

MC-420

wireless router ADSL

user's manual



MODECOM

Contents

1. Introduction	3	6.3.3 NAT Application	27
1.1 Introduction	3	6.3.4 NAT Mapping Types	28
1.2 Product Features	4	6.3.5 DMZ	28
2. Hardware Installation	6	6.3.6 Virtual Server	28
2.1 System Requirements	6	6.3.7 IP Address Mapping	29
2.2 Package Contents	6	6.4 ADSL	29
2.3 Front Panel Indicators and Description	6	6.5 QoS	30
2.4 Back Panel	6	6.6 VLAN	30
2.5 Connect Related Devices	7	7. Access Management	31
3. Connecting Wireless ADSL2+ Router via Ethernet	7	7.1 ACL	31
3.1 Setup Wireless ADSL2+ router via Ethernet Cable	7	7.2 IP Filter	32
3.2 Configure TCP/IP	7	7.3 SNMP	34
4. Configure Wireless ADSL2+ Router via HTML	14	7.4 UPnP	34
4.1 Login	14	7.5 DDNS	35
4.2 Navigating the Web Configurator	15	8. Maintenance	36
5. Interface Setup	16	8.1 Administration	36
5.1 Internet	16	8.2 Time Zone	37
5.1.1 ATM VC & QoS	17	8.3 Firmware	37
5.1.2 Encapsulation	17	8.4 System Restart	38
5.2 LAN	20	8.5 Diagnostic	38
5.2.1 Router Local IP	20	9. Status	38
5.2.2 Explaining RIP Setup	21	9.1 Device Info	38
5.2.3 DHCP Server	21	9.2 System Log	40
5.2.4 DHCP Relay	21	9.3 Statistics	40
5.2.5 DNS Relay	22	10. Troubleshooting	41
5.3 Wireless	22	10.1 Using LEDs to Diagnose Problems	41
5.3.1 Wireless LAN	22	10.1.1 Power LED	41
5.3.2 Access Point Settings	23	10.1.2 LAN LED	41
5.3.3 Multiple SSIDs Settings	23	10.1.3 ADSL LED	42
5.3.4 WDS Settings	23	10.2 Problems with the Web Interface	42
6 Advanced Setup	24	10.3 Problems with the Login Username and Password	42
6.1 Firewall	24	10.4 Problems with LAN Interface	42
6.2 Routing	24	10.5 Problems with WAN Interface	43
6.3 NAT	25	10.6 Problems with the Internet Access	43
6.3.1 What NAT Does	26		
6.3.2 How NAT Works	27		

MC-420

wireless router ADSL



Thank you for choosing our wireless ADSL router MC-420.

This broadband wireless ADSL router MC-420 is a all-in-one solution for home and SOHO network.

The built-in modem ADSL allows to reach fast Internet access. In addition, router has 4 port Ethernet switch 10/100 Mbps which allows to connect particular PC computers in local network using wired network.

The device is equipped with an Access Point of wireless network working in 802.11G standard. The built-in access point of wireless network allows to reach a connection up to 54 Mbps thanks to which using the Internet and working in the network is exceptionally convenient and efficient.

You can enjoy high-quality multimedia and real time applications such as on-line games, video on demand, VIP and other broadband services. The device also assures servicing many routing functions thanks to which users can configure their connection according to their demands and expectations.

In order to make using of our product easier, we recommend familiarizing yourself with the manual.

MODECOM takes care about the quality of its products not only by fulfilling, but also by forecasting its clients expectations.

MODECOM products users are used to high quality, advanced technology, reliability and functionality.

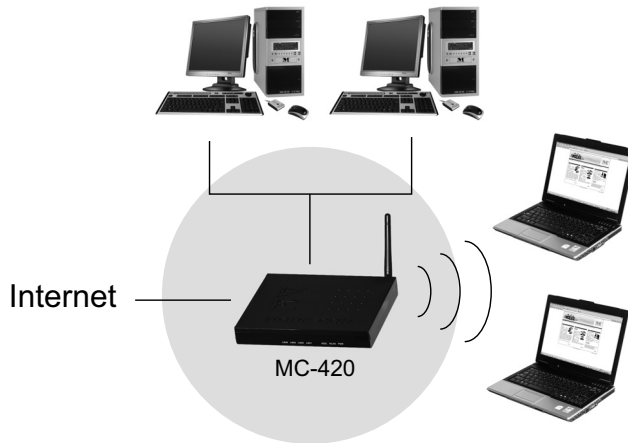
We make our exceptional products especially for YOU.

Choose better future - Choose MODECOM!

Copyright©2009 MODECOM S.A. All rights reserved. The MODECOM logo is registered trademark of MODECOM S.A.

1.2 Product Features

Application Diagram



High Speed Internet Access

This Wireless ADSL2+ router complies with ADSL / ADSL2 / ADSL2+ standards. It can support downstream rates of up to 24Mbps and upstream rates of up to 1Mbps. This ADSL2+ router is compliant with the following standards.

- ANSI T1.413 issue 2
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- G.994.1 (G.hs, Multimode)
- ITU-T G.992.3 (ADSL2 G.dmt.bis)
- ITU-T G.992.4 (ADSL2 G.lite.bis)
- ITU-T G.992.5 (ADSL2+; Annex A, I, J, L & M)
- Reach Extended ADSL (RE ADSL)

Quick Setup Wizard

Support Quick Setup Wizard Web GUI to configure this Wireless ADSL2+ router easily and quickly.

Multi-connection protocol support

- Multi Protocol over AAL5 (RFC1483 / 2684)
- Classical IP over ATM (RFC 1577)
- VC and LLC Multiplexing
- PPP over Ethernet (RFC 2516)
- PPP over ATM (RFC 2364)

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Universal Plug and Play (UPnP)

Universal Plug and Play is a standard that uses Internet and Web protocols to enable devices such as PCs, peripherals, intelligent appliances, and wireless devices to be plugged into a network and automatically know about each other. This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a centralized DHCP server. The ADSL router has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. It can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Device Management

- Web-based GUI Configuration / Management
- Command-line Interpreter (CLI)
- Telnet Remote Management
- Firmware upgrade via FTP / TFTP (Web-based GUI)
- Built-in Diagnostic tool and IP Ping

SNMP (Simple Network Management Protocol) Support

It's an easy way to remote control the router via SNMP.

10/100M Auto-negotiation Fast Ethernet switch

This auto-negotiation feature allows the router to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Multiple PVC (Permanent Virtual Circuits) Support

- Support up to 8PVCs.
- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells.
- ATM Forum UNI 3.1/4.0 PVC

Bridging / Routing support

- Ethernet to ADSL self-learning Transparent Bridging (IEEE 802.1D)
- IP routing-RIPv2 (backward compatible with RIPv1)
- Static IP routing
- Routing (TCP/IP/UDP/ARP/ICMP)
- IP Multicast IGMP v1/v2

Wireless

- IEEE802.11g compliance, backward compatible with 802.11b (at 11Mbps)
- 64/128 bits WEP Encryption
- WPA, WPA-TKIP/PSK
- MAC Address Filtering

Security

- PPP over PAP (Password Authentication Protocol; RFC1334)
- PPP over CHAP (Challenge Authentication Protocol; RFC1994)
- VPN (IPsec, PPTP, L2TP) pass through
- Built-in NAT Firewall
- IP-based Packet filtering
- Password Protected System Management

2. Hardware Installation

2.1 System Requirements

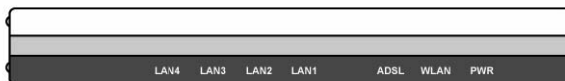
- Pentium III 266 MHz processor or higher
- 128 MB RAM minimum
- 20 MB of free disk space minimum
- RJ45 Ethernet Port

2.2 Package Contents

- Wireless ADSL2+ Router
- RJ-45 Ethernet cable
- RJ-11 Phone cable
- Power Adapter
- Quick Installation Guide

2.3 Front Panel Indicators and Description

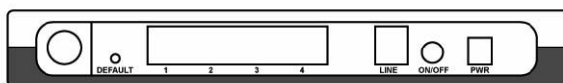
Front panel of this Wireless ADSL2+ router has LED indicators to display router's operating status.



Descriptions of LED status

PWR	When an active power adapter is connected with this router, this LED will light up.
WLAN	When WLAN card installed properly, this LED will be flashing. When transferring data, the LED will be steadily.
4	When port 4 connection with PC or Switch / Hub is established, this LED will light up.
3	When port 3 connection with PC or Switch / Hub is established, this LED will light up.
2	When port 2 connection with PC or Switch / Hub is established, this LED will light up.
1	When port 1 connection with PC or Switch / Hub is established, this LED will light up.
ADSL	When connection with Internet (ADSL Connected) is established, this LED will light up. When this LED is flashing: NO ADSL physical connection

2.4 Back Panel



PWR	Connect with power adapter
ON/OFF	Power switch button
LINE	Connect with phone cable
4	Connect with Ethernet Cable to Switch Hub or PC
3	Connect with Ethernet Cable to Switch Hub or PC
2	Connect with Ethernet Cable to Switch Hub or PC
1	Connect with Ethernet Cable to Switch Hub or PC
DEFAULT	Reset button

2.5 Connect Related Devices

- 1) Connect Router to LINE Plug the provided RJ-11 phone cable into LINE port on the back panel of the router and insert the other end into splitter or wall phone jack.
- 2) Connect Router to LAN Plug RJ-45 Ethernet Cable into LAN port on the back panel of the router and insert the other end of the Ethernet cable on your PC's Ethernet port or switch / hub.
- 3) Connect Router to Power Adapter Plug Power Adapter to PWR port on the back panel of the router and the other end to a power outlet.
- 4) Press ON/OFF button to start the router

Warning! Only use the power adapter provided in the package, otherwise it may cause hardware damage.

3. Connecting Wireless ADSL2+ Router via Ethernet

Your router can be managed from anywhere with the embedded Web configuration using a Web browser, such as Microsoft Internet Explorer or Netscape Navigator. Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled should be used. A screen resolution of 1024 by 768 pixels is recommended.

3.1 Setup Wireless ADSL2+ router via Ethernet Cable

If there is an available LAN card present on your PC, you just simply connect ADSL router and PC through the Ethernet cable. Once you establish Internet connection, you could browse the Web through the Ethernet cable.

3.2 Configure TCP/IP

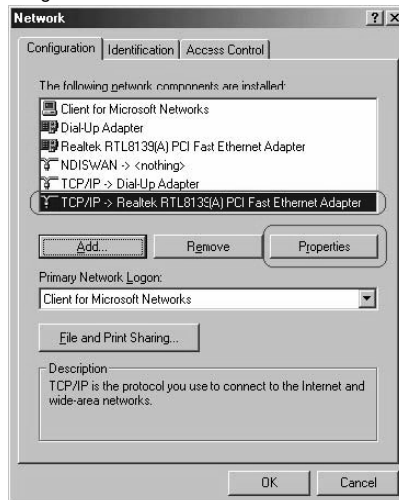
For Windows 98SE and ME

Step 1: Click Start then Settings and choose Control Panel

Step 2: Double click Network icon.

Step 3: Select Configuration tab, then choose TCP/IP from the list of installed network Components and click Properties button.

Step 4: You can setup the following configurations in two methods:

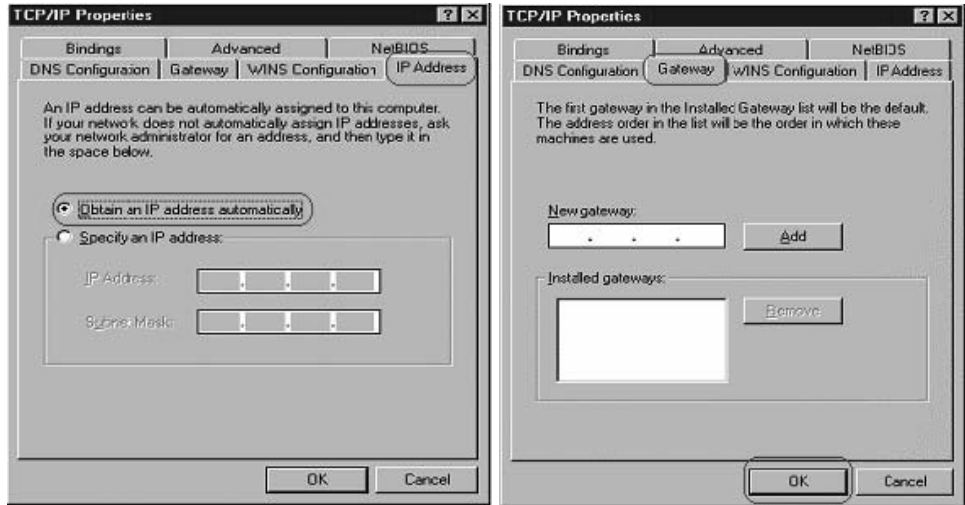


Option1: Get an IP from Router Automatically

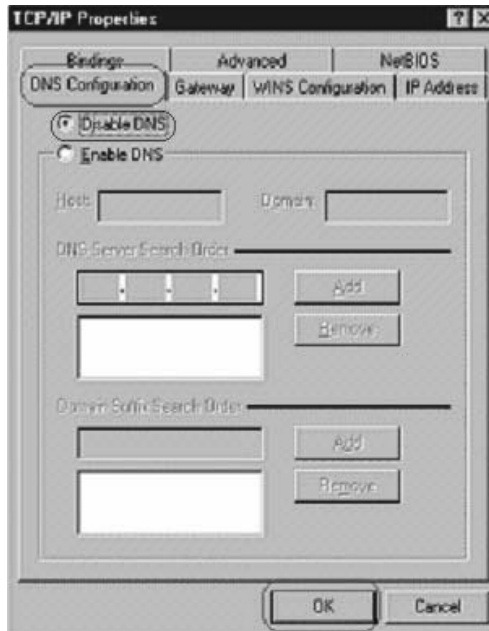
Select the IP Address tab.

In this page, click Obtain an IP address automatically radio button.

1) Select Gateway tab and click OK



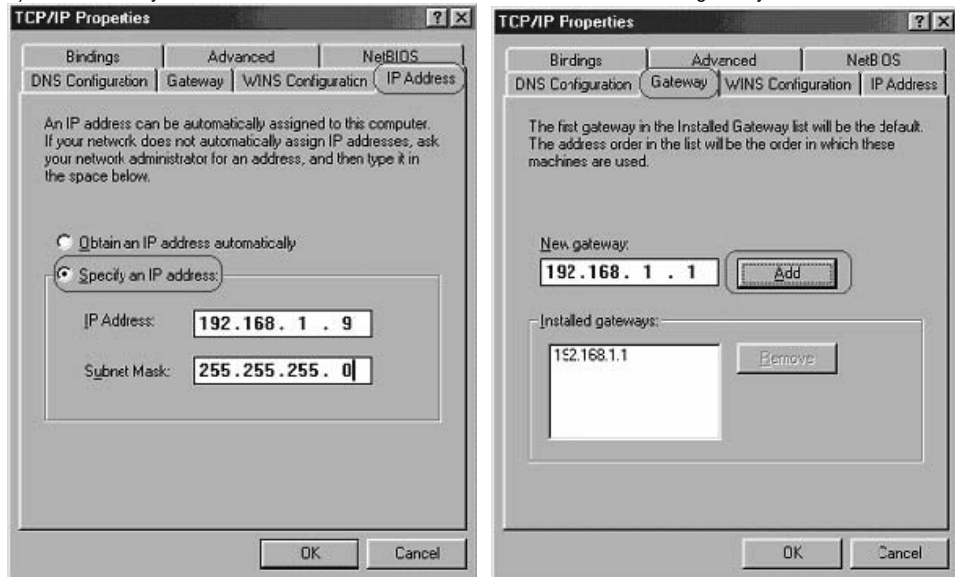
2) Then, select DNS Configuration tab and select Disable DNS then click OK to finish the configuration.



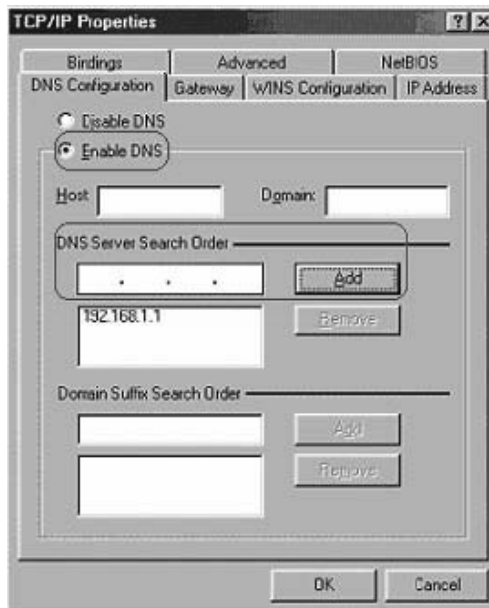
Option2: Configure IP Manually

1) At IP Address tab, select Specify an IP address, set default IP address for the Router is 192.168.1.1, so use 192.168.1.X (X is a number between 2 to 254) for IP Address field and 255.255.255.0 for Subnet Mask field.

2) Select Gateway tab and add default Router IP Address "192.168.1.1" in the New gateway field and click Add.



Under DNS Configuration tab, select Enable DNS and add DNS values (192.168.1.1) in DNS Server Search Order field then click Add.



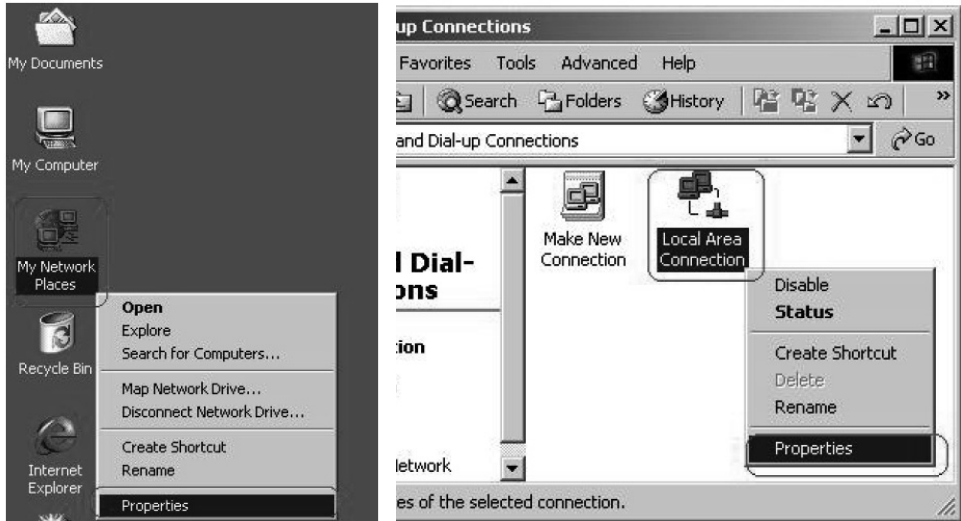
For Windows 2000

Step 1:

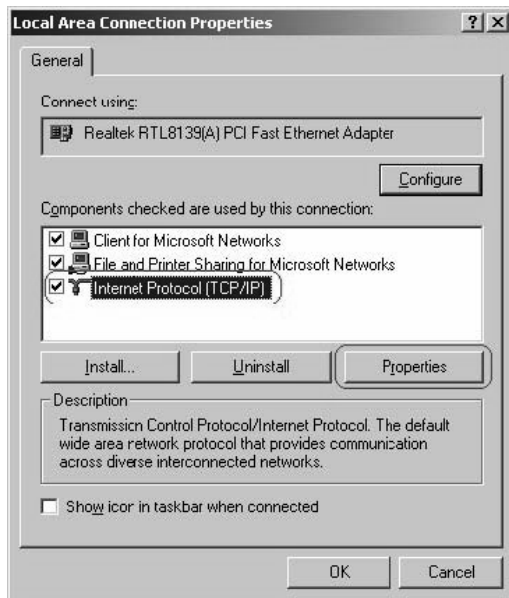
(a) Right-click My Network Places and select Properties in the main window screen

(b) Or, go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.

Step 2: Right click Local Area Connection (your local network hooked up with ADSL router) and select Properties:

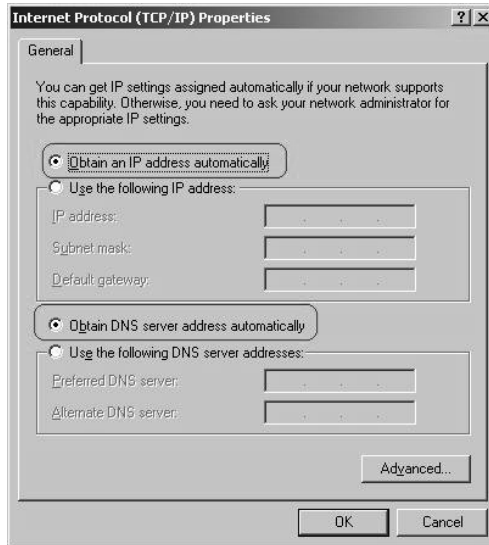


Step 3: Select Internet Protocol (TCP/IP) then click Properties:

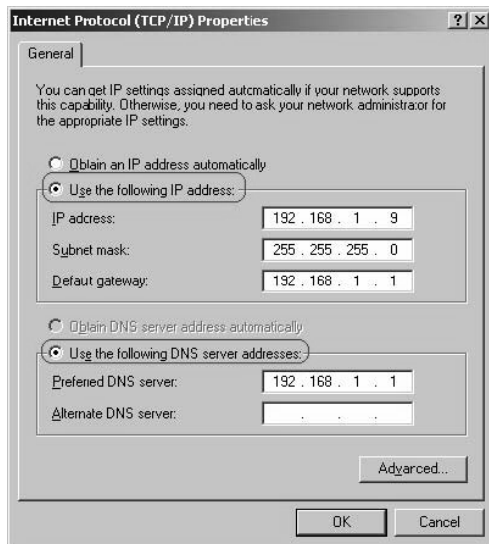


Configure IP Automatically:

Step 4: Select Obtain an IP address automatically and Obtain DNS server address automatically then click OK to complete IP configuring process.



Configure IP Manually: Step 4: Select Use the following IP address and Use the following DNS server addresses. IP address: Fill in IP address 192.168.1.x (x is a number between 2 to 254). Subnet mask: Default value is 255.255.255.0. Default gateway: Default value is 192.168.1.1. Preferred DNS server: Fill in preferred DNS server IP address. Alternate DNS server: Fill in alternate DNS server IP address.



WIRELESS ROUTER ADSL

For Windows XP

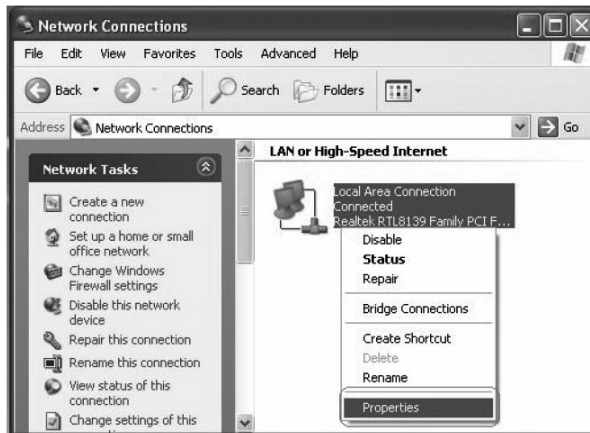
Step 1: Click Start then select Control Panel.



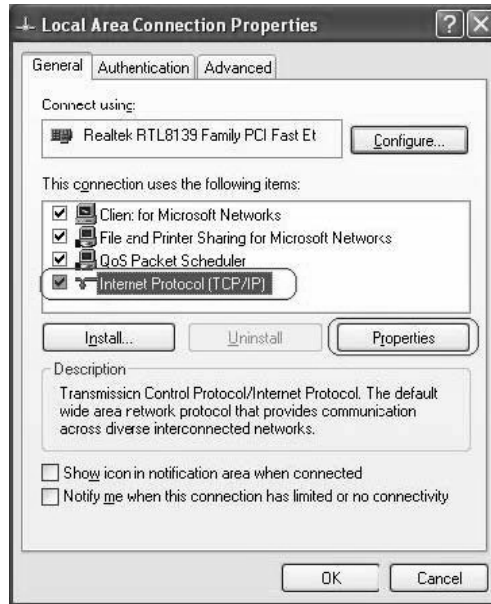
Step 2: Double-click Network Connections icon.



Step 3: Right-click Local Area Connection (local network your ADSL hooked up with) and select Properties:

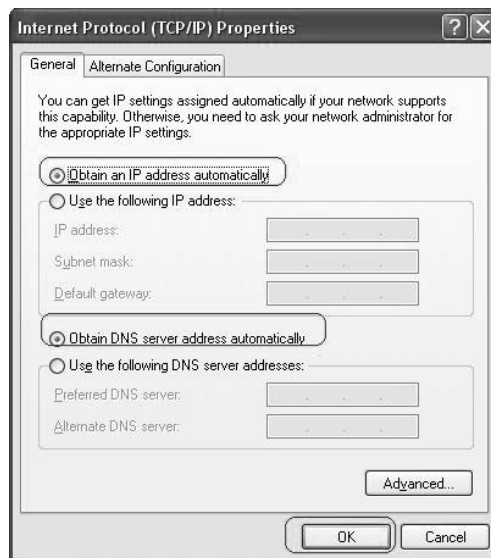


Step 4: Select Internet Protocol (TCP/IP) then click Properties:



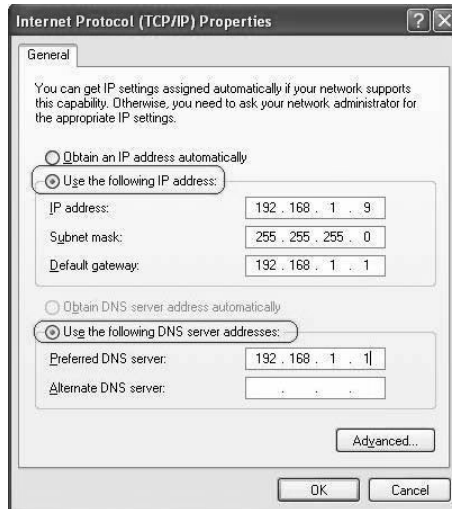
Configure IP address Automatically:

Step 5: Select Obtain an IP address automatically and Obtain DNS server address automatically. Click OK to finish the configuration.



