Wireless Router Serioux
User Guide

Thank you for choosing our wireless broadband router. Before using the router, please read this handbook carefully because it provides every basic setting. If your specification is mentioned in the handbook, the router mentioned refers to the SRX-WR150/300 series wireless router. Pictures of the interface in this manual provide references for users. If the product configuration interface does not provide a reference, you should set up the router according to your needs.

Product Features

- Integrates router, wireless access point, four-port switch and firewall in one device
- Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
- MIMO technology utilizes reflected signal to increase eight times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
- Provides 150/300Mbps transmission rates
- 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 auto wireless channel selection
- Supports WDS function (wireless distribution system)

Package Contents

Wireless-N 150/300M broadband router.
Power adapter: DC5V/2A ~~or~~ DC12V/1A
User manual.
Ethernet network cable.
Quick Installation Guide.
Warranty cards/certification.

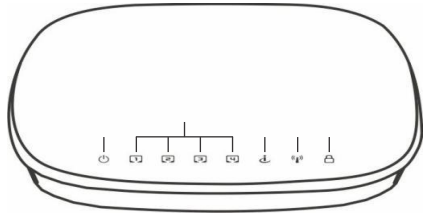
Important: When opening the package, please ensure that the package contents are as stated above. If not, please contact the distributor.

Product Specifications

Standards and Protocols		IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE.
Port	WAN	One 10/100 M self-adapting RJ-45 WAN port. (When working in gateway mode, it's a WAN port but when working in any other mode, it's aLAN port)
	LAN	Four 10/100M self-adapting RJ-45 LAN ports
	Frequency Range	2.4-2.4835GHz
	Wireless Signal Rates	11n: Up to 150/300Mbps 11g: Up to 54Mbps 11b: Up to 11Mbps
	Working Channel	1 to 14 channels (according to the country or region you choose)
	Spread Spectrum	DSSS (Direct Sequence Spread Spectrum)
Wireless parameters	Modulation Technology	DBPSK, DQPSK, CCK and OFDM (BPSK/QPSK/16-QAM/64-QAM)
	Receiver Sensitivity @PER	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER

	transmission range	Indoor: 300M, Outdoor: 500M (depending on environment)
Network Media		10Base-T: 3e UTP or above; 100Base-TX: 5e UTP
	WLAN	Status indicator for W LAN (on/off)
	WAN	Status indicator for WAN
LED	LAN	Status indicator for LAN
	WPS	WPS indicator
	POWER	Power indicator
Operating environment		Operation temperature: 0℃～4 5℃ Operating Humidity: 10%～90%(non-condensing) Storage temperature: -4 0℃～7 0℃ Storage Humidity: 5%～90%(non-condensing)
External power		Power adapter output: DC5V/2A or DC12V/1A

LED Indicators



Power indicator: LED will light when unit is powered on.
Status indicator for LAN: LED will light when link is established. LED will blink when packet is being transmitted or received.
Status indicator for WAN: LED will light when link is established . LED will blink when packet is being transmitted or received.
Status indicator for WLAN: LED will light when a function is enabled. LED will turn off when the wireless function is disabled. LED will blink when a packet is being transmitted or received.
WPS indicator: Indicates router setting WPS Mode . (PBC or PIN under WPS mode is optional)

Installation Warnings for Router

For a first-time wireless network installation, please follow the rules below in order to avoid damage or to decrease performance affected by an improper operation or location):
1.A router should be kept away from any cordless phone, microwave oven, refrigerator, or other source of interference.
2.When there are other 2.4G access points around, it is required that the interval be more than 12M and that any adjacent channel be avoided.
3.In order to receive the best wireless signal, the router should be placed properly in position.
4.Keep the router away from reinforced concrete walls or metal railings because these objects can block or absorb signals.
5.A router should be placed indoors, out of the way of sunshine, rain or lightning.
6.Keep the router away from fire and heat and keep it ventilated.

Notes

1.The maximum wireless signal rate based on IEEE standard 802.11n specifications, the actual data throughput will vary.
2.Network conditions and environmental factors, including network traffic, building materials and structures, and network expenses can reduce the actual data throughput.
3.This manual has been as far as possible try to provide you with accurate information, but only use as guidance.
4.Due to product upgrades or other reasons, the manual will be updated from time to time without notice!

Hardware Install Process

Establish WAN Connection

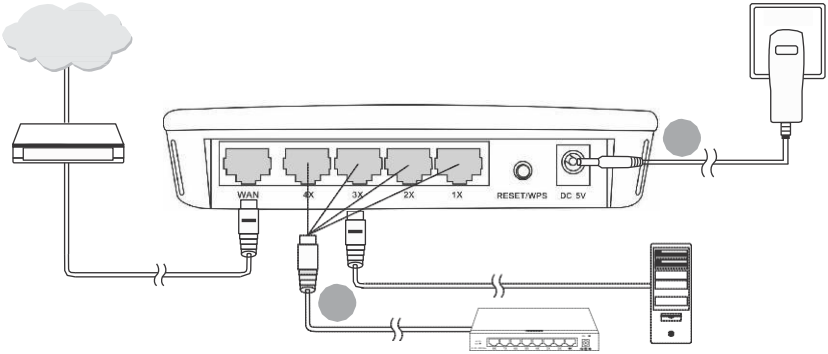
Connect the WAN port of router to xDSL Modem by a line.

Establish LAN Connection

Connect the port of router to HUB or switch by a line. You also can connect the computer LAN card directly.

Power Link

Link the power and the router will start automatically.

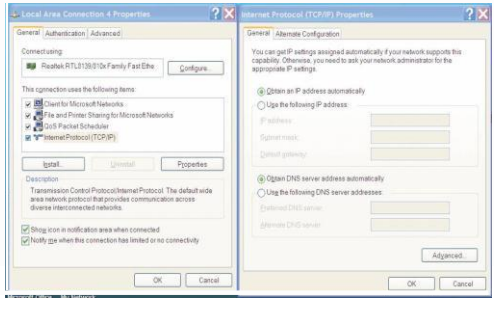


Management and Login

You should log into your web page before using the router. Here is an example, using the “Windows XP Home Edition Service Pack 3”operating system as an example to illustrate the configuration of the computer process:

1.Check “Network Connections”, making sure that the PC has an installed wireless card. If there is an icon, like “Local Area Connection 4 Connected” shown in the figure below, the wireless card has been already installed in the PC.

2.Set your IP address through the properties of “Internet Protocol (TCP/IP)”. Generally, the DHCP server of the router is on, so please select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, under the General tab.

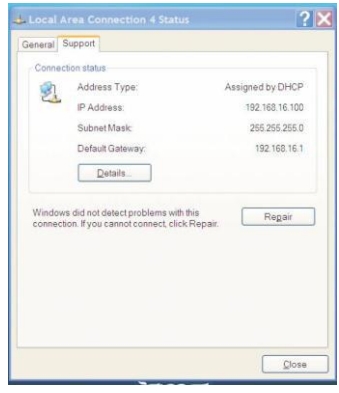


Tips:

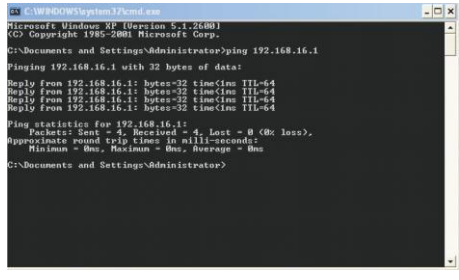
Only when the DHCP server of the router is enabled should you select “Obtain an IP address automatically”.

You can set the IP address by yourself instead. However, the IP address of the computer and router should be set within the same subnet and may not share an IP address . The default IP address is 192.168.16.1 and the subnet m ask is 255.255.255.0, so the IP address should not be 192.168.16.1.

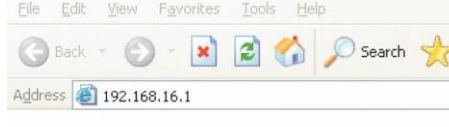
3.You can find the assigned address under the Support tab, as follows:



4.Click on Start | Programs | Accessories | Command Prompt, type ping 192.168.16.1, and press Enter (as shown below). If the screen displays the following figure, your PC has connected to the router successfully.



5.Access the interface of the router by opening a web browser. Input http://192.168.16.1 (the router’s default IP address) and press Enter.



6.The browser will open a login window as shown below. Enter **admin** for the administrator's User name and **admin** for the Password. Click on the OK button.

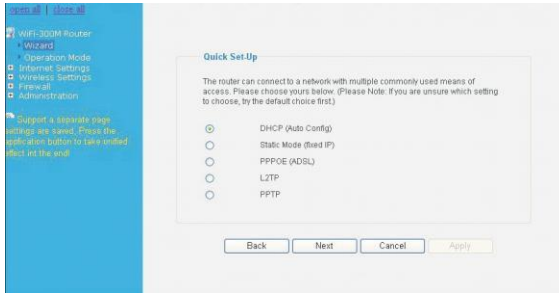
7.Click on the OK button. If the User name and Password are correct, you will enter the WEB settings screen.

8.You have now logged into the settings page successfully.

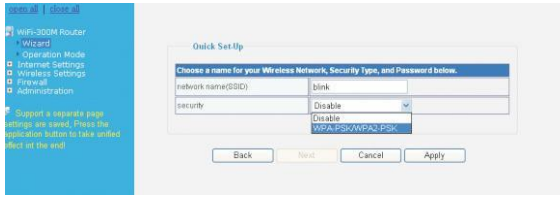
Wizard

The router supports various functions and provides a setup wizard. The wizard can guide you to finish the basic settings, even though you may be unfamiliar with the router.
1.Click on "Wizard" in the left margin and click on "Next" in the right margin under "Quick settings". This will start the procedure for setting the router.

2.This product supports any of five frequently-used modes to access a network. Choose a mode to suit your need. The default mode is pre-selected. The other four modes listed below the default mode would require parameter settings for the network connection. If you do not know the parameters,
please ask your ISP. After choosing a mode, click on the "Next" button.



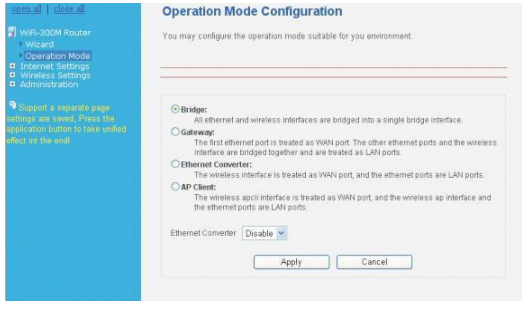
3.You can set a network name and corresponding encryption securit y for your wireless network settings, as shown below. Click on the “Apply” button to submit the setting information. The system will then reboot the router to complete the router’s basic settings.



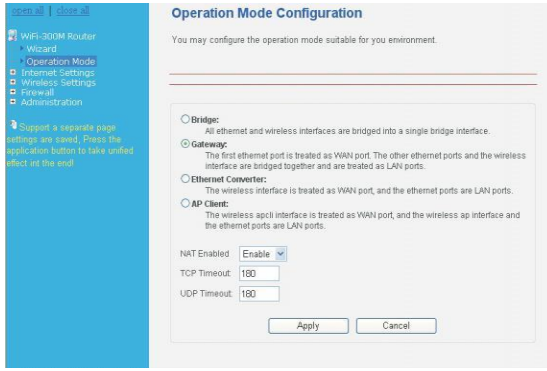
Operation Mode

The SRX-WR150/300 series wireless router is a powerful router because it can support four modes: Bridge mode, Gateway mode, Ethernet converter mode and AP client mode (The default mode is Gateway)

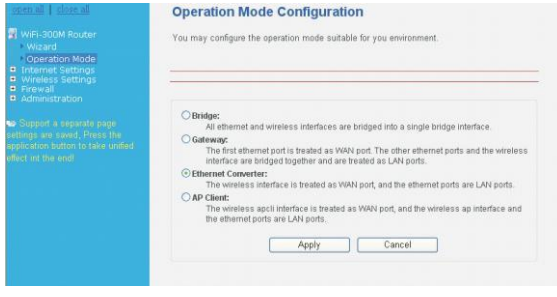
Operation mode set to Bridge mode:
All Ethernet and wireless interfaces are bridged into a single bridge interface. Until now, the router has been acting only as a switch, so the router has been unable to access the WAN and the firewall has been disabled)



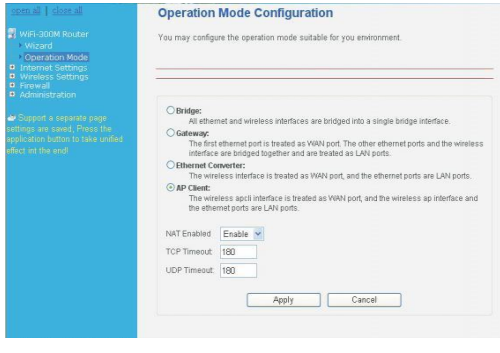
Operation mode set to Gateway mode:
Gateway is the default mode, The yellow Ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports (which is used to enable the NAT function to enable the router to transmit information easily with the Internet).



Operation mode set to Ethernet converter mode:
The wireless interface is treated as WAN port, and the ethernet ports are LAN ports.



Operation mode set to AP Client mode:
The wireless interface is treated as WAN port, the wireless interface and the ethernet ports are LAN ports.



Internet Setting

WAN

This router supports several common types of WAN connections . Select the connection method that your network operator uses and select the correct parameter information (likely provided by your ISP). Then, you can share the Internet normally. If you use a dynamic connection, dial-up connection, PPPoE dial-up connection, etc., there are two ways to verify whether the connection will work. One way is to browse the web site directly, and the other way is to distinguish it according to the Internet configuration state.

Internet Configurations	
Connected Type	PPPOE
WAN IP Address	58.60.132.45
Subnet Mask	255.255.255.255
Default Gateway	58.60.132.1
Primary Domain Name Server	202.96.134.33
Secondary Domain Name Server	202.96.128.86
MAC Address	00:0C:43:30:52:5A

Successful connection

An ISP may require a binding MAC address, which the ISP will usually offer to you. It may be entered on the MAC address bar. Otherwise, you may click the Fill my MAC button, in which case the MAC address of the current connecting host will be automatically filled in the text box for you.

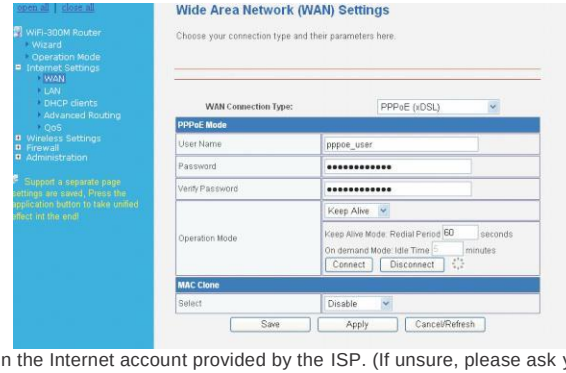
1.Connection Mode DHCP (Auto config)

This connection mode is more convenient because it can obtain information parameters such as IP and gateway addresses automatically and they can change while the ISP's operator network status changes.

2.Connection Mode Static (Fixed IP)
If your ISP uses the Static IP mode, please choose Static (fixed IP) to set the network parameters. If you are unsure about the mode, please contact your ISP.

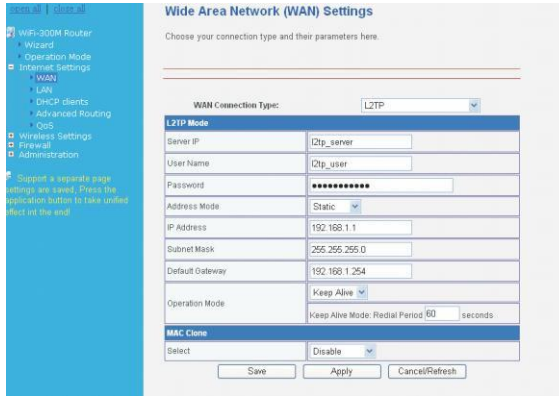
IP Address: Enter the static IP address provided by your ISP.
Subnet Mask: Enter the subnet mask .
Gateway: Enter the WAN gateway address.
Primary DNS Server: Enter the primary DNS server address provided by your ISP.
Secondary DNS Server: Enter the secondary DNS server address.

