in the Wireless Setting folder.

Station Mode: In this mode, router is used as a work station to be connected with an AP by scanning the AP's SSID and provides the security authentication. Generally speaking, AP mode is passive to be connected with work station, but Station mode always takes the initiative in connecting with AP.

SSID: SSID is the unique ID name of access point. The wireless work station must keep the same SSID name with the AP's for connections. By enabling Open Scanning button, the device can search available APs.

MAC: To connect certain AP, you need to know the AP's MAC address. By enabling Open Scanning button to find out the available AP's MAC address.

Channel: You can use the channel same as the AP. By enabling Open Scanning button to find out the available AP's channel.

Security Mode: router provides the following security authentication methods:

(1) **WEP:** selects ASCII format (5 or 13 ASCII characters except illegal characters,) or Hex format (10 or 26 Hex characters).

(2) **WPA/WPA2-personal (PSK)** is safer than other encryption methods because the key is subject to change all the time. WPA-PSK/WPA2-PSK utilizes the TKIP or AES encryption algorithm.

WEP Mode: The shared key requires the same WEP keys between the access point and work station.

Default KEY: After entering the WEP keys, select one key as the default one, for example, Key 1

KEY Format: AASCII: Enter 13 characters with case sensitive („a-z“, „A-Z“ and „0-9“). Hex: enter 26 Hex characters („A-F“, „a-f“ and „0-9“).

KEY 1: If the KEY 1 is selected as default key, the key will be enabled.

KEY 2: If the KEY 2 is selected as default key, the key will be enabled.

KEY 3: If the KEY 3 is selected as default key, the key will be enabled.

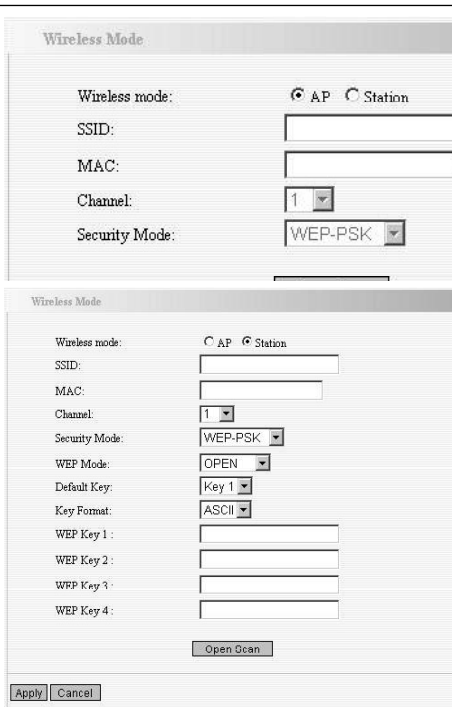
KEY 4: If the KEY 4 is selected as default key, the key will be enabled.

WPA/WPA2 Algorithm: When the WPA-PSK /WPA2-PSK authentication is selected, you can select one from two: TKIP and AES. For example, if the wireless provider selects TKIP, the wireless receiver (client) also needs to select TKIP for this authentication way.

Password: When WPA-PSK /WPA2-PSK authentication type is selected, enter the access password provided by AP users here.

Apply: Click “Apply” to make the settings go into effect.

Cancel: Click “Cancel” to throw all setting saved last time.



The image shows two screenshots of the 'Wireless Mode' configuration window. The top screenshot shows the 'AP' mode selected, with fields for SSID, MAC, Channel (set to 1), and Security Mode (set to WEP-PSK). The bottom screenshot shows the 'Station' mode selected, with fields for SSID, MAC, Channel (set to 1), Security Mode (set to WEP-PSK), WEP Mode (set to OPEN), Default Key (set to Key 1), Key Format (set to ASCII), and four WEP Key fields (Key 1 to Key 4). An 'Open Scan' button is visible in the bottom screenshot. At the bottom of the bottom screenshot are 'Apply' and 'Cancel' buttons.

Basic Settings

Network Mode: Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.

Main SSID: Main Service Set Identifier. It's the „name“ of your wireless network.

Minor SSID: Minor Service Set Identifier. It is optional.

Broadcast (SSID): Select "enable" to enable the device's SSID to be visible by wireless clients.

BSSID: It is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP

Channel: From the drop-menu, it is for selecting the working channels of the wireless network. Please select from 1 to 13, or select AutoSelect to select different channels.

Channel Bandwidth: Select wireless work frequency 20M or 20/40M.

HT TxStream: RF Transmit Stream.

HT RxStream: RF Receive Stream.