Configure IP Address Manually:

Step 5: Select Use the following IP address and Use the following DNS server addresses.



IP address: Fill in IP address 192.168.1.x (x is a number between 2 to 254).

Subnet mask: Default value is 255.255.255.0.

Default gateway: Default value is 192.168.1.1.

Preferred DNS server: Fill in preferred DNS server IP address.

Alternate DNS server: Fill in alternate DNS server IP address.

You can use ping command under DOS prompt to check if you have setup TCP/IP protocol correctly and if your computer has successfully connected to this router.

1) Type ping 192.168.1.1 under DOS prompt and the following messages will appear:

```
Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 times<2ms TTL=64 Reply from 192.168.1.1: bytes=32 times<1ms TTL=64 Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
```

2) If the communication link between your computer and router is not setup correctly, after you type ping 192.168.1.1 under DOS prompt following messages will appear:

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

Cable issue or something wrong might cause this failure in configuration procedure.

4. Configure Wireless ADSL2+ Router via HTML

This device supports a Web-based (HTML) GUI to allow users to configure Router setting via Web browser.

4.1 Login

1) Launch the Web browser.

2) Enter the default IP address http://192.168.1.1



3) Entry of the username and password will be displayed. Enter the default login User Name and Password: • The default login User Name of the administrator is admin, and the default login password is admin.



4.2 Navigating the Web Configurator

Steps to navigate the Web configuration from the Site Map are summarized as below.

Status	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Device Info	System Log	Statistics		
Device Information	Firmware Version : 2.11.6.1(RE0.C2B)3.7.6.1 MAC Address : 00:06:4f:11:22:33				
LAN	IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled				
WAN	Virtual Circuit : PVC0 Status : Not Connected Connection Type : PPPoE IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 DNS Server : 0.0.0.0 NAT : Enabled				
ADSL	ADSL Firmware Version : FwVer:3.7.6.1_A_TC3085 HwVer:T14.F7_3.0 Line State : Down Modulation : Multi-Mode Annex Mode : ANNEX_A				
		Downstream	Upstream		
	SNR Margin :	N/A	N/A	db	
	Line Attenuation :	N/A	N/A	db	
	Data Rate :	0	0	kbps	

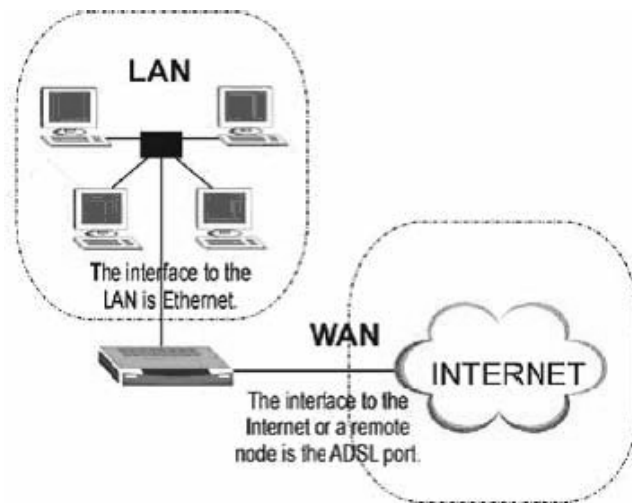
Steps to navigate the Web configuration from the Site Map are summarized below.

- Click on Quick Start to begin a wizard that helps to configure your router.
- Click on Interface Setup to configure Internet and LAN functions.
- Click on Advanced Setup to configure advanced features.
- Click on Access Management to manage Internet access options.
- Click on Maintenance to set a new password, to set the time zone, to upgrade or reload firmware and to run diagnostic tests on the router
- Click on Status to see router device information, system logs and performance statistics.
- Click on Help to see available help topics.

5. Interface Setup

The physical connections determine whether the router ports are local area network (LAN) ports or wide area network (WAN) ports. There are two kinds of IP networks. The local, private kind is the LAN network; the global, public kind is the WAN network. The following illustration shows the relationship between the router and the two different networks. A LAN is a shared communication system to which many computers are attached. A LAN is generally limited to the immediate area, usually the same building or floor of a building. A WAN is an outside connection to another network or to the Internet.

Click an Interface Setup link to set ATM VC values, ISP Encapsulation, configure multi-connection settings, and LAN configuration.



5.1 Internet

The Internet screen allows you to set up how your router connects to the Internet. If you already ran the Quick Start wizard, the information you provided to the wizard should be entered into the fields already. After you finish the changes, click on the SAVE button to save your changes.

Interface	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Internet	LAN	Wireless		
ATM VC	Virtual Circuit: PVC0 <input type="button" value="PVCs Summary"/>				
	Status: <input checked="" type="radio"/> Activated <input type="radio"/> Deactivated VPI: 0 (range: 0-255) VCI: 35 (range: 1-65535)				
QoS	ATM QoS: UBR				
	PCR: 0 cells/second				
	SCR: 0 cells/second				
	MBS: 0 cells				

5.1.1 ATM VC & QoS

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI, settings to you. In this Device, you can totally setup 8 PVCs on different encapsulations if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority. Virtual Circuit: Select the VC number you want to setup. VPI: Virtual Path Identifier. The valid range for the VPI is 0 to 255. VCI: Virtual Channel Identifier. The valid range for the VCI is 1 to 65635 (0 to 31 is reserved for local management of ATM traffic). ATM QoS: Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR(Constant Bit Rate), VBR(Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR, and MBS. PCR: Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed. SCR: Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec. MBS: Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR.

After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again. CBR is for connections that support constant rates of data transfer. The only parameter you need to worry about in CBR is PCR. UBR is for connections that have variable traffic. The only parameter you need to worry about in UBR is PCR. rtVBR is for connections that, while having variable traffic, require precise timing between traffic source and destination. PCR, SCR and MBS must all be set for rtVBR. nrtVBR is for connections that have variable traffic, do not require precise timing, but still require a set bandwidth availability. PCR, SCR and MBS must all be set for nrtVBR.

5.1.2 Encapsulation

Select the encapsulation protocol your ISP uses. The following section will vary depending on which encapsulation protocol you select.

Encapsulation
ISP : <input checked="" type="radio"/> Dynamic IP Address <input type="radio"/> Static IP Address <input type="radio"/> PPPoA/PPPoE <input type="radio"/> Bridge Mode

(1) Dynamic IP Address

Select this option if your ISP provides you an IP address automatically. Please enter the Dynamic IP information accordingly.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
TCP MTU Option	Enter TCP MTU Value here
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

(2) Static IP Address

Select this option to set static IP information. You will need to enter in the encapsulation type (1483 Bridged IP LLC, 1483 Bridged IP VC-Mux, 1483 Routed IP LLC (IPoA), 1483 Routed IP VC-Mux), IP address, subnet mask, and gateway address provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is 4 IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
Static IP Address	Enter the static IP Address here.
IP Subnet Mask	Enter the IP Subnet Mask here.
Gateway	Enter the Gateway address here.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

(3) PPPoA / PPPoE

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL service. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Selection Static PPPoE to use static IP address for your PPPoE connection. Please enter the information accordingly.

LABEL	DESCRIPTION
Username	Enter your username for your PPPoE/PPPoA connection.
Password	Enter your password for your PPPoE/PPPoA connection.
Encapsulation	Select your encapsulation type from the dropdown list.
Bridge Interface	Select whether the Interface will be Activated or Deactivated.
Connection	Select whether your connection is always on or if it connects on demand. If on demand, specify how many minutes the connection may be idle before it disconnects.
TCP MSS Option	Enter the TCP MSS you wish to use here.
Get IP Address	Choose whether the ROUTER obtains the IP address statically or dynamically.
Static IP Address	Enter the static IP address here. Only if you chose Static above.
IP Subnet Mask	Enter the IP subnet mask here. Only if you chose Static above.
Gateway	Enter the gateway here. Only if you chose Static above.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
TCP MTU Option	Enter TCP MTU Value here.
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

Connection Setting: For PPPoE/PPPoA connection, you can select Always on or Connect on-demand. Connect on-demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time, the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.

IP Address: For PPPoE/PPPoA connection, you need to specify the public IP address for this ADSL Router. The IP address can be either dynamically (via DHCP) or given IP address provide by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.

NAT: Select this option to Activate/Deactivated the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.

[Dynamic Route]

RIP (Routing Information Protocol): Select this option to specify the RIP version, including RIP1, RIP2-B and RIP2-M. RIP2-B & RIP2-M are both sent in RIP-2 format, the difference is that RIP2-M using Multicast and RIP2-B using Broadcast format. RIP Direction: Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. IN only means the ADSL router will only accept but will not send RIP packet. OUT only means the ADSL router will only sent but will not accept RIP packet.

[Multicast]

IGMP (Internet Group Multicast Protocol): It is a session-layer protocol used to establish membership in a multicast group. The ADSL supports both IGMP version IGMP-v1 & IGMP-v2. Select None to disable it.

Your ISP should provide the above information. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given.

(4) Bridge Mode

The modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable 2 or more networks to communicate as if they are 2 segments of the same physical LAN. Please set the Connection type.

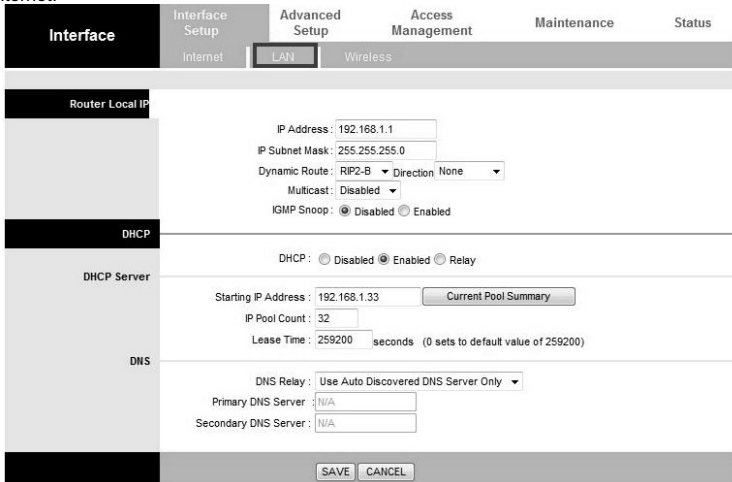


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.

5.2 LAN

There are the IP settings of the LAN Interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is provided to your internal network and cannot be seen on the Internet.



5.2.1 Router Local IP

IP Address: Enter the IP address of your ADSL router in dotted decimal notation, for example, 192.168.1.1 (default setting). IP Subnet Mask: Your ADSL router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing sub netting, use the subnet mask computed by the ADSL router.

Dynamic Route: Select the Dynamic Route from RIP1, RIP2-B, and RIP2-M. Please refer to Internet→Dynamic Route. The only difference is the interface.

5.2.2 Explaining RIP Setup

Routing Information Protocol (RIP) allows a router to exchange routing information with other routers. The RIP Direction field controls how RIP packets are allowed to enter and leave the router. Selecting Both means the router will broadcast its routing table and incorporate the RIP information that it receives. Selecting In Only means the router will only accept RIP packets received, not send RIP packets. Selecting Out Only means the router will only send RIP packets, not accept any RIP packets received. Selecting None means the router will not send any RIP packets nor will it accept any RIP packets received. The Dynamic Route field controls the format and the broadcasting method of RIP packets that the router sends. It recognizes both formats when receiving packets. RIP-1 is universally supported, but RIP-2 carries more information. RIP-1 is adequate for most networks. Only consider RIP-2 if your network has unusual topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format. RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Direction: Select the RIP direction from None, Both, In Only and Out Only. Multicast: IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL router supports both IGMP-v1 and IGMP-v2. Select None to disable it. Please refer to Internet→Multicast. The only difference is the interface.

5.2.3 DHCP Server

The DHCP Server gives out IP addresses when a device is booting up and request an IP to be logged on to the network. It must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the client on the network.

LABEL	DESCRIPTION
Starting IP Address	Enter the starting IP address you wish to use as the DHCP server's IP assignment.
IP Pool Count	Enter the maximum user pool size you wish to allow.
Lease Time	Enter the amount of time you wish to lease out a given IP address.
DNS Relay	Select the DNS relay option you wish to use from the dropdown list.
Primary DNS Server	Enter the primary DNS server IP address you wish to use. For user discovered DNS only.
Secondary DNS Server	Enter the secondary DNS server IP address you wish to use. For user discovered DNS only.

5.2.4 DHCP Relay

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enable, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

DHCP

DHCP Relay

DHCP : Disabled Enabled Relay

DHCP Server IP for Relay Agent :

DHCP Server IP for relay agent: The DHCP server IP Address runs on WAN side.

5.2.5 DNS Relay

The DNS Configuration allows the user to set the configuration of DNS.

DHCP

DHCP Server

DHCP : Disabled Enabled Relay

Starting IP Address :

IP Pool Count :

Lease Time : seconds (0 sets to default value of 259200)

DNS

DNS Relay :

Primary DNS Server :

Secondary DNS Server :

DNS Relay Selection: If user wants to disable this feature, he just needs to set both Primary & Secondary DNS to 0.0.0.0. Using DNS relay, users can setup DNS server IP to 192.168.1.1 on their computer. If not, device will perform as NO DNS relay. If you don't want to use the DNS Relay option, set the DNS relay to "Use User Discovered DNS Server Only" and set both Primary and Secondary DNS Servers to "0.0.0.0".

5.3 Wireless

5.3.1 Wireless LAN

Interface

Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status

Internet | LAN | **Wireless**

Access Point Settings

Access Point : Activated Deactivated

Channel : Undefined (range: 20-1000) Auto Current Channel: 1

Beacon Interval : 100 (range: 20-1000)

RTS/CTS Threshold : 2347 (range: 1500-2347)

Fragmentation Threshold : 2346 (range: 256-2346, even numbers only)

DTIM : 1 (range: 1-255)

802.11 b/g : 802.11b-g

Multiple SSIDs Settings

SSID Index : 1

SSID : Default_WLAN

Broadcast SSID : Yes No

Authentication Type : Disabled

WDS Settings

WDS Mode : Disabled

Mac Address #1 : 00:00:00:00:00

Mac Address #2 : 00:00:00:00:00

Mac Address #3 : 00:00:00:00:00

Mac Address #4 : 00:00:00:00:00

Wireless MAC Address Filter

Active : Activated Deactivated

Action : Allow Association the follow Wireless LAN station(s) association.

Mac Address #1 : 00:00:00:00:00

Mac Address #2 : 00:00:00:00:00

Mac Address #3 : 00:00:00:00:00

Mac Address #4 : 00:00:00:00:00

Mac Address #5 : 00:00:00:00:00

Mac Address #6 : 00:00:00:00:00

Mac Address #7 : 00:00:00:00:00

Mac Address #8 : 00:00:00:00:00

SAVE CANCEL

5.3.2 Access Point Settings

Access Point: Select this section for Activated or Deactivated AP function.

Channel: Select the local channel from the drop down list.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Set this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size TURNS OFF the RTS/CTS handshake. Set this attribute to ZERO TURNS ON the RTS/CTS handshake. Enter a value between 0 and 2432.

Fragment Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.

DTIM: This value is between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

802.11 b/g: Select the wireless mode in the section.

5.3.3 Multiple SSIDs Settings

SSID: The SSID is a unique name to identify the ADSL Router in the Wireless LAN. Wireless Clients associating to the ADSL Router must have the same SSID. The define SSID name is MC-420.

Broadcast SSID: Select No to hide the SSID such that a station can not obtain the SSID through passive scanning. Select Yes to make the SSID visible so a station can obtain in the SSID through Passive scanning.

Authentication Type: Select wireless authentication type to configure wireless AP. There have 4 types – WEP-64Bits, WEP-128Bits, WPA-PSK, WPA2-PSK.

[Authentication Type]

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select Disable to allow all wireless computers to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to use data encryption.

Key#1~Key#4 The WEP keys are used to encrypt data. Both the ADSL Router and the wireless clients must use the same WEP key for data transmission. If you chose 64-bit WEP, then enter any 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). If you choose 1280bit WEP, then enter 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). The values must be set up exactly the same on the Access Points as they are on the wireless client stations. The same value must be assigned to Key 1 on both access point (your ADSL Router) and the client adapters, the same value must be assigned to Key 2 on both access point and the client stations and so on, for all four WEP keys.

WPA-PSK Wi-Fi Protected Access, pre-shared key. Encrypts data frames before transmitting over the wireless network.

Pre-shared Key is used to encrypt data. Both the ADSL Router and the wireless clients must use the same WPA-PSK Key for data transmission.

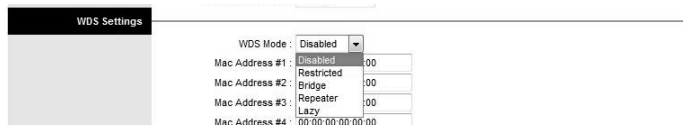
5.3.4 WDS Settings

A Wireless Distribution System is a system that enables the interconnection of access points wirelessly. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them.

WDS is another way for AP router to join an existing Wi-Fi network. The WDS feature is normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances. User can use this feature

to build up a large wireless network in a large space like airports, hotels and schools...etc. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.

WDS Mode: (1) Restricted – WDS peers must be registered with AP router (by MAC addresses). (2) Bridge – AP router will function as a wireless bridge, merely forwarding traffic between access points, and will not respond to wireless requests. The WDS peers must be manually stated and wireless stations will not be able to connect to AP router. (3) Repeater – AP router will act as a repeater, interconnecting between access points. WDS peers can be determined by the user (“Restricted” mode) or auto-detected (“Lazy” mode) (4) Lazy– Automatic detection of WDS peers: when a LAN user searches for a network, AP router will attempt to connect to WDS devices in its vicinity.



MAC address #1-#4: Specify the destination MAC address device. The MAC addresses filter tunneling lets you select exactly which stations should have access to your network.

5.3.4 Wireless MAC Address Filter

You can allow or deny a list of MAC addresses associated with the wireless stations access to the ADSL Router.

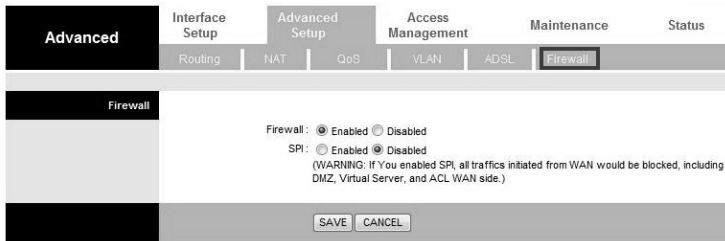
Active: Select this section to activated or deactivated Wireless MAC address filter.

Action: Select Deny Association to block access to the router, MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router, MAC addresses not listed will be denied access to the router.

6 Advanced Setup

6.1 Firewall

User can enable or disable firewall feature of the ADSL router in the page.



Firewall: Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack. SPI: Select this option to Enabled or Disabled the SPI feature. (NOTE: If you enable SPI, all traffics initiate from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side)

6.2 Routing

This table lists IP address of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Gateway IP to identify the first Internet router it should contact to

route the data most efficiently. Select this option will list the routing table information. You can press ADD ROUTE to edit the static route. (As below screen)

The screenshot shows the 'Advanced' configuration page with the 'Routing' tab selected. Below the navigation tabs, there is a 'Routing Table List' section containing a table with the following data:

#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.1	1	enet0	180		
2	default	0	Node1	2	Idle	0		

Below the table is an 'ADD ROUTE' button.

[Static Route]

Select this option to set Static Routing information.

The screenshot shows the 'Static Route' configuration page with the following fields and options:

- Destination IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
- Gateway IP Address: 0.0.0.0 (with a radio button selected) and PVC0 (with a dropdown arrow)
- Metric: 0
- Announced in RIP: No (with a dropdown arrow)

At the bottom of the page are buttons for 'SAVE', 'DELETE', 'BACK', and 'CANCEL'.

Destination IP Address: This parameter specifies the IP network address of the final destination of packets routed by this rule.

IP Subnet Mask: Enter the subnet mask for this destination.

Gateway IP Address: Enter the IP address of the gateway. A gateway does the actual forwarding of the packets. Enter the gateway's IP address in the field or select which PVC you wish to act as a gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.

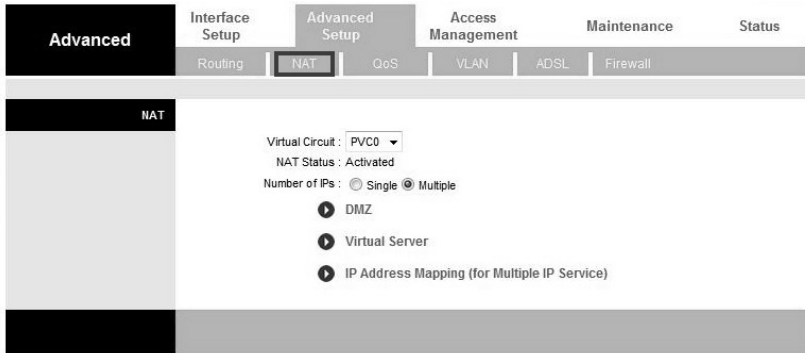
Metric: Metric represents the "cost" of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.

Announced in RIP: This parameter determines if the ADSL router includes the router to this remote node in its RIP broadcasts. If you choose Yes, the router in this remote node will be propagated to other hosts through RIP broadcasts. If you choose No, this route is kept private and is not included in the RIP broadcasts.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set, **BACK** to return to the previous screen or **CANCEL** to exit without saving.

6.3 NAT

Network Address Translation (NAT) is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses. Simply select this option to setup the NAT function for your ADSL router.



Virtual Circuit (VC): The Virtual Circuit (VC) properties of the ATM VC interface identify a unique path that your ADSL/Ethernet router uses to communicate via the ATM-based network with the telephone company central office equipment. NAT Status: This field shows the current status of the NAT function for the current VC. Number of IPs: This field is to specify how many IPs are provided by your ISP for current VC. It can be single IP or multiple IPs. Note: For VCs with single IP, they share the same DMZ & Virtual servers; for VCs with multiple IPs, each VC can set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

6.3.1 What NAT Does

NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed. The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. You may also designate servers, such as a Web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, your ROUTER filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

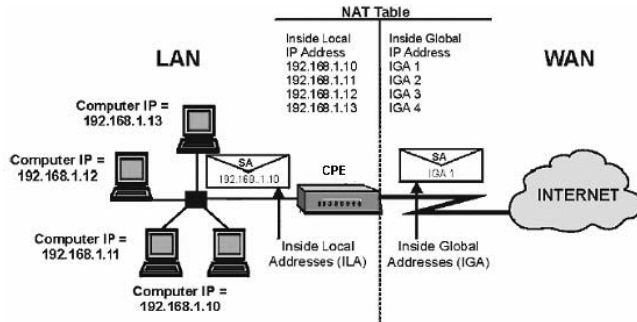
Inside/outside indicates where a host is located relative to the ROUTER. The computers hosts of your LAN are inside, while the Web servers on the Internet are outside. Global/local indicates the IP address of a host in a packet as the packet traverses a router. The local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host of a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

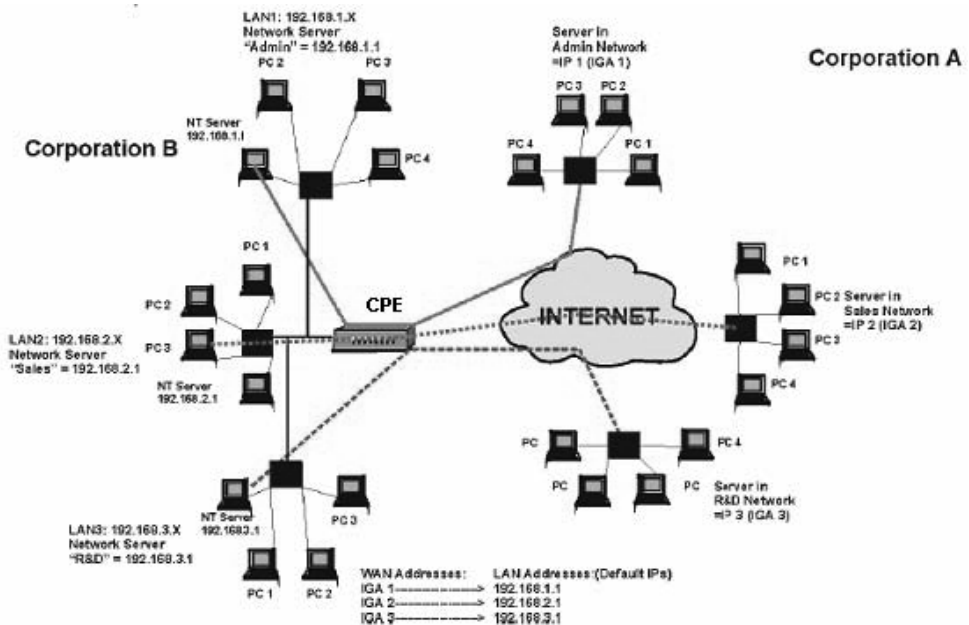
6.3.2 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ROUTER keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.



6.3.3 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.



6.3.4 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- a. One-to-One: In One-to-One mode, the TC3162 EVM maps one local IP address to one global IP address.
- b. Many-to-One: In Many-to-One mode, the TC3162 EVM maps multiple local IP addresses to one global IP address.
- c. Many-to-Many Overload: In Many-to-Many Overload mode, the TC3162 EVM maps multiple local IP addresses to shared global IP addresses.
- d. Many-to-Many No Overload: In Many-to-Many No Overload mode, the TC3162 EVM maps each local IP address to a unique global IP address.
- e. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. The following table summarizes these types.