3.Connection Mode PPPoE (xDSL)
PPPoE is commonly used for home and small office networks.



User Name: Fill in the Internet account provided by the ISP. (If unsure, please ask your ISP.)
Password: Fill in the password provided by the ISP. (If unsure, please ask your ISP.)
Operation Mode: Choose from three operation modes (Keep Alive, Dynamic demand, or Manual demand):
1.Keep Alive: The Keep Alive mode allows the router to connect automatically when turned on. If the network is disconnected from the router due to external factors, the system will try to reconnect to the network at regular intervals (default of 60s) until a connection is established.
2.Dynamic demand: The router connects automatically to the LAN when an access request is sent to it. If no access request is sent (free time), the router disconnects automatically from the network . (This connection mode is chosen by users who collect fees on time so they can save on the cost of Internet service.)
3.Manual demand: The user must dial manually when the router is turned on. Click on Connection to connect to the network . Click on Disconnect to disconnect from the network.

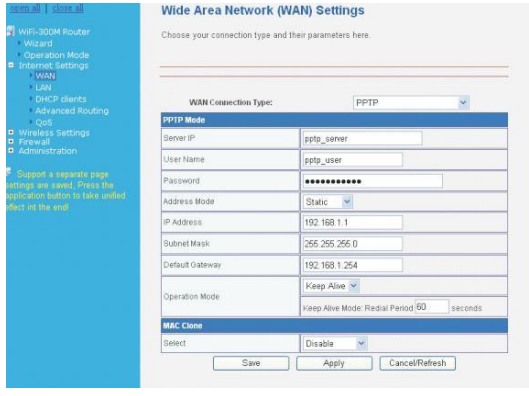
4.Connection Mode L2TP



Server IP: Enter the required (not optional) Server IP address, provided by your ISP.

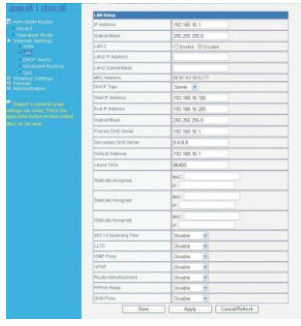
User Name: Enter the required (not optional) L2TP User Name, provided by your ISP.
Password: Enter the required (not optional) L2TP password, provided by your ISP.
Address Mode: Obtain an IP address:
Dynamic: Choose this mode if the router can obtain an IP address automatically.
Static: Choose this mode if your ISP has provided you with a static IP address.
IP Address: Choose “Static” and enter the L2TP IP address provided by your ISP.
Subnet Mask: Enter the Subnet Mask address supplied by your ISP.
Default Gateway: Enter the Default Gateway address supplied by your ISP.
Operation Mode (2 modes):
Keep Alive: The router connects automatically to the LAN when an access request is sent to it. If the network is disconnected from the router due to external factors, the system will try to connect to the network at regular intervals until a connection is established.
Manual demand: If the network disconnects from the router, choose this mode to dial manually to the network.

5.Connection Mode PPTP
If the connection is the PPP Tunneling Protocol, your ISP can provide you with the User Name and Password . For related parameter settings, please refer to the L2TP mode.



LAN

Select “Internet Settings | LAN” to set the parameters of the LAN ports (IP address, subnet mask , DHCP, etc.).



Hostname: Name of the network to which the router connects.
IP Address: LAN IP address of the router. (The default is 192.168.16.1.)
Subnet Mask: Subnet mask of the router, according to the network state. (The default is 255.255.255.0.)
LAN2: Enable or disable the second LAN port address, according to the request. To enable it, set the IP address and subnet mask of the second LAN port.
LAN 2 IP Address: Second IP address.
LAN 2 Subnet Mask: Second Subnet mask.
MAC Address: MAC address of the LAN port of the router.
DHCP Type: Distribute the PC’s IP address to the LAN network automatically by using the built-in DHCP Server. To enable it, select DHCP as the server. Otherwise, select Disable. (The default is Server.)

Start IP Address: Set the initial IP address, which the DHCP Server distributes automatically according to the router’s LAN IP address.

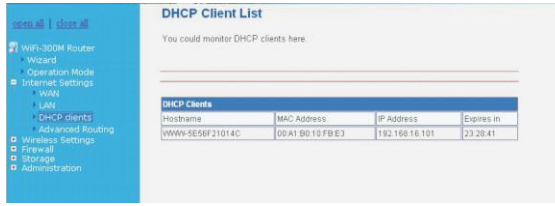
End IP Address: Set the end IP address, which the DHCP Server distributes automatically according to the router’s LAN IP address.
Subnet Mask: Set a matching subnet mask according to the initial/end IP address.
Primary DNS Server: Fill in the Primary DNS server address (optional) provided by your ISP.

Secondary DNS Server: Fill in the Secondary DNS server address (optional) provided by your ISP.
Default Gateway: Set the gateway of the DHCP server according to the router’s LAN IP address. The router’s default gateway is 192.168.16.1.
Release time: The effective time (in seconds) of the dynamic IP address that the DHCP server allocates to the client host. (The default is 86400. 86,400 seconds = 1 day.) During this time, the server will not assign IP addresses to other hosts. (You can set the time according to your preference, which can improve the void IP address recovery efficiency of the DHCP server.)
Static specifies: You can set a scheme for DHCP to comply. Every time that the DHCP server assigns IP addresses automatically, it assigns a fixed IP address to the user’s device. If necessary, fill in the designated MAC address and IP address.
MAC address: The MAC address of the PC that reserves a static IP address. (Example: 00:0C:43:80:88.)
IP address: The reserved IP address for a host in a network. (Example: 192.168.16.254.)
802.11d Spanning Tree: The Spanning Tree protocol, defined in 802.1d, is a bridge-to-bridge protocol in the link management. It provides a redundancy of pathways to prevent a cycle path. (There is no default value.)
LLTD: Options include Enabled, Disabled, and Open. If there is an LLTP client, information about the router will display automatically.

Enable the IGMP agent: It inhibits the occurrence of a multicast flood by effectively obtaining and controlling the user’s information. This helps to reduce a network side agreement and the network load. (There is no default)
UPNP: The router provides UPNP to P2P intranet software. (There is no default.)
Router advertising: The router will send out or reply to broadcast information between each node at a fixed cycle to indicate its existence. (There is no default.)
PPPOE Forward: This function makes a local computer dial PPPoE separately and directly in the gateway mode. (There is no default.)

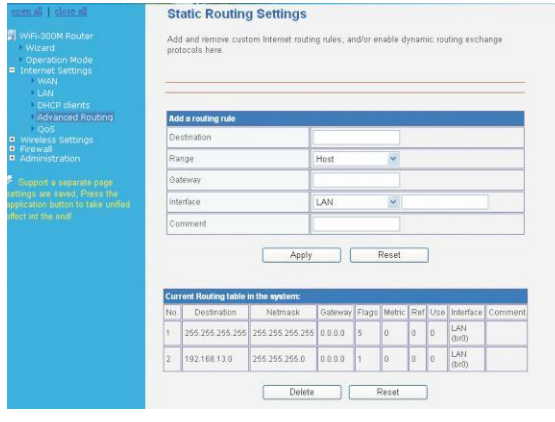
DHCP Clients

Select “Internet Settings | DH CP clients” to check the related computer information of the DHCP that automatically assigns IP addresses in the LAN (such as network name, MAC address, IP address and expiration time).



Advanced Routing

This function is an option to add specific routing to a specific hos t if necessary. The appropriate use of static routers in a network can reduce routing selection problems and data overload of routing streams, so its use can increase the transmitting speed of data packets. By setting the addresses of the IP, subnet mask, and gateway, a routing table can be set up. The destination IP address and subnet mask are used to determine a target network/host so that the router can send data packets to designated target network/hosts through the gateway.

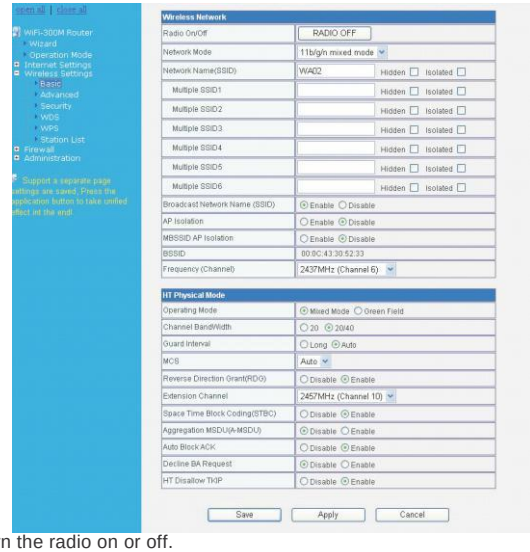


QOS

QOS is Quality of service, its primary function is to limit the bandwidth usage of a certain server and IP, to meet the bandwidth that’s needed by specific application and priority of service, and share bandwidth with the rest of users, so there can be more stable and reliable data transfer service

Prompt:
The formula of unit conversion between bandwidth and Kbyte is 1Mbit= 128K byte (kilobyte) Generally the ADSL ratio of upload and download bandwidth is one to three, upload bandwidth of 1M ADSL is 42Kbyte and the download is 128Kbyte.

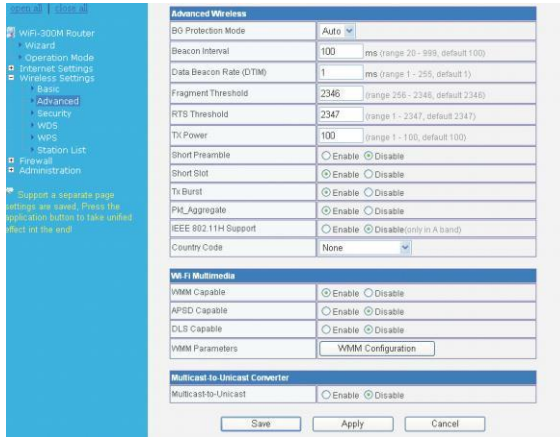
Wireless Settings
Basic:



Radio On/Off: Turn the radio on or off.
Network Mode: Choose one of router working modes: 802.11b, 802.11g, 802.11b/g, and 802.11b/g/n.
Network Name (SSID): Network name (32 characters max.) of wireless signals set to distinguish a separate network.
Broadcast Network Name (SSID): Enable or disable SSID broadcast machine. Select Disable, The SSID is hidden so that a wireless client will be unable to scan the SSID equipment. The client must know the equipment SSID before it can communicate with the equipment. (The default is Enabled).
BSSID (Basic Service Set ID): It applies to the MAC address site. In wireless access points, a group of wireless workstations and wireless LAN workstations called access points (AP) form a basic service device (BSD). The BSS device of each computer must configure the same BSSID, namely the wireless- access-point wireless logo.
Frequency (Channel): Select the wireless-network work channel. The two choices are Automatic Selection and Manual of Choice. Different countries or regions use different channel numbers. For national or regional settings, please see the section on advanced settings.
Operation Mode: Mixed Mode or Green Field:
Mixed Mode: The former wireless card can identify the Pre-N AP and connect to it but the transmission will be affected somewhat. (The default is Mixed Mode.)
Green Field: You can achieve a higher transmission rate but it will affect backwards compatibility and the security of the system.
Channel Bandwidth: Choose 20 or 20/40. (The default is 20/40.)
Guard interval: Choose Long or Auto. (The default is Auto.)
MCS: Modulation Code Lists: The 802.11n standard of the wireless LAN (W LAN) communications rate. (The default is Auto.)
Reverse Direction Access (RDG): Enable or disable this permission.
Extensions channel: Choose from the defined band expanded channels.
Space Time Block Coding(STBC): Choose Enable or Disable. (The default is Enabled)
Polymerization MAC Business Data Unit (A-MSDU): The multiple Ethernet message is clumped into a larger load in a certain way. (The default is Disabled)
Auto Block ACK: Choose Enable or Disable. (The default is Enabled)
Decline BA Request: Choose Enable or Disable. (The default is disabled)
HT Disallow TKIP: Choose Enable or Disable. (The default is Enabled)

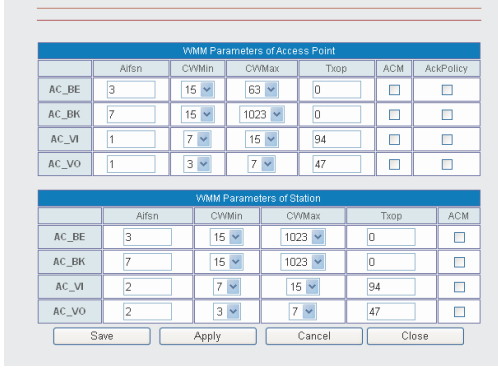
Advanced

Select “Wireless Settings | Advanced” to access the advanced wireless settings interface. It includes advanced parameters like Beacon Interval and transmitting power to set an optimal allocation for your network. Please do not modify the contents unless you are an advanced user.



BG Protection Mode: You can select On or Off. (The default is Auto.)
Beacon Interval: It can be set to obtain the access interval time of a nearby wireless network. (The default is 100ms.)
Data Beacon Rate (DTIM): It is the time (in ms) used to transfer information, which is shown in the next client window that receives broadcast and multicast messages. The range is 1 to 255. (The default is 1.)
Fragment Threshold: It sets the data’s packet size before the data is transmitted. When a wireless network is busy or is working in a high-interference environment, you should enable this function. A packet should be divided to reduce the number of retransmissions, which improves the wireless network’s performance. If the fragment threshold is above the data packet value, the data will not be divided when it is transmitted. Otherwise, it will be divided one packet (not all packets) at a time. Its range is 256-2346. (The default is 2346.) We recommend using the default value or a value that is slightly lower than the default value.
RTS Threshold: An appropriate setting can avoid a hidden node problem that occurs when both radios share the same access point but vary in range. The RTS packet size that radios send depends on the RTS Threshold. The range of the RTS Threshold is 1-2347. (The default is 2347.) When the packet size exceeds the RST limits, this device will send an RTS notice before sending the packets. When you set a transfer request limit, consider the pros and cons. A low value enables RTS notifications but a higher frequency will occupy more bandwidth. However, the more often that an RTS packet transmits, the sooner the system will recover from a data collision. So, we recommend using the default value or a value that is slightly lower than the default value.
TX Power: It defines the transmitting power size for the SSID of the current machine. 50 is half power. (The default is 100, which is full power.)
Short Preamble: It is used to provide a leading frame for the default setting. You can enable or disable it. (The default is Disabled, which is recommended.)Shot slot: You can enable or disable it. (The default is Enabled, which is recommended)
TX Burst: This property belongs to the MAC address layers, which can improve the balance of the wireless network TCP transmission. You can enable or disable it. (The default is Enabled, which is recommended)
PKT Aggregate: Aggregation technologies put multiple packets together, which enhances each LAN packet to be sent to its destination correctly. This improves the transmitting efficiency. You can enable or disable it. (The default is Enabled, which is recommended.)

IEEE 802.11H Support: It is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military radar systems and medical devices. The rules for 802.11h were recommended by the International Telecommunication Union, which is an addition to the 802.11a standards. The 802.11h standard is compliant with European standards on 5GHz wireless LANs. (The default is disabled.)
Country Code: Select the appropriate country code to meet local requirements according to the country or region where you are. Different countries or regions have different wireless controls, such as the channel number. (The default is None, which means it has no set value.)
WMM Capable: It is used to set the Wi-Fi service (QoS) ability for multimedia quality. When this function is enabled, the router will prioritize wireless data according to the type of data. (The default is enabled.)
Note: In order to apply the WMM function, both client and router must support it.
AP SD Capable: It shows expandability. You can enable or disable this function. (The default is Disabled)
Wi-Fi WMM settings: Click on the Wi-Fi WMM settings button. A settings page will then pop up:



Security

Select “Wireless Settings | Security”. This interface is used to set up wireless network security encryption. You can choose the SSID that you need to encrypt. Select a safe mode, and then set the encryption keys to prevent unauthorized access to a wireless client connection . You can also allow or prohibit an illegal connection by setting up a strategy based on MAC.