Basic Settings

Network Mode: 11b/g/n mixed mode

Main SSID: Tenda

Minor SSID: guest

Broadcast(SSID): ☒ Enable ☐ Disable

BSSID: 00:0C:41:86:0A:B2

Channel: 2437MHz (Channel 6)

Operating Mode: ☒ Mixed Mode ☐ Green Field

Channel Bandwidth: ☐ 20 ☒ 20/40

Guard Interval: ☐ long ☒ Auto

MCS: Auto

Reverse Direction Grant(RDG): ☐ Disable ☒ Enable

Extension Channel: 2457MHz (Channel 10)

Aggregation MSDU (A-MSDU): ☒ Disable ☐ Enable

HT TxStream: 2

HT RxStream: 2

Save Cancel

Wireless Security Settings

This page is to configure the wireless security of your Router. Six wireless security modes, WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise and RADIUS, are supported. If you do not want to use wireless security, select Disable from the drop-down menu.

1.Mixed WEP

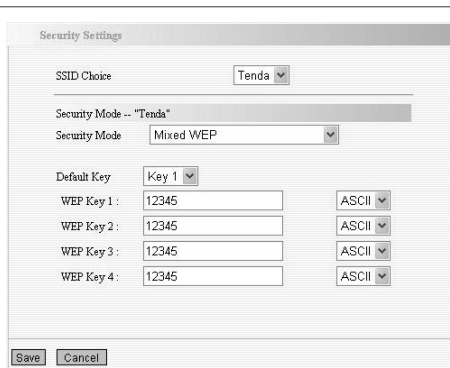
WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources.

SSID Choice: Select SSID to be configured security. The device supports to configure different security classes between the main SSID and the subordinate SSID.

Security Mode: There are several different security modes; you can choose one from mixed WEP, WPA-Personal, WPA-Enterprise, etc.

Default Key: Select a valid encryption key.

WEP Key 1, 2, 3, 4: Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be ASCII Characters or Hexadecimal Digits



Security Settings

SSID Choice: Tenda

Security Mode -- "Tenda"

Security Mode: Mixed WEP

Default Key: Key 1

WEP Key 1: 12345 ASCII

WEP Key 2: 12345 ASCII

WEP Key 3: 12345 ASCII

WEP Key 4: 12345 ASCII

Save Cancel

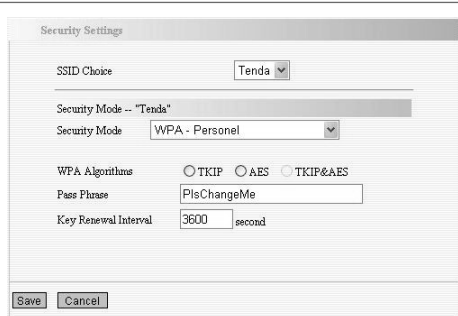
2. WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.

WPA Algorithms: Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

Pass Phrase: Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval: Enter the key renewal period. It is to tell the Router how often to change the keys.



The screenshot shows the 'Security Settings' page. At the top, 'SSID Choice' is set to 'Tenda'. Below it, 'Security Mode -- "Tenda"' is selected. The 'Security Mode' dropdown is set to 'WPA - Personal'. Under 'WPA Algorithms', the radio buttons for 'TKIP', 'AES', and 'TKIP&AES' are visible, with 'AES' being the selected option. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Save' and 'Cancel' buttons.

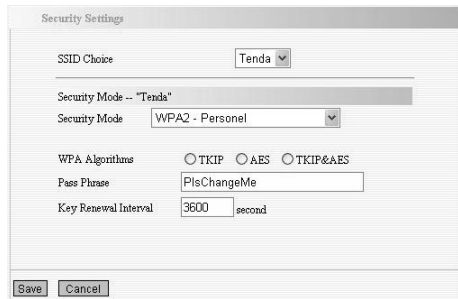
3. WPA2-Personal

WPA2 (Wi-Fi Protected Access version 2), It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.

WPA Algorithms: Select key Algorithms such as TKIP, AES and TKIP&AES.

Pass Phrase: Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval: Enter the key renewal period. It is to tell the Router how often to change the keys.



The screenshot shows the 'Security Settings' page. At the top, 'SSID Choice' is set to 'Tenda'. Below it, 'Security Mode -- "Tenda"' is selected. The 'Security Mode' dropdown is set to 'WPA2 - Personal'. Under 'WPA Algorithms', the radio buttons for 'TKIP', 'AES', and 'TKIP&AES' are visible, with 'AES' being the selected option. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Save' and 'Cancel' buttons.

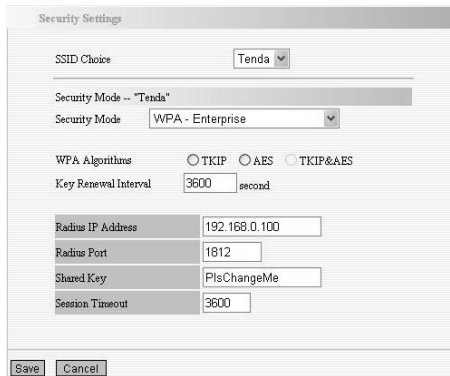
4. WPA-Enterprise

This Authentication protocol based on RADIUS server. This security mode is used when a RADIUS server is connected to the Router.
Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.