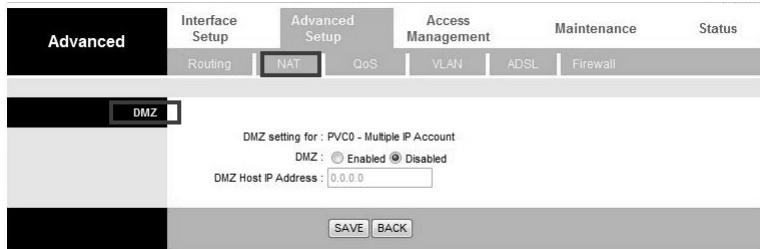
TYPE	IP MAPPING
One-to-One	ILA1 IGA1
Many-to-One (SUA/PAT)	ILA1 IGA1 ILA2 IGA1 ...
Many-to-Many Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA1 ILA4 IGA2 ...
Many-to-Many No Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA3 ...
Server	Server 1 IP IGA1 Server 2 IP IGA1 Server 3 IP IGA1

6.3.5 DMZ

A DMZ (de-militarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Users of the public network outside the company can access only the DMZ host. DMZ: Toggle the DMZ function Enabled or Disabled.

DMZ Host IP Address: Enter the specified IP Address for DMZ host on the LAN side

When you are done making changes, click on SAVE to save your changes or on BACK to return to the previous screen.



6.3.6 Virtual Server

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world. Rule Index: The Virtual server rule index for this VC. You can specify up to 10 rules. All the VCs with single IP will use the same Virtual Server rules. Start & End port number: Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, set the FTP Virtual server, you can set the start and end port number to 21. Local IP Address: Enter the IP Address for the Virtual Server in LAN side. Virtual Server Listing: This is a listing of all virtual servers you have set.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

Advanced | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status

Routing | **NAT** | QoS | VLAN | ADSL | Firewall

Virtual Server

Virtual Server for : PVC0 - Multiple IP Account

Rule Index : 1

Application : -

Protocol : ALL

Start Port Number : 0

End Port Number : 0

Local IP Address : 0.0.0.0

Virtual Server Listing

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

SAVE DELETE BACK CANCEL

6.3.7 IP Address Mapping

The IP Address Mapping is for those VCs that with multiple IPs. The IP Address Mapping rule is per-VC based. (only for Multiple IPs' VCs). Rule Index: The Virtual server rule index for this VC. You can specify up to 10 rules. All the VCs with single IP will use the same Virtual Server rules. Rule Type: There are 4 types of One-to-One, Many-to-One, Many-to-Many Overload, and Many-to Many No-Overload. Local Start & End IP: Enter the local IP address you plan to map to. Local Start IP is the starting local IP address & Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255. Public Start & End IP: Enter the Public IP Address you want to do NAT. Public Start IP is the starting Public IP Address and Public End IP is the ending Public IP Address. If you have a Dynamic IP, enter 0.0.0.0 as the Public Start IP. When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

Advanced | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status

Routing | **NAT** | QoS | VLAN | ADSL | Firewall

IP Address Mapping

Address Mapping Rule : PVC0

Rule Index : 1

Rule Type : One-to-One

Local Start IP : 0.0.0.0

Local End IP : N/A

Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)

Public End IP : N/A

Address Mapping List

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

SAVE DELETE BACK CANCEL

6.4 ADSL

Select this option to set ADSL Mode and ADSL Type information.

ADSL Mode: Select which mode your ADSL connection uses from the dropdown list. The option has Auto Sync-up, ADSL2+, ADSL2, G.DMT, T1.413, G.LITE

ADSL Type: Select the ADSL type you use from the dropdown list. ANNEX A, ANNEX I, ANNEX A/L, ANNEX M, ANNEX A/I/J/L/M

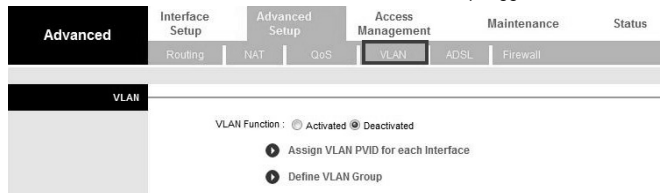
When you are done making changes, click on SAVE to save your changes.

6.5 QoS

QoS (Quality of Service). This option will provide better service of selected network traffic over various technologies. Deploying QoS management to guarantee that all application receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modem enterprise network.

6.6 VLAN

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs. ATM VLAN-using LAN Emulation(LANE) protocol to map Ethernet packets into ATM cells and deliver then to their destination by converting an Ethernet MAC address into an ATM address. The key for the IEEE 802.1Q to perform the above functions is in its tags. 802.1Q-compliant switch ports can be configure to transmit tagged or untagged frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. However, it is important to ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many NICs for PCs and printers are not 802.1Q-compliant. If they received a tagged frame, they will not understand the VLAN tag and will drop the frame. Also, the maximum legal Ethernet frame size for tagged frames was increased in 802.1Q (and its companion, 802.3ac) from 1518 to 1522 bytes. This could cause network interface cards and older switches to drop tagged frames as "oversized"



Assign VLAN PVID for each interface: You can assign ATM VC, Ethernet (LAN) port, and Wireless LAN port's PVID in this section. Define VLAN Group: Based on each VLAN group, you can configure each group's VLAN setting. You can configure up to 8 VLAN settings.

7. Access Management

7.1 ACL

Go to Access Management → ACL to enable remote management. Access Control Listing (ACL) is a management tool that acts as a filter for incoming or outgoing packets, based on application. You may use telnet or Web to remotely manage the ADSL Router. User just needs to enable Telnet or Web and give it an IP address that wants to access the ADSL Router. The default IP 0.0.0.0 allows any client to use this service to remotely manage the ADSL Router.



ACL: There has Activated & Deactivated option. The default setting is Deactivated which means all IP can access via router. If you choose Activated, you only can access via router bylisted IP addresses.ACL Rule Index: Index number from 1 and up to 16.Active: Once you choose Yes then you can access the IP via router.Application: Each of these labels denotes a service that you may use to remotely manage the Router. Choices are Web, FTP, Telnet, SNMP, Ping, ALL.Interface: Select the access interface. Choices are WAN, LAN and Both.

For Example:

How to set your ACL?

You must choose Activated to enable your ACL function.

Select the ACL Rule Index number (up to 16 number)

You can set the specific Secure IP address or set 0.0.0.0 for all IPs.

Choose the Application which you want to access for this ACL Rule index.

Select the Interface you want to access from.

After all settings are ready, click SAVE and continue next ACL Rule Index setting.

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	Web	LAN
2	Yes	0.0.0.0-0.0.0.0	Telnet	LAN
3	No	0.0.0.0-0.0.0.0	FTP	Both
4	No	0.0.0.0-0.0.0.0	SNMP	Both
5	No	0.0.0.0-0.0.0.0	Ping	LAN
6	No	0.0.0.0-0.0.0.0	ALL	LAN

[Note]

You must set one ACL index to access your router via LAN interface. If you don't, your router cannot access other listed IP Address. (Refer to Index 1).

Remember! Once you active your ACL function, you only can access via router by listed Secure IP Address.

7.2 IP Filter

The Router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attackers. Go to Access Management →IP Filtering to set different IP filter rules of a given protocol (TCP, UDP, or ICMP) and a specific direction (incoming, outgoing, or both) to filter the packets. IP Filter is a more complex filtering tool, based more on IP and custom rules. Each of the indices can hold six rules, and each interface can have four associated indices, allowing 24 rules per interface. If all six rules in an index are Next rules, the data will be sent to the next index for filtering.

Access Management | Interface Setup | Advanced Setup | Access Management | Maintenance | Status

ACL | **Filter** | SNMP | UPnP | DDNS | CWMP

Filter

Filter Type

Filter Type Selection : IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index : 1
 Interface : PVC0
 Direction : Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index : 1
 Rule Type : IP
 Active : Yes No

Source IP Address : (0.0.0.0 means Don't care)
 Subnet Mask :
 Port Number : 0 (0 means Don't care)

Destination IP Address : (0.0.0.0 means Don't care)
 Subnet Mask :
 Port Number : 0 (0 means Don't care)

Protocol : TCP
 Rule Unmatched : Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index		Interface		Direction			
#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE DELETE CANCEL

IP Filter Set Index: The IP Filter Set Index from 1 to 12 and each index can set up to 6 IP Filter.

Interface: Choices from PVC0 to PVC7 and LAN.

Direction: Choices are Both, Incoming and Outgoing. Select which direction of data flow you wish to apply the filters to. Note that Incoming and Outgoing are from the point of view of your router, relative to the interface you select. For WAN, data coming from outside your system is considered Incoming and data leaving your system is Outgoing. For LAN, data leaving your system is considered Incoming and data entering your system is Outgoing.

IP Filter Rule Editing: Select the IP Filter Rule Index you wish to modify.

Active: Toggle this rule index on or off with Yes or No, respectively.

Source IP Address: Enter the source IP address you wish to deny access to your system.

Subnet Mask: Enter the subnet mask of the source IP address.

Port Number: Enter the port number of the source IP address. Note that 0 means that all ports are allowed.

Destination IP Address: Enter the destination IP address that you wish to deny access to your system.

Subnet Mask: Enter the subnet mask of the destination IP address

Port Number: Enter the port number of the destination IP address. Note that 0 means that all ports are allowed

Protocol: Select the protocol to filter. Choices are TCP, UDP, and ICMP.

Rule Unmatched: Choices are Forward and Next. Select what happens to the data in question if the rule you are currently editing is unmatched. Next means that the data is then compared to the next IP filter rule. Forward means that the data will be allowed into your system. Note that a Forward rule should be the last rule, as no data will be compared to rules after a Forward rule.

IP Filter Set Index: Select the IP filter set you wish to view.

For Example

Please follow below steps to set your IP Filter:

IP Filter Set Editing: Choose your IP Filter Set Index, Interface and Direction options. Remember, Interface and Direction functions are affected with IP Filter Set Index. EX: if your 1st index set of IP filter set PVC0 as Interface and Outgoing as Direction, so the list of 1st IP Filter will be PVC0 and Outgoing as their settings.

2. IP Filter Rule Editing: Select the IP Filter Rule Index (up to 6 numbers for each set index) and choose Active option. As below example, Source IP Address is 192.168.1.4, Subnet Mask is 255.255.255.255, Destination IP Address & Subnet Mask is 0.0.0.0, Port Number is 80. And, Protocol sets TCP. From this setting, it filters 192.168.1.14, so it cannot access the web. Notice, each IP Filter Set Index can has up to 6 filters IP. At "Rule Unmatched" option, you must choose NEXT until the last filter IP choose Forward.

After every setting is done, click SAVE to continue next IP Filter Editing.

7.3 SNMP

The Simple Network Management Protocol (SNMP) is used for exchanging information between network devices. It enables a host computer to access configuration, performance, and other system data that resides in a database on the modem. The host computer is called a management station and the modem is called an SNMP agent. The data that can be accessed via SNMP is stored in a Management Information Database (MIB) on the modem.



Get Community: Select to set the password for incoming Get- and GetNext request from management station. Set Community: Select to set the password for incoming Set request from management station. The default password is 'public'. When you are done making changes, click on SAVE to save your changes.

7.4 UPnP

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly an automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN. How do I know if I'm using UPnP? UPnP hardware is identified as an icon in the Network Connections folder (in Windows XP & Windows ME). Each UPnP-compatible device that is installed on your network will appear as a separate icon.



UPnP (Universal Plug and Play): You can choose “Activated” or “Deactivated” option from this session.

Auto-Configured (by UPnP Application): UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. Choose “Activated” option to allow UPnP-enabled applications to automatically configure the ADSL Router so that they can communicate through the ADSL Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. If you don't want to make configuration changes through UPnP, just choose “Deactivated”.

SAVE: Click SAVE to save the setting to the ADSL Router.

7.5 DDNS

The Dynamic Domain Name System allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dns.org, where my host is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address. First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

Dynamic DNS: Choose the option for Activated or Deactivated DDNS.

Service Provider: The default Dynamic DNS service provider is www.dyndns.org.

My Host Name: Type the domain name assigned to your ADSL by your Dynamic DNS provider.

E-mail Address: Type your e-mail address.

Username: Type your user name.

Password: Type the password assigned to you.

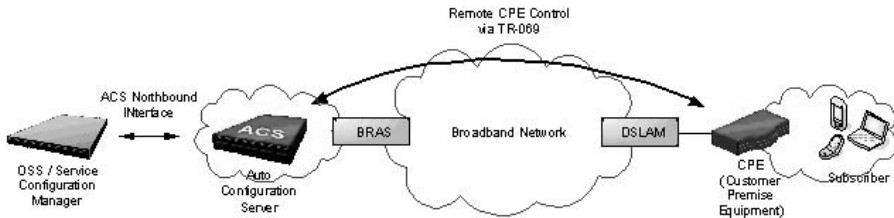
Wildcard support: Select Yes or No to turn on DYNDNS Wildcard.

DYNDNS Wildcard --> Enabling the wildcard feature for your host causes `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`. This feature is useful if you want to be able to use, for example, `www.yourhost.dyndns.org` and still reach your hostname.

SAVE: Click SAVE to save your changes. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of `user@domain` where domain identifies a service name, enter it exactly as given. When you are done making changes, click on SAVE to save your changes.

7.6 CWMP

TR-069 is a CPE WAN Management Protocol (CWMP). As a bidirectional SOAP/ HTTP based protocol it provides the communication between CPE and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. In the course of the boom of the broadband market, the number of different Internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, paddles, VoIP-phones). At the same time the configuration of this equipment became more complicated -- too complicated for the end-users. For this reason the TR-069 standard was developed. It provides the possibility of auto configuration of these access types. The technical specifications are managed and published by the DSL Forum. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically. Accordingly other service functions can be provided. TR-069 is the current standard for activation of terminals in the range of DSL broadband market.



Access Management	Interface Setup	Advanced Setup			Access Management		Maintenance	Status
	ACL	Filter	SNMP	UPnP	DDNS	CWMP		
CWMP Setup								
CWMP : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated								
Login ACS								
URL: <input type="text"/>								
User Name: <input type="text"/>								
Password: <input type="password"/>								
Connection Request								
Path: <input type="text" value="tr-069"/>								
Port: <input type="text" value="80"/>								
Username: <input type="text"/>								
Password: <input type="password"/>								
Periodic Inform								
Periodic Inform : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated								
Interval: <input type="text" value="0"/>								
SAVE CANCEL								

8. Maintenance

8.1 Administration

There is only one account that can access Web-Management interface-Administration. Admin has read/write access privilege. In this web page, you can set new password for admin.

Maintenance	Interface Setup	Advanced Setup	Access Management		Maintenance	Status
	Administration	Time Zone	Firmware	SysRestart	Diagnostics	
Administrator						
Username : admin						
New Password : <input type="password"/>						
Confirm Password : <input type="password"/>						
SAVE CANCEL						

New Password: Type the new password in this field.

Confirm Password: Type the new password again in this field.

Note: If you ever forget the password to log in, you may press the RESET button up to 6 second to restore the factory default settings. The Factory Default Settings for User Name & Password are admin & admin.

8.2 Time Zone

The system time is the time used by the device for scheduling services. You can manually set the time or connect to a NTP (Network Time Protocol) server. If an NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

The screenshot shows the 'Time Zone' configuration page. At the top, there are tabs for 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', and 'Status'. Under 'Advanced Setup', there are sub-tabs for 'Administration', 'Time-Zone', 'Firmware', 'SysRestart', and 'Diagnostics'. The 'Time-Zone' sub-tab is active. The page displays the following information and controls:

- Current Date/Time:** 01/01/2000 00:15:34
- Time Synchronization:**
 - Synchronize time with:
 - NTP Server automatically
 - PC's Clock
 - Manually
 - Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (dropdown menu)
 - Daylight Saving: Enabled Disabled
 - NTP Server Address: 0.0.0.0 (0.0.0.0: Default Value)
- Buttons: SAVE, CANCEL

Current Date/Time: This field displays an updated Date and Time when you reenter this menu.

[Time Synchronization]

Synchronize time with: You can choose "NTP Server automatically", "PC's Clock", or "Manually" to coordinate the time. Time Zone: Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). Daylight Saving: Choose "Enabled" or "Disabled" to use daylight savings time. NTP Server Address: Type the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. A Network Time Protocol (NTP) server can automatically set the router time for you. If you use an NTP server, you will only need to select your time zone. If you manually set the time, you can enable Daylight Saving. The router will automatically adjust when Daylight Saving goes into effect.

When you are done making changes, click on SAVE to save your changes or on CANCEL to exit without saving.

8.3 Firmware

You can upgrade the firmware of the router in this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to browse the local had drive and locate the firmware to be used for the update. Then press UPGRADE to upload new Firmware. It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade!! After a success upload, the system automatically restarts. Please wait for the device to finish restarting. This should take about 2 minutes or more. You need to log in again if you want to access the device.

The screenshot shows the 'Firmware/Romfile Upgrade' page. At the top, there are tabs for 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', and 'Status'. Under 'Advanced Setup', there are sub-tabs for 'Administration', 'Time Zone', 'Firmware', 'SysRestart', and 'Diagnostics'. The 'Firmware' sub-tab is active. The page displays the following information and controls:

- Firmware/Romfile Upgrade:**
 - Current Firmware Version : 2.11.6.1(RE0.C2B)3.7.6.1
 - New Firmware Location :
 - New Romfile Location :
 - Romfile Backup :
- Status:**
 - ⓘ It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.
- Buttons: UPGRADE

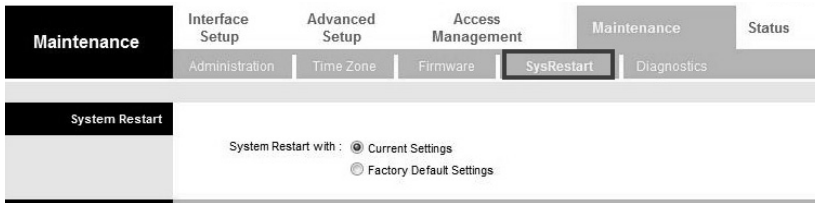
Current Firmware Ver.: This field displays the current firmware version.

New Firmware Location: Type in the location of the file you want to upload in this field or click Browse... to find it.

vUPGRADE: Click UPGRADE to begin the upload process.

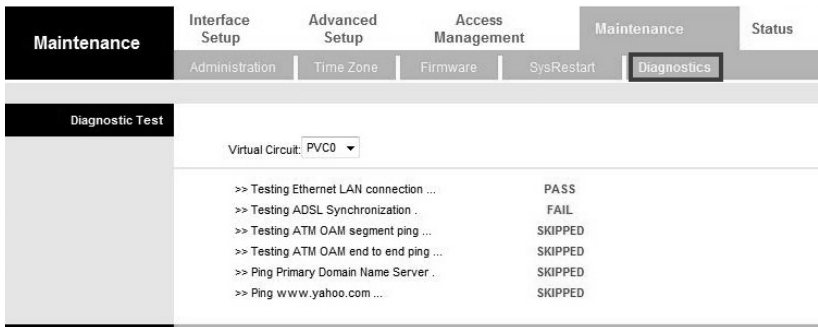
8.4 System Restart

The SysRestart screen allows you to restart your router with either its current settings still in place or the factory default settings. If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Otherwise, you can select Current Settings. You may also reset your router to factory settings by holding the DEFAULT button on the back panel of your router in for 10-12 second while the router is turned on.



8.5 Diagnostic

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for LAN & WAN sides.



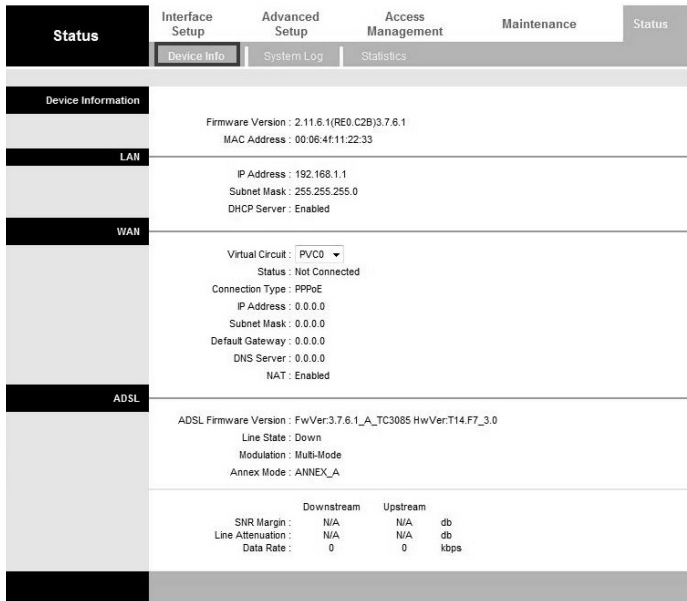
Select which PVC you wish to test from the dropdown list. The router will automatically run diagnostic tests on that circuit. A green PASS means that the given test was passed, a red FAIL means that the test was failed and a green SKIPPED means that the test was skipped.

Note: 1) User ONLY can view PVC0's Diagnostic Test connection. 2) "Testing ADSL Synchronization" might take 30 sec to execute the Diagnostic Test.

9. Status

9.1 Device Info

The Device Info screen is a tool that you use to monitor your ADSL Router. It shows the Firmware Version, WAN, LAN, and MAC address information. Note that these fields are read-only and are not meant for diagnostic purposes. Except the Virtual Circuit, click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.



[Device Information]

Firmware Version: This field displays current firmware version.

MAC Address: The MAC (Media Access Control) or Ethernet address unique to your modem.

[LAN]

IP Address: The LAN port IP address Subnet Mask: The LAN port IP subnet mask. DHCP Server: The status of DHCP Server (Enabled or Disabled)

[WAN]

Virtual Circuit: Click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.

Status: Connected or Not Connected

Connection Type: The WAN Connection Type.

IP Address: The WAN port IP address

Subnet Address: The WAN port IP subnet mask.

Default Gateway: The IP address of the default gateway, if applicable.

DNS Server: The IP address of the DNS Server

[ADSL]

ADSL Firmware Version: This field displays current ADSL firmware version.

Line States: This field displays the ADSL connection process and status.

Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode: This field displays the ADSL annex modes for Annex A or Annex B.

Downstream and Upstream: Status of SNR Margin, Line Attenuation and Data Rate

SNR Margin: Amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate). The SNR Margin is set by Central Office DSLAM. If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease,

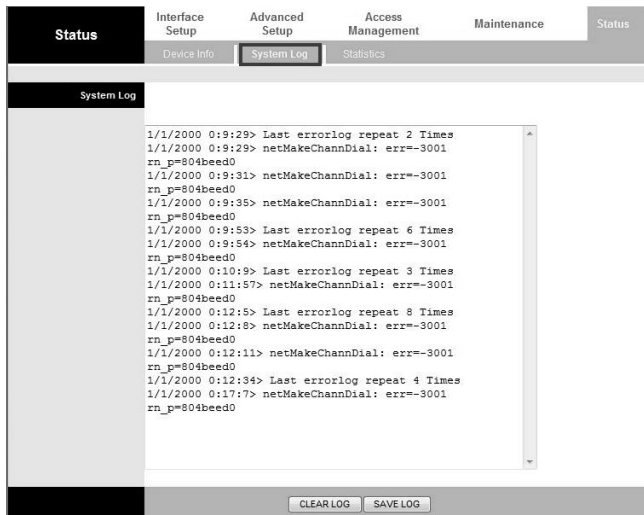
but the data rate will increase.

Line Attenuation: Attenuation is the decrease in magnitude of the ADSL line signal between the transmitter (Central Office DSLAM) and the receiver (Client ADSL Modem), measured in dB. It is measured by calculating the difference in dB between the signal power level received at the Client ADSL Router and the reference signal power level transmitted from the Central Office DSLAM.

Data Rate: This field displays the ADSL data rate.

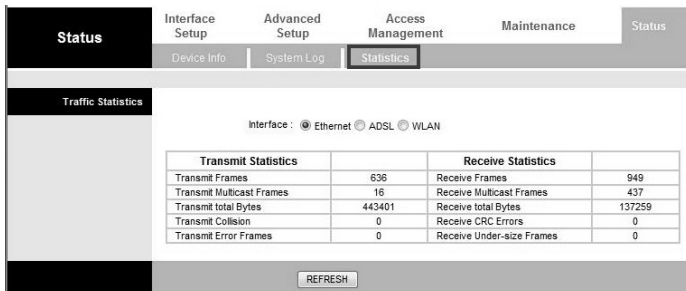
9.2 System Log

The System Log displays data generated or acquired by routine system communication with other devices, such as the results of negotiations with the ISP's computers for DNS and gateway IP addresses. The device keeps a running log of events and activities occurring on the Router. You can click Save Log to display a Windows File Download dialog box that enables opening or saving the contents of the log to your PC. To remove all entries from the list, click Clear Log. New entries will begin accumulating. If the device is rebooted, the logs are automatically cleared.



9.3 Statistics

The ADSL Router keeps statistic of traffic that passes through it. You are able to view the amount of packets that passes through the Router on both the WAN port & the LAN port. The traffic counter will reset if the device is rebooted. You can select Ethernet/ADSL to view the statistics report of LAN/WAN.



[Ethernet]

The Ethernet screen gives you information on how much data your router has transmitted and received across the Ethernet connection. Click on REFRESH to update the screen.

Traffic Statistics			
Interface: <input type="radio"/> Ethernet <input type="radio"/> ADSL			
Transmit Statistics		Receive Statistics	
Transmit Frames	344	Receive Frames	237
Transmit Multicast Frames	16	Receive Multicast Frames	0
Transmit total Bytes	107747	Receive total Bytes	50877
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

[ADSL]

The ADSL screen gives you information about how much data your router has transmitted or received across the ADSL connection. Click on REFRESH to update the screen.