OPEN WEP

WEP encryption is the earliest wireless encryption, which is accomplished by using a 64/128/152 key for encryption of data transmission. The router work s at a slower rate under this encryption method. New 802.11n agreements do not support this encryption method, so this encryption method is not recommended unless your wireless client is incompatible with another encryption method.

Default key: Select the current default key number.
WEP Keys (1 to 4): Set up different keys according to the encryption length and type. There are two kinds of encryption lengths which are available: 64-bit and 128-bit. There are two kinds of key types available: Hex (Hexadecimal) and ASCII. If you use Hex, the key characters can be 0 to 9 and/or A to F. If you use ASCII, then any ASCII characters on the keyboard can be used. If you choose the Hex key type, the key would be 10 or 26-bit hex characters. If you choose the ASCII key type, the key would be with 5 or 13-bit ASCII characters.

WPA-PSK
This is a pre-sharing key called Wi-Fi Protect Access. It is a standard new encryption technology that provides two more powerful encryption methods than WEP does: TKIP (Temporary Key Integration Agreements) and AES (Advanced Encryption Standard). The setting of this key can change the password dynamically, improve the WEP security effectively, and resist hacking more effectively. It is one of the most common encryption methods used.

WPA algorithm: Select an encryption method such as AES or TKIP. The TKIP algorithm would jumble the code by using a hash algorithm and by adding a complete-checking character, ensuring against tampering with the password.
Pass Phrase: Enter the key which should have 8-63 ASC II characters or a 64-bit hexadecimal (0 to 9 and/o r A to F) character.
Key Renewal Interval: Enter the key-renewal length of time (seconds). (The default is 3600.)

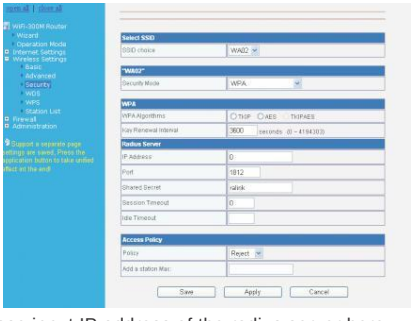
WPA2-PSK
This is a pre-sharing key called Wi-Fi Protect Access Version 2, which can be compared with WPA-PSK. The encryption that WPA2-PSK offers is better than the encryption that WPA-PSK offers but it does not adapt to all LAN cards . Please refer to the WPA-PSK section for the settings procedure .

WPA-PSK/WPA2-PSK

It supports the WPA-PSK /WPA2-PSK encryption so that clients can access the Internet using WPA-PSK or WPA2-PSK encryption. Please refer to the WPA-PSK section or the WPA2-PSK section for the setting procedure.

WPA

This authentication protocol is based on RADIUS server. This security mode is used when a RADIUS server is connected to the Router.



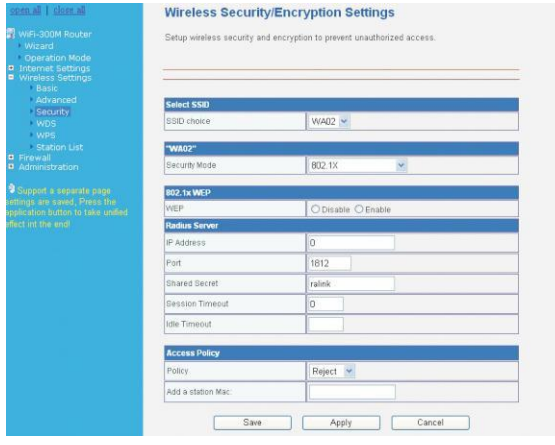
Radius IP Address: P lease input IP address of the radius server here.
Radius Port: Please input the port number of the radius server here.
Shared key: The encryption key that the router is authenticated through RADIUS server.
Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.

WPA2

This authentication protocol is 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.

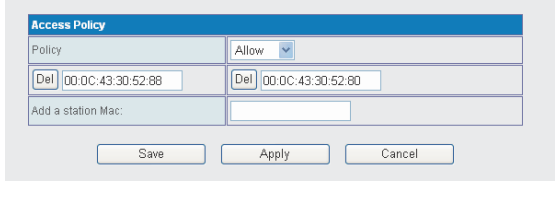
802.1X
This security mode is used when a RADIUS server is connected to the Router. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel.
The final purpose of 802.11x 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

⚠ **Note**: In order to improve your security level, please do not use a password which is simple or easy to remember.

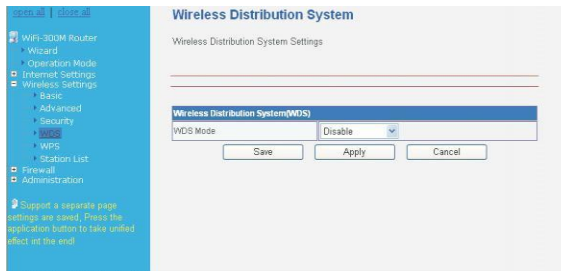
Access Policy
You may provide wireless-access setting strategies based on MAC to allow or refuse the access of selected MAC addresses. Within the same SSID, only the Enable or Disable functions may be set:



Disable: When the Disable function (in the pull-down menu under the security mode) is selected, the access strategy function is disabled. It stops access control of the wireless devices listed on the MAC list. When the Disable function in the pull-down menu of Policy is selected, you can delete a relevant MAC by clicking on the Del button in the MAC list and then by clicking on the Apply button to submit the order and to restart the router.
Enable: When the Enable function is selected, the MAC address is added to the list to connect the router to it.

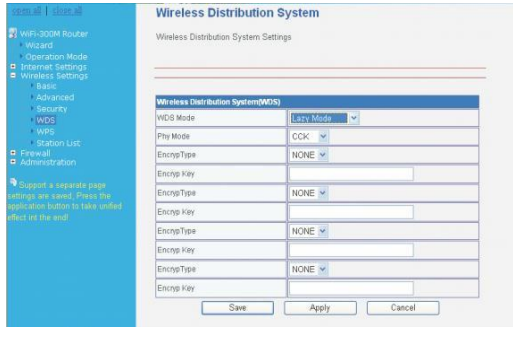
WDS

Click on “Wireless Settings | WDS”, enter your wireless distribution system interface to enable the WDS, or select the WDS (Wireless Distribution System) mode. WDS opens the W DS function on the radio equipment, establishes WDS trust and communication, extends the expansion wireless signal, and enables wide wireless network coverage.
Note: In order to use this function, the users must all be equipped with the WDS function and must all be WDS members. Also, the channel of each transmission point must not set the automatic channel choice. The same channel and same working mode are required to be set at each transmission point. WDS member machines are located at different IP addresses of an identical network segment. If the DHCP function is needed, enable just one of the machines and disable the other DHCPs. Use the identical product brand (model and series) to obtain better compatibility and to enable the connection for as long as possible. All SRX-WR products can support three modes: Lazy Mode, Bridge Mode, and Repeater Mode:



1.Lazy Mode:

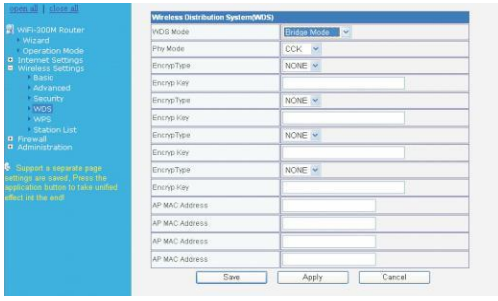
There is no need to fill in the BSSID of the opposite party in this mode. The W DS connection is now a passive connection, so the other party should fill in the BSSID address of the router. This means that the WDS mode of the other party’s machine can only be in a non-Lazy mode (Bridge or Repeater mode). Also, the WDS connections of the machines must be in the same physical mode, they must be on the same wireless channel (not on Auto), and they must have the same wireless encryption type (not supporting the Mix encryption type like WPAPSK/WPA2PSK). The machines must each have unique IP addresses on the same network. Open only the DHCP function; close all other DHCP functions.



Phy Mode: Select the supporting Physical mode (CCK, OFDM, or HTMIX) . The same physical mode must exist for all of the connecting equipment.
Encrypt Type: Select NONE (no encryption type). There are 3 types: WEP, TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) . You can set a maximum of four different types and can use these types to connect to four different clients.
Note: The same encryption type must exist for all of the equipment to the connection to be established.
Encrypt Key: Input a new key here after choosing the Encrypt Type.

2.Bridge Mode

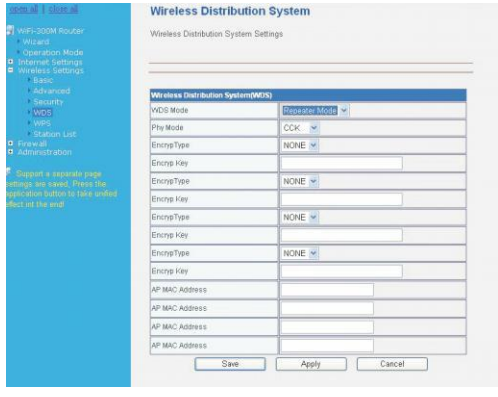
The Bridge mode requires the BSS ID of the other client to be filled in. The AP SSID of this router will be shielded so that the wireless client will not be able to determine this router. The wired client can use a WAN port to access the Internet.



Phy Mode: Select the supporting physical mode (CCK, OFDM, or HTMIX) . The same physical mode is required for all connecting equipment .
Encryp Type: Select NONE (no encryption type) . There are 3 types: WEP, TKIP (Temporal Key Integrity Protocol), and AES (Advanced Encryption Standard). You can set a maximum of four different types and can use these types to connect to four different clients.
Note: The same Encrypt Type must exist for all connecting equipment in order to establish a connection .
AP MAC address: Fill in the BSS ID of the WDS connecting equipment. You can fill in four different BSS IDs in order to enable one-to-many connections.

3.Repeater Mode

You have to input the BSSID of the connected equipment. Either a wireless client or a wired client (not a bridge) can connect to the network in the WDS mode.



WPS (Wi-Fi Protected Setup)
WPS is a standard used to establish an easy and secure wireless client and router. It is created by the Wi-Fi Alliance, so you don't need to choose the encryption type or to set the key. You can set the WPS by inputting the right PIN code or by pressing the WPS/RESET button on the panel.

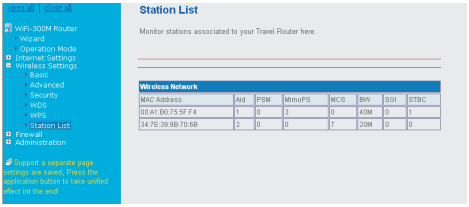
WPS Config: Select the Enable or Disable WPS function. You need to enable the WPS before you can use the WPS button on the panel to set the PBC encryption. (The default is Disabled)
WPS Summary: This displays the parameters of the current W PS settings,
including: WPS current status, SSID, authentication mode, encryption type, AP PIN, etc.
Reset OOB: Click this button to restore all WPS configurations to the default value.
WPS Progress: It supports 2 ways to configure WPS settings: PBC (Push-Button Configuration) and PIN (Personal Identification Number).
PBC: Select PBC or press the WPS button on the panel of the Router to 1 second. The WPS indicator will blink, allowing you to enable the client to implement the WPS/PBC.
PIN: You have to know the PIN code of the client to use this option. Fill in the code and save it; then use the same code for the client.
WPS Status: It displays the WPS current status. There are three states:
WSC Idle: It shows that the WPS current status is free.
WSC Start WSC Process: It shows that the WPS current status is sending a message.
WSC Success: It shows that access of the client to the AP is successful and that a WPS connection has been established.

AP client
AP client settings option, only when the router works in "AP client" mode , the option can be set. Including the wireless base station to be connected (wireless access point) of the SSID, BSSID and other parameters.

SSID: enter the name of wireless base station.
MAC Address (optional): enter the BSSID name which is connected to wireless base station.
Security Mode: Select the security mechanism.
Encryption Type: Select the wireless encryption type.
Pass Phrase: Enter the password for the encrypti on key.

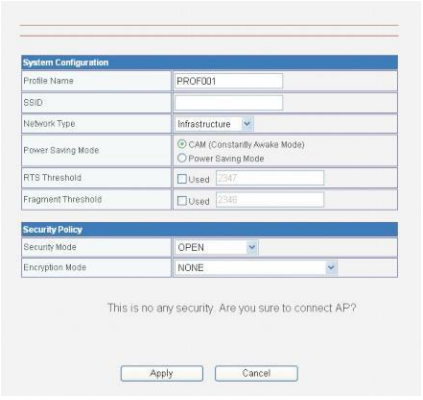
Station List

You may monitor stations associated with the AP here.



Profile

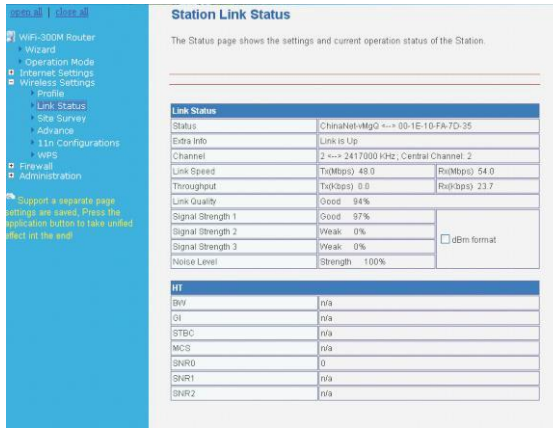
When the router works in Ethernet converter mode, click "Add button" on the "Profile" option, in the popup page, connect to the wireless base station to set the relevant parameters (such as the Service Set Identifier, encryption, etc.) , and confirm the submission, it can be set on the wireless base station (wireless access point) to implement binding settings.



You also can set the file list in the profile list, select the appropriate file, and then to operate by clicking the "delete ", "Edit", "activate" button.
Note: Only after the wireless base station to activate its binding come into effect.

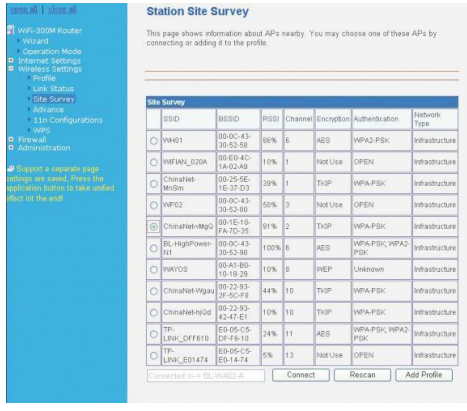
Link Status

When the router works in Ethernet converter mode, it acts as a wireless client that associated with the wireless base station its connection status information shown in the online status, such as l in e speed, the signal strength.

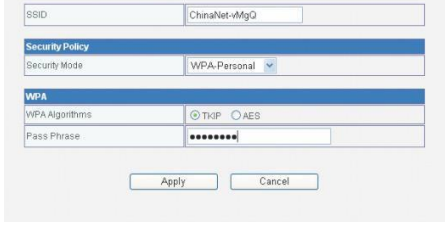


Site Survey

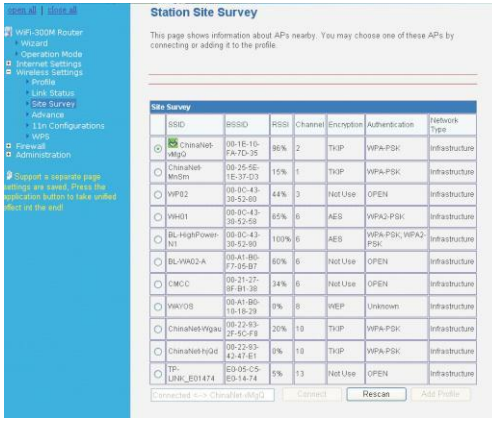
When the router works in Ethernet converter mode, scan the base station, the wireless router based near the station can be searched out, there will be a list shows service set identifier base station (SSID), the basic service set identifier (BSSID), received signal strength , channel , encryption type and other information.