The screenshot shows the 'Security Settings' window with the following configuration:

- SSID Choice: Tenda
- Security Mode -- "Tenda": WPA - Enterprise
- WPA Algorithms: ☐ TKIP ☐ AES ☐ TKIP&AES
- Key Renewal Interval: 3600 second
- Radius IP Address: 192.168.0.100
- Radius Port: 1812
- Shared Key: PlsChangeMe
- Session Timeout: 3600

Buttons: Save, Cancel

5. WPA2-Enterprise

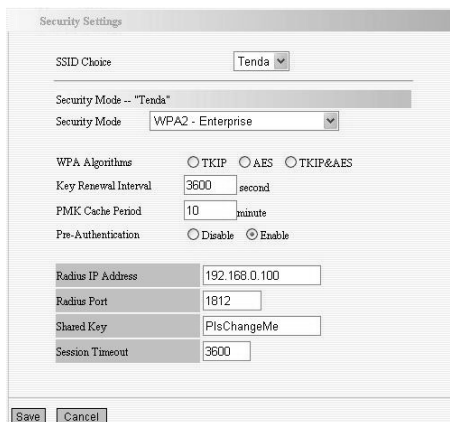
This security mode is also used when a RADIUS server is connected to the Router.

WPA Algorithms: Select key Algorithms such as TKIP and AES.
Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.



The screenshot shows the 'Security Settings' window with the following configuration:

- SSID Choice: Tenda
- Security Mode -- "Tenda": WPA2 - Enterprise
- WPA Algorithms: ☐ TKIP ☐ AES ☐ TKIP&AES
- Key Renewal Interval: 3600 second
- PMK Cache Period: 10 minute
- Pre-Authentication: ☐ Disable ☒ Enable
- Radius IP Address: 192.168.0.100
- Radius Port: 1812
- Shared Key: PlsChangeMe
- Session Timeout: 3600

Buttons: Save, Cancel

This security mode is used when a RADIUS server is connected to the Router. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.1x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass.


WEP: Select "enable/disable" WEP encryption which indicates the authentication process between wireless adapter and wireless router.

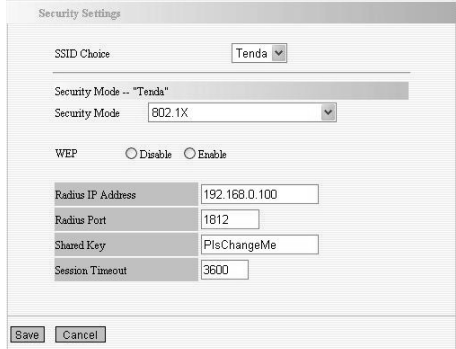
Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server.

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.

 **NOTE:** To improve security level, do not use those words which can be found in a dictionary or too easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it's worth to use complicated WEP key to improve security level.



The screenshot shows the 'Security Settings' window. At the top, 'SSID Choice' is set to 'Tenda'. Below it, 'Security Mode -- "Tenda"' is displayed. The 'Security Mode' dropdown is set to '802.1X'. There are two radio buttons for 'WEP': 'Disable' (selected) and 'Enable'. Below these are four input fields: 'Radius IP Address' (192.168.0.100), 'Radius Port' (1812), 'Shared Key' (PlsChangeMe), and 'Session Timeout' (3600). At the bottom are 'Save' and 'Cancel' buttons.

WPS Settings

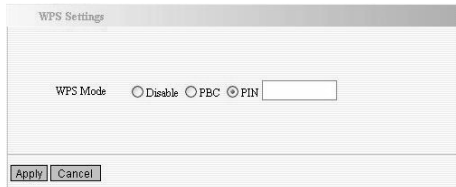
WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the Router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

WPS Mode: Supports two ways to configure WPS settings:

PBC (Push-Button Configuration) and PIN code.

PBC: Select the PBC or press the WPS button on the panel of the Router (Press the button for one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another Router to implement the WPS/ PBC negotiation between them. At present, the WPS only support one client access. Two minutes later, the WPS indicator will be off.).

PIN: If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the client.



The screenshot shows the 'WPS Settings' window. It has a title bar 'WPS Settings'. Below it, there are three radio buttons: 'Disable', 'PBC', and 'PIN'. The 'PIN' radio button is selected, and next to it is an empty text input field. At the bottom are 'Apply' and 'Cancel' buttons.

WDS Settings

In this mode, you can expand the scope of network by combining up to four other access points together, and every access point can still accept wireless clients.

Lazy Mode: You need configure the router's BSSID into another device, not need input another router's BSSID in it, and then connect together automatically.


Bridge Mode: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table. At the same time, the connecting device should be in Lazy, Repeater or Bridge mode.