Traffic Statistics			
Interface: <input type="radio"/> Ethernet <input checked="" type="radio"/> ADSL			
Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

10. Troubleshooting

If the router is not function properly, first check this session for simple troubleshooting before contacting your Internet service provider (ISP) for support.

10.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

10.1.1 Power LED

The PWR LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Make sure that the power adaptor is connected to the router and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the router and the power source are both turned on and the router is receiving sufficient power.
3	Turn the router off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

10.1.2 LAN LED

The LAN LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

10.1.3 ADSL LED

The ADSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between the router ADSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for ADSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

10.2 Problems with the Web Interface

I cannot access the web Interface.

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the router. Check the IP address of the router.
2	Make sure that there is not a console session running.
3	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
4	For WAN access, you must configure remote management to allow server access from the WAN (or all).
5	Your computer's and the router's IP addresses must be on the same subnet for LAN access.
6	If you changed the router's LAN IP address, then enter the new one as the URL.
7	Remove any filters in LAN or WAN that block web service.

The web Interface does not display properly.

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

10.3 Problems with the Login Username and Password

I forgot my login username and/or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the DEFAULT button for five seconds, and then release it. When the ADSL LED begins to blink, the defaults have been restored and the router restarts.
3	The default username is "admin". The default password is "admin". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.

It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

10.4 Problems with LAN Interface

I cannot access the router from the LAN or ping any computer on the LAN.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
2	Make sure that the IP address and the subnet mask is consistent between the router and the workstation.

10.5 Problems with WAN Interface

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The ADSL LED on the front panel of the router should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart the router. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by the qualified and licensed electrician), and ensure that all line filters are correctly installed and right way around.
2	Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnects.

Frequent loss of ADSL line sync (disconnections).

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPOA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct casing).

10.6 Problems with the Internet Access

I cannot access the Internet.

STEPS	CORRECTIVE ACTION
1	Make sure the router is turned on and connected to the network.
2	If the ADSL LED is off, refer to Section 10.1.3
3	Verify your WAN settings.
4	Make sure you entered the correct user name and password.
5	For wireless stations, check that both the router and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

If you have any troubles to configure or setup this ADSL Ethernet Router, please feel free to contact us. Before contacting us, make sure collect following information. Submit complete detailed information of your problem will help us to provide you accurate answers.

Model Name:

Serial Number:

PC Settings:

Other:

Spis treści

1. Wstęp	45	6.3.4 Typy odwzorowywania NAT	73
1.2 Cechy szczególne wyrobu	45	6.3.5 DMZ	74
2. Instalacja sprzętu	47	6.3.6 Serwer wirtualny	74
2.1 Wymagania systemu	47	6.3.7 Odwzorowywanie adresów IP	75
2.2 Zawartość pakietu	47	6.4 ADSL	76
2.3 Wskaźniki na przednim panelu i ich opis	48	6.5 QoS	76
2.4 Tylny panel	48	6.6 VLAN	77
2.5 Przyłączenie powiązanych urządzeń	48	7. Zarządzanie dostępem	78
3. Przyłączenie routera ADSL2+ poprzez Ethernet	49	7.1 ACL	78
3.2 Konfigurowanie TCP/IP	49	7.2 Filtr IP	79
4. Konfiguracja routera bezprzewodowej sieci ADSL2+ poprzez HTML	58	7.3 SNMP	81
4.1 Logowanie	58	7.4 UPnP	82
4.2 Nawigacja za pomocą konfiguratora sieci	59	7.5 DDNS	83
5. Ustawianie interfejsu	59	7.6 CWMP	84
5.1 Internet	60	8. Konserwacja	85
5.1.1 ATM VC & QoS	60	8.1 Administracja	85
5.1.2 Enkapsulacja	61	8.2 Strefa czasowa	85
5.2 LAN	64	8.3 Oprogramowanie urządzenia	86
5.2.1 Lokalny IP routera	65	8.4 Ponowne uruchomienie systemu	86
5.2.2 Objasnienie ustawień RIP	65	8.5 Diagnostyka	87
5.2.3 Serwer DHCP	66	9. Status	87
5.2.4 Przełącznik DHCP	66	9.1 Informacja o urządzeniu	87
5.2.5 Przełącznik DNS	66	9.2 System Log	89
5.3 Sieci bezprzewodowe	67	9.3 Statystyka	90
5.3.1 Ustawienia punktu dostępowego	68	10. Rozwiązywanie problemów	90
5.3.2 Ustawienia SSID	68	10.1 Użycie diod świecących do problemów diagnostyki	91
5.3.3 Ustawienia WDS	68	10.1.1 Diody świecące zasilania	91
5.3.4 Filtr adresu MAC	69	10.1.2 Dioda świecąca LAN	91
6. Zaawansowane ustawienia	69	10.1.3 Dioda świecąca ADSL	91
6.1 Zabezpieczenia Firewall	69	10.2 Problemy z interfejsem sieciowym	91
6.2 Routing	70	10.3 Problemy z nazwą Użytkownika Login i hasłem	92
6.3 NAT	71	10.4 Problemy z interfejsem LAN	92
6.3.1 Co robi NAT?	71	10.5 Problemy z interfejsem WAN	92
6.3.2 W jaki sposób działa NAT?	72	10.6 Problemy z dostępem do Internetu	93
6.3.3 Zastosowanie NAT	73	OCHRONA ŚRODOWISKA:	94

MC-420

wireless router ADSL

Dziękujemy za wybór bezprzewodowego routera sieci MC-420 ADSL.

Szerokopasmowy router bezprzewodowy MC-420 ADSL jest kompleksowym rozwiązaniem do zastosowań domowych i SOHO. Wbudowany modem ADSL pozwala na szybki dostęp do Internetu. Router ma ponadto 4-portowy switch Ethernet 10/100 Mbps, który pozwala na połączenie poszczególnych komputerów osobistych w sieci lokalnej przy użyciu sieci przewodowej. Jednocześnie urządzenie wyposażone jest w punkt dostępowy (Access Point) sieci bezprzewodowej, pracujący w standardzie 802.11g. Wbudowany punkt dostępowy sieci bezprzewodowej pozwala na uzyskiwanie połączenia z prędkości do 54Mbps, dzięki czemu praca w sieci i korzystanie z Internetu jest wyjątkowo komfortowe i wydajne. Możecie Państwo cieszyć się multimediami wysokiej jakości oraz aplikacjami czasu rzeczywistego takimi jak na przykład: gry on-line, wideo na żądanie, VoIP i inne szerokopasmowe usługi konsumenckie. Urządzenie zapewnia także obsługę wielu funkcji routowania dzięki czemu użytkownicy mogą skonfigurować połączenie zgodnie ze swoimi wymaganiami i oczekiwaniami.

Aby ułatwić Państwu korzystanie z naszego produktu, zalecamy dokładne poznanie instrukcji obsługi.

MODECOM dba o jakość swoich produktów, nie tylko by spełniać, ale także by wyprzedzać oczekiwania swoich Klientów. Przyzwyczajaliśmy Użytkowników do wysokiej jakości naszych produktów, ich zaawansowanej technologii oraz niezawodności i funkcjonalności.

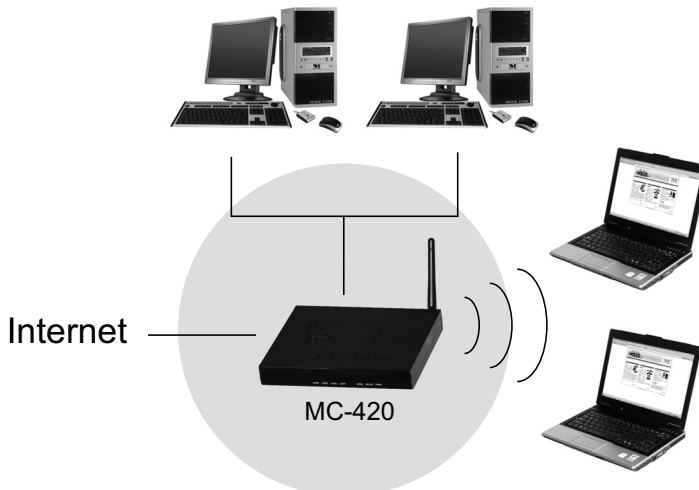
Dla Państwa tworzymy rzeczy wyjątkowe pod każdym względem!

Wybierz lepszą przyszłość - wybierz MODECOM!

1. Wstęp

1.2 Cechy szczególne wyrobu

Schemat zastosowań



Szybki dostęp do Internetu

MODECOM MC-420 ADSL jest zgodny z wymaganiami norm ADSL / ADSL2 / ADSL2+. Urządzenie to może być użyte przy szybkościach ściągania danych do 24 Mbps i wysyłania do 1 Mbps. Router ten jest zgodny z następującymi normami:

- ANSI T1.413, wydanie 2
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- G.964.1 (G.hs, Multimode)
- ITU-T G.992.3 (ADSL 2 G.dmt.bis)
- ITU-T G.992.4 (ADSL2 G.lite.bis)
- ITU-T G.992.5 (ADSL2+; załączniki A, I, J, K, L i M)
- Wzbogacone rozszerzone wydanie ADSL (RE ADSL)
- Rozpoznawanie do 8 PVCs.
- Rozpoznawanie pętli wstecznej OAM F4/F5, AIS i komórek RDI OAM.
- ATM Forum UNI 3.1/4.0 PVC.

Wsparcie protokołów wielopołączeniowych

- Protokół o wielu połączeniach dotyczący AAL5 (RFC 1483 / 2684)
- Klasyczny IP obejmujący ATM (RFC 1577)
- Multipleksowanie VC i LLC
- Wsparcie PPP przez Ethernet (RFC 2516)
- Wsparcie PPP przez ATM (RFC 2364)

Translacja adresu sieciowego (NAT)

Translacja adresu sieciowego (NAT) umożliwia translację adresu IP, używanego w ramach jednej sieci (na przykład prywatnego adresu IP, używanego w sieci lokalnej) na inny adres IP znany w innej sieci (na przykład publiczny adres sieci IP, używany w Internecie).

Uniwersal Plug and Play (UPnP)

Uniwersal Plug and Play jest to norma, która wykorzystuje protokoły Internetu i sieci Web do umożliwienia włączenia do sieci takich urządzeń, jak komputery osobiste, urządzenia peryferyjne, urządzenia inteligentne i urządzenia bezprzewodowe, które zostają automatycznie powiadomione jedno o drugim. Protokół ten jest stosowany do umożliwienia prostego i pewnego połączenia niezależnych urządzeń i komputerów osobistych.

Wsparcie dla dynamicznego DNS (DDNS)

Korzystając z wsparcia dynamicznego DNS można mieć statyczną nazwę komputera w sieci (nazwę umowną) dla dynamicznego adresu IP, co umożliwia łatwiejszy dostęp do hosta z różnych miejsc Internetu.

Należy jednak zarejestrować tę usługę z klientem dynamicznego DNS.

Wsparcie DHCP

DHCP (protokół konfiguracji dynamicznej hosta) umożliwia poszczególnym klientom otrzymanie konfiguracji TCP/IP z serwera DHCP.

Router ADSL ma wbudowany serwer DHCP włączony domyślnie. Może on przypisać adresy IP, domyślne łącze IP i serwery DNS klientom DHCP. Może on także działać jako serwer uboczny (zastępczy) lub DHCP (przełącznik DHCP) przekazując klientom przypisany adres IP z innego serwera DHCP.

Zarządzanie urządzeniem

- Konfiguracja / zarządzanie na bazie sieci GUI
- Interpreter wiersza poleceń (CLI)
- Zdalne zarządzanie Telnet

- Uaktualnianie (rozbudowa) oprogramowania sprzętowego poprzez FTP /TFTP (GUI na bazie sieci)
- Wbudowane narzędzie diagnostyczne IP Ping

Pomoc techniczna (rozpoznawanie SNMP (Protokół zarządzania prostą siecią)

Jest to łatwy sposób zdalnej kontroli routera poprzez SNMP.

Szybki przełącznik Ethernet 10/100M z automatyczną negocjacją połączenia

Autonegociacja połączenia umożliwia routerowi wykrywanie prędkości i trybu podłączanego interfejsu i odpowiednie ustawianie urządzenia bez interwencji ręcznej. Umożliwia on przekazywanie danych z prędkością 10 Mbps lub z prędkością 100 Mbps w trybie albo półduplexu albo pełnego duplexu, w zależności od Twojej sieci Ethernet.

Wsparcie mostkowania / routowania

- Ethernet do ADSL, samouczące się przezroczyste mostkowanie (IDEE 802.1D)
- Routowanie IP - RIPv2 (wstecznie zgodne z RIPv1)
- Statyczne routowanie IP
- Routowanie (TCP/IP/UDP/ARP/ICMP)
- Multicast IGMP v1/v2

Sieć bezprzewodowa

- IEEE802.11g wstecznie zgodne z 802.11b (przy 11Mbps)
- 64/128 bit WEP Encryption
- WPA, WPA-TKIP/PSK, WPA2-TKIP/PSK
- Filtracja adresu MAC
- Wsparcie dla technik wspomaganie jakości usługi (QoS), 802.11e, WMM

Bezpieczeństwo

- PPP (protokół uwierzytelnienia hasła, RFC 1334)
- Protokół dwupunktowy PPP z CHAP (protokół uwierzytelniania wezwania; RFC 1994)
- Przepuszczanie VPN (IPSec, PPTP, L2TP)
- Wbudowane zabezpieczenie NAT
- Filtrowanie pakietu na bazie IP
- Zarządzanie (administrowanie systemem zabezpieczone przez hasło).

2. Instalacja sprzętu

2.1 Wymagania systemu

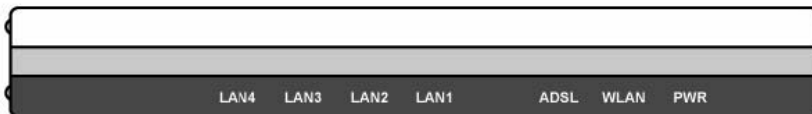
- Procesor Pentium III 266 MHz lub wyższe
- Minimalna pamięć RAM 128 MB
- Minimalna ilość wolnej przestrzeni na dysku 20 MB
- Port Ethernet RJ45

2.2 Zawartość pakietu

- Router ADSL2+
- Przewód Ethernet RJ45
- Przewód telefoniczny RJ11
- Adapter zasilający
- Instrukcja instalacji
- Płyta CD

2.3 Wskaźniki na przednim panelu i ich opis

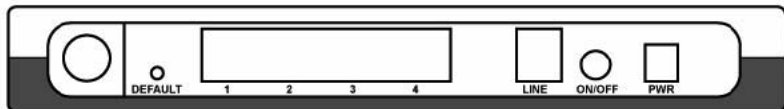
• Przednia tablica tego routera ruchów sieci bezprzewodowej ADSL2+ ma diody świecąca wyświetlające stan roboczy routera ruchu w sieci.



Opisy sygnalizacji za pomocą diod świecących

PWR	Ta dioda świecąca zapala się po przyłączeniu aktywnego adaptera zasilającego do tego routera.
WLAN	Po prawidłowym zainstalowaniu karty WLAN zapala się ta dioda świecąca paląca się światłem przerywanym (zaczyna migać). Podczas przekazywania danych dioda ta pali się światłem ciągłym.
4	Ta dioda świecąca zapala się po ustanowieniu połączenia portu 4 z komputerem osobistym lub przełącznikiem / koncentrATOREM.
3	Ta dioda świecąca zapala się po ustanowieniu połączenia portu 3 z komputerem osobistym lub przełącznikiem / koncentrATOREM.
2	Ta dioda świecąca zapala się po ustanowieniu połączenia portu 2 z komputerem osobistym lub przełącznikiem / koncentrATOREM.
1	Ta dioda świecąca zapala się po ustanowieniu połączenia portu 1 z komputerem osobistym lu przełącznikiem /koncentrATOREM.
ADSL	Ta dioda świecąca zapal się po ustanowieniu połączenia z Internetem (połączenie ADSL). Gdy dioda ta pali się światłem migającym, oznacza to, że nie ma fizycznego połączenia ADSL.

2.4 Tylny panel



PWR	Połączenie z adapterem zasilającym
ON/OFF	Przycisk wyłącznika zasilania
LINE	Połączenie z przewodem telefonicznym
4	Połączenie z kablem Ethernet połączonym z przełącznikiem – koncentrATOREM lub komputerem osobistym
3	Połączenie z przewodem Ethernet połączonym z przełącznikiem – koncentrATOREM lub komputerem osobistym
2	Połączenie z przewodem Ethernet połączonym z przełącznikiem – koncentrATOREM lub komputerem osobistym
1	Połączenie z przewodem Ethernet połączonym z przełącznikiem - koncentrATOREM lub komputerem osobistym
DEFAULT (Wartość domyślna)	Przycisk resetowania

2.5 Przyłączenie powiązanych urządzeń

1) Przyłączenie routera do LINE (Linii)

Wetknij wtyk dostarczonego przewodu telefonicznego RJ-11 do portu LINE (linia) na tylnym panelu routera i wetknąć drugi koniec do splittera lub gniazdka telefonicznego ściennego.

2) Przyłączenie router do LAN

Wetknij wtyczkę przewodu Ethernet RJ-45 do portu LAN na tylnym panelu routera i wetknąć drugi koniec przewodu Ethernet do portu Ethernet Twojego komputera osobistego lub przełącznika.

3) Połącz router z zasilaniem. Wetknij wtyczkę zasilacza do portu PWR, znajdującego się na tylnym panelu routera i drugi koniec przewodu do gniazdka zasilania

4) Wciśnij przycisk wyłącznika, aby uruchomić router.

Ostrzeżenie! Używaj jedynie zasilacza dostarczonego w pakiecie. Używanie innego zasilacza grozi uszkodzeniem sprzętu.

3. Przyłączenie routera ADSL2+ poprzez Ethernet

Twój router może być zarządzany z dowolnego miejsca w sieci poprzez budowany konfigurator przy użyciu przeglądarki sieciowej takiej, jak Microsoft Internet Explorer lub Netscape Navigator. Należy używać przeglądarek Internet Explorer 6.0 i późniejszych wersji i/lub Navigator Netscape 7.0 i późniejszych wersji z włączoną obsługą JavaScript. Zaleca się stosowanie ekranu o rozdzielczości równej 1024 x 768 pikseli.

3.1 Ustawianie routera ADSL2+ poprzez kabel Ethernet

Jeżeli dostępna jest karta LAN w Twoim komputerze osobistym, wystarczy po prostu przyłączyć router do sieci ADSL i komputer osobisty za pomocą kabla Ethernet. Po ustanowieniu połączenia z Internetem można będzie korzystać z zasobów Internetu przy użyciu połączenia Ethernet.

3.2 Konfigurowanie TCP/IP

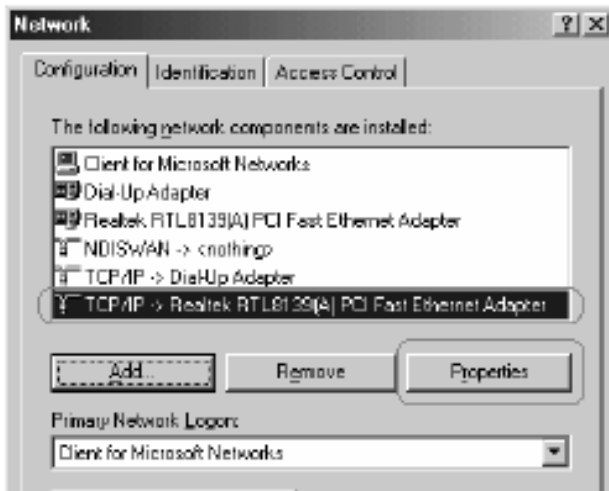
Dla Windows 98SE i ME

Krok 1: Kliknij Start a następnie Setting (Ustawienia) i wybrać Control Panel (Panel sterowania).

Krok 2: Kliknij dwukrotnie ikonę Network (Sieć).

Krok 3: Wybierz zakładkę Configuration (Konfiguracja), a następnie wybierz TCP/IP z listy zainstalowanych składników sieci i kliknij przycisk Properties (Właściwości).

Krok 4: Możesz teraz ustawić następujące konfiguracje, stosując dwie metody:



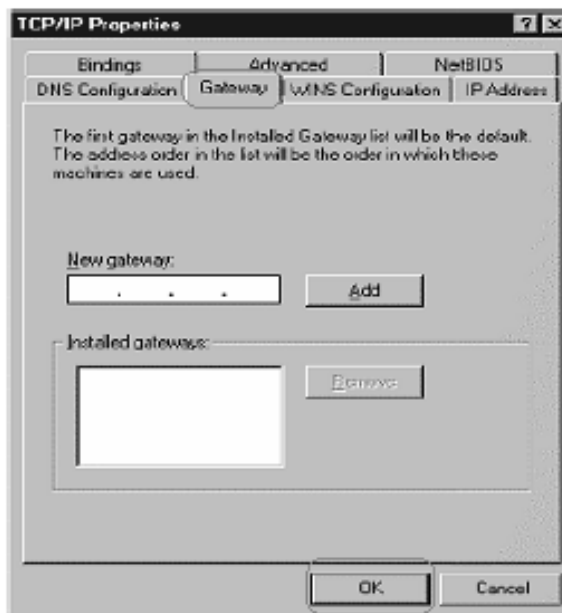
Opcja 1: Automatyczne otrzymywanie IP z routera (sterownika ruchem w sieci)

Wybrać pasek adresu IP.

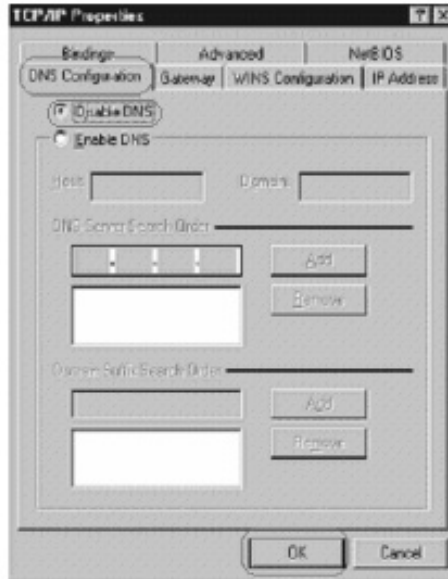
Na tej stronie należy kliknąć przycisk Obtain an IP address automatically (Automatyczne otrzymywanie adresu IP).



1) Wybierz pasek bramki i kliknij OK



2) Następnie należy wybrać zakładkę DNS Configuration (Konfiguracja DNS) i wybrać Disable DNS (Wyłączenie DNS), a potem kliknąć OK, aby zakończyć konfigurację.



Opcja 2: Ręczne skonfigurowanie IP

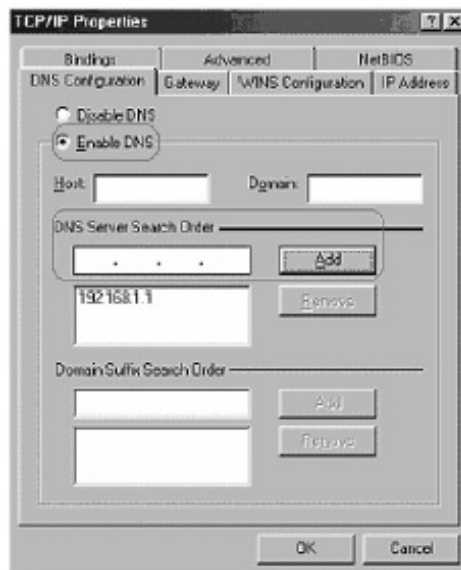
1) Na zakładce IP Address (Adres IP) wybierz odpowiedni adres IP i ustaw domyślny adres IP – dla routera domyślnie to 192.168.1.1, więc należy zastosować adres w postaci 191.168.1.X (gdzie X jest to liczba z zakresu od 2 do 254) dla pola adresu IP i 255.255.255.0 dla pola maski podsieci.



2) Wybierz pasek Gateway (Bramka), dodaj adres IP routera (domyślny „192.168.1.1”) do pola New gateway (Nowa bramka) i kliknij Add (Dodaj).



Na zakładce DNS Configuration (Konfiguracja DNS) należy wybrać Enable DNS (Włączenie DNS) i dodać wartości DNS (192.168.1.1) w polu DNS Server Search Order (kolejność poszukiwania serwera DNS), a następnie kliknij Add (Dodaj).



Dla Windows 2000

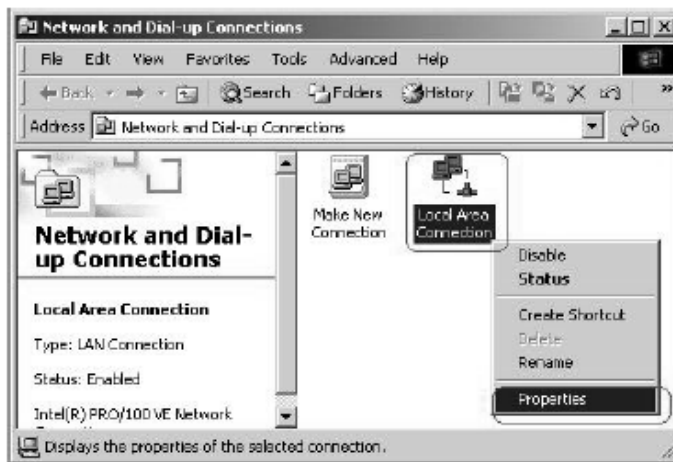
Krok 1: (a) kliknij prawym przyciskiem na My Network Places (Moje miejsca sieciowe) i wybierz Properties (Właściwości) w głównym oknie ekranu.

(b) lub przejdź do Start / Settings /Control Panel (Uruchomienie / Ustawienia / Panel sterowniczy).