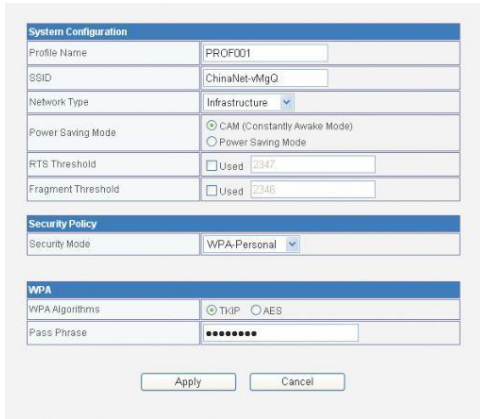
Select the appropriate base station, then click on "Connect" button, in the popup page you can set the password which associated with online authentication access.



When connection is successful, the service set identifier (SSID) can be shown as an green symbol, a shaking hands on the top.



In addition, you also can click on the "Add Profile", in the popup pages you can operate some associated settings, click "Apply" button, and then see the information by clicking the "Profile" .

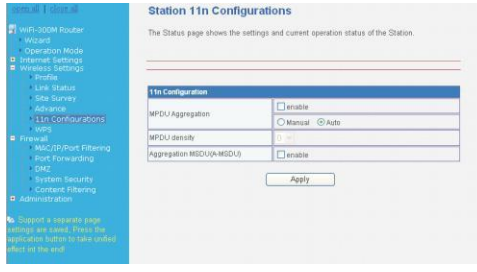


Advanced

When the router works in Ethernet converter mode, through the advanced settings option, you can set the parameters of wireless client mode, the number of wireless channel, B/G/N protection mechanisms and so on.

11n Configurations

When the router works in Ethernet converter mode, it acts as a wireless client working in 11n mode, you set some parameters through the "11n Configurations" option.



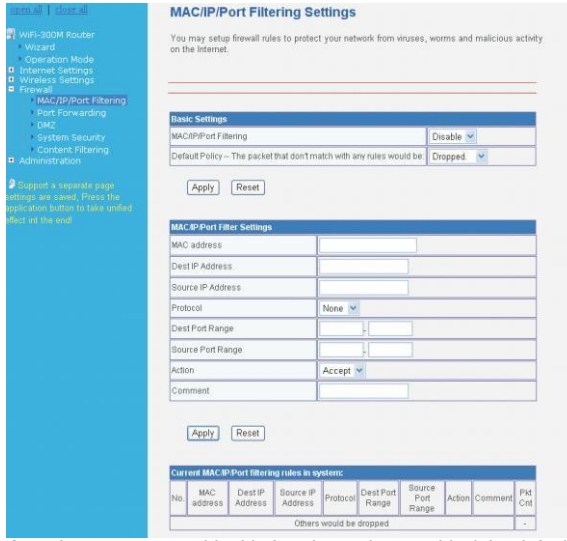
WPS

When the router works in Ethernet converter mode, you can set the WPS client function through the "WPS" settings option.

Firewall

MAC/IP/PORT Filtering

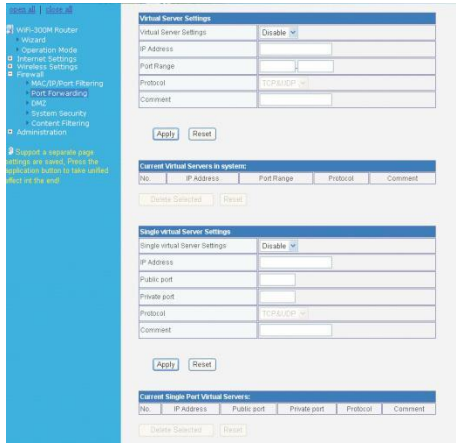
This function is used to manage the clients connected to the router, so that you can limit the client's Internet access. Before using this function, you need to choose Accept or Drop so that a data package that does not match the rule will be categorized as Accept or Drop accordingly. Then, fill in the corresponding rules. The rules depend on your needs, not all of the information needs to be filled in.
Example: If you want to prohibit a client whose IP address is 192.168.16.146 from accessing the Internet,
just choose Accept and fill in 192.168.16.146 for the source IP address. This function can improve LAN user security and manageability.



MAC/IP/Port Filtering: If you want to enable this function, select Enable (The default is Disabled).
Default Policy: You can state that packets that don't match any rules are to be dropped or accepted.
MAC address: Enter the MAC address for which you want to define a rule.
Dest IP Address: Enter the destination IP address you want to filter.
Source IP Address: Enter the source IP address you want to filter.
Protocol: Select a protocol to control data packages.
Dest Port Range: Enter the destination IP address you want to control. The start port number must not be greater than the end port number.
Source Port Range: Enter the source IP address you want to control. The start port number must not be greater than the end port number.
Action: Drop or accept the defined rule.
Comment: Describe the rule.

Port Forwarding

Port forwarding (port mapping) is the process of setting a virtual server to establish mapping relations between: WAN IP address, external port LAN server IP address, and internal port and LAN server IP addresses. This function allows the WAN user to access services (web, email, FTP, etc.) via the LAN server. By default, the wireless router will block initiating connection requests from the Internet to guarantee the security of the LAN. If you want to allow Internet users to access a serve r within the LAN, set up a virtual server.



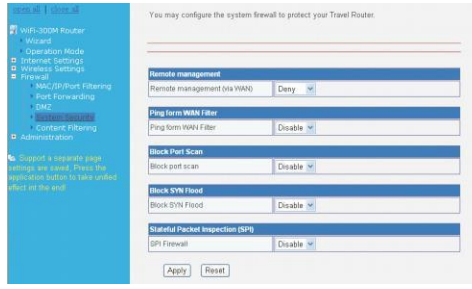
Virtual Server Settings: Enable or Disable the virtual server. (The default is Disabled)
IP address: Enter the IP address of the internal network which you want to set up as a virtual server (like 192.168.16.254).
Port Range: Server port range of the host in the internal network (like 80).
Protocol: Select the program protocol (TCP/UDP/TCP&UDP). (The default is TCP&UDP.)
Comment: Enter a comment. Example for the configuration above: “Visit 80 port. It will turn to the host whose IP address is 192.168.16.254”). Current Virtual Servers in system: Displays a list of virtual servers.
Single Virtual Server Settings: Enable or disable a single virtual server. (The default is Disable.)
IP address: Enter the IP address of the internal network which you want to set up a single virtual server.
Common Port: It is the port used to access the virtual server by a client.
Private Port: It is the real port opened by the virtual server.
Protocol: Select a program protocol (TCP/UDP/TCP&UDP).
Comment: Enter a comment. Current Single Virtual Server in system: It shows a list of virtual servers.

DMZ

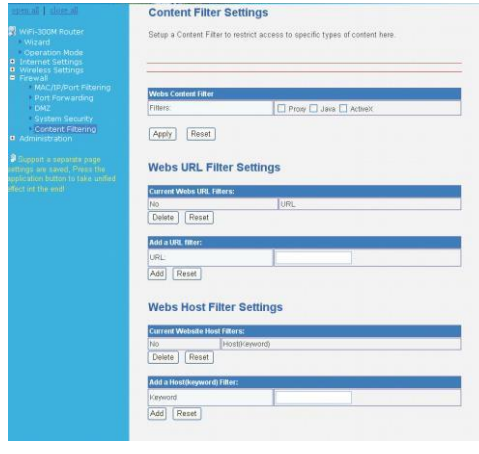
The DMZ host is the default virtual server. Its priority is lower than that of a virtual server. When a wireless router receives a connection request from an external network, the router scans the server list according to the number of the server port. If there is a matching port, it sends this request to the corresponding virtual server. If there is not, it checks for a matching DMZ host and sends a request to it; if it can’t find the host, it abandons the request. As for a detailed setting, you only need to fill in the host IP address, choose Enable, and click on Apply to save it.
Note: If you enable the DMZ function, this host will be exposed in the WAN, which would compromise its security. When you set the DMZ function, ensure that the number of port that is accessed is the same as the number of the port which the DMZ host enables.

DMZ Settings: Enables or disables DMZ host.
DMZ IP Address: Enables the IP address of the computer you want to display.

System Security
Select “Firewall | System Security” to enable or disable the remote management. You can allow or forbid a PC in the WAN network management router by using the WAN IP address of the router to access a web page. You can enable or disable ping packages and ping requests in the WAN filter, port scan block, SYN flood and in the SPI firewall function. **Caution**: If you enable the SPI firewall function, some firewall functions (like IP/MAC/PORT filtering) may stop working.



Content Filtering
In this interface, you can set Proxy, Java, and ActiveX content filtering in a web page when you browse the Web. You can al so set URL filtering rules according to your demand (by domain name, host name, and keywords) to prohibit a LAN PC from accessing a website.



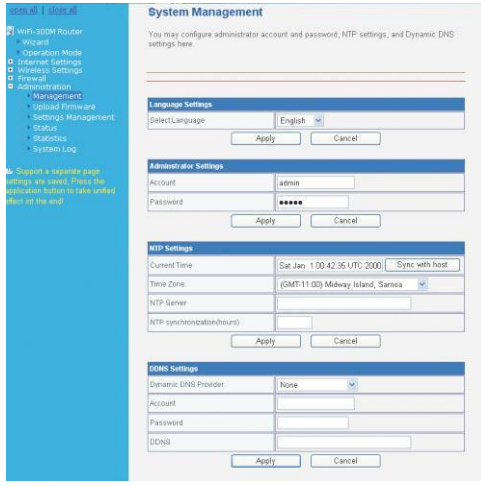
Webs Content Filtering: Select appropriate filter rules according to your demand.

There are 3 types of filters:
Proxy: Filter out web pages offered by agencies.
Java: Filter out Java in web pages.
Active-X: Filter out Active-X controls in web pages. Current Web URL Filtrates (filters): It is the set rule of URL filters. If you wish, you can delete the rule: select it and click on the Delete button.
Add a URL filter: Enter the URL address you want to filter. Click on the Add button to prohibit a website from being accessed. The new URL filter will appear at the top of the list.
Current Web Host Filters: It shows the defined rule of host filtrates. If you want to remove it, please select it and click on the Delete button.
Add a Host filter: Enter the keywords of the hostname you want to filter and click on the Add button to prohibit the access of a website. The new keywords will appear at the top of the list.

Administration

Management

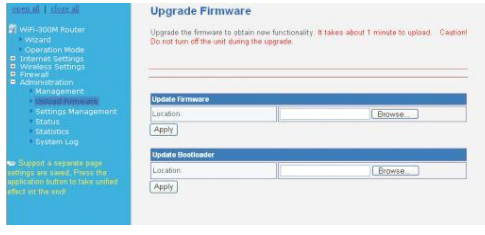
In the left pane, click on “Administration | Management” to set configurations such as: language, administration account, password, current time, NTP (Network Time Protocol), and DNS server.



Select Language: Choose one of three languages and click on the Apply button to complete the language setting.
Account: Enter a new user name for the device. (The default is **admin**)
Password: Enter a new password. (The default is **admin**). Click on the Apply button. The system will reboot and then ask you to enter the changed account name or password. If you forget the account name or password, then press and hold the reset button on the rear panel for 5 seconds to allow the system to reboot and restore all configurations to the factory-default settings.
Current time: The current time displays. Click on Sync with host to set time on the router to the time of the host.
Time zone: Choose your time zone (such as GMT+02:00 Romania).
NTP server: Input the URL address of the NTP server.
NTP synchronization (hours): This is the synchronization interval time with the NTP server.
DNS ISP: Select the DDNS (Dynamic DNS) service provider you wish to use.
DDNS Account: Input the account you registered with the DDNS service provider.
DDNS Password: Input the password you registered on the DDNS service provider.
DNS: Input the domain name you registered.

Upload Firmware

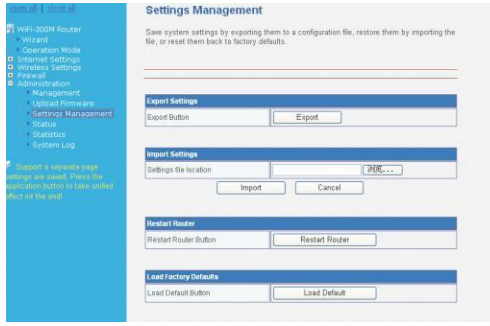
Click on “Administration | Upload Firmware” in the left pane to upgrade the firmware and update the system startup loader program.



Update Firmware: Click on Browse to choose the latest firmware file for the router. Click on the Apply button to upgrade it. The firmware will upgrade and then the system will reboot.
Update Boot-loader: Click on Browse to choose the latest system-loader program file for the router and then click on the Apply button to update it.
Important note: Do not turn off the power or disconnect the network from the router while the router is upgrading, otherwise the process may hang up or the equipment may get damaged.
Note: Before upgrading the router, ensure that the file is the latest one and that the corresponding product is the product of the same series.

Settings Management

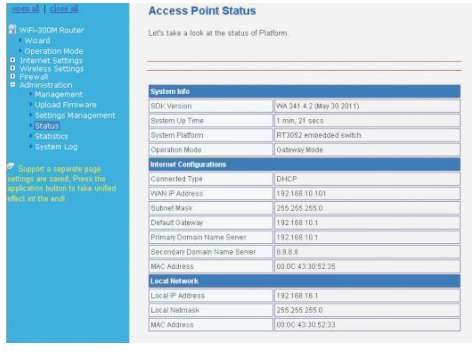
In the left pane, click on “Administration | Settings Management”. You can save the system settings by exporting them to a configuration file. Restore the settings by importing the file and resetting them to the factory defaults.



Export Settings: Click on Export to export the current system settings to a certain point. The filename is the default value and cannot be changed.
Import Settings: Click on Browse to see the directory to which you exported the system setting files, then choose the file, then click on the Import button, and then reboot the system.
Restart Router Button: Click this button, the device will restart the router.
Load Defaults: Click on this button to reset all of the configurations to the default values, which means that you will lose all of the settings that you previously set for the router. The system will then reboot.
Note: Please save the current configurations before importing another configuration file or restoring the factory settings.

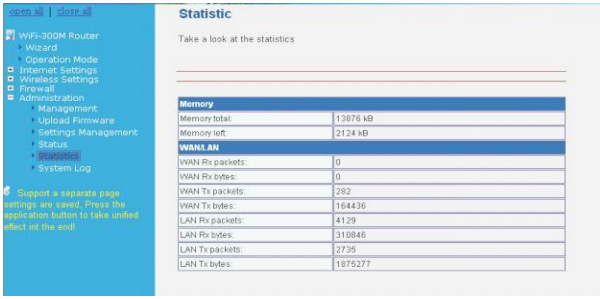
Status

In the left pane, click on “Administration | Status” to see on this page: SDK version, system uptime, system platform, operation mode, Internet configurations, and local network.



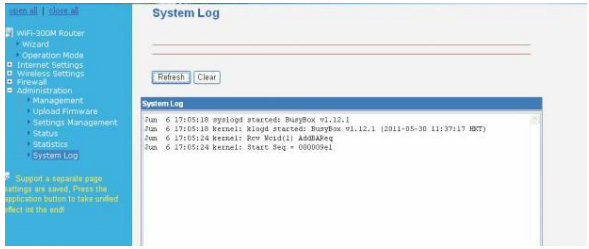
Statistics

Click on “Administration | Statistics” in the left pane to see the current system memory usage and the number of packets sent and received on the WLAN, LAN and WAN networks.



System Log

In the left pane, click on “System Log” to display the system login of the router. Query and easily troubleshoot the local system or remote monitoring to know which system has logged into the router. Click on the Clear button to delete the current login record.