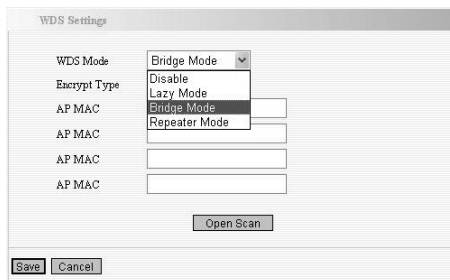
Repeater Mode: You can select the mode to extend the distance between the two WLAN devices. Functioning as a WDS repeater, the W306R connects to both a client card as an AP and to another AP. In typical repeater applications, APs connecting to other APs equipped with WDS functionality must also support WDS. In this mode, you need to add the MAC address of the connecting device into the Router's AP MAC address table and the connecting client should be in Lazy, Repeater or client mode.

Encrypt Type: You can select WEP mode, TKIP mode, AES mode for security here.

Pass phrase: Enter the key, the key format according to encryption you selected.

AP MAC: Input the MAC address of another wireless router.

 **NOTE:** Two wireless routers must use the same band, channel number, and security setting!



Advanced Wireless Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, Beacon Period and DTIM Interval.

BG protection Mode: Auto by default. You can select On or Off.

Basic Data Rates: For different requirement, you can select one of the suitable Basic Data Rates.

Here, default value is (1-2-5.5-11Mbps...).

Beacon Interval: Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.

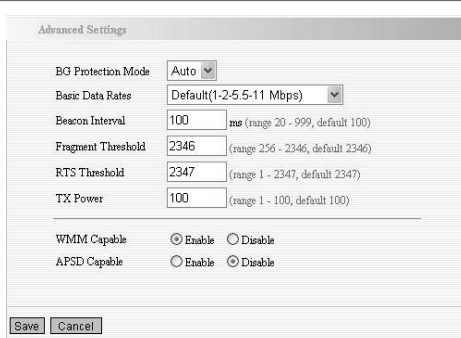
Fragment Threshold: Do not modify default value if you don't know what it is, default value is 2346.

RTS Threshold: Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.

TX Power: You can set the output power of wireless radio. Unless you're using this wireless router in a really big space, you may not have to set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).

WMM Capable: It will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is / not sure if you need it, it's safe to set this option to 'Enable', however, default value is enabling.

APSD Capable: It is used for auto power-saved service. The default is disabled.



Advanced Settings

BG Protection Mode	Auto
Basic Data Rates	Default(1-2-5.5-11 Mbps)
Beacon Interval	100 ms (range 20 - 999, default 100)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Save Cancel

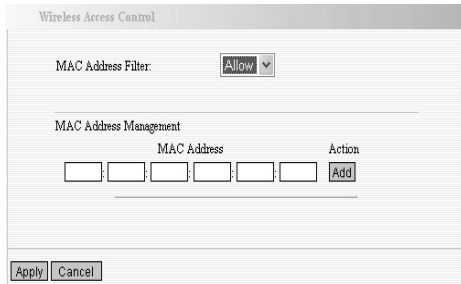
Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management.

MAC Address Filter: If you want to access the Router from any external IP Address, please select the "Disable".

MAC Address: To specify an external IP address, please add the MAC address manually and click "Add".

MAC Address List: The added MAC addresses are listed here. Click "Delete" to delete the filter management for this MAC address.



Wireless Access Control

MAC Address Filter:

MAC Address Management

MAC Address	Action
<input type="text"/>	<input type="button" value="Add"/>

Apply Cancel

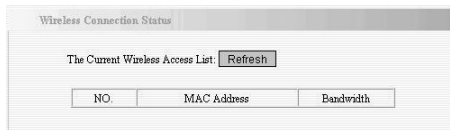
Wireless Connection Status

This page is to show the current wireless access status. Click “**Refresh**” to update the wireless connection information.

MAC Address:

Shows the connecting PC’s MAC address.

Bandwidth: displays the channel bandwidth of the host to be connected.



Wireless Connection Status

The Current Wireless Access List:

NO.	MAC Address	Bandwidth

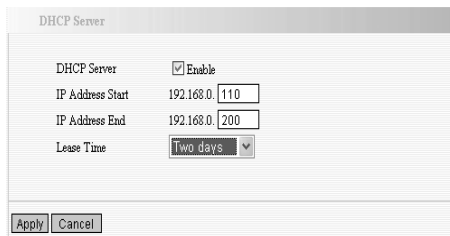
Chapter 7: DHCP Server

DHCP (Dynamic Host Control Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating “**Obtain an IP Address Automatically**”. So specifying the starting and ending address of the IP Address pool is needed.

DHCP Server: Activate the checkbox to enable DHCP server.

IP Address Start/End: Enter the range of IP address for DHCP server distribution.

Lease Time: The length of the IP address lease.