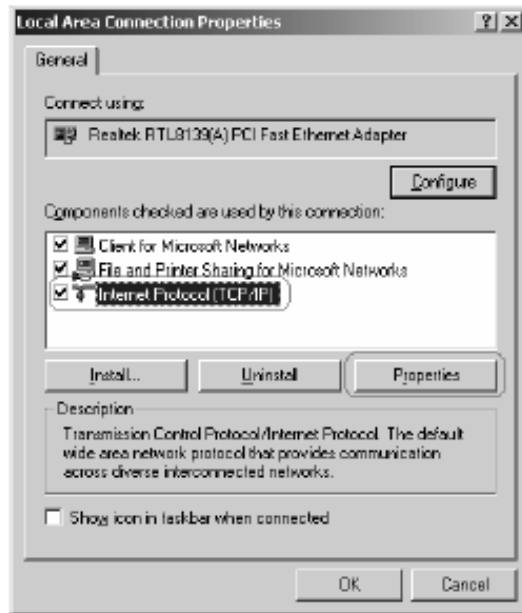
Kliknij dwukrotnie na Control Panel (Panel sterowania) Network and Dial-up Connections (Połączenia sieci i wybierania).



Krok 2: kliknij prawym przyciskiem Local Area Connection (Połączenie sieci lokalnej) i wybierz Properties (Właściwości):

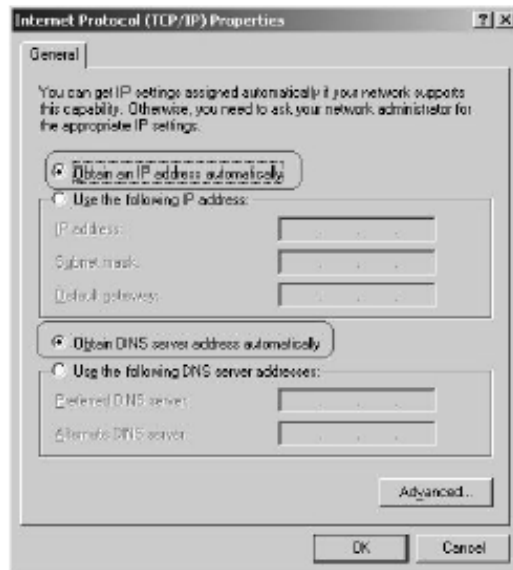


Krok 3: Wybierz Internet Protocol (TCP/IP) a następnie kliknij Properties (Właściwości)



Automatyczna konfiguracja IP

Krok 4: Wybierz Obtain an IP address automatically (Automatyczne otrzymywanie adresu IP) i Obtain DNS server address automatically (Automatyczne otrzymywanie adresu serwera DNS), a następnie kliknij OK, aby zakończyć proces konfiguracji IP.



Ręczne konfigurowanie IP:

Krok 4: Wybierz „Use the following IP address „Użyj następującego adresu IP” i użyj następujących adresów serwera DNS:

Adres I: wpisz adres IP 192.168.1.x (gdzie x jest liczbą mieszczącą się w zakresie od 2 do 254).

Maska podsieci: Wartość domyślna to 255.255.255.0.

Domyślna bramka: Wartość domyślna to 192.168.1.1

Preferowany serwer DNS: wpisz adres IP preferowanego serwera DNS.

Alternatywny serwer DNS: wpisz adres IP alternatywnego serwera DNS



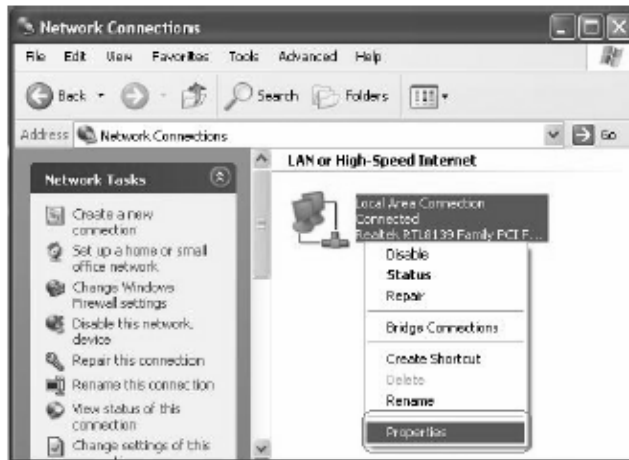
Dla Windows XP

Krok 1: Kliknij Start, a następnie wybierz Control Panel (Panel sterowania).

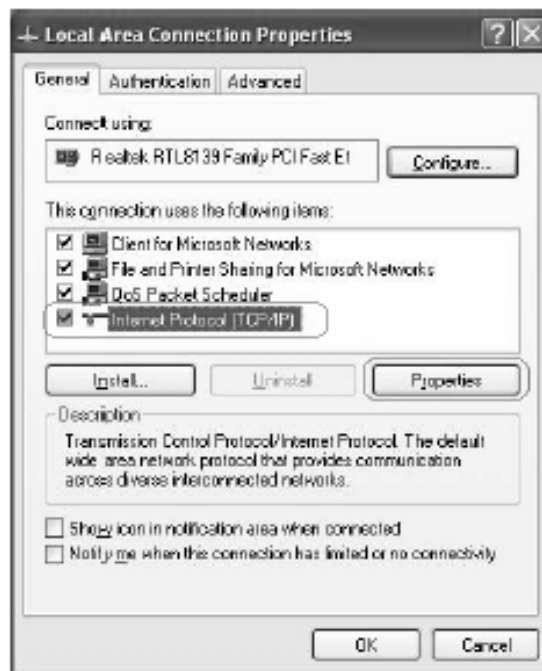
Krok 2: Kliknij dwa razy ikonę Network Connection (Połączenia sieciowe)



Krok 3: Kliknij prawym przyciskiem Local Area Connection (Połączenie sieci lokalnej) i wybierz Properties (Właściwości).

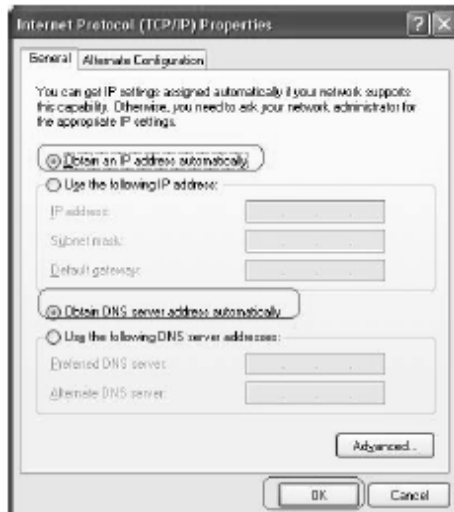


Krok 4: Wybierz Internet Protocol (TCP/IP) (Protokół internetowy), a następnie kliknij Properties (Właściwości)



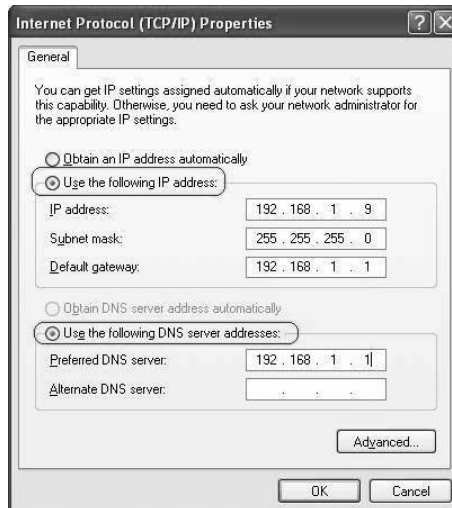
Automatyczne konfigurowanie adresu IP:

Krok 5: Wybierz Obtain an IP address automatically (Automatyczne otrzymywanie adresu IP) i Obtain DNS server address automatically (Automatyczne otrzymywanie adresu serwera DNS). Kliknik OK., aby zakończyć konfigurację.



Ręczna konfiguracja adresów IP:

Krok 5: Wybierz Use the following IP address (Użyj następującego adresu IP) i Use the following DNS server addresses (Użyj następującego adresu serwera DNS):



Adres IP: Wpisz adres IP 192.168.1.x (gdzie x jest liczbą z przedziału od 2 do 254).

Maska podsieci: Wartość domyślna to 255.255.255.0.

Domyślna bramka: Wartość domyślna to: 192.168.1.1.

Preferowany serwer DNS: Wpisz adres IP preferowanego serwera DNS.

Alternatywny serwer DNS: Wpisz adres IP alternatywnego serwera DNS.

Możecie użyć komendy ping z linii poleceń DOS do sprawdzenia, czy ustawiliście prawidłowo protokół TCP/IP i czy Wasz komputer został pomyślnie przyłączony do tego routera.

1) Wpisz komendę ping 192.168.1.1 w linii poleceń: po dokonaniu tego pojawią się następujące komunikaty:

Komenda ping 192.168.1.1: z 32 bajtami danych:

Odpowiedź od 192.168.1.1: bajty = 32 razy < 2 ms TTL = 64

Odpowiedź od 192.168.1.1: bajty = 32 razy <1 ms TTL = 64

Odpowiedź od 192.168.1.1: bajty = 32 razy < 10 ms TTL = 64

2) Jeśli nie ustawiono prawidłowo połączenia Twojego komputera i sterownika, po wpisaniu ping 192.168.1.1 pod znakiem zachęty DOS pojawią się następujące komunikaty:

Wpisanie komendy ping 192.186.1.1 z 32 bajtami danych:

Upłynął limit czasu żądania.

Upłynął limit czasu żądania.

Upłynął limit czasu żądania.

Przedstawiony tutaj błąd w sposobie konfiguracji może być spowodowany przez kabel lub inne źródła błędów.

4. Konfiguracja routera bezprzewodowej sieci ADSL2+ poprzez HTML

Urządzenie to pozwala na konfigurację przy użyciu graficznego interfejsu użytkownika opartego na wbudowanym lokalnym serwerze WWW.

4.1 Logowanie

1) Uruchomić przeglądarkę sieciową.

2) Wpisać adres domyślny IP http:192.168.1.1



3) Wyświetlona zostaje prośba o wpisanie nazwy użytkownika i hasła. Domyślnie User Name (Nazwa Użytkownika): admin i Password (Hasło): admin.



4.2 Nawigacja za pomocą konfiguratora sieci

Poniżej podano zbiorczy wykaz kroków, jakie należy podjąć, aby zapewnić nawigację konfiguracji sieciowej od Mapy miejsca instalacji.

Status	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Device Info	System Log	Statistics		
Device Information	Firmware Version : 2.11.6.1(RE0.C2B)3.7.6.1 MAC Address : 00:06:4f:11:22:33				
LAN	IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled				
WAN	Virtual Circuit : PVC0 Status : Not Connected Connection Type : PPPoE IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 DNS Server : 0.0.0.0 NAT : Enabled				
ADSL	ADSL Firmware Version : FwVer:3.7.6.1_A_TC3085 HwVer:T14.F7_3.0 Line State : Down Modulation : Multi-Mode Annex Mode : ANNEX_A				
		Downstream	Upstream		
	SNR Margin :	N/A	N/A	db	
	Line Attenuation :	N/A	N/A	db	
	Data Rate :	0	0	kbps	

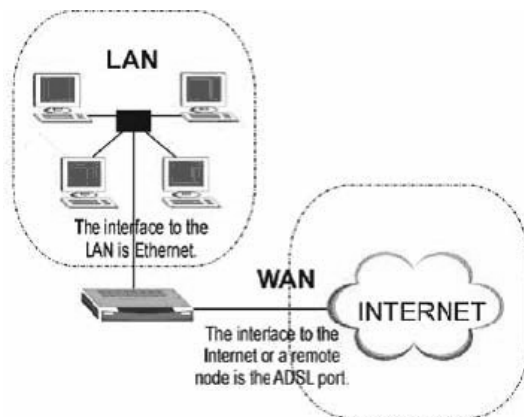
Poniżej zestawiono kroki, jakie należy podjąć, aby zapewnić nawigację konfiguracji sieciowej od mapy miejsca zainstalowania:

- Kliknij Interface Setup, aby skonfigurować funkcje LAN i funkcje internetowe.
- Kliknij Advanced Setup, aby skonfigurować cechy zaawansowane.
- Kliknij Access Management, aby móc zarządzać opcjami dostępu do Internetu.
- Kliknij Maintenance, aby ustawić nowe hasło, strefę czasową, aby zaktualizować lub załadować ponownie oprogramowanie sprzętowe i aby przeprowadzić próby diagnostyczne na urządzeniu.
- Kliknij Status, aby otrzymać informacje o urządzeniu sterownika, dziennikach i statystyce pracy.
- Kliknij Help, aby zobaczyć, jakie są dostępne tematy pomocy.

5. Ustawianie interfejsu

Fizyczne połączenia określają, czy porty routera są portami sieci lokalnej (LAN), czy też są portami rozległej sieci komputerowej (WAN). Istnieją dwa rodzaje sieci IP. Lokalna prywatna sieć jest to sieć LAN. Globalna publiczna sieć jest to sieć WAN. Poniższy rysunek przedstawia zależność pomiędzy routerem i dwoma różnymi sieciami. LAN jest to wspólny system łączności, do którego przyłączono wiele komputerów. LAN jest najczęściej ograniczony do bezpośredniej strefy sąsiedztwa, zazwyczaj tego samego budynku lub tej samej kondygnacji budynku.

WAN stanowi zewnętrzne połączenie z inną siecią lub z Internetem.



5.1 Internet

Zakładka Internet umożliwia Ci ustalenie, w jaki sposób Twój router zostanie połączony z Internetem. Zachęcamy do skorzystania z aplikacji umieszczonej na płycie CD, służącej do automatycznej konfiguracji łącza ADSL dla Twojego dostawcy Internetu.

Interface	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Internet	LAN	Wireless		
	ATM VC				
	QoS				
		Virtual Circuit: PVC0 <input type="button" value="PVCs Summary"/>			
		Status: <input checked="" type="radio"/> Activated <input type="radio"/> Deactivated			
		VPI: 0 (range: 0-255)			
		VCI: 35 (range: 1-65535)			
		ATM QoS: UBR			
		PCR: 0 cells/second			
		SCR: 0 cells/second			
		MBS: 0 cells			

5.1.1 ATM VC & QoS

Do przyłączenia Twojego ISP używane są ustawienia ATM. Twój ISP (dostawca usługi internetowej) powinien dostarczyć Ci ustawienia VPI i VCI. W urzędzeniu tym możecie w sumie skonfigurować do 8 PVCs", jeśli otrzymasz 8 różnych obwodów wirtualnych od Twojego ISP. Aby uzyskać efekt, musicie włączyć VC. W przypadku zarządzania PVC możecie użyć ATM QoS do ustawiania każdego priorytetu linii ruchu PVC.

Wirtualny obwód: Wybierz liczbę VC, którą chcesz ustawić.

VPI: Wirtualny identyfikator drogi. Ważnym zakresem VPI jest zakres od 0 do 255.

VCI: Identyfikator kanału wirtualnego. Ważnym zakresem VCI jest zakres od 1 do 65635 (zakres od 0 do 31 został zarezerwowany dla lokalnego zarządzania ruchem ATM).

ATM QoS: Wybierz jakość usługi dla tego obwodu wirtualnego. Typy ATM QoS obejmują CBR (stałą prędkość transmisji w bitach na minutę), VBR (zmienną prędkość transmisji w bitach na minutę) i UBR (nie wyszczególnioną prędkość transmisji w bitach na minutę). Te typy QoS są wszystkie kontrolowane przez parametry podane poniżej, w tym PCR, SCR i MBS.

PCR: Szczytowa prędkość komórek (PCR) jest to maksymalna prędkość z jaką nadajnik może przesyłać komórki. Parametr ten może być niższy (lecz nie może on być wyższy) od maksymalnej prędkości linii. Komórka 1 ATM ma 53 bajty (424 bity) tak, iż maksymalna prędkość równa 832 Kbps daje maksymalną PCR wynoszącą 1962 komórki na se-

kundę. Ta prędkość nie jest jednak gwarantowana ze względu na to, że zależy ona od prędkości linii.

SCR: Prędkość nie przerwane go ruchu komórek (SCR) jest to średnia prędkość komórek podczas przesyłania pakietów ze źródła ruchu włączanego / wyłączanego, które mogą być przesyłane ze szczytową prędkością I parametru ruchu typu cechy przesyłania pakietów. SCR nie może być większe od PCR. System domyślny wynosi 0 komórek na sekundę.

MBS: Maksymalny wymiar przesyłanych pakietów (MBS). Jest to maksymalna liczba komórek, które mogą być wysłane przez PCR.

Po osiągnięciu MBS prędkości komórek opadają poniżej SCR, dopóki prędkość komórek SCR nie zbliży się z powrotem do wartości SCR. W tym momencie można przesłać wiele komórek (do MBS) przez PCR z powrotem.

CBR: Służy do połączeń obsługujących stałe prędkości przekazywania danych. Jedynym parametrem o który powiniście się zająć w CBR jest parametr PCR.

UBR: Służy do połączeń, które mają zmienny ruch. Jedynym parametrem, jakim tutaj powiniście się zająć w UBR jest PCR.

rtVBR Służy do połączeń, które charakteryzując się zmiennym ruchem wymagają dokładnej synchronizacji w czasie pomiędzy źródłem ruchu a miejscem przeznaczenia. PCR, SCR i MBS muszą być ustawione na rtVBR.

nrtVBR Służy do połączeń, które charakteryzują się zmiennym ruchem i nie wymagają dokładnej synchronizacji w czasie, lecz wymagają w dalszym ciągu dostępnej ustawionej szerokości pasm. PCR, SCR i MBS muszą być ustawione na nrtVBR.

5.1.2 Enkapsulacja

Wybierz protokół stosowany przez Twojego dostawcę łącza internetowego. Poniższy ustęp będzie inny w zależności od tego, jaki wybierze cie protokół.

(1) Dynamiczny adres IP

Wybierz tę opcję, jeśli Twój ISP dostarcza Ci automatycznie adres IP. Prosimy wpisać odpowiednie informacje odnoszące się do dynamicznego IP.

W poniższej tablicy opisano etykiety figurujące na tym ekranie.

ETYKIETA	OPIS
Enkapsulacja	Wybierz Wasz typ Enkapsulacji z Twojej listy rozwijanej w dół.
NAT	Wybierz czy NAT powinien być włączony czy wyłączony.
Trasa domyślna	Wybierz, czy ten PVC stworzy trasę domyślną dla danych Internetu.
Opcja TCP MTU	Wpisz tutaj wartość TCP MTU
Trasa dynamiczna	Wybierz typ RIP z listy rozwijanej.
Multiemisja	Wybierz protokół multiemisji z listy rozwijanej.

(2) Statyczny adres IP1

Wybierz tę opcję, aby ustawić informację o statycznym IP. Będziesz wówczas musiał wpisać typ enkapsulacji (1483 IP LLC, 1483 IP VC-Mux, 1483 IP LLC (IPoA), 1483 IP VC-Mux), adres IP, maskę podsieci i adres bramek wskazanych Ci przez Twojego ISP. Każdy adres IP wpisany w odpowiednich polach musi mieć odpowiednią formę IP, to jest formę czterech bajtów 8-bitowych, 4 IP oddzielonych kropkami (x.x.x.x). Router nie przyjmie adresu IP, który nie będzie podany w tym formacie.

W poniższej tablicy opisano etykiety widoczne na tym ekranie.

ETYKIETA	OPIS
Enkapsulacja	Wybierz Swój typ enkapsulacji z listy rozwijanej.
Stacyjny adres IP	Wpisz w tym miejscu statyczny adres IP.
Maska podsieci IP	Wpisz w tym miejscu adres podsieci IP.
Bramka	Wpisz w tym miejscu adres bramki.
NAT	Wybierz, czy NAT ma być włączony czy wyłączony.
Trasa domyślna	Wybierz, czy ten PVC ma być trasą domyślną danych internetowych.
Trasa dynamiczna	Wybierz typ RIP i kierunek z listy rozwijanej.
Multiemisja	Wybierz protokół emisji, którego chcesz używać z listy rozwijanej.

(3) PPPoA / PPPoE

Wybierz tę opcję, jeśli Wasz ISP wymaga zastosowania połączenia PPPoE. Opcja ta jest typowo stosowana do serwisu DSL. Wybierz dynamiczne PPPoE, gdy będziecie chcieli uzyskać adres automatyczny IP dla Twojego połączenia PPPoE. Wybierz statyczne PPPoE, gdy będziecie chcieli użyć statycznego adresu do Twojego połączenia PPPoE. Prosimy wpisać odnośnie informacje.

PPPoE/PPPoA

Connection Setting

Servicename:

Username:

Password:

Encapsulation: PPPoE LLC

Half Bridge: Activated Deactivated

Connection: Always On (Recommended)
 Connect On-Demand (Close if idle for 0 minutes)
 Connect Manually

TCP MSS Option: TCP MSS(0:default) 0 bytes

IP Address

Get IP Address: Static Dynamic

Static IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

NAT: Disabled

Default Route: Yes No

TCP MTU Option: TCP MTU(0:default) 0 bytes

Dynamic Route: RIP2-B Direction Both

Multicast: Disabled

MAC Spoofing: Enabled Disabled

00:00:00:00:00:00

ETYKIETA	OPIS
Nazwa Użytkownika	Wpisz swoją nazwę użytkownika dla Twojego połączenia PPPoE/PPPoA.
Hasło	Wpisz swoje hasło dla Twojego połączenia PPPoE/PPPoA.
Enkapsulacja	Wybierz typ Twojej enkapsulacji z listy rozwijanej.
Mostkowanie	Wybierz, czy mostkowanie ma być włączone, czy też wyłączone
Połączenia	Wybierz, czy Twoje połączenie jest zawsze włączone, czy też zostaje ono włączone tylko na życzenie. Jeśli jest ono włączane na życzenie, należy podać ile minut połączenie ma być w stanie biernym zanim zostanie ono rozłączone.
Opcja TCP MSS	Wpisz pożądane TCP MSS do zastosowania w tym miejscu.
Otrzymanie adresu IP	Wybierz, czy router ma otrzymywać adres IP statycznie, czy dynamicznie.
Statyczny adres IP	Wpisz w tym miejscu statyczny adres IP. Należy tego dokonywać tylko wówczas, jeśli wybrano powyżej statyczny adres.
Maska podsieci IP	Wpisz tutaj maskę podsieci IP. Należy tego dokonywać tylko wówczas, gdy powyżej wybrano statyczny adres.
Bramka	Wpisz tutaj bramkę. Należy tego dokonać tylko wówczas, gdy poprzednio wybrano statyczny adres.
NAT	Wpisz czy NAT ma być włączone, czy wyłączone
Trasa domyślna	Wybierz, czy ten PVC będzie trasą domyślną danych internetowych.
Opcja TCP MTU	Wpisz w tym miejscu wartość TCP MTU.
Trasa dynamiczna	Wybierz typ RIP i kierunek z list rozwijanych.
Multiemisja	Wybierzprotokół multiemisji, jakiego pragniecie użyć z listy rozwijanej w dół.

Ustawienia połączenia: Dla połączenia PPPoE/PPPoA możesz wybrać stałe połączenie lub połączenie na żądanie. Połączenie na żądanie jest zależne od istniejącego ruchu. Jeśli nie ma w ogóle ruchu w sieci (lub też jest ruch martwy) przez ustalony uprzednio okres czasu, wówczas połączenie automatycznie rozłącza się. W chwili pojawienia się ruchu, to jest przesłania lub odebrania wiadomości, połączenie to automatycznie włącza się.

Adres IP: Dla połączenia PPPoE/PPPoA musisz wyszczególnić adres publicznego IP dla tego routera ADSL. Adres IP może być albo dynamiczny (poprzez DHCP), lub też może to być adres IP podany przez Twojego ISP. Dla statycznego adresu IP musicie wyszczególnić adres IP, maskę podsieci i adres bramki IP.

NAT: Wybierz tę opcję, aby włączyć / wyłączyć funkcję NAT (tłumaczenie adresu sieci) dla tego VC. Funkcja NAT może być włączona lub wyłączona na podstawie PVC.

[Trasa dynamiczna]

RIP (Protokół zawierający informację o trasowaniu): Wybierz tę opcję, aby wyszczególnić wersję RIP, zawierającą RIP1, RIP2-B i RIP2-M. RIP2-B i RIP2-M są obydwa przesyłane w takim samym formacie RIP2. Jedyną różnicę pomiędzy nimi stanowi to, że RIP2-M używa multiemisji, a RIP2-B używa formatu nadawania.

Kierunek RIP: Wybierz tę opcję, aby wyszczególnić kierunek RIP. Jeśli będziecie chcieli wyłączyć opcję RIP, Wpisz None (brak). Wpisanie Both (oba) oznacza, że router ADSL będzie okresowo przysyłał informacje o trasowaniu i przyjmował informacje o trasowaniu, które zostają włączone do tablicy trasowania. In only (Tylko przyjmowanie) oznacza, że router ADSL będzie tylko przyjmował pakiet RIP, lecz nie będzie wysyłał pakietu RIP. Out only (Tylko wysyłanie) oznacza, że router ADSL będzie jedynie wysyłał pakiety RIP, lecz nie będzie ich przyjmował.

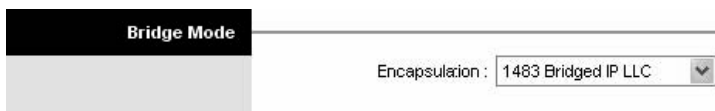
[Multiemisja]

IGMP: Jest to protokół warstwy sesji używany do ustalenia członkostwa w grupie przeprowadzającej multiemisję. ADSL obsługuje obie wersje IGMP, to znaczy, że zarówno IGMP-v1 jak i IGMP-v2. Gdy chce się wyłączyć to działanie, należy wybrać None (Brak).

Twój ISP powinien dostarczać powyższe informacje. Prosimy zauważyć, że musia wpisać nazwę Użytkownika dokładnie w takim brzmieniu, jak została ona przydzielona przez ISP. Jeśli przydzielona nazwa ma formę user@domain , gdzie domena identyfikuje nazwę serwisu, należy wpisać ją dokładnie w tej formie, jak została ona podana.