Appendix A: Common Troubleshooting Methods

Appendix A provides some methods to resolve problems you may meet when you install the router and some steps to take to analyze the problems using diagnostic tools.
If you cannot resolve a problem, please contact the Technical Support department.
1.Problem: Power indicator does not light.
Solution: Check that the power supply is working and that you are using the proper power adapter.
2.Problem: WAN indicator does not light when a network cable is plugged in.
Solution: Check that the network cable has been inserted correctly into the WAN port.
3.Problem: LAN indicator does not light when a network cable is plugged in.
Solution: Check that the power connector and Internet cables are ok.
Check the connection from the cable to the port.
Check whether the Ethernet card is installed correctly in the PC.
4.Problem: Failed to visit the WEB setting page.
Solution: Ensure that your browser (IE6+ or Firefox 1.5+) is the latest version and that you have Java installed on your computer.
5.Problem: Cannot save the setting that I altered on the web page.
Solution: Ensure that after you complete your configuration changes on the interface that you click on the Apply button and that you then reload the system.
6.Problem: What should a user do if he knows nothing about the router's firewall when he enables the firewall function?
Solution: A router's firewall has strict rules, so a common user should disable the firewall. Only a user who is familiar with setting a router should consider setting a firewall. Before setting the rules, please plan all of the Internet activities that the LAN users need.

Appendix B: Technical Terms

1.DHCP (Dynamic Host Configuration Protocol)
It dynamically allocates IP address, subnet mask, and gateway for a host in a network.
2.DHCP Server (Dynamic Host Configuration Protocol Server)
It runs DHCP to allocate an IP address for a DHCP client.
3.DNS (Domain Name Server)
It resolves a domain name (like www.yahoo.com) into a corresponding IP address (like 216.115.108.243). A DNS message is distributed in the DNS server for the entire Internet, so the DNS server will check the domain name that we send a request to and search for the corresponding IP address when we visit a website. If this DNS server can't find the IP address, it will send the request to a superior DNS server to continue searching for an IP address.
4.FTP (File Transfer Protocol)
A protocol that describes how to transfer files between each computer in the network.
5.HTTP (Hypertext Transfer Protocol)
It is a standard protocol for transmission of a web page.
6.ICMP (Internet Control Message Protocol)
It is used to send an error message and some important network information (like ping command).
7.IEEE (Institute of Electrical and Electronics Engineers)
It is a technical institution that specially defines international standards.
8.ISP (Internet Service Provider)
It is the Internet accessing service.
9.LAN (Local Area Network)
It is a home network or an intranet (internal private network of a small or medium-sized business).
10.MAC (Media Access Control)
The MAC address is the hardware (permanent physical) address of a device that is specified by the manufacturer, connected to a shared network medium. It is composed of 6 pairs of hexadecimal characters (like 00-0F-E2-80-65-25). Each network component has a globally unique MAC address.

11.NAT (Network Address Translation)
It allows for more than one computer to be in a LAN, sharing an IP address of the public network. It shields LAN users who access the Internet and it plays an important role in ensuring network security. It is usually used by broadband routers.
12.NIC (Network Interface Card)
Located in a PC, it provides a physical port to a cable connected to it. If it is an Ethernet NIC, it usually uses an RJ-45 port.
13.Ping
The ping command sends a message from one computer to another one to check whether it is reachable and active. It is a tool used to test whether the local computer can interchange information with another computer on the network. The local computer sends a message to a specified computer and if that computer receives the message, it responds to the local computer.
14.PPP (Point-to-Point Protocol)
It is the link layer communication protocol.
15.RJ-45
It is a standard plug used to connect to an Ethernet switch, a concentrator, and a router. A direct connecting cable and a crossover cable usually make use of this plug, along with a route function.
16.TCP/IP (Transmission Control Protocol/Internet Protocol)
It defines a group of protocols.
17.Telnet
It is an interactive program based on characters to enable a client (user on a computer) to log on to a distant host (another computer) via the Internet. Telnet allows a user a remote login and setting device.
18.WAN (Wide Area Network)
It is a data communication network covering a large geographic range (like the Internet).
19.Web page
It is a website file on the WWW (World Wide Web). A website may contain hyperlinks (text or images) to open other web pages. A homepage is the top-level web page of a website.
20.Broadcast
It sends data to all computers in a network.
21.Domain name
It is the unique key component of a URL that identifies a file by its name on the Web. The domain name is much easier to remember than the corresponding IP address (a series of numbers).
22.Ethernet
It is a network technology used for LANs. A twisted-pair cable is usually used for transmission. Ethernet data transfer rates (radio frequency signals) between computers are either 10 Mbps or 100 Mbps.
23.Firewall
It can protect a computer or LAN from an unwelcome visit or a malicious attack.
24.Package
It is made up of data and other information, including the source and destination addresses, on a network.
25.Port
It is physical interface on a computer or router in which a connector is plugged to allow data in or out.
26.Protocol
It is a group of rules used to manage data transmission. Interconnected equipment must follow the rules to transfer data successfully.
27.Long distance
It is a long way between two points (like a staff member on a business trip logging in to a company network far away).
28.Route
It is the path taken for data to travel between computer networks. A router forwards the data between them.

Router Wireless Serioux

Ghid de utilizare

Vă mulţumim pentru alegerea acestui router wireless broadband. Înainte de utilizarea routerului, vă rugăm să citiţi cu atenţie prezentul ghid de utilizare, acesta conţinând informaţii despre toate setările de bază. Specificaţiile menţionate în ghidul de utilizare fac referire la routerele wireless broadband seria SRX-WR150 şi seria SRX-WR300. Imaginile din prezentul manual referitoare la interfaţă furnizează informaţii pentru utilizatori. În cazul în care interfaţa de configurare a produsului nu furnizează informaţii cu privire la o anumită setare, veţi configura routerul în funcţie de necesităţile dumneavoastră.

Caracteristicile produsului

◆Reuneşte într-un singur dispozitiv un router, un punct de acces wireless, un switch cu patru porturi şi un firewall.
◆Se conformează standardelor IEEE802.11n, IEEE802.11b şi IEEE802.11g.
◆Tehnologia MIMO utilizează semnalul reflectat pentru a mări de opt ori distanţa de transmisie faţă de standardul iniţial 802.11g şi restrânge zonele fără semnal din aria de acoperire wireless.
◆Asigură rate de transmisie de până la 150/300Mbps.
◆Suportă WMM pentru o mai bună transmisie a semnalelor audio şi video.
◆Suportă metode de criptare 64/128-biţi WEP, WPA, WPA2 şi autentificare 802.1x.
◆Metodă de criptare WPS (PBC şi PIN) pentru a elimina necesitatea memorării parolelor lungi.
◆Suportă management web de la distanţă sau local.
◆Suportă tehnologia Roaming wireless şi asigură conexiuni wireless cu eficienţă ridicată.
◆Suportă modul stealth SSID wireless şi controlul accesului pe bază de adresă MAC.
◆Suportă Auto MDI/MDIX.
◆Asigură un jurnal de sistem pentru înregistrarea stării routerului.
◆Suportă filtrare adresă MAC, NAT, NAPT.
◆Suportă UPnP şi DDNS.
◆Suportă controlul accesului asupra 30 de adrese MAC.
◆Suportă server şi client DHCP.
◆Suportă SNTP.
◆Suportă selectare automată a canalelor wireless.
◆Suportă funcţia WDS (wireless distribution system - sistem de distribuţie wireless).

Conţinutul pachetului

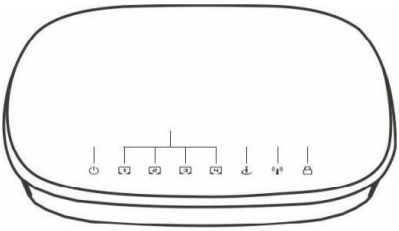
Router broadband wireless-N 150/300Mbps.
Adaptor de alimentare : DC5V/2A sau DC12V/1A (în funcţie de modelul achiziţionat) .
Manual de utilizare / ghid
Cablu de reţea Ethernet .
Ghid de instalare rapidă .

Important: La deschiderea pachetului, asiguraţi-vă că acesta conţine elementele de mai sus.
În caz contrar, vă rugăm să contactaţi distribuitorul.

Specificaţiile produsului

Standarde şi protocoale		IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE
Porturi	WAN	Port WAN RJ -45 10/100Mbps. (În ca zul funcţi onări i în modul gateway, este un port WAN, în celelalte moduri fiind port LAN.
	LAN	Patru port uri LAN RJ-45 10/100Mbps
	Domeniu de frecvenţe	2.4 - 2.4835 GHz
	Rate de semnal wireless	11n: Până la 150 / 300Mbps 11g: Până la 54Mbps 11b: Până la 11Mbps
	Canale de frecvenţe	De la 1 la 14 canale (în funcţie de ţara sau regiunea pe care o alegeţi)
	Spectru frecvenţe	DSSS (Direct Sequence Spread Spectrum)
Parametrii wireless	Tehnologie de modulaţie	DBPSK, DQPSK, CCK şi OFDM (BPSK/QPSK/16-QAM/64-QAM)
	Sensibilitate receptor	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
	Distanţă de transmisie	În interior: 300M. În aer liber: 500M (în funcţie de medi u)
Medii Ethernet		10Base-T: 3e UTP sau superioare; 100Base-TX: 5e UTP
	WLAN	Indicator de stare pentru WLAN (pornit/oprit)
Indicaţii	WAN	Indicator de stare pentru WAN
LED	LAN	Indicator de stare pentru LAN
	WPS	Indicator WPS
	POWER	Indicator de alimentare cu energie electrică
Condiţii de funcţionare		Domeniu de temperatură de funcţionare: 0ºC~45 ºC Domeniu de umiditate de funcţionare: 10%~90% (fără condens) Domeniu de temperatură pentru depozitare: -40ºC~70 ºC Domeniu de umiditate pentru depozitare: 5%~90% (fără condens)
Alimentare externă		Adaptor alimentare DC5V/2A sau DC12V/1A.

Indicatoare LED



Indicator de alimentare cu energie: ledul se aprinde când dispozitivul este alimentat cu energie.

Indicator de stare pentru LAN: ledul se aprinde când conexiunea este stabilită. Ledul clipeşte când sunt transmise sau recepţionate pachete de date.
Indicator de stare pentru WAN: ledul se aprinde când conexiunea este stabilită. Ledul clipeşte când sunt transmise sau recepţionate pachete de date.
Indicator de stare pentru WLAN: ledul se aprinde la activarea unei funcţii. Ledul se stinge când funcţia wireless este dezactivată. Ledul clipeşte când sunt transmise sau recepţionate pachete de date.
Indicator WPS: Indică activarea modului WPS (PBC sau PIN sunt opţionale în modul WPS).

Atenţionări privind instalarea routerului

În cazul unei prime instalări a reţelei wireless, vă rugăm să respectaţi regulile de mai jos pentru a evita deteriorarea dispozitivului sau diminuarea performanţelor din cauza unei utilizări sau a unei amplasări necorespunzătoare:
1. Routerul nu trebuie amplasat în apropierea telefoanelor fără fir, a cuptoarelor cu microunde, a frigiderelor sau a altor surse de interferenţă.
2. În cazul în care există alte puncte de acces 2.4G în apropriere, se recomandă ca distanţa dintre dispozitive să fie de cel puţin 12 m şi evitarea oricăror canale adiacente.
3. Pentru recepţionarea în cele mai bune condiţii a semnalului wireless, routerul trebuie poziţionat corespunzător.
4. Nu amplasaţi routerul în apropierea pereţilor din beton armat sau a grilajelor metalice, aceste obiecte putând bloca sau absorbi semnalele.
5. Routerul trebuie amplasat în interior, ferit de lumina soarelui, ploaie sau descărcări electrice.
6. Feriţi routerul de foc şi căldură şi păstraţi-l într-un loc care să permită aerisirea acestuia.

Observaţii

1. Rata maximă a semnalului wireless reiese din specificaţiile standardului IEEE 802.11n, volumul efectiv al transferului de date putând varia.
2. Condiţiile reţelei şi factorii din mediul ambiant , inclusiv traficul de reţea, materialele de construcţie, structura construcţiei, precum şi cheltuielile alocate pentru reţea pot reduce volumul efectiv al transferului de date.
3. La realizarea prezentului manual, au fost luate toate măsurile necesare pentru a vă furniza informaţii corecte, dar acesta trebuie utilizat numai ca ghid.
4. Date fiind îmbunătăţirea produsului şi alte motive, manualul poate fi actualizat periodic fără nicio notificare!

Procedura de instalare hardware

Stabilirea conexiunii WAN

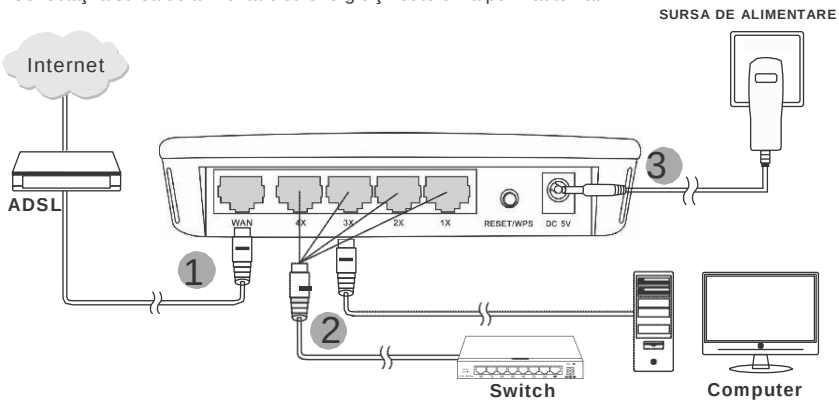
Conectaţi portul WAN al routerului la modemul xDSL cu ajutorul unui cablu.

Stabilirea conexiunii LAN

Conectaţi portul routerului la switch cu ajutorul unui cablu. De asemenea, puteţi conecta direct placa de reţea a computerului.

Conectare la sursa de curent

Conectaţi la sursa de alimentare cu energie şi routerul va porni automat.

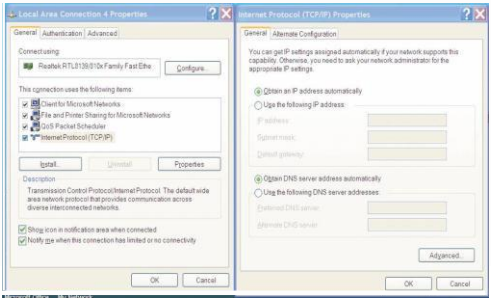


Management

Înainte de a utiliza routerul, trebuie să vă autentificaţi în pagina web. În continuare, este exemplificată procedura de autentificare utilizând sistemul de operare „Windows HP Home Edition Service Pack 3”:

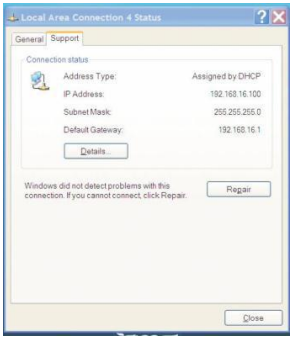
1. Accesaţi „Network Connections”, asigurându-vă că în computer este instalată o placă wireless. Dacă este afişată o pictogramă precum cea din imaginea de mai jos, adică ”Local Area Connection 4 Connected”, placa wireless a fost deja instalată în computer.

2. Setaţi adresa IP prin intermediul proprietăţilor „Internet Protocol (TCP/IP)”. În general, serverul DHCP al routerului este activ, deci vă rugăm să selectaţi „Obtain an IP address automatically” şi „Obtain DNS server address automatically” din fila General.