DHCP Server

DHCP Server ☒ Enable

IP Address Start 192.168.0.110

IP Address End 192.168.0.200

Lease Time

DHCP Server List

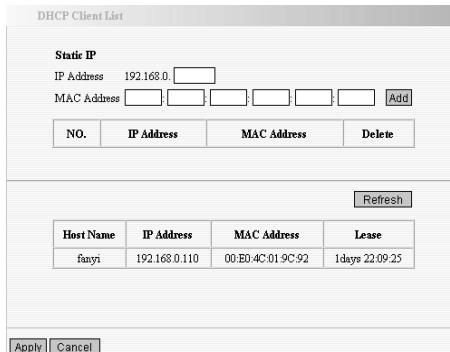
The Static IP assignment is to add a specifically static IP address to the assigned MAC address. You can view the related information in the DHCP server list.

IP Address: Enter one IP address for the computer on the LAN network.

MAC Address: Enter the MAC address of the computer you want to assign the above IP address. Click “**Add**” to add the entry in the list.

Hostname: The name of the computer which is added a new IP address.

Lease Time: The time length of the corresponding IP address lease.



DHCP Client List

Static IP

IP Address 192.168.0.

MAC Address


NO.	IP Address	MAC Address	Delete

Host Name	IP Address	MAC Address	Lease
flany1	192.168.0.110	00:E0:4C:01:9C:92	1days 22:09:25

Chapter 8: Virtual Server

Single Port Forwarding

The W306R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

 **NOTE:** the virtual server uses known host-name or public IP address.

External Port: This is the external port number for server or Internet application, for example, port 21 for ftp service.

Internal Port: This is the port number of LAN computer set by the Router. The Internet traffic from the external port will forward to the internal port.


For example, you can set the internal port NO.66 to act as the external port NO.21 for ftp service.

IP Address: Enter the IP address of the PC where you want to set the applications.

Protocol: Select the protocol (TCP/UDP/Both) for the application.

Well-Known Service Port: Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

Delete/Enable: Click to check it for corresponding operation.

 **NOTE:** If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

Single Port Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port	To IP Address	Protocol	Enable	Delete
1.	66 21	192.168.0.10	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) Add ID 1

Apply Cancel

Single Port Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port	To IP Address	Protocol	Enable	Delete
1.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
2.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) Add ID 1

Apply Cancel

Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.

Start/End Port: Enter the start/end port number which ranges the External ports used to set the server or Internet applications.

IP Address: Enter the IP address of the PC where you want to set the applications.

Protocol: Select the protocol (TCP/UDP/Both) for the application.

Well-Known Service Port: Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

Delete/Enable: Click to check it for corresponding operation.

Port Range Forwarding

The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53) Add ID 1

Port Trigger Settings

When internal clients have access to external server in the Internet for some application, the clients request to connect with servers, and the server will also ask to connect with client. But in the default setting, router will refuse to accept any request from WAN, which will bring communication halt. The port triggering is used to define triggering rules. So when clients have access to the server, the device will open the port through which the server sends the request to client.

IP Range: The internal IP address range for requesting external server application.

Trigger Port: The port range through which the internal clients send request traffics to external server with the range of 1~65535. Note that the low number first and two blanks can keep the same number if needed.

External Port: The port range through which the external server send request traffics to internal clients with the range of 1~65535. Note that the low number first and two blanks can keep the same number if needed.


Apply: To enable or disable the rule.

Add: After edit the rule, click the "add" button to add the current entry to port triggering list.

Apply: Click "Apply" to activate the current rule.

Cancel: Click "Cancel" to drop all setting saved last time.

It is allowed to delete or modify the previous rules in the list table.

 **Note:** The special application can be only used in one PC. If there is more than one PC to open the same triggering port, the external port will be connected to the last PC for the application.

Port Trigger Settings

Port Trigger ☒

IP Range	Trigger Port	External Port
192.168.0. <input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>

Protocol: TCP&UDP

Apply ☐

Num	IP	Trigger Port	External Port	Protocol	Apply	Edit	Del
-----	----	--------------	---------------	----------	-------	------	-----

ALG Service Settings

ALG (Application Layer Gateway)

In the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer „control/ data“ protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications etc.

In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

Usually allowing client applications to use dynamic ephemeral TCP/UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.

In the default ALG settings, the following protocols have enabled. It is recommended to keep the settings unchanged.

- 1,FTP
- 2,TFTP
- 3,PPTP
- 4,IPSec
- 5,L2TP

ALG Service Settings

FTP ☒ Enable
TFTP ☒ Enable
PPTP ☒ Enable
IPSEC ☒ Enable
L2TP ☒ Enable

Apply Cancel

DMZ Settings

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.

DMZ Host IP Address: The IP address of the computer you want to expose.

Enable: Click the checkbox to enable the DMZ host.
IMPORTANT: When enabled the DMZ host, the firewall settings of the DMZ host will not function.

DMZ Settings

IMPORTANT: When enabled the DMZ host, the firewall settings of the computer will not function.

DMZ host IP ☐ Enable

Apply Cancel

UPnP Settings

It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.

Enable UPnP: Click the checkbox to enable the UPnP.

UPnP Settings

Enable UPnP ☒

Apply Cancel

Chapter 9: Traffic Control

Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.

Enable Traffic Control: To enable or disable the internal IP bandwidth control.