(4) Tryb mostka

Modem może być tak skonfigurowany, aby działał on jako urządzenie mostkujące pomiędzy Twoją siecią LAN i Twoim ISP. Mostki są to urządzenia, które umożliwiają przyłączenie dwóch lub więcej sieci, jeśli istnieją dwa segmenty takiego samego fizycznie LAN. Prosimy ustawić typ połączenia.



W poniższej tabeli podano opisy etykiet widocznych na tym ekranie.

ETYKIETA	OPIS
Przedstawienie w sposób ukryty	Wybierz Wasz typ przedstawienia w sposób ukryty z listy rozwijanej w dół.

5.2 LAN

Istnieją ustawienia IP interfejsu LAN dla urządzenia. O ustawieniach tych można powiedzieć, że są to ustawienia prywatne. W razie potrzeby możecie zmienić adres IP LAN. Adres IP LAN jest przekazywany do Twojej sieci wewnętrznej i nie można go zobaczyć w Internecie.

Interface	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Internet	LAN	Wireless		
Router Local IP	IP Address : 192.168.1.1 IP Subnet Mask : 255.255.255.0 Dynamic Route : RIP2-B Direction : None Multicast : Disabled IGMP Snoop : <input checked="" type="radio"/> Disabled <input checked="" type="radio"/> Enabled				
DHCP	DHCP : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay				
DHCP Server	Starting IP Address : 192.168.1.33 <input type="button" value="Current Pool Summary"/> IP Pool Count : 32 Lease Time : 259200 seconds (0 sets to default value of 259200)				
DNS	DNS Relay : Use Auto Discovered DNS Server Only Primary DNS Server : N/A Secondary DNS Server : N/A				
<input type="button" value="SAVE"/> <input type="button" value="CANCEL"/>					

5.2.1 Lokalny IP routera

Adres IP: Wpisz adres IP Twojego sterownika ADSL w zapisie dziesiętnym z kropkami, na przykład 192.168.1.1 (ustawienia domyślne).

Maska podsieci IP: Wasz router ADSL automatycznie przeliczy maskę podsieci opartą na adresie IP, który został Wam przydzielony. Jeśli nie wprowadzacie podsieciowania, powinniście użyć maski podsieci obliczonej przez sterownik ADSL.

Dynamiczna trasa: Wybierz dynamiczną trasę z RIP1, RIP2-B i RIP2-M. Patrz trasa Internet → Dynamic. Jedną różnicę stanowi interfejs.

5.2.2 Objaśnienie ustawień RIP

Protokół zawierający informację o trasowaniu (RIP) pozwala routerowi (sterownikowi) wymieniać informacje o trasowaniu z innymi routerami (sterownikami). Pole kierunkowe RIP kontroluje w jaki sposób pakiety RIP mogą wchodzić do routera (sterownika) i wychodzić z niego. Wybór Both (Oba) oznacza, że router będzie nadawał swoją tablicę tras, a jednocześnie odbierał informacje RIP, które otrzymuje. Wybór In Only (Tylko odbiór) oznacza, że router będzie tylko przyjmował otrzymywane informacje RIP, a nie będzie wysyłał pakietów RIP. Wybór Out Only (Tylko wysyłanie) oznacza, że router będzie tylko wysyłał pakiety RIP, a nie będzie odbierał przychodzących pakietów RIP. Wybór None (żaden) oznacza, że router ani nie będzie wysyłał pakietów RIP, ani też nie będzie odbierał żadnych pakietów RIP.

Pole trasy dynamicznej kontroluje format i metodę nadawania pakietów RIP wysyłanych przez Reuter. Rozpoznaje on oba formaty przy otrzymywaniu pakietów. RIP-1 jest uniwersalnie rozpoznawane, lecz RIP-2 przynosi więcej informacji. W przypadku większości sieci odpowiednim pakietem jest RIP-1. Z pakietu RIP-2 korzystać należy jedynie wówczas, gdy sieć ma niezwykłą topologię.

Zarówno RIP-2B jak i RIP2-M przesyłają dane trasowania w formacie RIP-2. RIP-2B wykorzystuje przesyłanie do podsieci, natomiast RIP-2M korzysta z multi - emisji.

Kierunek: Należy wybrać odpowiedni kierunek RIP, klikając jeden z następujących napisów None (żaden), Both (Oba), In Only (Tylko odbieranie) i Out Only (Tylko wysyłanie).

Multiemisja (połączenie wielopunktowe): IGMP, jest to protokół warstwy sesji używanej do ustalenia członkostwa w grupie składającej się z wielu rozmówców. Router ADSL obsługuje zarówno IGMP-v1, jak i IGMP-v2. Gdy chce się go wyłączyć, należy wcisnąć None (Brak). Prosimy porównać z Internet → Multicast. Jedyną różnicę stanowi tutaj interfejs.

5.2.3 Serwer DHCP

Serwer DHCP podaje adresy IP w czasie, gdy urządzenie inicjuje system operacyjny i żąda, aby IP został zarejestrowany w sieci. Urządzenie musi być ustawione jako klient DHCP, aby otrzymać automatycznie adres IP. W routerze domyślnie włączony jest serwer DHCP. Zbiór adresów DHCP zawiera zakres adresów IP, który automatycznie zostaje przydzielony klientowi w sieci.

ETYKIETA	OPIS
Adres początku puli adresów IP	Wpisz początkowy adres IP, którego chcesz używać jako pierwszy z adresów przypisywanych przez serwer DHCP.
Ilość adresów IP w puli adresów serwera	Wstaw maksymalną dopuszczaną ilość adresów do przydzielenia
Czas dzierżawy	Wpisz czas, na jaki wydierżawiany jest klientom adres IP.
Przełącznik DNS	Wybierz opcję przełącznika DNS, z którego chcesz korzystać z listy rozwijanej
Podstawowy serwer DNS	Wpisz adres IP podstawowego serwera DNS, z którego chcesz korzystać. Tylko dla DNS widocznych dla użytkownika.
Pomocniczy serwer DNS	Wpisz adres IP pomocniczego serwera DNS, z którego chcesz korzystać. Tylko dla DNS widocznych przez użytkownika.

5.2.4 Przełącznik DHCP

Przełącznik DHCP jest to komputer, który przesyła dane DHCP pomiędzy komputerami, które żądają podania adresów IP i serwerem DHCP, który przydziela adresy. Każdy z interfejsów urządzenia można skonfigurować jako przełącznik DHCP. Jeśli zostanie on włączony, wówczas żądania DHCP od lokalnych komputerów osobistych, przekazuje do serwera DHCP po stronie WAN. Aby jednak ta funkcja działała prawidłowo, prosimy działać tylko w trybie routera, wyłączyć serwer DHCP na porcie LAN i upewnić się, czy tablica routingu ma prawidłowy wpis dotyczący trasowania.

IP serwera DHCP dla agenta przełącznika: Adres IP serwera DHCP działającego po stronie WAN.

5.2.5 Przełącznik DNS

Konfiguracja DNS umożliwia użytkownikowi ustawienie konfiguracji DNS.

DHCP	
DHCP Server	DHCP: <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay
	Starting IP Address: <input type="text" value="192.168.1.33"/>
	IP Pool Count: <input type="text" value="32"/>
	Lease Time: <input type="text" value="253200"/> seconds (0 sets to default value of 253200)
DNS	DNS Relay: <input type="text" value="Use Auto Discovered DNS Server Only"/>
	Primary DNS Server: <input type="text" value="N/A"/>
	Secondary DNS Server: <input type="text" value="N/A"/>

Wybór przekąźnika DNS: Jeśli pragniesz wyłączyć tę funkcję, wystarczy jeżeli ustawisz zarówno podstawowy, jak i pomocniczy DNS na 0.0.0.0. Używając przekąźnika DNS Użytkownicy mogą ustawić IP serwera DNS na wartość 192.168.1.1 w swoim komputerze. Jeśli tego nie uczynią, urządzenie będzie działało jako przekąźnik NO DNS (BRAK DNS).

Jeżeli nie będziesz chciał korzystać z opcji przekąźnika DNS, powinieneś ustawić przekąźnik DNS na „Use User Discovered DNS Server Only” („Używaj tylko serwera DNS, wykrytego przez Użytkownika”) i ustawić podstawowe i pomocnicze serwery DNS na 0.0.0.0.

5.3 Sieci bezprzewodowe

Interface	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Internet	LAN	Wireless		
Access Point Settings					
Access Point: <input checked="" type="radio"/> Activated <input type="radio"/> Deactivated					
Channel: Undefined <input type="text"/> Auto <input type="text"/> Current Channel: <input type="text" value="1"/>					
Beacon Interval: <input type="text" value="100"/> (range: 20-1000)					
RTS/CTS Threshold: <input type="text" value="2347"/> (range: 1500-2347)					
Fragmentation Threshold: <input type="text" value="2346"/> (range: 256-2346, even numbers only)					
DTM: <input type="text" value="1"/> (range: 1-255)					
802.11 b/g: <input type="text" value="802.11b-g"/>					
Multiple SSIDs Settings					
SSID Index: <input type="text" value="1"/>					
SSID: <input type="text" value="Default_WLAN"/>					
Broadcast SSID: <input checked="" type="radio"/> Yes <input type="radio"/> No					
Authentication Type: <input type="text" value="Disabled"/>					
WDS Settings					
WDS Mode: <input type="text" value="Disabled"/>					
Mac Address #1: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #2: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #3: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #4: <input type="text" value="00:00:00:00:00:00"/>					
Wireless MAC Address Filter					
Active: <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated					
Action: <input type="text" value="Allow Association"/> the follow Wireless LAN station(s) association.					
Mac Address #1: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #2: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #3: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #4: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #5: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #6: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #7: <input type="text" value="00:00:00:00:00:00"/>					
Mac Address #8: <input type="text" value="00:00:00:00:00:00"/>					
<input type="button" value="SAVE"/> <input type="button" value="CANCEL"/>					

5.3.1 Ustawienia punktu dostępowego

Access Point: Dokonaj wyboru w tej sekcji, aby uaktywnić (Activate) lub dezaktywować (Deactivate) funkcje punktu dostępowego

Channel: Dokonaj wyboru kanału sieci bezprzewodowej z rozwijanej listy

Beacon Interval: Określ jak często wysyłany jest pakiet synchronizacji sieci bezprzewodowej.

RTS/CTS Threshold: Próg RTS (żądania wysłania) (liczba bajtów) mający na celu umożliwienie inicjacji RTS/CTS. Dane mające wymiar ramki większy od tej wartości podlegają potwierdzeniu RTS/CTS. Należy ustawić ten atrybut większy niż maksymalna wartość MSDU (MAC Service Data Unit), gdy chce się wyłączyć potwierdzenie RTS/CTS. Gdy chce się włączyć potwierdzenie RTS/CTS należy ustawić ten atrybut równy ZERO. Wpisać wartość pomiędzy 0 a 2432.

Fragment Threshold: Wartość progowa (liczba bajtów) dla granicy fragmentacji dla ukierunkowanych komunikatów. Jest to maksymalny wymiar fragmentu danych, który może być przesłany. Należy wpisać wartość pomiędzy 256 i 2432.

DTIM: Wartość ta mieszcząca się w zakresie o1 do 255 wskazuje odstęp komunikatów ruchu dochodzącego (DTIM). 802.11 b/g: Wybierz tryb pracy sieci bezprzewodowej.

5.3.2 Ustawienia SSID

SSID: SSID jest to unikalna nazwa identyfikująca router ADSL w sieci bezprzewodowej. Bezprzewodowi klienci związani z routerem ADSL muszą mieć ustawiony taki sam SSID. Domyślny SSID to: MC-420.

Rozsyłanie SSID Jeżeli zechcesz ukryć SSID tak, aby stacja nie mogła otrzymać SSID za pomocą biernego skanowania musisz wybrać No (Nie). Aby SSID było widoczne wybierz Yes (Tak).

Authentication Type: Wybierz rodzaj szyfrowania stosowanego przez punkt dostępowy. Dostępne są 4 rodzaje szyfrowania – WEP-64Bits, WEP-128Bits, WPA-PSK, WPA2-PSK.

[Rodzaj szyfrowania]

WEP (Wired Equivalent Privacy) szyfruje ramki danych przed przesłaniem ich siecią bezprzewodową. Gdy chcesz pozwolić, aby wszystkie bezprzewodowo połączone komputery połączyły się z punktami dostępu bez jakichkolwiek zakodowania danych, wybierz Disable (Wyłączyć). Jeśli chcesz korzystać z zaszyfrowanych danych, wybierz 64-bit WEP lub 128-bit WEP.

Key#1~Key#4 (Klucz#1-Klucz#4) Klucze WEP są wykorzystywane do szyfrowania danych. Zarówno router ADSL, jak klienci bezprzewodowych sieci muszą używać tego samego klucza WEP do nadawania danych. Jeśli wybierzesz 64-bitowy WEP, wówczas możesz wpisać dowolną 10-cyfrową szesnastkową liczbę („0-9”, „A-F”) poprzedzonych przez 0x dla każdego klawisza (1-4). Jeśli wybierzesz 128-bitowy WEP, wówczas wpisz 26-cyfrową szesnastkową liczbę („0-9”, „A-F”) poprzedzoną przez 0x dla każdego klucza (1-4). Wartości powinny być ustawione dokładnie takie same w punktach odstępu, jakie występują w stacjach bezprzewodowych klienta. Ta sama wartość musi być przypisana do klucza 1 w obu punktach dostępu (Wasz router ADSL) i adaptery klienta. Ta sama wartość musi być przypisana do klucza 2 w obu punktach dostępu i na stacjach klienta itd. dla wszystkich czterech kluczy WEP.

WPA-PSK Dostęp zabezpieczony Wi-Fi, klawisz wstępnie udostępniony (wspólny). Ramki są szyfrowane przed przesłaniem przez sieć bezprzewodową.

Wstępnie udostępniony (Pre-Shared) klucz jest wykorzystywany do szyfrowania danych. Zarówno router ADSL, jak i klienci bezprzewodowej instalacji muszą używać takiego samego klawisza WPA-PSK do przekazywania danych.

5.3.3 Ustawienia WDS

WDS (Wireless Distribution System) to system umożliwiający bezprzewodowe połączenie kilku routerów. Umożliwia to rozszerzenie obszaru sieci bezprzewodowej przy użyciu kilku punktów dostępowych, bez potrzeby zastosowania przewodowego połączenia między nimi.

WDS jest sposobem dołączenia routera do istniejącej sieci Wi-Fi. Najczęściej WDS stosowany jest w dużych otwartych przestrzeniach gdzie jest ograniczona możliwość przeprowadzenia kablowego połączenia.

Tryby WDS

WDS Mode: (1) Restricted – Uczestnicy WDS muszą być zarejestrowani w routerze (przy użyciu adresu MAC).

(2) Bridge – Punkt dostępowy pełnić będzie rolę bezprzewodowego mostu, przesyłając jedynie ruch pakietów pomiędzy innymi punktami dostępowymi. Uczestnicy WDS muszą być ręcznie ustalen i stacje bezprzewodowe nie będą w stanie połączyć się z routerem.

(3) Repeater – Router pełnić będzie funkcję regeneratora łączącego między punktami dostępowymi. Uczestnicy WDS mogą być ustalen przez użytkownika ("Restricted mode") lub automatycznie ("Lazy" mode)

(4) Lazy – Automatyczne wykrywanie uczestników WDS: kiedy użytkownik sieci lokalnej poszukuje sieci, router spróbuje połączyć go do urządzeń pracujących w WDS znajdujących się w jego okolicy.

WDS Settings

WDS Mode: **Disabled**

Mac Address #1: **Disabled** :00

Mac Address #2: **Restricted** :00

Mac Address #3: **Bridge** :00

Mac Address #4: **Repeater** :00

Mac Address #5: **Lazy** :00

Mac Address #6: 00:00:00:00:00:00

MAC address #1-#4: Określ tu adres MAC urządzenia docelowego. Filtr ten pozwala określić, które stacje będą miały dostęp do Twojej sieci.

5.3.4 Filtr adresu MAC

Możesz pozwolić lub nie pozwolić na to, aby pewne adresy MAC związane z Twoimi stacjami bezprzewodowymi miały dostęp do routera ADSL.

Stan: Użyj listy rozwijanej przy włączaniu lub wyłączeniu filtrów adresu MAC.

Działanie: Gdy chce się zablokować dostęp do routera, należy wybrać Deny Association (Odmowa przypisania). Adresy MAC nie wymienione na liście będą wówczas miały dostęp do routera .

Gdy chce się umożliwić dostęp do routera, należy wybrać Allow Association (Pozwolić na połączenie). Adresy MAC, które nie znajdują się w zbiorze, nie będą miały dostępu do routera.

6. Zaawansowane ustawienia

6.1 Zabezpieczenia Firewall

Użytkownik może włączyć lub wyłączyć zabezpieczenie firewall routera ADSL na tej stronie.

Advanced

Interface Setup | Advanced Setup | Access Management | Maintenance | Status

Routing | NAT | QoS | VLAN | ADSL | **Firewall**

Firewall

Firewall: Enabled Disabled

SPI: Enabled Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

SAVE CANCEL

Zabezpieczenie Firewall: Wybierz tę opcję, aby móc automatycznie wykrywać i blokować ataki typu DoS (Denial Of Service) takich jak: Ping of death, SYN Flood, skanowanie portu i Land attack.

SPI: Wybierz tę opcję, aby włączyć lub wyłączyć funkcję SPI. (UWAGA: Jeśli włączysz SPI, wówczas wszystkie elementy ruchu zainicjowane przez WAN zostaną zablokowane wraz z DMZ, wirtualnym serwerem oraz stroną ACL WAN).

6.2 Routing

Tablica ta podaje adresy IP miejsc w Internecie, do których często uzyskiwany jest dostęp z Twojej sieci. Gdy komputer poprosi o przesłanie danych do podanego miejsca przeznaczenia, urządzenie wykorzystuje bramkę IP do identyfikacji pierwszego routera Internetu, z którym należy nawiązać kontakt, aby można było ustalić najbardziej odpowiednią trasę przesyłania danych. Po wyborze tej opcji otrzymuje się tablicę trasowania, zawierającą potrzebne informacje. Gdy chce się wyedytować trasę statyczną (tak, jak na poniższym ekranie), można wcisnąć ADD ROUTE (Dodaj trasę).

#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.1	1	enet0	180		
2	default	0	Node1	2	Idle	0		

[Statyczna trasa]

Chcąc uzyskać informacje o statycznym routingu, należy wybrać tę opcję.

Adres docelowy (miejsca przeznaczenia) IP: Parametr ten określa adres sieci IP docelowego miejsca przeznaczenia pakietów, które są kierowane odpowiednimi trasami zgodnie z tą regułą.

Maska podsieci IP: Wpisz maskę podsieci dla tego miejsca przeznaczenia.

Adres IP bramki: Bramka jest bezpośrednim sąsiadem Twojego routera ADSL, który przesyła pakiet do miejsca przeznaczenia. W przypadku LAN bramka musi być routerem w tym samym segmencie, jak i Wasz router; w przypadku Internetu (WAN) bramka musi być adresem IP jednego ze zdalnych węzłów.

Zapis metryczny: Zapis metryczny reprezentuje „koszt” transmisji dla celów trasowania. Trasowanie IP wykorzystuje obliczenie hopów (jednostek odległości internetowych) jako pomiar kosztów, przy czym minimalna wartość kosztów wynosi 1 w przypadku sieci połączonych bezpośrednio. Wpisz liczbę, która podaje przybliżoną wartość kosztów dla tego połączenia. Liczba ta nie musi być dokładna, lecz musi ona mieścić się w granicach od 1 do 15. W praktyce dobrą liczbą jest na przykład 2 albo 3.

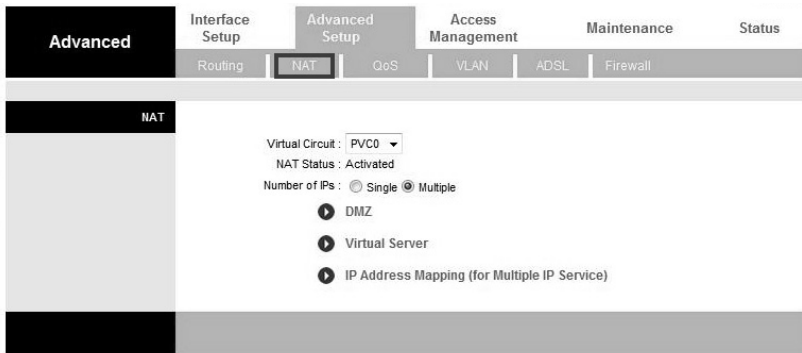
Zapowiedź w RIP: Parametr ten określa, czy router ADSL zawiera router do tego zdalnego węzła w transmisjach RIP.

Jeśli wybierzesz Yes (Tak), router znajdujący się w tym odległym węźle zostanie przesłany dalej do innych stacji bazowych (komputerów) przez transmisję RIP. Jeśli wybierzesz No (Nie), trasa ta zostaje utrzymana jako prywatna i nie wchodzi do transmisji RIP.

Jeśli wprowadzacie zmiany, powinniście kliknąć SAVE (Zapamiętaj), aby zapisać zmianę, DELETE (Skasuj), gdy chcesz skasować zasadę wraz z ustawionymi parametrami a BACK (Wstecz), jeśli chcesz powrócić do poprzedniego ekranu lub CANCEL (Anuluj), gdy chcesz wyjść bez zapisywania wprowadzonych zmian.

6.3 NAT

Tłumaczenie adresu sieciowego (NAT) jest to metoda ukrywania prywatnych adresów IP, którego używasz w Twoim LAN jako publicznego adresu IP, którego używasz w Internecie. Należy zdefiniować zasady NAT, które dokładnie określą w jaki sposób i kiedy należy dokonać tłumaczenia pomiędzy publicznym i prywatnymi adresami IP. Gdy chcesz ustawić funkcję NAT Twojego Routera ADSL, powinieneś po prostu wybrać tę opcję.



Wirtualny obwód (VC): Właściwości wirtualnego obwodu (VC) interfejsu ATM VC identyfikują jedną szczególną drogę, której używa Wasz router ADSL/Ethernet, aby połączyć się poprzez sieć na bazie ATM z urządzeniami centrali telekomunikacyjnej.

Status NAT: W polu tym pokazano aktualny stan funkcji NAT bieżącego VC.

Liczba IP: W polu tym podano ile adresów IP przewidziane zostało przez Twojego IP dla aktualnego VC. Może to być pojedynczy IP lub kilka IP.

Uwaga: W przypadku VC z pojedynczym IP korzystają one z tych samych DMZ i serwerów wirtualnych. Każdy VC ustawia DMZ i serwery wirtualne. Ponadto w przypadku VC z kilkoma IP należy określić zasady mapowania (odzworowywania) adresu. W przypadku VC z jednym IP, gdyż mają one tylko jeden IP, nie ma potrzeby indywidualnego zdefiniowania zasad odzworowywania adresu.

6.3.1 Co robi NAT?

NAT zmienia źródłowy adres IP w pakiecie otrzymanym od abonenta (adres w sieci lokalnej) na inny (publiczny adres w sieci globalnej) przed przesłaniem pakietu na stronę WAN. Po nadejściu odpowiedzi NAT tłumaczy adres docelowy (publiczny adres w sieci globalnej) z powrotem na adres w sieci lokalnej przed przesłaniem go do stacji w sieci lokalnej. Prosimy zauważyć, że adres IP (zarówno lokalny albo globalny) zewnętrznej stacji (komputera) nigdy nie zostaje zmieniony.

Globalne adresy IP dla wewnętrznych stacji centralnych mogą być albo statycznie, albo dynamicznie przypisane przez ISP. Możesz także wyznaczyć serwery takie, jak serwer sieciowy i serwer telnet Twojej lokalnej sieci i udostępnić je dla

zewnątrznego świata. Jeśli nie zdefiniuje się żadnych serwerów, Twój Router będzie odfiltrowywał wszystkie przychodzące zapytania, chroniąc w ten sposób przed przedostaniem się intruzów do Twojej sieci. Więcej informacji na temat tłumaczenia adresu IP znaleźć możesz w RFC 1631, translator adresu sieciowego IP (NAT).

Ustawienia wewnętrzne / zewnętrzne wskazuje, w którym miejscu komputer znajduje się stosunku do Twojego Routera. Komputery Twojego LAN są wewnętrzne, podczas gdy serwery sieciowe Internetu są zewnętrzne. Określenie globalne / lokalne podaje adres IP stacji bazowej w pakiecie w chwili, gdy pakiet przechodzi przez router. Lokalny adres odnosi się do adresu IP stacji bazowej, gdy pakiet znajduje się w lokalnej sieci, podczas gdy globalny adres odnosi się do adresu IP stacji bazowej, gdy ten sam pakiet przechodzi na stronę WAN.

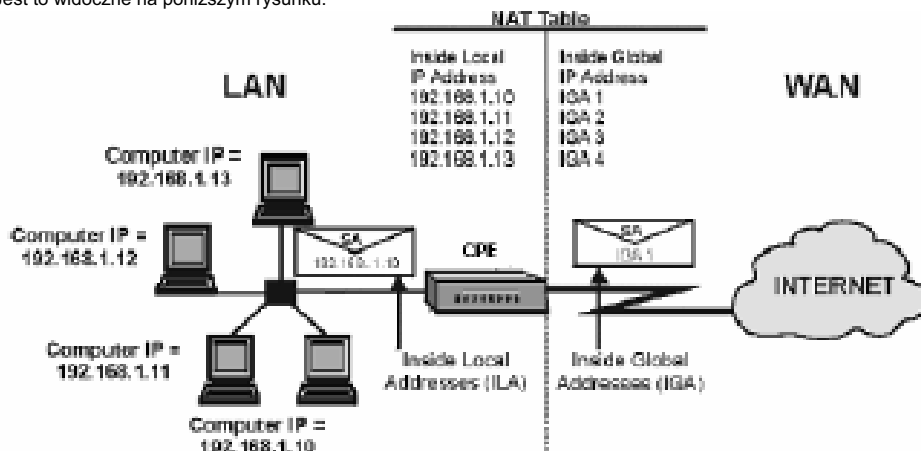
Prosimy zauważyć, że określenie wewnętrzny / zewnętrzny odnosi się do miejsca zajmowanego przez stację bazową, podczas gdy określenie globalny / lokalny odnosi się do adresu IP stacji bazowej używanego w pakiecie. Tak więc wewnętrzny lokalny adres (ILA) jest to adres IP wewnętrznej stacji bazowej pakietu, gdy pakiet ten znajduje się nadal jeszcze w sieci lokalnej, podczas gdy wewnętrzny globalny adres (IGA) jest to adres IP tej samej wewnętrznej stacji bazowej, gdy pakiet znajduje się już po stronie WAN.