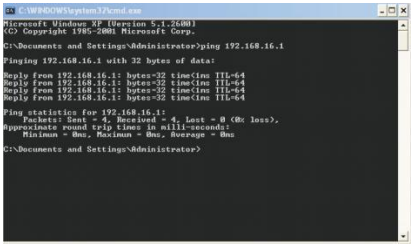


Sfaturi:

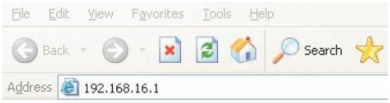
Selectaţi “Obtain an IP address automatically” numai atunci când serverul DHCP al routerului este activ.
De asemenea, puteţi seta dumneavoastră adresa IP. Cu toate acestea, adresa IP a computerului şi cea a routerului trebuie setate în aceeaşi subreţea şi nu poate fi alocată aceeaşi adresă IP. Adresa IP implicită este 192.168.16.1, iar masca de subreţea este 255.255.255.0, deci adresa IP nu trebuie să fie 192.168.16.1.
3. Puteţi găsi adresa atribuită în fila Support, după cum este prezentat mai jos:



4. Faceţi click pe Start | Programs | Accessories | Command Prompt, tastaţi ping 192.168.16.1, apoi apăsaţi Enter (după cum este arătat mai jos). Dacă pe ecran este afişată imaginea de mai jos, computerul dumneavoastră s-a conectat cu succes la router.

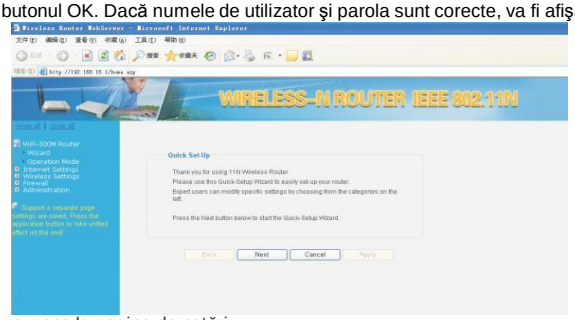


5. Accesaţi interfaţa routerului prin deschiderea unui browser web. Introduceţi http://192.168.16.1 (adresa IP implicită a routerului) şi apăsaţi Enter.



6. Browserul va deschide o pagină de autentificare după cum este arătat mai jos. Introduceţi ***admin*** în câmpul User name (numele de utilizator al administratorului) şi ***admin*** în câmpul Password (Parolă). Faceţi click pe butonul OK.

7. Faceţi click pe butonul OK. Dacă numele de utilizator şi parola sunt corecte, va fi afişat un ecran de configurare WEB.

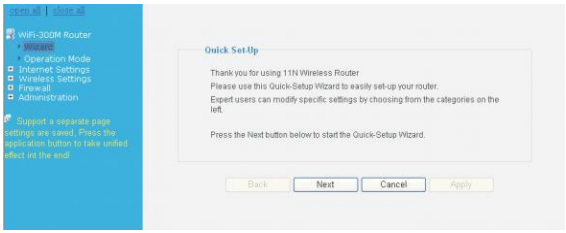


8. V-aţi conectat cu succes la pagina de setări.

Asistentul de configurare

Routerul dispune de diverse funcţii şi include un asistent de configurare. Asistentul de configurare vă îndrumă în vederea finalizării setărilor de bază, chiar dacă nu sunteţi familiarizaţi cu routerul.

1. Faceţi click pe „Wizard” în partea stângă a ecranului şi click pe “Next” în partea dreaptă, sub „Quick Set-Up”. Va fi demarată procedura de configurare a routerului.



2. Acest produs suportă oricare dintre cele cinci cel mai frecvent utilizate moduri de accesare a unei reţele. Selectaţi un mod în funcţie de preferinţele dumneavoastră. Modul implicit este preselectat. Celelalte patru moduri afişate sub modul implicit necesită configurarea parametrilor pentru conexiunea în reţea. Daca nu cunoaşteţi parametrii, contactaţi furnizorul de servicii Internet. După selectarea modului, faceţi click pe butonul “Next”.

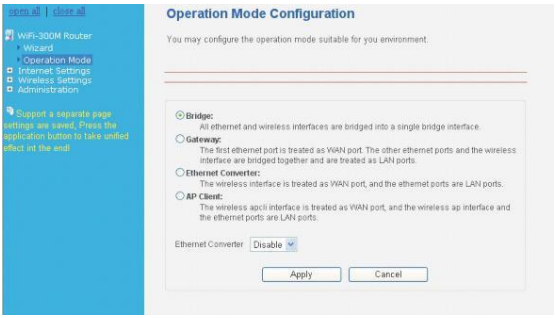
3. Puteţi seta un nume de reţea şi tipul de criptare corespunzător pentru setările reţelei wireless, după cum este prezentat mai jos. Faceţi click pe butonul “Apply” pentru a valida informaţiile de configurare. Sistemul va reporni computerul pentru a finaliza configurarea de bază a routerului.

Moduri de funcţionare

Routerele wireless din seria SRX-WR150 sau SRX-WR300 sunt routere puternice, deoarece pot suporta patru moduri de funcționare: mod Bridge, mod Gateway, mod Ethernet Converter şi mod AP Client (modul implicit este Gateway)

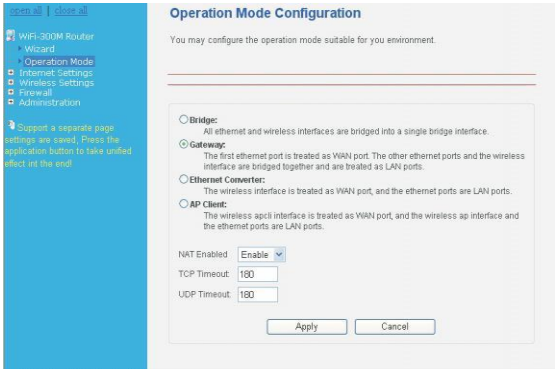
Modul Bridge:

Toate interfeţele Ethernet şi wireless sunt interconectate într-o singură interfaţă. Până în acest punct, routerul a funcţionat numai ca switch, nefiind capabil să acceseze WAN, iar firewall-ul a fost dezactivat)



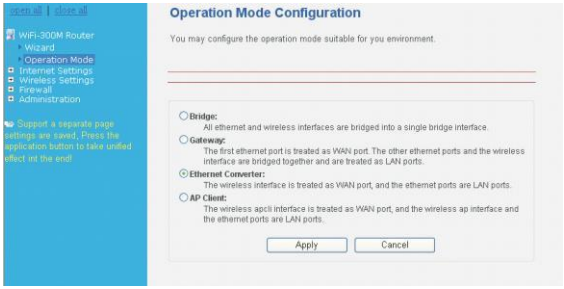
Modul Gateway:

Modul Gateway este modul implicit. Portul galben Ethernet este tratat ca port WAN. Celelalte porturi Ethernet şi interfaţa wireless sunt interconectate şi tratate ca porturi LAN (situaţie care face ca funcţia NAT să permită routerului schimbul de informaţii cu Internetul).

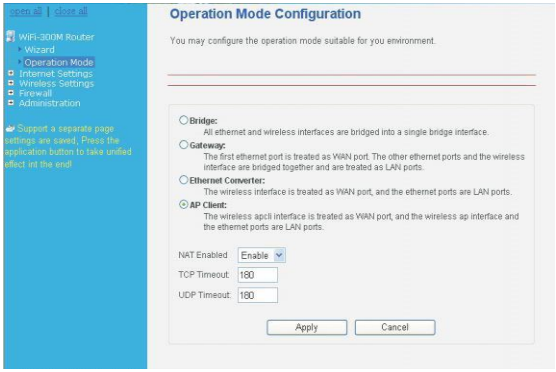


Modul Ethernet Converter:

Interfaţa wireless este tratată ca port WAN, iar porturile Ethernet sunt porturi LAN.



Modul AP Client:
Interfaţa wireless este tratată ca port WAN, iar interfaţa wireless AP şi porturile Ethernet sunt porturi LAN.



Configurare WAN

Acest router suportă mai multe tipuri obişnuite de conexiuni WAN. Selectaţi metoda de conectare utilizată de operatorul de reţea şi selectaţi informaţiile corecte privind parametrii (comunicate de către furnizorul de servicii Internet). După această etapă, puteţi partaja Internetul în mod normal. Dacă utilizaţi o conexiune dinamică, o conexiune dial-up, o conexiune dial-up PPPoE etc., există două metode prin care puteţi verifica funcţionalitatea conexiunii. Una dintre metode este accesarea directă a site-ului web, iar cealaltă este verificarea conexiunii în funcţie de starea configuraţiei Internet.

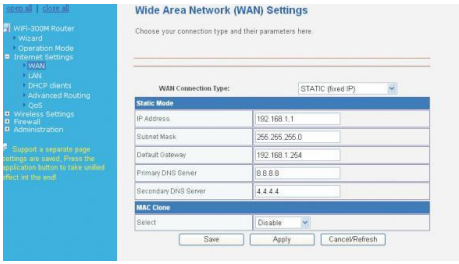
Internet Configurations	
Connected Type	PPPOE
WAN IP Address	58.60.132.45
Subnet Mask	255.255.255.255
Default Gateway	58.60.132.1
Primary Domain Name Server	202.96.134.33
Secondary Domain Name Server	202.96.128.86
MAC Address	00:0C:43:30:52:5A

Conexiune reuşită

Furnizorul de servicii Internet poate solicita o adresă MAC obligatorie oferită de acesta. Aceasta poate fi introdusă în bara pentru adresa MAC. Altfel, puteţi face click pe butonul Fill my MAC, caz în care adresa MAC a gazdei curente a conexiunii va fi completată automat în caseta de text.

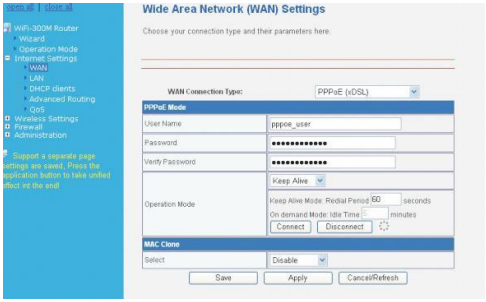
1. Conexiune DHCP (Auto Config)
Acest tip de conexiune este mai convenabil deoarece poate obţine în mod automat informaţii cu privire la parametri cum ar fi adresele IP şi gateway, aceştia putându-se modifica odată cu modificările realizate de operatorul de reţea al furnizorului de servicii Internet.

2. Conexiune Static IP (IP fix)
Dacă furnizorul de servicii Internet utilizează tipul de conexiune Static IP, vă rugăm să selectaţi Static (fixed IP) pentru configurarea parametrilor reţelei. Dacă aveţi nelămuriri cu privire la tipul de conexiune, vă rugăm să contactaţi furnizorul de servicii Internet.



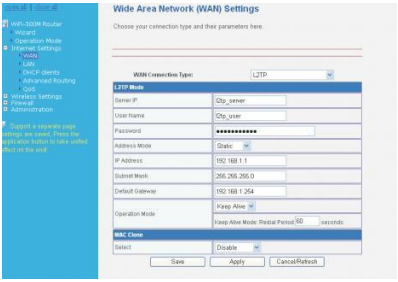
IP Address: Introduceţi adresa IP comunicată de furnizorul de servicii Internet.
Subnet Mask: Introduceţi masca de subreţea.
Gateway: Introduceţi adresa gateway WAN.
Primary DNS Server: Introduceţi adresa serverului DNS primar comunicată de furnizorul de servicii Internet. Fiecare domeniu are propriul DNS.
Secondary DNS Server: Introduceţi adresa serverului DNS secundar. Fiecare domeniu are propriul DNS.

3. Conexiune PPPoE (xDSL)
Conexiunea PPPoE este utilizată în special pentru reţele locale şi reţele pentru birouri mici.



User Name: Completaţi contul de internet obţinut de la furnizorul de servicii Internet. (Dacă aveţi neclarităţi, contactaţi furnizorul de servicii internet.)
Password: Completaţi parola comunicată de furnizorul de servicii Internet. (Dacă aveţi neclarităţi, contactaţi furnizorul de servicii internet.)
Operation Mode: Selectaţi unul dintre cele trei moduri de funcţionare (Keep Alive, Dynamic demand sau Manual demand):
1.Keep Alive: Modul Keep Alive permite routerului să se conecteze automat atunci când este pornit. Dacă reţeaua este deconectată de la router din cauza unor factori externi, sistemul va încerca să se reconecteze la reţea la intervale regulate (interval implicit 60 s), până la stabilirea unei conexiuni.
2.Dynamic demand: Routerul se conectează automat la LAN atunci când este trimisă o solicitare de acces.
Dacă nu este trimisă nicio solicitare de acces (perioadă liberă), routerul se deconectează de la reţea în mod automat. (Conexiunea de acest tip este aleasă de utilizatorii taxaţi în funcţie de durata conexiunii pentru a diminua costurile generate de serviciile Internet.)
3.Manual demand: Utilizatorul trebuie să formeze manual atunci când routerul este pornit. Faceţi click pe Connection pentru conectare la reţea. Faceţi click pe Disconnection pentru deconectare de la reţea.

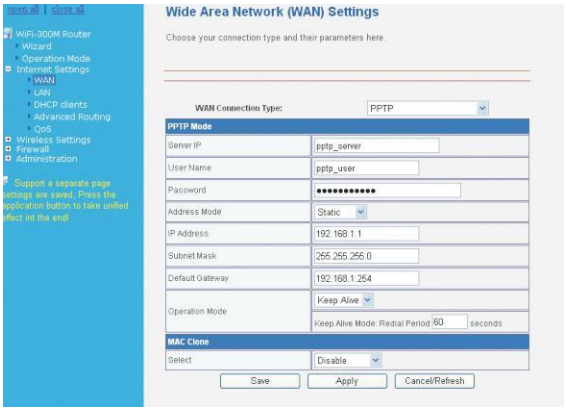
4. Conexiune L2TP



Server IP: Introduceţi adresa IP a serverului (obligatoriu) comunicată de către furnizorul de servicii Internet.
User Name: Introduceţi numele de utilizator L2TP (obligatoriu) comunicat de către furnizorul de servicii Internet.
Password: Introduceţi parola L2TP (obligatoriu) comunicată de către furnizorul de servicii Internet.
Address Mode: Obţineţi o adresă IP:
Dynamic: Selectaţi acest mod dacă routerul poate obţine o adresă IP în mod automat.
Static: Selectaţi acest mod dacă furnizorul de servicii Internet v-a comunicat o adresă IP statică.
IP Address: Selectaţi „Static" şi introduceţi adresa IP L2TP comunicată de furnizorul de servicii Internet.
Subnet Mask: Introduceţi adresa Subnet Mask comunicată de furnizorul de servicii Internet.
Default Gateway: Introduceţi adresa Default Gateway comunicată de furnizorul de servicii Internet.
Operation mode (2 moduri):
Keep Alive: Routerul se conectează automat la LAN atunci când este trimisă o solicitare de acces. Dacă nu este trimisă nicio solicitare de acces (perioadă liberă), routerul se deconectează de la reţea în mod automat. Dacă reţeaua este deconectată de la router din cauza unor factori externi, sistemul va încerca să se reconecteze la reţea la intervale regulate, până la stabilirea unei conexiuni.
Manual demand: Dacă reţeaua se deconectează de la router, selectaţi acest mod pentru a forma conexiunea manual.

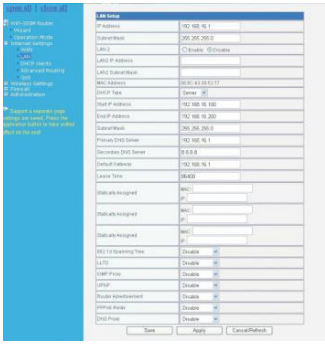
5. Conexiune PPTP

În cazul în care conexiunea este PPP Tunneling Protocol, furnizorul de servicii Internet vă poate comunica numele de utilizator şi parola. Pentru configurarea parametrilor, consultaţi instrucţiunile aferente conexiunii tip L2TP.



Configurare LAN

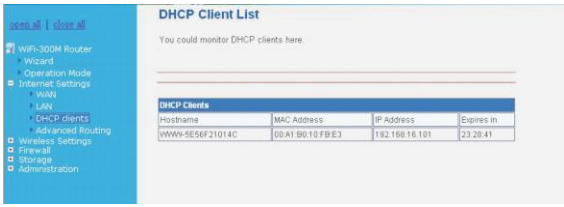
Selectaţi “Internet Settings | LAN” pentru a seta parametrii porturilor LAN (adresa IP, masca de subreţea, DHCP etc.).