Interface: To limit the uploading and downloading bandwidth in WAN port.

Service: To select the controlled service type, such as HTTP service.

IP Starting Address: The first IP address for traffic control.

IP Ending Address: The last IP address for traffic control.

Uploading/Downloading: To specify the traffic heading way for the selected IP addresses: uploading or downloading.

Bandwidth: To specify the uploading/downloading Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.

Apply: To enable the current editing rule. If not, the rule will be disabled.

Add: After edit the rule, click the "add to list" button to add the current rule to rule list.

Apply: Click "Save" to activate the current rule.

Cancel: Click "Cancel" to drop all setting saved last time.

It is allowed to delete or modify the previous rules in the list table.

Traffic Control Settings

Traffic Control ☒

Interface **Upload BW** **Download BW**

WAN: 512 2048 (KB/s, The bandwidth can not be zero)

Protocol Port Service

Services: TCP&UDP 0 All

IP: 192.168.0. -

Up/Down: Up

BW Range: - (KB/s, The bandwidth can not be zero)

Apply: ☐

Add

Num	Port	IP	Up/Down	BW Range	Apply	Edit	Del
-----	------	----	---------	----------	-------	------	-----

Apply Cancel

Chapter 10: Security Settings

Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.

Client Filter: Check to enable client filter.

Access Policy: Select one number from the drop-down menu.

Enable: Check to enable the access policy.

Clear the Policy: Click "Clear" button to clear all settings for the policy.

Filter Mode: Click one radio button to enable or disable to access the Internet.

Policy Name: Enter a name for the access policy selected.

IP Start/End: Enter the starting/ending IP address.

Port No.: Enter the port range based over the protocol for access policy.

Protocol: Select one protocol (TCP/UDP/Both) from the drop-down menu.

Times: Select the time range of client filter.

Days: Select the day(s) to run the access policy.



The screenshot shows the 'Client Filter' configuration window. The 'Client Filtering Settings' checkbox is checked. The 'Access Policy' is set to '10'. The 'Enable' checkbox is checked, and the 'Delete the Policy' button is visible. The 'Filtering' mode is set to 'Disable', and the 'Mode' is set to 'Enable' with the note 'access the Internet'. The 'Policy Name' field is empty. The 'Start IP' and 'End IP' are both set to '192.168.0'. The 'Port' field is empty. The 'Type' is set to 'TCP'. The 'Times' are set to '0' for all days. The 'Date' is set to 'Everyday'. The 'Apply' and 'Cancel' buttons are at the bottom.

URL Filter Settings

In order to control the computer to have access to websites. You can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.

URL Filter: Check to enable URL filter.

Access Policy: Select one number from the drop-down menu.

Enable: Check to enable the access policy.

Clear the Policy: Click "Clear" button to clear all settings for the policy.

Filter Mode: Click one radio button to enable or disable to access the Internet.

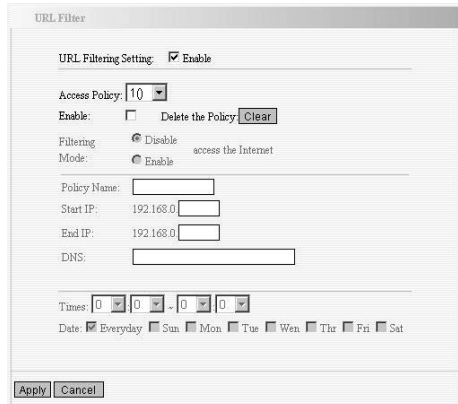
Policy Name: Enter a name for the access policy selected.

Start/End IP: Enter the starting/ending IP address.

DNS: Specify the text strings or keywords in the DNS. If any part of the URL contains these strings or words, the web page will not be accessible and display.

Times: Select the time range of client filter.

Days: Select the day(s) to run the access policy.



The screenshot shows the 'URL Filter' configuration window. The 'URL Filtering Setting' checkbox is checked and labeled 'Enable'. The 'Access Policy' is set to '10'. The 'Enable' checkbox is checked, and the 'Delete the Policy' button is visible. The 'Filtering' mode is set to 'Disable', and the 'Mode' is set to 'Enable' with the note 'access the Internet'. The 'Policy Name' field is empty. The 'Start IP' and 'End IP' are both set to '192.168.0'. The 'DNS' field is empty. The 'Times' are set to '0' for all days. The 'Date' is set to 'Everyday'. The 'Apply' and 'Cancel' buttons are at the bottom.

MAC Address Settings

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.

MAC Address Filter: Check to enable MAC address filter.

Access Policy: Select one number from the drop-down menu.
Enable: Check to enable the access policy.

Clear the Policy: Click "Clear" button to clear all settings for the policy.