Podane tutaj informacje zostały zebrane w poniższej tabeli:

POZYCJA	OPIS
Wewnętrzny	Określenie to odnosi się do stacji bazowej w LAN.
Zewnętrzny	Określenie to odnosi się do stacji bazowej w WAN.
Lokalny	Określenie to odnosi się do adresu pakietu (źródłowego lub docelowego) w chwili, gdy pakiet ten przechodzi przez LAN.
Globalny	Określenie to odnosi się do adresu pakietu (źródłowego lub docelowego) w chwili, gdy pakiet ten przechodzi przez WAN.

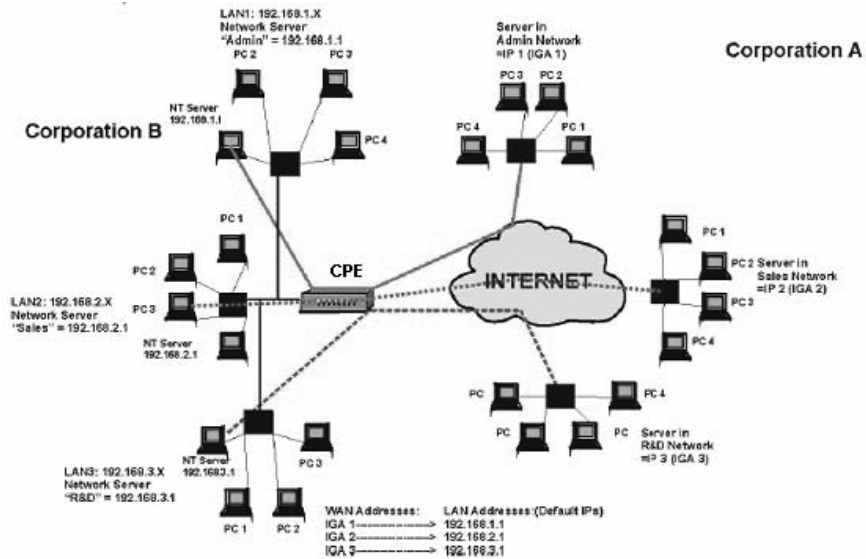
6.3.2 W jaki sposób działa NAT?

Każdy pakiet ma dwa adresy: adres źródłowy i adres docelowy. Dla wychodzących pakietów ILA stanowi adres źródłowy w LAN, a IGA jest adresem źródłowym w WAN. W przypadku przychodzących pakietów ILA jest adresem docelowym w LAN, a IGA - adresem docelowym w WAN. NAT odwzorowuje prywatne (lokalne) adresy IP na unikalne adresy globalne, wymagane dla nawiązywania kontaktu ze stacjami bazowymi w innych sieciach. Zastępuje on oryginalny adres źródłowy IP (oraz numery portów źródłowych TCP lub UDP dla odwzorowania NAT przeciążenia kilka na jeden i kilka na kilka) w każdym pakiecie, a następnie przesyła go do Internetu. Router śledzi drogę oryginalnych adresów i numery portów, dzięki czemu nadchodzące pakiety z odpowiedzią mogą mieć przywrócone swoje wyjściowe wartości. Jest to widoczne na poniższym rysunku.



6.3.3 Zastosowanie NAT

Poniższa tablica przedstawia możliwe zastosowania NAT w przypadku których trzy wewnętrzne LAN (logiczne LAN używające nazwy umownej IP), znajdujące się za routerem mogą nawiązywać łączność z trzema wyraźnymi sieciami WAN. Więcej przykładów zamieszczono na końcu tego rozdziału.



6.3.4 Typy odwzorowywania NAT

NAT wspiera pięć typów odwzorowywania IP / port. Są to następujące typy:

- Jeden na jeden: W trybie jeden na jeden TC3162 EVM odwzorowuje jeden lokalny adres IP na jeden globalny adres IP.
- Kilka na jeden: W trybie kilka na jeden TC3162 EVM odwzorowuje kilka lokalnych adresów IP na jeden globalny adres IP.
- Wiele na wiele z przeciążeniem: W trybie wiele na wiele z przeciążeniem TC3162 EVM odwzorowuje kilka lokalnych adresów IP na wspólne globalne adresy IP.
- Wiele na wiele bez przeciążenia: W trybie wiele na wiele bez przeciążenia TC3162 EVM odwzorowuje każdy lokalny adres IP na jedyny istniejący adres globalny IP.
- Serwer: Typ ten umożliwi Wam określenie wewnętrznych serwerów różnych usług poza NAT, dostępnych dla zewnętrznego świata.

W poniższej tablicy zebrano powyższe typy.

TYP	ODWZOROWANIE IP
Jeden na jeden	ILA1 IGA1
Kilka na jeden (SUA/PAT)	ILA1 IGA 1
	ILA2 IGA1
	...

Wiele na wiele z przeciążeniem	ILA1	IGA1
	ILA2	IGA2
	ILA3	IGA1
	ILA4	IGA2
	...	
Wiele na wiele bez przeciążenia	ILA1	IGA1
	ILA2	IGA2
	ILA3	IGA3
	...	
Serwer	Serwer 1 IP	IGA1
	Serwer 2 IP	IGA1
	Serwer 3 IP	IGA1

6.3.5 DMZ

DMZ (strefa zdemilitaryzowana) jest to komputer/serwer w sieci lokalnej dostępny z sieci publicznej. Nie pozwala on zewnętrznym użytkownikom na bezpośredni dostęp do serwera, na którym znajdują się dane firmy. Użytkownicy sieci publicznej spoza przedsiębiorstwa mogą uzyskać dostęp tylko do stacji DMZ.

DMZ: Może być włączony lub wyłączony.

Adres IP stacji bazowej DMZ: Należy wpisać podany adres IP stacji bazowej DMZ po stronie LAN.

Przy wprowadzaniu zmian należy kliknąć SAVE (Zapisz), aby zapisać wprowadzone zmiany lub BACK (Wstecz), aby powrócić do poprzedniego ekranu.

6.3.6 Serwer wirtualny

Wirtualny serwer jest to serwer lub serwery, znajdujące się poza NAT (w LAN). Na przykład: serwer sieciowy lub serwer FTP, który możecie uwidocznili dla zewnętrznego świata nawet wtedy, gdy NAT sprawi, że Twoja cała sieć będzie dla zewnętrznego świata przedstawiała się jako jedno urządzenie.

Wskaźnik zasady: Wskaźnik zasady wirtualnego serwera dla tego VC. Możecie wyszczególnić do 10 zasad. Wszystkie VC z pojedynczymi IP korzystają z tych samych zasad serwera wirtualnego.

Liczba portu początkowego i końcowego: Wpisz liczbę portu początkowego i końcowego, którą chcesz przekazać do danego komputera (serwera). Jeśli jest tylko jeden port, możesz wpisać taką samą liczbę portu końcowego, jak liczbę portu początkowego. Tak na przykład przy ustawianiu serwera wirtualnego FTP możesz ustawić numer portu początkowego i końcowego równy 21.

Lokalny adres IP: Wpisz adres IP dla wirtualnego serwera po stronie LAN.

Lista serwerów wirtualnych: Jest to lista wszystkich serwerów wirtualnych ustawionych przez Ciebie.

Przy wprowadzaniu zmian kliknij SAVE (Zapamiętaj), aby zapisać wprowadzone zmiany, DELETE (Skasuj), aby skasować zasadę (regulę) z ustawionymi przez Ciebie parametrami, BACK (Wstecz), aby powrócić do poprzedniego ekranu lub CANCEL (Anuluj), aby wyjść bez zapisywania wprowadzonych zmian.

Advanced

Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status

Routing | **NAT** | QoS | VLAN | ADSL | Firewall

Virtual Server

Virtual Server for: PVC0 - Multiple IP Account

Rule Index: 1

Application: -

Protocol: ALL

Start Port Number: 0

End Port Number: 0

Local IP Address: 0.0.0.0

Virtual Server Listing

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

SAVE DELETE BACK CANCEL

6.3.7 Odwzorowywanie adresów IP

Odwzorowywanie adresów IP dotyczy tych VC, które mają kilka IP. Zasadą odwzorowywania adresów IP jest przyjęcie za podstawę VC (tylko dla kilku IP VC).

Wskaźnik zasady (reguły): Wskaźnik zasady (reguły) dla tego VC. Możesz podać do 10 reguł (zasad). Wszystkie VC z pojedynczym IP używają tych samych reguł (zasad) serwera wirtualnego.

Typ zasady (reguły): Istnieją 4 typy: jeden na jeden, kilka na jeden, kilka na kilka z przeciążeniem, kilka na kilka bez przeciążenia.

Lokalny IP adres początkowy i końcowy: Wpisz lokalny adres IP, który chcesz odwzorować. Lokalny początkowy IP jest to lokalny początkowy adres IP, a lokalny końcowy IP jest to lokalny końcowy adres IP. Jeśli dana zasada (reguła) odnosi się do wszystkich lokalnych IP, wówczas początkowy IP wynosi 0.0.0.0 a końcowy IP wynosi 255.255.255.255.

Publiczny początkowy i końcowy IP: Wpisz publiczny adres, którego chcesz użyć w NAT. Publiczny początkowy IP jest to początkowy publiczny adres IP, a końcowy publiczny IP jest to końcowy publiczny adres IP. Jeśli masz dynamiczny IP, wpisz 0.0.0.0 jako publiczny początkowy IP.

Przy wprowadzaniu zmian kliknij SAVE (Zapamiętaj), aby zapisać wprowadzone zmiany, DELETE (Skasuj), aby skasować zasadę (regułę) z ustawionymi przez Ciebie parametrami, BACK (Wstecz), aby powrócić do poprzedniego ekranu lub CANCEL (Anuluj), aby wyjść bez zapisywania wprowadzonych zmian.

Advanced
Interface Setup
Advanced Setup
Access Management
Maintenance
Status

Routing
NAT
QoS
VLAN
ADSL
Firewall

IP Address Mapping

Address Mapping List

Address Mapping Rule : PVC0

Rule Index : 1

Rule Type : One-to-One

Local Start IP : 0.0.0.0

Local End IP : N/A

Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)

Public End IP : N/A

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

SAVE
DELETE
BACK
CANCEL

6.4 ADSL

Wybierz tę opcję, gdy będziesz chciał ustawić informacje o trybie ADSL oraz typie ADSL.

Tryb ADSL: Wybierz, którego trybu połączenia z listy rozwijanej używa Twój ADSL.

Opcja ta ma następujące tryby: Auto Sync-up, ADSL2+, ADSL2, G.DMT, T1.413, G.LITE.

Typ ADSL: Wybierz typ ADSL, którego będziesz używać z listy rozwijanej:

ANNEX A, ANNEX I, ANNEX A/L, ANNEX M, ANNEX A/t/J/L/M.

Gdy wprowadzisz zmiany kliknij SAVE (Zapisz), aby zapisać wprowadzone zmiany.

Advanced
Interface Setup
Advanced Setup
Access Management
Maintenance
Status

Routing
NAT
QoS
VLAN
ADSL
Firewall

ADSL

ADSL Mode : Auto Sync-Up

ADSL Type : ANNEX A/t/J/L/M

SAVE

6.5 QoS

QoS (Quality of Service – Jakość usługi). Opcja ta pozwala dostarczyć lepszą jakość usługi dla wybranego ruchu sieciowego przy użyciu różnych technologii. Zastosowanie zarządzania QoS gwarantuje, że wszystkie aplikacje będą mogły skorzystać z przepustowości sieci na poziomie spełniającym oczekiwania.

Advanced	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Routing	NAT	QoS	VLAN	ADSL
Quality of Service					
QoS : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated					
Summary : <input type="button" value="QoS Settings Summary"/>					
Rule	Rule Index : 1				
	Active : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated				
	Application : <input type="text"/>				
	Physical Ports : <input type="checkbox"/> WLAN <input type="checkbox"/> Enet1 <input type="checkbox"/> Enet2 <input type="checkbox"/> Enet3 <input type="checkbox"/> Enet4				
	Destination MAC : <input type="text"/>				
	IP : <input type="text"/>				
	Mask : <input type="text"/>				
	Port Range : <input type="text"/> ~ <input type="text"/>				
	Source MAC : <input type="text"/>				
	IP : <input type="text"/>				
	Mask : <input type="text"/>				
	Port Range : <input type="text"/> ~ <input type="text"/>				
	Protocol ID : <input type="text"/>				
	Vlan ID Range : <input type="text"/> ~ <input type="text"/>				
	IPIDS Field : <input type="radio"/> IPPITOS <input checked="" type="radio"/> DSCP				
Action	IP Precedence Range : <input type="text"/> ~ <input type="text"/>				
	Type of Service : <input type="text"/>				
	DSCP Range : <input type="text"/> ~ <input type="text"/> (Value Range: 0 ~ 63)				
	802.1p : <input type="text"/> ~ <input type="text"/>				
	IPIDS Field : <input type="radio"/> IPPITOS <input checked="" type="radio"/> DSCP				
	IP Precedence Remarking : <input type="text"/>				
	Type of Service Remarking : <input type="text"/>				
	DSCP Remarking : <input type="text"/> (Value Range: 0 ~ 63)				
	802.1p Remarking : <input type="text"/>				
	Queue # : <input type="text"/>				
<input type="button" value="ADD"/> <input type="button" value="DELETE"/> <input type="button" value="CANCEL"/>					

6.6 VLAN

Virtual LAN (VLAN – Wirtualna sieć lokalna) to grupa urządzeń w jednej lub wielu sieciach lokalnych (LAN) skonfigurowanych w ten sposób aby mogły komunikować się ze sobą tak, jakby były ze sobą połączone, podczas gdy w rzeczywistości znajdują się w różnych segmentach sieci LAN. Ponieważ VLAN oparty jest o połączenia logiczne a nie fizyczne, jest bardzo łatwe w zarządzaniu stacjami oraz określaniu dostępu do pasma oraz innych zasobów.

Port-Based VLAN (VLAN w oparciu o porty): każdy fizyczny port jest skonfigurowany przy użyciu listy dostępowej, określającej członków każdej wirtualnej sieci lokalnej.

ATM VLAN- używanie protokołu emulacji sieci lokalnej (LAN Emulation(LANE)) do przypisania pakietów Ethernet do komórek ATM i dostarczanie ich do celu poprzez przekształcenie adresów MAC w adresy ATM.

Klucz dla IEEE 802.1Q do wypełnienia powyższych funkcji znajduje się w jego znacznikach. Koncentratory przełączające (switche) kompatybilne z protokołem 802.1Q, mogą być skonfigurowane do przesyłania oznakowanych lub nieoznakowanych ramek. Pole znacznika zawierającego informację o VLAN (i/lub priorytecie 802.1p) może być umieszczone w ramce Ethernet. Jeżeli port ma podłączone urządzenie zgodne z 802.1Q (np. inny koncentrator przełączający), takie oznakowane ramki mogą przenieść informacje o przynależności do VLAN, co za tym rozszerzać się na inne switche. Jednakże należy pamiętać o tym, że aby porty do których podłączone są urządzenia niezgodne z 802.1Q,

skonfigurowane były do przesyłania pakietów nieoznakowanych. Wiele interfejsów sieciowych dla komputerów i drukarek nie jest zgodnych z 802.1Q. Jeżeli urządzenie takie, otrzyma ramkę oznakowaną, nie będą one w stanie rozpoznać informacji o VLAN i odrzucą tę ramkę.

The screenshot shows the 'Advanced' configuration page with the following structure:

- Advanced** (selected)
- Interface Setup**: Routing
- Advanced Setup**: NAT, QoS
- Access Management**: **VLAN** (selected), ADSL, Firewall
- Maintenance**: Firewall
- Status**

The 'VLAN' section contains:

- VLAN Function**: Activated Deactivated
- Assign VLAN PVID for each Interface** (with a right-pointing arrow)
- Define VLAN Group** (with a right-pointing arrow)

→ Assign VLAN PVID for each interface (przydziel identyfikator sieci VLAN dla każdego z portów): W tej sekcji możesz przydzielić PVID dla ATM VC, Ethernet (LAN port) oraz port bezprzewodowego.

→ Define VLAN Group (zdefiniuj grupę VLAN): Na podstawie grupy VLAN, możesz skonfigurować ustawienia każdej VLAN. Możesz skonfigurować do 8 ustawień VLAN.

7. Zarządzanie dostępem

7.1 ACL

Aby umożliwić zdalne zarządzanie należy przejść do Access Management → ACL (Zarządzanie dostępem → ACL). Lista kontrolna dostępu (ACL) jest to narzędzie zarządzania, które działa jak filtr dla przychodzących i wychodzących pakietów w zależności od zastosowania. Możecie używać telnetu lub sieci Web do zdalnego zarządzania ADSL. Użytkownik musi po prostu włączyć telnet lub sieć Web i podać im adres IP, który chce udostępnić routerowi ADSL. Domyślny IP 0.0.0.0 umożliwia wszystkim klientom skorzystanie z tej możliwości zdalnego zarządzania routerem ADSL.

The screenshot shows the 'Access Management' configuration page with the following structure:

- Access Management** (selected)
- Interface Setup**: ACL (selected), Filter
- Advanced Setup**: SNMP, UPnP
- Access Management**: DDNS, CWMP
- Maintenance**: DDNS, CWMP
- Status**

The 'ACL' section contains:

- Access Control Setup**: ACL: Activated Deactivated
- Access Control Editing**:
 - ACL Rule Index: 1
 - Active: Yes No
 - Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
 - Application: Web
 - Interface: LAN
- Access Control Listing**:

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	Web	LAN
2	Yes	0.0.0.0-0.0.0.0	FTP	LAN
3	Yes	0.0.0.0-0.0.0.0	Telnet	LAN
4	Yes	0.0.0.0-0.0.0.0	SNMP	Both
5	Yes	0.0.0.0-0.0.0.0	Ping	Both

Buttons: SAVE, DELETE, CANCEL

ACL: Istnieją dwie opcje: włączenie (aktywizacja) i wyłączenie (dezaktywizacja). Ustawieniem domyślnym jest wyłączenie (dezaktywizacja) co oznacza, że dostęp do wszystkich IP można uzyskać się przez router. W przypadku wyboru Activated (włączone) możesz mieć dostęp do Twojego routera tylko poprzez wyszczególnione w liście adresy IP.

Wskaźnik reguły (zasady) ACL: Wskaźnik ten powinien mieścić się w zakresie od 1 do 16.

Aktywność: Po wybraniu Yes (Tak) masz dostęp do IP przez router .

Zastosowanie: Każda z tych etykiet oznacza usługę, jakiej możesz użyć do zdalnego zarządzania routerem. Masz następujące możliwości do wyboru: Web, FTP, Telnet, SNOP, Ping, ALL (Wszystkie).

Interfejs: Wybierz interfejs dostępu. Możesz wówczas wybrać: WAN, LAN i Both.

Na przykład:

Jak ustawić ACL?

1. Wybierz Activated (włączone), aby uaktywnić funkcję ACL (włączyć działanie Twojego ACL).
2. Wybierz wartość wskaźnika zasady (reguły) ACL (do 16 numerów).
3. Możesz ustawić specjalny Secure IP address (Bezpieczny adres IP), lub też ustawić 0.0.0.0 dla wszystkich IP.
4. Wybierz Application (Aplikacje) której dotyczyć ma ta reguła.
5. Wybierz interfejs, do którego chcesz mieć dostęp.
6. Po zakończeniu wszystkich ustawień kliknij SAVE (Zapisz) i kontynuuj ustawienia następnej reguły ACL.

Access Control Setup

ACL : Activated Deactivated

ACL Rule Index :

Active : Yes No

Secure IP Address : - (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application :

Interface :

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	Web	LAN
2	Yes	0.0.0.0-0.0.0.0	Telnet	LAN
3	No	0.0.0.0-0.0.0.0	FTP	Both
4	No	0.0.0.0-0.0.0.0	SNMP	Both
5	No	0.0.0.0-0.0.0.0	Ping	LAN
6	No	0.0.0.0-0.0.0.0	ALL	LAN

[Uwagi]

1. Musisz ustawić jeden wskaźnik ACL, aby uzyskać dostęp do Twojego routera przez interfejs LAN. Jeśli tego nie uczynisz, Twój router nie może uzyskać dostępu do innych adresów IP wymienionych w liście (patrz wskaźnik 1).
2. Pamiętaj! Po uaktywnieniu Twojej funkcji ACL możesz mieć dostęp przez router jedynie przez wymieniony w liście bezpieczny adres IP.

7.2 Filtr IP

Router zapewnia bardzo pewną ochronę Firewall przez ograniczenie parametrów połączenia w celu ograniczenia niebezpieczeństwa wtargnięcia nieuprawnionych intruzów i dla obrony przed wieloma różnymi niebezpiecznymi hakera-
mi. Aby ustawić różne reguły filtrowania IP danego protokołu (TCP, UDP lub ICMP) i specjalnego kierunku filtrowania pakietów (przychodzące, wychodzące lub jedno i drugie) należy skorzystać z filtrowania IP. Filtr IP jest bardziej skomplikowanym narzędziem filtrowania opartym w większym stopniu na IP i przyjętych regułach. Każdy ze wskaźników może spełniać 6 reguł (zasad) i każdy interfejs może mieć 4 dodatkowe wskaźniki, co pozwala na uzyskanie 24 reguł (zasad) na interfejs. Jeśli wszystkie 6 reguł we wskaźniku są to reguły następne, dane będą przesłane do następnego wskaźnika do przefiltrowania.

Access Management
Interface Setup
Advanced Setup
Access Management
Maintenance
Status

ACL
Filter
SNMP
UPnP
DDNS
CWMP

Filter

Filter Type

Filter Type Selection : IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index : 1

Interface : PVC0

Direction : Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index : 1

Rule Type : IP

Active : Yes No

Source IP Address : (0.0.0.0 means Don't care)

Subnet Mask :

Port Number : (0 means Don't care)

Destination IP Address : (0.0.0.0 means Don't care)

Subnet Mask :

Port Number : (0 means Don't care)

Protocol : TCP

Rule Unmatched : Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index 1 Interface - Direction -

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE
DELETE
CANCEL

Wskaźnik ustawiania filtru IP: Wskaźnik ustawiania filtru IP powinien mieścić się w granicach od 1 do 12 przy czym każdy wskaźnik może ustawić do 6 filtrów IP.

Interfejs: Należy wybrać interfejs spośród PVC0 do PVC7 i LAN.

Kierunek: Masz do wyboru Both (Oba), Incoming (Przychodzący) i Outgoing (Wychodzący). Wybierz do jakiego kierunku przepływu danych chcesz dostosować swój filtr. Uwaga: Incoming (Przychodzący) i Outgoing (Wychodzący) z punktu widzenia Twojego routera odnoszą się do wybranego przez Ciebie interfejsu. W przypadku WAN dane pochodzące z zewnątrz Twojego systemu są traktowane jako przychodzące, a dane opuszczające Twój system - jako wychodzące. W przypadku LAN dane opuszczające Twój system są traktowane jako przychodzące, a dane wchodzące do Twojego systemu - jako wychodzące.

Edycja reguły (zasady) filtru IP: Wybierz wskaźnik reguły (zasady) filtru IP, który chcesz zmienić.

Aktywność: Ten wskaźnik reguły (zasady) może być włączony i wyłączony – odpowiednio Yes (Tak) lub No (Nie).

Adres źródłowy IP: Wpisz adres źródłowy IP, któremu chcesz odmówić dostępu do Twojego systemu.

Maska podsieci: Wpisz maskę podsieci źródłowego adresu IP.

Numer portu: Wpisz numer portu źródłowego adresu IP. Zwróć uwagę, że 0 oznacza dopuszczenie wszystkich portów.

Adres docelowy (miejsca przeznaczenia) IP: Wpisz adres docelowy (miejsca przeznaczenia) IP, któremu chcesz odmówić dostępu do Twojego systemu.

Maska podsieci: Wpisz maskę podsieci adresu docelowego (miejsca przeznaczenia) IP.

Numer portu: Wpisz numer portu adresu docelowego (miejsca przeznaczenia) IP. Zwróć uwagę, że 0 oznacza wszystkie dopuszczalne porty.

Protokół: Wybierz protokół, który ma być przefiltrowany. Masz do wyboru następujące możliwości: TCP, UDP i ICMP.
Reguła niedostosowana: Masz do wyboru dwie możliwości: Forward (Do przodu) i Next (Następny). Wybierz, co ma się zdarzyć z rozpatrywanymi danymi, jeśli reguła, która jest aktualnie poddawana edycji i jest niedostosowana. Next (Następny) oznacza, że dane są wówczas porównywane z następną regułą filtra IP. Forward (Do przodu) oznacza, że dane uzyskają dostęp do Twojego systemu. Prosimy zwrócić uwagę, że reguła (zasada) Forward (Do przodu) powinna być ostatnią regułą, gdyż po wprowadzeniu tej reguły (zasady) żadne inne dane nie będą porównywane z regułami.
Wskaźnik ustawienia filtra IP: Wybierz wskaźnik ustawień filtra IP jaki chcesz obejrzeć.