Hostname: Denumirea reţelei la care se conectează routerul.
IP Address: Adresa IP LAN a routerului. (Adresa implicită este 192.168.16.1).
Subnet Mask: Masca de subreţea a routerului, în funcţie de starea reţelei. (Adresa implicită este 255.255.255.0.)
LAN2: Activaţi sau dezactivaţi adresa celui de al doilea port LAN, conform solicitării. Pentru activare, setaţi adresa IP şi masca de subreţea ale celui de al doilea port LAN.
LAN 2 IP Address: A doua adresă IP.
LAN 2 Subnet Mask: A două mască de subreţea.
MAC Address: Adresa MAC a portului LAN al routerului.
DHCP Type: Distribuiţi în mod automat adresa IP a computerului către reţeaua LAN utilizând serverul DHCP încorporat. Pentru activare, selectaţi DHCP ca server. În caz contrar, selectaţi Disable. (Setarea implicită este Server).
Start IP Address: Setaţi adresa IP iniţială pe care serverul DHCP o distribuie automat în funcţie de adresa IP LAN a routerului.
End IP Address: Setaţi adresa IP finală pe care serverul DHCP o distribuie automat în funcţie de adresa IP LAN a routerului.
Subnet Mask: Setaţi o mască de subreţea corespunzătoare, în funcţie de adresa IP iniţială/finală.
Primary DNS Server: Completaţi (opţional) adresa serverului DNS primar comunicată de către furnizorul de servicii Internet.
Secondary DNS Server: Completaţi (opţional) adresa serverului DNS secundar comunicată de către furnizorul de servicii Internet.
Default Gateway: Setaţi gateway-ul serverului DHCP în funcţie de adresa IP LAN a routerului. Gateway-ul implicit al routerului este 192.168.16.1.
Release time: Durata efectivă (în secunde) a adresei IP dinamice pe care serverul DHCP o alocă clientului gazdă. (Durata implicită este 86400. 86.400 secunde =1 zi.) În acest interval, serverul nu va aloca adrese IP altor gazde. (Puteţi seta durata în funcţie de preferinţele dumneavoastră, putând mări eficienţa serverului DHCP în ceea ce priveşte recuperarea adreselor IP neutilizate.)
Static specifies: De fiecare dată când serverul DHCP alocă adrese IP automat, acesta alocă dispozitivului utilizatorului o adresă IP fixă. Dacă este cazul, completaţi adresa MAC şi adresa IP.
MAC Address: Adresa MAC a computerului care rezervă o adresă IP statică.(Exemplu: 00:0C:43:80:88)
IP Address: Adresa IP rezervată pentru o gazdă în cadrul unei reţele. (Exemplu: 192.168.16.254).
802.11d Spanning Tree: Protocolul Spanning Tree, definit în 802.1d, este un protocol bridge-to-bridge din managementul conexiunilor. Acesta asigură o redundanţă de căi pentru prevenirea buclelor în reţea. (Nu există o setare implicită.)
LLTD: Opţiunile includ Enabled, Disabled şi Open. Dacă există un client LLTP, informaţiile cu privire la router vor fi afişate în mod automat.
Enable the IGMP agent: Împiedică apariţia unui „multicast flood” prin obţinerea şi controlarea în mod eficace a informaţiilor utilizatorului. Acesta ajuta la reducerea unui acord suplimentar în reţea şi a încărcării reţelei.
UPNP: Routerul asigură software intranet UPNP to P2P. (Nu există o setare implicită.)
Router advertising: Routerul va emite sau va răspunde la informaţii difuzate între fiecare nod la un ciclu fix, pentru indicarea existenţei acestuia. (Nu există o setare implicită.)
PPPOE Forward: Această funcţie permite unui computer local să formeze conexiunea PPPoE separat şi direct în modul gateway. (Nu există o setare implicită.)

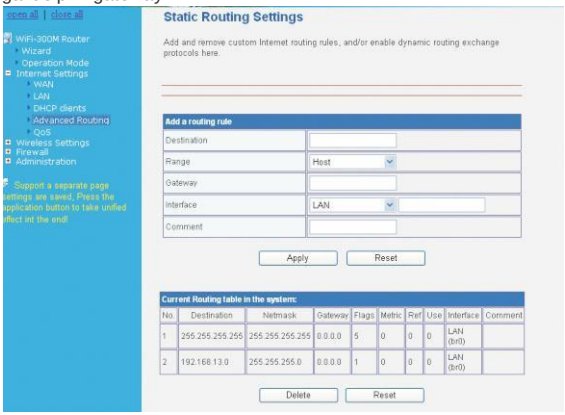
Clienţi DHCP

Selectaţi “Internet Settings | DHCP clients” pentru a verifica informaţiile cu privire la computerul pentru care DHCP alocă în mod automat adrese IP în LAN (cum ar fi denumirea reţelei, adresa MAC, adresa IP şi ora expirării).



Rutare avansată

Această funcţie reprezintă o opţiune pentru adăugarea unei rutări specifice unei anumite gazde, dacă este cazul. Utilizarea corespunzătoare a routerelor statice în cadrul unei reţele poate reduce problemele de selectare a rutării şi supraîncărcarea cu date a fluxurilor de rutare, aceasta putând mări viteza de transmitere a pachetelor de date. Prin setarea adreselor IP pentru masca de reţea şi gateway poate fi organizat un tabel de rutare. Adresa IP şi masca de subreţea de destinaţie sunt utilizate pentru a stabili o reţea/gazdă ţintă, astfel încât routerul să poată transmite pachetele de date către reţea/gazde prin gateway.



QOS

QOS este prescurtarea de la Quality of service (calitatea serviciului), funcţia sa principală fiind limitarea utilizării lăţimii de bandă a unui anumit server şi IP, în vederea asigurării necesarului de lăţime de bandă pentru o anumită aplicaţie şi prioritate de serviciu, precum şi în vederea partajării lăţimii de bandă cu restul utilizatorilor, astfel încât să se poată asigura un serviciu de transfer de date mai stabil şi mai fiabil.

Notă:

Formula de transformare dintre lăţimea de bandă şi Kbyte este 1Mbit=128Kbyte (kilobyte). În general, raportul ADSL de lăţime de bandă pentru încărcare şi descărcare este de unu la trei, lăţimea de bandă pentru încărcare a 1M ADSL este 42Kbyte şi pentru descărcare este 128Kbyte.

Setări wireless

Radio On/Off: Radio pornit/oprit.
Network Mode: Selectaţi unul dintre cele patru moduri de funcţionare a routerului: 802.11b, 802.11g, 802.11b/g şi 802.11b/g/n.
Network Name (SSID): Denumirea de reţea (cel mult 32 caractere) a semnalelor wireless setată pentru distingerea unei reţele individuale.
Broadcast Network Name (SSID): Activaţi sau dezactivaţi funcţia de difuzare SSID. Selectaţi disable. SSID este ascuns astfel încât un client wireless nu va putea scana echipamentul SSID. Clientul trebuie să cunoască SSID pentru comunicarea cu echipamentul.(Setarea implicită este Enable.)
BSSID (Basic Service Set ID): Se aplică pentru locul adresei MAC. În cazul punctelor de acces wireless, un grup de staţii de lucru wireless şi staţii de lucru wireless LAN denumite puncte de acces (AP) formează un dispozitiv de servicii de bază (BSD). Dispozitivul BSS al fiecărui computer trebuie să configureze acelaşi BSSID, adică logoul wireless al punctului de acces wireless.
Frequency(Channel): Selectaţi canalul de lucru al reţelei wireless. Cele două opţiuni sunt Automatic Selection şi Manual of Choice. Diferitele ţări şi regiuni utilizează numere de canale diferite. Pentru setări naţionale sau regionale, vă rugăm să consultaţi secţiunea privind setările avansate.
Operation Mode: Mixed Mode sau Green Field:
Mixed Mode: Placa wireless anterioară poate identifica Pre-N AP şi se poate conecta la acesta, dar transmisia va fi afectată într-o oarecare măsură. (Setarea implicită este Mixed Mode.)
Green field: Puteţi obţine o rată mai mare de transmisie, dar vor fi afectate negativ compatibilitatea şi securitatea sistemului.
Channel Bandwidth: Selectaţi 20 sau 20/40. (Setarea implicită este 20/40.)
Guard Interval: Selectaţi Long sau Auto. (Setarea implicită este Auto.)
MCS: Liste de Coduri de Modulaţie**:** Standardul 802.11n al ratei comunicaţiilor wireless LAN (WLAN). (Setarea implicită este Auto.)
Reverse Direction Access(RDG): Activaţi sau dezactivaţi această autorizare.
Extension channel: Selectaţi unul dintre canalele de extensie definite.
Space Time Block Coding (STBC): Selectaţi Enable sau Disable. (Setarea implicită este Enable.)
Polymerization MAC Business Data Unit (A-MSDU): Mesajul multiplu Ethernet este grupat într-un pachet mai mare printr-o anumită metodă. (Setarea implicită este Disable).
Auto Block ACK: Selectaţi Enable sau Disable. (Setarea implicită este Enable.)
Decline BA Request: Selectaţi Enable sau Disable. (Setarea implicită este Disable.)
HT Disallow TKIP: Selectaţi Enable sau Disable. (Setarea implicită este Enable.)

Anexa A: Metode generale de soluţionare a problemelor

Anexa A prezintă câteva metode de soluţionare a problemelor pe care le puteţi întâlni când instalaţi routerul broadband seria WA02-03 şi seria WP02-03, precum şi câteva măsuri necesare în vederea analizării problemelor prin intermediul instrumentelor de diagnosticare. În cazul în care nu puteţi soluţiona o problemă, vă rugăm să contactaţi serviciul de Asistenţă Tehnică.

1. Problemă: Indicatorul de alimentare cu energie nu se aprinde.
Soluţie: Verificaţi funcţionarea sursei de alimentare cu energie şi utilizarea unui adaptor corespunzător.
2. Problemă: Indicatorul WAN nu se aprinde la conectarea unui cablu de reţea.
Soluţie: Verificaţi introducerea corectă a cablului de reţea în portul WAN.
3. Problemă: Indicatorul LAN nu se aprinde la conectarea unui cablu de reţea.
Soluţie: Verificaţi racordul de alimentare cu energie şi cablurile Internet.
Verificaţi conexiunea dintre cablu şi port.
Verificaţi dacă placa Ethernet este instalată corect în computer.
4. Problemă: Nu poate fi accesată pagina de configurare WEB.
Soluţie: Asiguraţi-vă că browser-ul dumneavoastră (IE6+ sau Firefox 1.5+) este actualizat şi verificaţi instalarea Java pe computerul dumneavoastră.
5. Problemă: Nu poate fi salvată setarea modificată pe pagina Web.
Soluţie: Asiguraţi-vă că, după finalizarea modificării setărilor în interfaţă, aţi făcut click pe butonul Apply şi că aţi reiniţializat sistemul.
6. Problemă: Cum ar trebui să procedeze un utilizator care nu cunoaşte informaţii despre firewall-ul routerului în momentul în care activează funcţia firewall?
Soluţie: Firewall-ul unui router are reguli stricte, deci utilizatorii obişnuiţi ar trebui să dezactiveze această funcţie. Numai utilizatorii familiarizaţi cu setarea unui router vor avea în vedere configurarea unui firewall. Înainte de a stabili regulile, vă rugăm să luaţi în calcul toate activităţile legate de Internet de care utilizatorii LAN au nevoie.

Produsul achiziționat este conform cu următoarele standarde europene:

1999/5/EC Directive
ETSI EN 300 328 V1.7.1 (2006-05)
EN 301 489-1 V1.8.1 (2008-04)
EN 301 489-17 V1.3.2 (2008-04)
EN 50385:2002
IEC 60950-1:2005
EN 60950-1:2006+A11:2009

CE

Безжичен рутер Serioux

Благодарим Ви, че закупихте рутера Serioux. Прочетете ръководството преди употреба. Продукта се намира в три версии: с вградена антена N150, в външна антена N150 и с 2 антени N300 .

Характеристики

◆ Интегрира рутер, безжична точка за достъп, четири-портов суич и защитна стена (firewall) в едно устройство.

◆ Отговаря на стандартите: IEEE802.11n, IEEE802.11b и IEEE802.11g
◆ Технологията MIMO увеличава до 8 пъти разстоянието на предаване на сигнала спрямо стандартният 802.11g и намалява „мъртвите точки" на безжичното покритие.
◆ Осигурява 150/300Mbps скорост на предаване.
◆ Поддържа WMM, което увеличава качеството на аудио-видеото.
◆ Поддържа методи за кодиране 64/128-bit WEP, WPA, WPA2 и 802.1x стандарти за аутентификация и сигурност.
◆ WPS (PBC и PIN) метод за криптиране, който ви освобождава от запомнянето на дългите пароли.
◆ Поддържа remote/local Web management
◆ Поддържа технологията wireless Roaming и осигурява високо ефективна безжична връзка.
◆ Поддържа wireless SSID стелт режим и MAC контрол до адреса за достъп
◆ Поддържа Auto MDI/MDIX.
◆ Осигурява системен регистър, за да записва статуса на рутера.
◆ Поддържа филтър на MAC адресите, NAT, NAPT.
◆ Поддържа UPnP и DDNS.

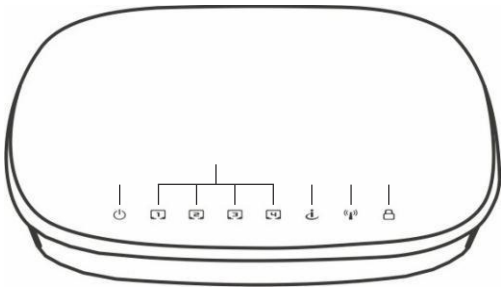
Съдържание на пакета

Рутър Wireless-N 150/300M.
Рутър: DC5V/2A или DC12V/1A.
Ръководство за употреба.

Особености на продукта

Стандарти и протоколи		IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE.
Порт	WAN	One 10/100M self-adapting RJ-45 WAN port. (When working in gateway mode, it's a WAN port but when working in any other mode, it's a LAN port.)
	LAN	4 порта 10/100M self- adapting RJ-45 LAN порта
	Честотен обхват	2.4-2.4835GHz
	Безжичен сигнал	11n: Up to 300Mbps 11g: Up to 54Mbps 11b: Up to 11Mbps
	Канали	1 до 14 канала(според страната, в която се използва)
Разширяване на спектъра		DSSS (Direct Sequence Spread Spectrum)
Параметри Wireless	Модулация на технологията	DBPSK, DQPSK, CCK и OFDM (BPSK/QPSK/16-QAM/64-QAM)
	Чувствителност на приемника @PER	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Разстояние на трансмисиите		Indoor: 300M, Outdoor: 500M (depending on environment)
Network Media		10Base-T: 3e UTP or above; 100Base-TX: 5e UTP
Инструкции LED	WLAN	Статус индикатор WLAN (on/off)
	WAN	Status indicator for WAN
	LAN	Статус индикатор за LAN
	WPS	WPS индикатор
	POWER	Power индикатор (вкл./изкл.)
Работна среда		Работна температура: 0℃～45℃ Работна влажност: 10%～90%(non-condensing) Storage temperature: -40℃～70℃ Съхранение при влажност: 5%～90%(без кондензация)
Външно захранване		Изход за адаптор: DC5V/2A или DC12V/1A

LED индикатори



Индикатор мощност: LED-а ще свети, когато устройството е включено.

Статус индикатор за LAN: LED-а ще свети, когато е установена връзка. LED-а ще примигва, когато данните са били предадени или приети.

Статус индикатор за WAN: LED-а ще свети когато е установена връзка. LED-а ще примигва, когато се предават данни.

Статус индикатор за WLAN: LED-а ще свети когато някоя функция е активна. LED-а ще се изключва, когато безжичната функция е недостъпна. LED-а ще примигва, когато се предават данни.