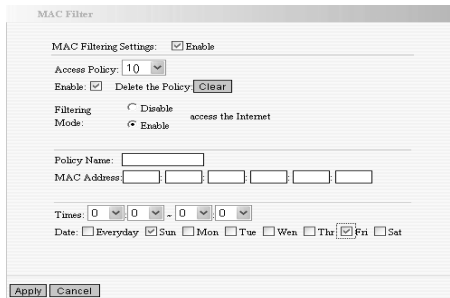
Filter Mode: Click one radio button to enable or disable to access the Internet.

Policy Name: Enter a name for the access policy selected.

MAC Address: Enter the MAC address you want to run the access policy.

Times: Select the time range of client filter.

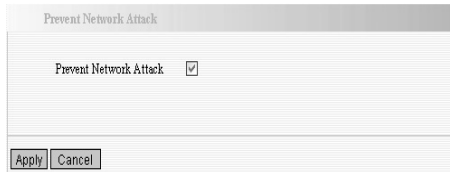
Days: Select the day(s) to run the access policy.



Prevent Network Attack

W tej części zawarte są ustawienia ochrony sieci wewnętrznej przed atakami zewnętrznymi, takimi jak SYN Flooding, Smurf, LAND itd. Po wykryciu nieznanego ataku, router automatycznie ogranicza szerokość pasma. Adres IP urządzenia atakującego można znaleźć w dzienniku systemowym („System Log”).

Prevent Network Attack (Zapobiegaj atakom sieciowym):
Zaznacz, aby włączyć ochronę przed atakami.



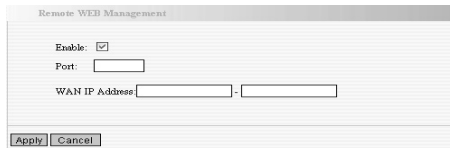
Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the “Enable”.

Enable: Check to enable remote web management.

Port: The management port open to outside access The default value is 80.

WAN IP Address: Specify the range of the WAN IP address for remote management.

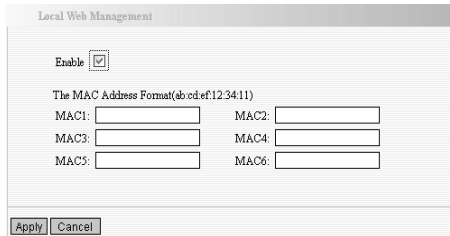


Local Web Management

Local web management, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.

Enable:
Check to enable the local web management

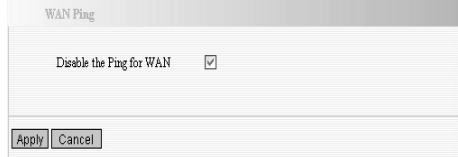
MAC1/2/3...:
Enter the MAC addresses of LAN computers.



WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.

Disable the Ping for WAN: Check to enable it.



WAN Ping

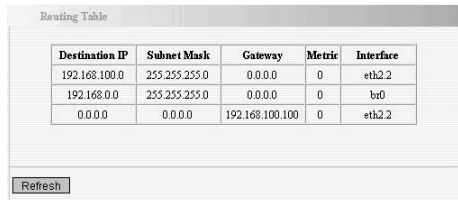
Disable the Ping for WAN ☒

Apply Cancel

Chapter 11: Routing Settings

Routing Table

The main duty for router is to look for a best path for every data frame, and transfer this data frame to destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.



Routing Table

Destination IP	Subnet Mask	Gateway	Metric	Interface
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.100	0	eth2.2

Refresh

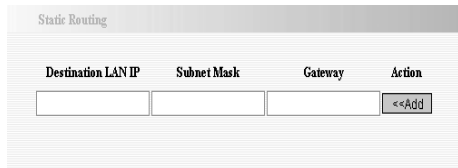
Static Route

Static Route is set by administrator in advance is called static route. Usually, it is set according to network configuration when installing the operation system. It would not be changed according to network structure's change.

Destination LAN IP: The address of the remote host with which you want to construct a static route.

Subnet Mask: The network portion of the Destination LAN IP.

Gateway: The gateway of the next hop.



Static Routing

Destination LAN IP	Subnet Mask	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add

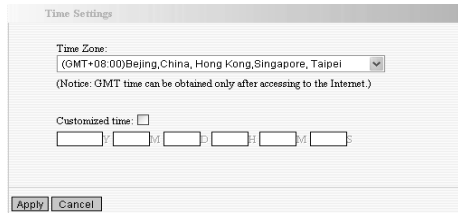
Chapter 12: System Tools

Time

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.

Time Zone: Select your time zone from the drop-down menu.

Customized time: Enter the time you customize.



Time Settings

Time Zone:
 (GMT+08:00)Beijing,China, Hong Kong,Singapore, Taipei v

(Notice: GMT time can be obtained only after accessing to the Internet.)

Customized time: ☐

: / / : : :

Apply Cancel

DDNS

The DDNS (Dynamic Domain Name System) is supported in this router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select "Enable" and a DDNS service provider to sign up.

DDNS: Click the radio button to enable or disable the DDNS service. Service Provider: Select one from the drop-down menu and press "Sign up" for registration.