Предупреждения за инсталирането на рутера

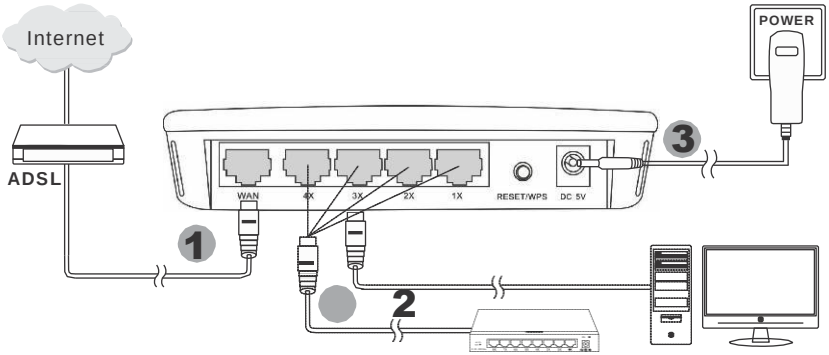
При първата инсталация на рутера, моля следвайте описаните правила, за да избегнете повредата на устройството или намаляването на капацитета му поради неправилно боравене или инсталиране:

1. Рутера трябва да бъде държан далеч от мобилни телефони, микровълнови печки, хладилници или други източници на смущения.
2. Препоръчва се да се спазва разстояние от 12 м. между две подобни устройства.
3. За да се получи максимален сигнал, дръжте рутера в нормално положение.
4. Дръжте рутера далеч от бетонни стени или метални парапети, тъй като тези обекти могат да блокират или абсорбират сигналите.
5. Рутера трябва да бъде държан на закрито, далеч от слънчева светлина, дъжд или мълнии.
6. Дръжте рутера далеч от топлина и огън.

Бележки

1. Прехвърлянето на данни варира в зависимост от мястото на разположение.
2. Използвайте това ръководство за обща употреба, настройките могат да бъдат направени различно от професионисти.
3. Ръководството може да бъде променяно без това да се оповестява предварително

Инструкции за свързване

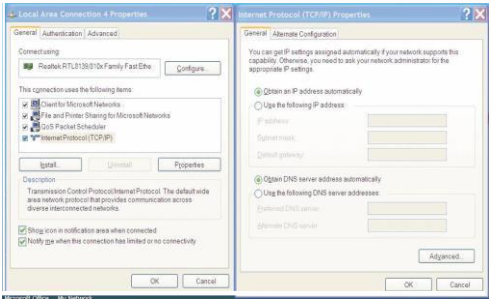


Управление и свързване

Преди първата употреба на рутера, следвайте инструкциите (пример с “Windows XP):

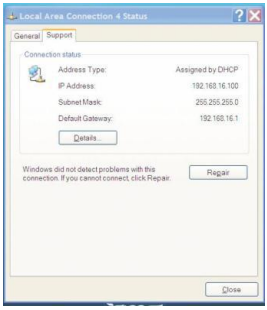
1. Проверете в “Network Connections”, дали компютъра има вградена мрежова карта.

2. Настройте вашият IP address през “Internet Protocol (TCP/IP)”. Обикновено, DHCP сървъра на рутера е включен, така че изберете “Obtain an IP address automatically” и „Obtain server address automatically”, под основният т

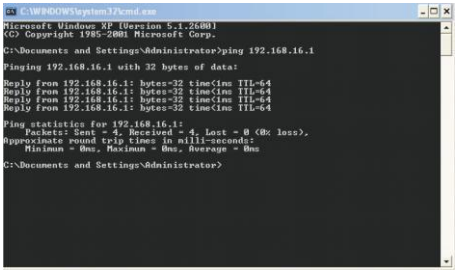


Съвети:

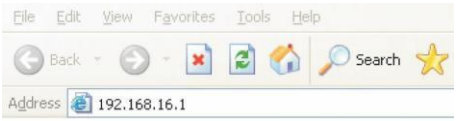
Изберете “Obtain an IP address automatically” само когато сървъра DHCP на рутера е активен. Също така, можете да настроите сами IP адреса. Въпреки това, IP адреса на компютъра и на рутера трябва да бъдат настроени в една и съща подмрежа и не може да бъде записан един IP адрес. IP адреса по подразбиране е 192.168.16.1, а маска на подмрежата е 255.255.255.0, така че IP адреса не трябва да бъде 192.168.16.1.
3. Можете да намерите зададения адрес в прозореца Support, както е показано по-долу:



4. Кликнете на Start | Programs | Accessories | Command Prompt, напишете 192.168.16.1, и натиснете Enter (както е показано по-долу). Ако на екрана се появи снимката от по-долу, това означава, че сте се свързали.



5. Влезте в интерфейса на рутера отваряйки един уеб браузър. Въведете http://192.168.16.1 (IP адреса на рутера) и натиснете Enter.



6. Ще се появи един прозорец за вписване, въведете user name/password

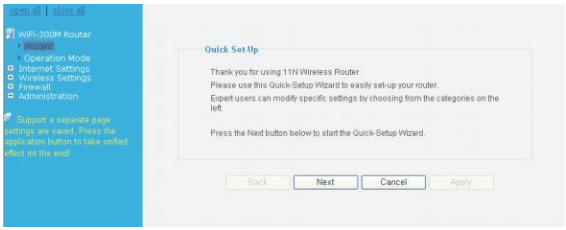
7. Кликнете на бутона OK. Ако потребителя и паролата са били правилни, ще се свържете.

8. Вече сте влезли в страницата за настройки.

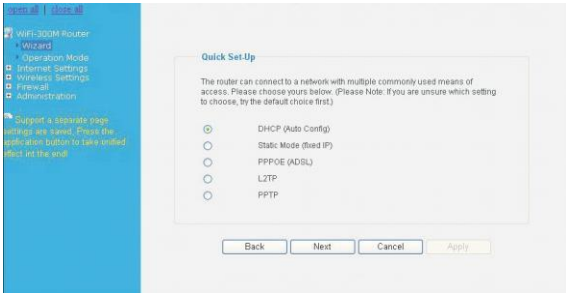
Wizard

Можете да изберете бързо конфигуриране с Wizard, дори и да не сте запознат с рутера.

1. Кликнете на „Wizard" в левия край и кликнете на „Next" в десния край "Quick setting". Така ще започне процедурата по настройката на рутера.



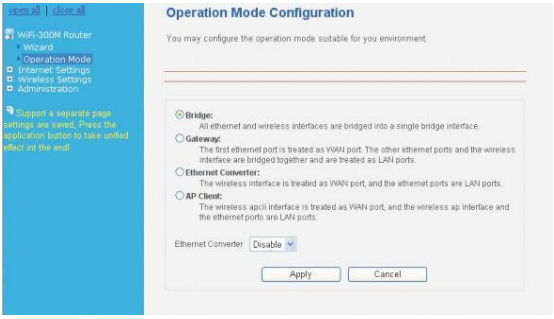
2. Това устройство поддържа всичките пет често използвани начина за свързване към мрежата. Режима по подразбиране е предварително избран. Изберете желаният вариант. Натиснете Next.



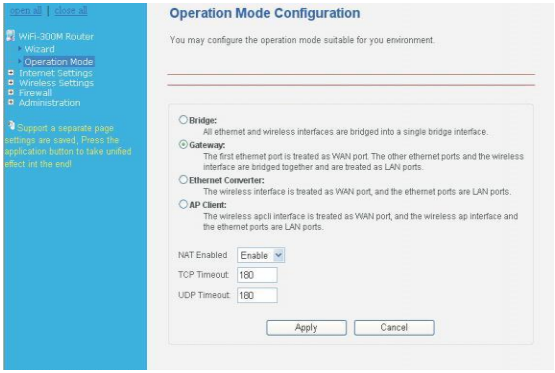
3. Можете да настроите името на мрежата и типа парола. Кликнете на бутона "Apply". Системата ще рестартира компютъра, за да завърши настройките.

Режим на работа

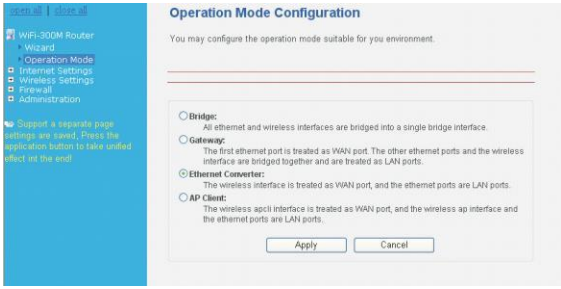
Рутерите SRX-WR150/300 поддържат 4 режима: Bridge mode, Gateway mode, Ethernet converter mode и AP клиент (режима по подразбиране е Gateway). Режима на работа е настроен на Bridge mode. Всички портове Ethernet и wireless-а са събрани на едно. Работи като един суич, като връзката wireless и firewall са дезактивирани.



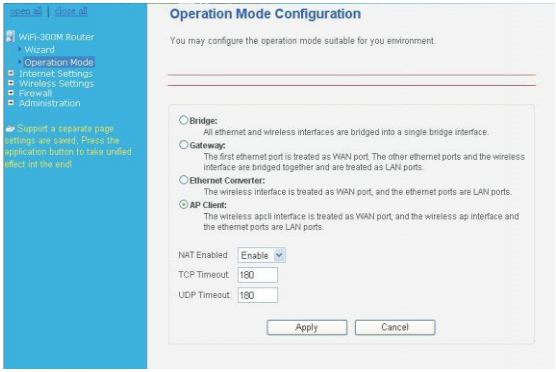
Настройка режим Gateway:
Gateway е режим по подразбиране. Жълтият Ethernet порт е за WAN port.



Настройка на режим Ethernet:
Wireless-а е разглеждан като WAN port, и портовете ethernet са LAN портове.



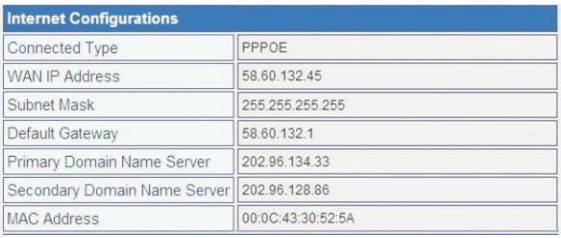
Режим на работа AP Client mode:
Wireless-а е разглеждан като WAN порт, wireless AP interface и ethernet портовете са LAN портове.



Интернет настройки

WAN

Този рутър поддържа няколко типа WAN връзки. Изберете връзката в зависимост от интернет доставчика ви. Ако използвате динамична връзка, dial-up връзка, PPPoE dial-up връзка, etc., има два начина да проверите дали връзката ще работи. Единият начин е да заредите директно една страница, а другият е да се разграничи според състоянието на интернет конфигурацията.



Internet Configurations	
Connected Type	PPPOE
WAN IP Address	58.60.132.45
Subnet Mask	255.255.255.255
Default Gateway	58.60.132.1
Primary Domain Name Server	202.96.134.33
Secondary Domain Name Server	202.96.128.86
MAC Address	00:0C:43:30:52:5A

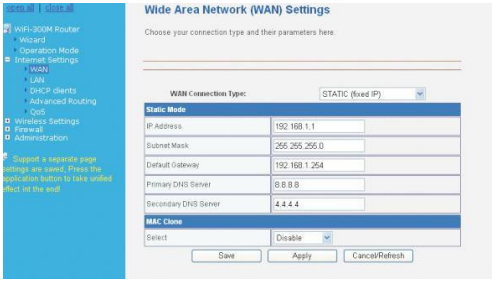
Успешна връзка

Някои интернет доставчици могат да искат блокиране на MAC адреса.

1. Режим на връзка 1: DHCP (Auto Config)

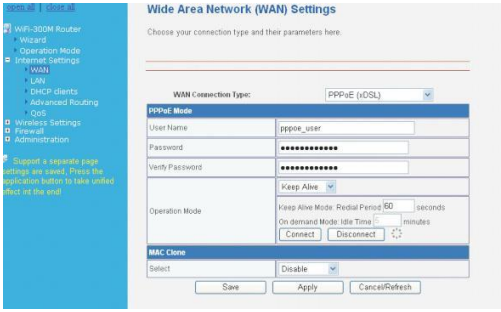
Този режим на свързване е удобен, тъй като търси автоматично IP адреса и адреса gateway.

2. Режим на връзка 2: Static (Fixed IP)
Ако вашият доставчик използва Static IP mode, моля изберете Static (fixed IP), за да настроите параметрите на мрежата. Ако не сте сигурни за режима, свържете се с вашият

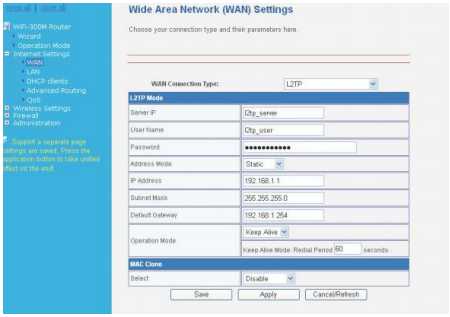


IP Address: Въведете статичният IP адрес даден ви от интернет доставчика.
Subnet Mask: Въведете subnet mask.
Gateway: Въведете адреса WAN gateway.
Primary DNS Server: Въведете главният DNS server address даден от интернет доставчика. Всеки доставчик има собствен DNS адрес.
Secondary DNS Server: Въведете DNS сървър адресите.

3. Режим на връзка 3: PPPoE (xDSL)
PPPoE се използва за домашни и малки офис мрежи.

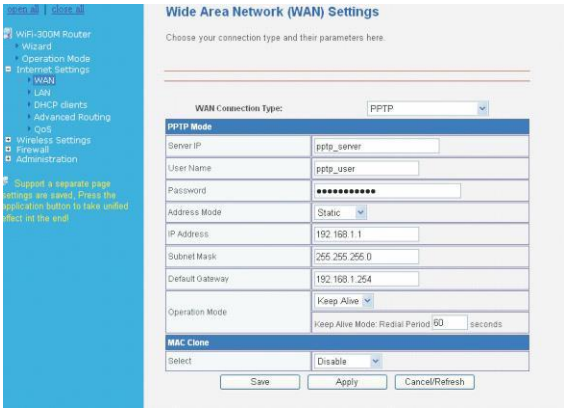


User Name: Въведете името на потребителя, дадено от интернет доставчика.
Password: Въведете паролата дадена ви от интернет доставчика.
Operation Mode: Изберете един от трите режима (Keep Alive, Dynamic demand, или Manual demand):
1. Keep Alive: този режим позволява на рутера да се свързва автоматично когато е включен. Ако се загуби връзката, периодично се опитва възстановяването ѝ.
2. Dynamic demand: Рутера се свързва автоматично към LAN, когато това се зададе. Препоръва се когато сте таксувани на трафик.
3. Manual demand: Потребителя свързва ръчно рутера към мрежата. Кликнете на Connection to the network. Кликнете на Disconnection to disconnect from the network.
4.Режим на връзка 4: L2TP



Server IP: Въведете IP адреса на сървъра даден ви от интернет доставчика и потребителското име L2TP User Name.
Password: Въведете парола L2TP, дадена ви от доставчика.
Address Mode: Получаване на IP address:
Dynamic: Изберете този режим ако рутера може да открие автоматично IP адреса.
Static: Изберете този режим ако доставчика ви е дал статичен IP адрес.
IP Address: Изберете “Static” и въведете L2TP IP адреса.
Subnet Mask: Въведете Subnet Mask .
Default Gateway: Enter the Default Gateway address supplied by your ISP.Operation Mode (2 modes):
Keep Alive: Рутера се свързва автоматично към LAN.
Manual demand: ако мрежата се изключва от рутера, изберете този режим за ръчно свързване.

5. Режим на връзка 5: PPTP
Протокола PPP Tunneling изисква данните от интернет доставчика.



Следните европейски стандарти са били следвани:

1999/5/EC Directive
ETSI EN 300 328 V1.7.1 (2006-05) EN 301 489-1 V1.8.1 (2008-04)
EN 301 489-17 V1.3.2 (2008-04) EN 50385:2002
IEC 60950-1:2005
EN 60950-1:2006+A11:2009

CE