User Name: Enter the user name the same as the registration name.

Password: Enter the password you set.

Domain Name: Enter the domain name which is optional.



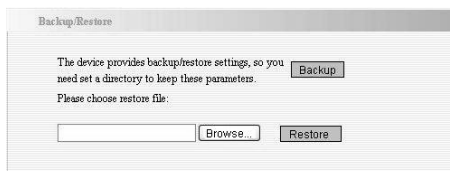
Backup/Restore

The device provides backup/restore settings, so you need set a directory to keep these parameters.

Backup: Click this button to back up the Router's configurations.

Browse: Click this button to browse the directory where you Back up or save files.

Restore: Click this button to restore the Router's configurations



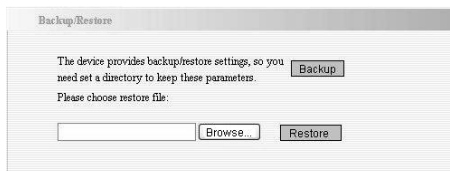
Firmware Upgrade

The Router provides the firmware upgrade by clicking the "Upgrade" after browsing for the firmware upgrade packet which you can download from www.tenda.cn. After the upgrade is completed, the Router will reboot automatically.

Browse: Click this button to browse the directory where you download the firmware upgrade files.

Upgrade: Click this button to start upgrade.

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the device. The Router will reboot after the upgrade.



Restore to Factory Default Settings

This button is to reset all configurations to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.

Restore to Factory Default Settings: Click this button to restore to default settings.


Factory Default Settings:

User Name: admin

Password: admin

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

 **NOTE:** After restoring to default settings, please restart the device, then the default settings can go into effect.

Restore to Factory Default Settings

Restore to Factory Default Settings.

Reboot

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.

Reboot the router: Click this button to reboot the device.

Reboot

Click here to reboot the router.

Change Password


This section is to set a new user name and password to better secure your router and network. Please Note that the new password should be less than 14 characters.

User Name: Enter a new user name for the device.

Old Password: Enter the old password.

New Password: Enter a new password.

Re-enter to Confirm: Re-enter to confirm the new password.

 **NOTE:** It is highly recommended to change the password to secure your network and the Router.

Change Password

Note: User Name and Password makeup only by number or land letter.

User Name

Old Password

New Password

Re-enter to Confirm

System Log

The section is to view the system log. Click the "Refresh" to update the log. Click "Clear" to clear all shown information. If the log is over 150 records, it will clear them automatically.

Refresh: Click this button to update the log.

Clear: Click this button to clear the current shown log.

System Log

Page 1 content

1	2000-01-01 00:00:09	DHCP	Send discover
2	2000-01-01 00:00:12	DHCP	Send discover
3	2000-01-01 00:00:15	DHCP	Send discover
4	2000-01-01 00:00:21	System	system start.
5	2000-01-01 00:01:18	DHCP	Send discover
6	2000-01-01 00:01:21	DHCP	Send discover
7	2000-01-01 00:01:24	DHCP	Send discover
8	2000-01-01 00:00:09	DHCP	Send discover
9	2000-01-01 00:00:12	DHCP	Send discover
10	2000-01-01 00:00:15	DHCP	Send discover

[1] [2] [3]

Appendix A: Product Features

- Integrates router, wireless access point, four-port switch and firewall in one
- Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
- MIMO technology utilizes reflection signal to increase eight times transmission distance of original 802.11g standard and reduces the „dead spots“ in the wireless coverage area
- Provides 300Mbps receiving rate and 300Mbps sending rate
- Supports WMM to make your voice and video more smooth
- Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
- WPS (PBC and PIN) encryption method to free you from remembering long passwords
- Supports remote/local Web management
- Supports wireless Roaming technology and ensures high-efficient wireless connections
- Supports wireless SSID stealth mode and MAC address access control
- Supports Auto MDI/MDIX
- Provides system log to record the status of the router
- Supports MAC address filtering, NAT, NAPT
- Supports UPnP and DDNS
- Supports the access control over 30 MAC addresses
- Supports DHCP server/client
- Supports SNTP
- Supports virtual server and DMZ host
- Supports auto wireless channel selection
- Supports WDS function (wireless distribution system)



Symbol odpadów pochodzących
ze sprzętu elektrycznego i elektronicznego
(WEEE - ang. Waste Electrical and Electronic Equipment)

Użycie symbolu WEEE oznacza, że niniejszy produkt nie może być traktowany jako odpad domowy. Zapewniając prawidłową utylizację pomagasz chronić środowisko naturalne. W celu uzyskania bardziej szczegółowych informacji dotyczących recyklingu niniejszego produktu należy skontaktować się z przedstawicielem władz lokalnych, dostawcą usług utylizacji odpadów lub sklepem, gdzie nabyto produkt.



Importer:
Megabajt Sp. z o.o., ul. Rydygiera 8, 01-793 Warszawa