Na przykład:

Aby ustawić filtr IP, wykonaj poniższe czynności:

1. Edycja ustawienia filtra IP: Wybierz wskaźnik ustawienia filtra IP i opcje interfejsu i kierunku. Pamiętaj, że wskaźnik ustawienia filtra IP ma wpływ na działanie interfejsu i na kierunek. **PRZYKŁAD:** Jeśli pierwszy ustawiony wskaźnik filtra IP w PVCO ustawionym przez filtr jest ustawiony jako interfejs i wyjście jako kierunek, wówczas lista pierwszego filtra IP będzie miała ustawienia VPCO i wyjście.
2. Edycja reguły (zasady) filtra IP: Wybierz wskaźnik reguły (zasady) filtra IP (do 6 numerów dla każdego ustawionego wskaźnika) i wybierz opcję aktywną. Tak jak to podano w poniższym przykładzie, źródłowym adresem IP jest 192.168.1.4, maską podsieci jest 255.255.255.255, adresem docelowym (miejsca przeznaczenia) IP i maską podsieci jest 0.0.0.0, numerem portu jest 80 a ustawionym protokołem TCP. Od tej ustawienia odfiltrowuje on 192.168.1.14 tak, że nie może on uzyskać dostępu do sieci Web.

Uwaga: Każdy wskaźnik ustawienia filtra IP może mieć do 6 filtrów IP. W przypadku opcji „Rule Unmatched” (Reguła niedostosowana) musisz wybierać NEXT (Następny), dopóki ostatni filtr IP nie wybierze Forward (Do przodu).

3. Po zakończeniu ustawiania, należy kliknąć SAVE (Zapisz), aby móc kontynuować edycję następnego filtra IP.

IP Filter Listing							
#	Active	Src IP/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	192.168.1.14/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	80	TCP	Next

7.3 SNMP

Prosty protokół zarządzania siecią (SMNP) jest używany do wymiany informacji pomiędzy urządzeniami sieciowymi. Umożliwia on komputerowi centralnemu uzyskanie dostępu do konfiguracji, przepustowości i innych danych systemu, które znajdują się w bazie danych na modemie. Komputer centralny jest nazywany stacją centralną, a modem jest nazywany agentem SNMP. Dane do których można uzyskać dostęp poprzez SNMP są zapisane w bazie danych informacji o zarządzaniu (MIB) na modemie.

Access Management	Interface Setup	Advanced Setup		Access Management		Maintenance	Status
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	
SNMP							
Get Community : public							
Set Community : public							

Uzyskanie dostępu do sieci publicznej: Wybierz to ustawienie, aby uzyskać hasło dla prób o ustawienie Get i Get Next przychodzących ze stacji zarządzania.

Ustawienie dostępu do sieci publicznej: Wybierz to ustawienie, aby uzyskać hasło dla prób o ustawienie przychodzących ze stacji zarządzania

Hasłem domyślnym jest Public (Publiczny). Po wprowadzeniu zmian należy Kliknij SAVE (Zapisz), aby zapisać wprowadzone zmiany.

7.4 UPnP

UPnP (Uniwersalna funkcja Plug and Play) jest to norma rozłożonej otwartej pracy sieciowej, która wykorzystuje TCP/IP do nawiązywania prostej łączności w sieci typu peer-to-peer (każdy z każdym) pomiędzy urządzeniami. Urządzenie UPnP może dynamicznie przyłączyć się, otrzymać adres IP, przekazać jej możliwości i uzyskać informacje o innych urządzeniach, znajdujących się w sieci. Z kolei urządzenie może opuścić bez przeszkód sieć automatycznie, gdy nie jest ono już dłużej używane. Transmisje UPnP są dozwolone tylko w LAN.

Skąd wiem, że korzystam z UPnP?

Sprzęt UPnP jest pokazany w postaci ikony w folderze połączeń sieciowych (w Windows XP i Windows ME). Każde urządzenie kompatybilne z UPnP, które jest zainstalowane w Twojej sieci pojawi się w postaci oddzielnej ikony.

Access Management	Interface Setup	Advanced Setup		Access Management		Maintenance	Status
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	
Universal Plug & Play							
UPnP : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated							
Auto-configured : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)							
SAVE							

UPnP (Uniwersalna funkcja Plug & Play): Możesz wybrać opcje „Activated” (włączona) lub „Deactivated” (wyłączona) z tej sesji.

Automatyczna konfiguracja (przy zastosowaniu UPnP): Przyrządy sieciowe UPnP mogą automatycznie skonfigurować sporządzanie adresów sieciowych, informować o ich obecności w sieci innym urządzeniom UPnP i umożliwiać wymia-

nę prostego produktu i opisów usług. Wybierz opcję „Activated” (włączone), aby umożliwić zastosowaniom zależnym od UPnP automatyczną konfigurację routera ADSL tak, aby mogły one nawiązywać łączność poprzez router ADSL na przykład przy zastosowaniu traversalu. Aplikacje UPnP automatycznie rezerwują port przesyłania NAT w celu nawiązania łączności z innymi urządzeniami włączonymi przez UPnP. Eliminuje to potrzebę ręcznej konfiguracji portu przesyłającego dla aplikacji włączonych przez UPnP. Jeśli nie chcesz dokonać żadnych zmian w konfiguracji poprzez UPnP, wystarczy jeżeli wybierzesz opcję „Deactivated” (wyłączone).

SAVE (ZAPISZ): Kliknij SAVE (Zapisz), aby zapisać ustawienia w routerze ADSL.

7.5 DDNS

System dynamicznej nazwy domeny umożliwi Ci aktualizację bieżącego dynamicznego adresu z jedną lub kilkoma dynamicznymi usługami DNS tak, aby każdy mógł skontaktować się z Tobą (w NetMeeting, CU-SeeMe, itd.). Możesz również uzyskać dostęp do Twojego serwera FTP lub witryny www na swoim własnym komputerze przy użyciu adresu podobnego do DNS (na przykład, myhost.dhs.org, gdzie my host jest nazwą wybraną przez Was), która nigdy nie ulega zmianie zamiast używania adresu IP, który ulega zmianie w czasie każdego połączenia. Wasi przyjaciele lub krewni będą zawsze mogli zatelefonować do Was nawet, jeśli nie znają Twojego adresu IP. Przede wszystkim musicie mieć zarejestrowane dynamiczne konto DNS z adresem www.dynds.org. Możliwość ta jest przeznaczona dla ludzi z dynamicznym IP z serwera ISP lub DHCP, którzy chcieli by mieć nazwę DNS.

Dostawca dynamicznych usług DNS da Wam hasło lub klucz.

Access Management	Interface Setup	Advanced Setup		Access Management		Maintenance	Status
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	
Dynamic DNS							
Dynamic DNS: <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated							
Service Provider: <input type="text" value="www.dynds.org"/>							
My Host Name: <input type="text"/>							
E-mail Address: <input type="text"/>							
Username: <input type="text"/>							
Password: <input type="text"/>							
Wildcard support: <input type="radio"/> Yes <input checked="" type="radio"/> No							
<input type="button" value="SAVE"/>							

Dynamiczny DNS: Wybierz opcję z Activated (włączone) lub Deactivated (wyłączone) DDNS.

Dostawca usług (internetu): Domyślnym dostawcą dynamicznych usług DNS jest www.dyns.org.

Nazwa mojej stacji roboczej: Wpisz nazwę domeny przypisaną Twojemu routerowi ADSL przez Twojego dostawcę dynamicznego DNS.

Adres poczty elektronicznej: Wpisz Twój adres poczty elektronicznej.

Nazwa Użytkownika: Wpisz Twoją nazwę Użytkownika.

Hasło: Wpisz przydzielone Ci hasło.

Obsługa maski: Wybierz Yes (Tak) lub No (Nie), aby wyłączyć maski DYNDNS.

Wildcard DYNDNS: Włączenie obsługi maski sprawia, że *.yourhost.dynds.org stanowić będzie alias tego samego adresu IP, jak .yourhost.dynds.org. Funkcja ta jest użyteczna wówczas, jeżeli chcesz móc na przykład korzystać z www.yourhost.dynds.org i bez zmieniania uzyskiwać nazwę stacji bazowej (komputera centralnego).

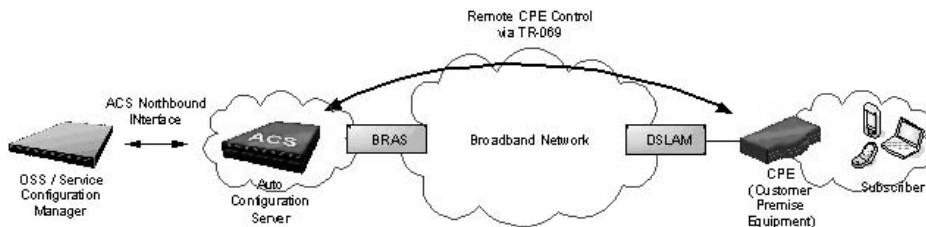
SAVE (Zapisz): Kliknij SAVE (Zapisz), gdy chcesz aby układ zapisał wprowadzone zmiany.

Prosimy pamiętać o tym, że trzeba wpisać dokładnie taką nazwę Użytkownika, jak Twoja przypisana ISP. Jeśli nazwa Użytkownika ma postać user@domain, gdzie domena identyfikuje nazwę usługi, należy wpisać ją dokładnie tak,

jak została ona podana. W przypadku wprowadzania zmian należy Kliknij SAVE (Zapisz), aby zapisać wprowadzone zmiany.

7.6 CWMP

TR-069 to protokół zarządzania CPE (CPE WAN Management Protocol (CWMP)). Jest to dwukierunkowy protokół oparty o SOAP/HTTP, zapewniający komunikację pomiędzy CPE oraz ACS (Auto Configuration Server). Zapewnia funkcje bezpiecznej automatycznej konfiguracji oraz kontroli innych urządzeń CPE w ramach sieci. Ze względu na szybki rozwój sieci szerokopasmowego dostępu do Internetu rozwinęła się również liczba rozwiązań dla tego typu sieci (np. modemy, routery, bramy itp.) Jednocześnie konfiguracja tego typu urządzeń staje się coraz bardziej skomplikowana – zbyt skomplikowana dla użytkownika końcowego. Z tego względu stworzony był standard TR-069. Zapewnia on możliwość automatycznej konfiguracji dla takich urządzeń. Specyfikacja techniczna tego protokołu zarządzana i publikowana jest przez DSL Forum. Przy użyciu TR-069, terminale mogą połączyć się z serwerem automatycznej konfiguracji i pobrać ustawienia automatycznie.



Access Management	Interface Setup		Advanced Setup		Access Management		Maintenance		Status
	ACL	Filter	SNMP	UPnP	DDNS	CWMP			
CWMP Setup									
CWMP : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated									
Login ACS									
URL : <input type="text"/>									
User Name : <input type="text"/>									
Password : <input type="password"/>									
Connection Request									
Path : <input type="text" value="/tr069"/>									
Port : <input type="text" value="80"/>									
UserName : <input type="text"/>									
Password : <input type="password"/>									
Periodic Inform									
Periodic Inform : <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated									
Interval : <input type="text" value="0"/>									
SAVE CANCEL									

8. Konserwacja

8.1 Administracja

Istnieje tylko jedno konto, do którego może mieć dostęp interfejs zarządzania siecią - Administration (Administracja). Admin ma uprzywilejowany dostęp do odczytu / zapisu. Na tej stronie sieci Web możesz ustawić nowe hasło dla admin.

Nowe hasło: W tym polu należy wpisać nowe hasło.

Potwierdzenie hasła: Wpisać nowe hasło w tym polu jeszcze raz.

Uwaga: Jeśli kiedykolwiek zapomnicie hasła i nie będziecie się mogli zalogować, możecie wcisnąć przycisk RESET (Resetowanie) i przytrzymać go przez 6 sekund, co spowoduje przywrócenie fabrycznych ustawień domyślnych. Fabrycznymi ustawieniami domyślnymi nazwy użytkownika i hasła są: admin i admin.

8.2 Strefa czasowa

Czas systemowy jest to czas używany przez urządzenie do celów obsługi harmonogramów dostępu. Możesz ręcznie ustawić czas, albo połączyć się z serwerem NTP (Protokół czasu sieci). W przypadku ustawienia serwera NTP, potrzebujesz tylko ustawić strefę czasową. Jeśli natomiast ręcznie ustawiasz czas, możesz także ustawić daty przejścia czasu z czasu letniego na czas zimowy i z czasu zimowego na czas letni a urządzenie będzie automatycznie w tym czasie przestawiał czas.

Aktualna data / czas: Przy powtórny wejściu do tego menu w polu tym wyświetlona zostaje uaktualniona data i czas.

[Synchronizacja czasu]

Synchronizuj czas z: Możesz wybrać następujące opcje „NTP serwer automatically” (Automatyczne ustawianie serwe-

ra NTP), „PC Clock” (Zegar komputera) lub „Manually” (Ustawienia ręczne) do koordynacji czasu.

Strefa czasowa: Wybierz strefę czasową Twojego miejsca pobytu. Otrzymasz różnicę czasu pomiędzy Swoją strefą czasową i Greenwich Mean Time (GMT).

Zmiana czasu letniego na zimowy i czasu zimowego na czas letni: Wybierz „Enabled”(Włączony) lub „Disabled” (Wyłączony), aby skorzystać z czasu letniego.

Adres serwera NTP: Wpisz adres IP lub nazwę domeny Twojego serwera czasowego. Sprawdź z Twoim administratorem ISP/sieci, jeśli nie jesteś pewny tej informacji.

Serwer protokołu czasu sieci: Serwer protokołu czasu sieci (NTP) może automatycznie ustawić czas routera dla Was. Jeśli używasz serwera NTP, wystarczy jeśli wybierzesz Waszą strefę czasową. Jeśli natomiast ręcznie ustawisz czas, możecie uaktywnić przejście z czasu letniego na czas zimowy i na odwrót. Router będzie automatycznie zmienił godzinę przy przejściu na czas zimowy i czas letni.

Przy wprowadzaniu zmian musisz kliknąć SAVE (Zapisz), aby zapisać wprowadzone zmiany lub CANCEL (Anuluj), aby wyjść bez zapisywania wprowadzonych zmian.

8.3 Oprogramowanie urządzenia

Na tej stronie możesz uaktualnić oprogramowanie urządzenia Twojego routera. Upewnij się, czy oprogramowanie sprzętowe, którego chcesz używać, znajduje się na lokalnym twardym dysku komputera. Kliknij Browse (Przeglądaj), gdy będziesz chciał przejrzeć lokalny twardy dysk i ustalić położenie oprogramowania sprzętowego, którego będziesz używać do uaktualnienia. Następnie wciśnijcie UPGRADE (Uaktualnienie), aby załadować nowe oprogramowanie sprzętowe. Czynność ta może zająć kilka minut, dlatego też nie wyłączajcie zasilania podczas uaktualniania. Po uaktualnieniu urządzenie ponownie zaskartuje!

Po pomyślnym załadowaniu system automatycznie zostaje uruchomiony. Prosimy poczekać, aż zakończy się rozruch urządzenia. Zajmie to około 2 minut lub więcej. Jeśli chcesz uzyskać dostęp do urządzenia, musisz ponownie zalogować się.

The screenshot shows the router's web interface for firmware upgrade. The navigation tabs are: Maintenance (selected), Interface Setup, Advanced Setup, Access Management, Maintenance, and Status. Under the Maintenance tab, the sub-tabs are: Administration, Time Zone, Firmware (selected), SysRestart, and Diagnostics. The main content area is titled 'Firmware/Romfile Upgrade'. It displays the current firmware version as 2.11.6.1(RE0.C2B)3.7.6.1. There are two input fields for 'New Firmware Location' and 'New Romfile Location', each with a 'Browse...' button. Below these is a 'Romfile Backup' button labeled 'ROMFILE SAVE'. A status message with an information icon states: 'It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.' At the bottom of the form is an 'UPGRADE' button.

Bieżąca wersja oprogramowania sprzętowego: W polu tym wyświetlona zostaje aktualna wersja oprogramowania sprzętowego.

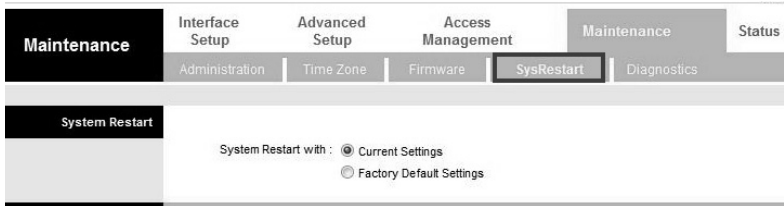
Nowe miejsce oprogramowania sprzętowego: Należy wpisać miejsce pliku, który chcesz załadować w tym polu lub Kliknij Browse... (Przeglądaj), aby znaleźć go.

UAKTUALNIENIE: Kliknij UPGRADE (Uaktualnienie), aby rozpocząć proces załadowania.

8.4 Ponowne uruchomienie systemu

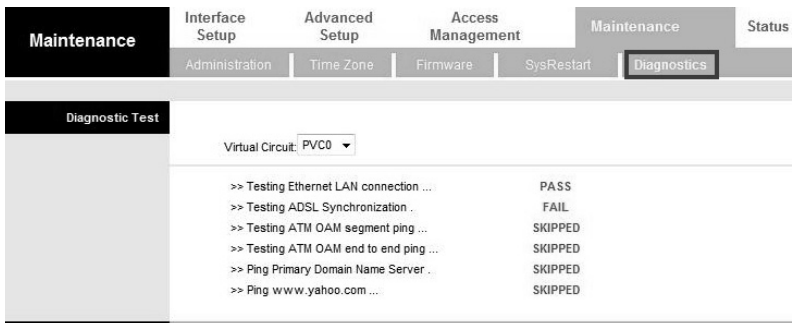
Ekran SysRestart (Ponownego uruchomienia systemu) umożliwi Ci ponowne uruchomienie Twojego routera albo z aktualnymi ustawieniami, które nie uległy zmianie lub z domyślnymi ustawieniami fabrycznymi.

Jeżeli chcesz ponownie uruchomić router używając domyślnych ustawień fabrycznych (na przykład po aktualizacji sprzętowego oprogramowania lub też jeśli zapisałeś nieprawidłową konfigurację), wybierz Factory Default Settings (Ustawienia domyślne fabryczne), aby zresetować urządzenie i otrzymać domyślne ustawienia fabryczne. W innym przypadku możecie wybrać Current Settings (Aktualne ustawienia). Możecie również zresetować Wasz router przywracając ustawienia fabryczne przez wciśnięcie i przytrzymanie przycisku DEFAULT (Domyślnie), znajdującego się na tylnym panelu Twojego routera przez 10 do 12 sekund przy włączonym urządzeniu.



8.5 Diagnostyka

Strona testu diagnostycznego pokazuje wyniki testu łączności faktycznej warstwy i warstwy protokołu stron LAN i WAN.



Wybierz PVC, którego chcielibyście użyć z listy rozwijanej. Router automatycznie włączy kontrolę diagnostyczną tego obwodu. Zielony napis PASS (Przejęcie) oznacza, że kontrola ta została przeprowadzona pomyślnie a czerwony napis FAIL (Niepowodzenie) oznacza, że kontrola dała wynik ujemny, natomiast zielony napis SKIPPED (Pominięto) oznacza, że kontrola ta została pominięta.

Uwaga: 1) Użytkownik może widzieć TYLKO kontrolne połączenie diagnostyczne PVC0. 2) „Testing ADSL Synchronization” (Synchronizacja kontroli ADSL) może potrzebować 30 sekund na przeprowadzenie kontroli diagnostycznej.

9. Status

9.1 Informacja o urządzeniu

Ekran Device Info (Informacja o urządzeniu) jest to narzędzie, którego użyć można do monitorowania routera ADSL. Pokazuje ono wersję oprogramowania sprzętowego WAN, LAN oraz informacje o adresie MAC. Prosimy zauważyć, że pola te są polami przeznaczonymi tylko do odczytu i nie służą one do celów diagnostycznych. Za wyjątkiem obwo-

du wirtualnego, należy kliknąć na listę opuszczaną i wybrać nazwę obwodu wirtualnego w którym ma być pokazany stan Twojego systemu.

Status	Interface Setup	Advanced Setup	Access Management	Maintenance	Status
	Device Info	System Log	Statistics		
Device Information	Firmware Version : 2.11.6.1(RE0.C2B)3.7.6.1 MAC Address : 00:06:4f:11:22:33				
LAN	IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled				
WAN	Virtual Circuit : PVC0 Status : Not Connected Connection Type : PPPoE IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 DNS Server : 0.0.0.0 NAT : Enabled				
ADSL	ADSL Firmware Version : FwVer:3.7.6.1_A_TC3085 HwVer:T14.F7_3.0 Line State : Down Modulation : Multi-Mode Annex Mode : ANNEX_A				
		Downstream	Upstream		
	SNR Margin :	N/A	N/A	db	
	Line Attenuation :	N/A	N/A	db	
	Data Rate :	0	0	kbps	

[Informacja o urządzeniu]

Wersja oprogramowania sprzętowego: W polu tym pokazano aktualną wersję oprogramowania firmowego.
Adres MAC: MAC (Kontrola dostępu do mediów) lub adres Ethernet jest jedyny dla Twojego modemu.

[LAN]

Adres IP: Adres IP portu LAN.

Maska podsieci: Maska podsieci IP portu LAN.

Serwer DHCP: Stan serwera DHCP (włączony lub wyłączony).

[WAN]

Obwód wirtualny: Kliknij na listę rozwijaną i wybierz nazwę obwodu wirtualnego, dla którego ma być pokazany stan systemów.

Stan: Połączony lub nie połączony.

Typ połączenia: Typ połączenia WAN.

Adres IP: Adres IP portu WAN.

Adres podsieci: Maska podsieci IP portu WAN.

Domyślna bramka: Adres IP domyślnej bramki, jeśli ma on zastosowanie.

Serwer DNS: Adres IP serwera DNS.

[ADSL]

Wersja oprogramowania sprzętowego ADSL: W polu wyświetlana jest aktualna wersja oprogramowania sprzętowego ADSL.

Stan linii: W polu tym wyświetlany jest proces i stan połączenia ADSL.

Modulacja: W polu tym wyświetlany jest stan modulacji ADSL dla G.dmt lub T1.413.

Tryb załącznika: W polu tym wyświetlane są tryby załącznika ADSL dla załącznika A lub załącznika B.

W kierunku przepływu i w kierunku przeciwnym do przepływu: Stan marginesu SNR, tłumienie łącza i szybkość transmisji.

Margines SNR: Ilość zwiększonych zakłóceń, który może być tolerowany przy utrzymywaniu znamionowego BER (Bitowy błąd transmisji). Margines SNR ustawia się za pomocą DSLAM centralnego biura. Przy zwiększeniu marginesu SNR poprawia się stosunek bitowego błędu w transmisji, lecz zmniejsza się szybkość transmisji. I na odwrót, jeśli zmniejszy się margines SNR, zmniejsza się również ilość błędów transmisji lecz szybkość transmisji zwiększa się.

Tłumienie łącza: Tłumienie jest to osłabienie wielkości sygnału łącza ADSL pomiędzy nadajnikiem (DSLAM centralnego biura) i odbiornikiem (modem ADSL klienta) zmierzony w decybelach (dB). Mierzy się go, obliczając różnicę decybeli pomiędzy poziomem mocy otrzymanego sygnału na routerze ADSL Klienta i odnośnym poziomem sygnału mocy, nadawanym z centralnego biura DSLAM.

Szybkość transmisji: W polu tym wyświetlana jest szybkość transmisji ADSL.

9.2 System Log

System Log wyświetla dane wytworzone lub nabyte przez rutynowy system łączności z innymi urządzeniami takie, jak wyniki negocjacji z komputerami ISP dla adresów DNS i bramki IP. Urządzenie prowadzi bieżący rejestr wydarzeń i czynności mających miejsce w Twoim routerze. Możesz kliknąć Save Log (Zapisz rejestr), aby wyświetlić okno dialogowe pobierania pliku z Windows, co umożliwi otwieranie lub zapisywanie do zawartości rejestru w Twoim komputerze osobistym. Aby wykasować wszystkie wpisy z listy, należy kliknąć Clear Log (Skasuj rejestr). Zaczynają się wówczas gromadzić nowe wpisy. W przypadku zainicjowania Twojego urządzenia, pliki zostają automatycznie wykasowane.

The screenshot shows the 'System Log' page of a wireless router. The navigation menu at the top includes 'Status', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', and 'Status'. The 'Advanced Setup' section is active, and 'System Log' is selected. The log content is as follows:

```

1/1/2000 0:9:29> Last errorlog repeat 2 Times
1/1/2000 0:9:29> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:9:31> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:9:35> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:9:53> Last errorlog repeat 6 Times
1/1/2000 0:9:54> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:10:9> Last errorlog repeat 3 Times
1/1/2000 0:11:57> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:12:5> Last errorlog repeat 8 Times
1/1/2000 0:12:8> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:12:11> netMakeChannDial: err=-3001
rn_p=804beed0
1/1/2000 0:12:34> Last errorlog repeat 4 Times
1/1/2000 0:17:7> netMakeChannDial: err=-3001
rn_p=804beed0
  
```

At the bottom of the log area, there are two buttons: 'CLEAR LOG' and 'SAVE LOG'.

9.3 Statystyka

Router ADSL prowadzi statystykę ruchu przechodzącego przez niego. Jesteście w stanie zobaczyć ilość pakietów przechodzących przez router zarówno przez port WAN, jak i przez port LAN. Licznik ruchu zostaje zresetowany (wykasowany) przy ponownym zainicjowaniu urządzenia. Aby zobaczyć sprawozdanie statystyczne LAN/WAN należy wybrać Ethernet/ADSL.

The screenshot shows the 'Traffic Statistics' page for the ADSL interface. The 'Statistics' tab is selected under the 'Access Management' menu. The interface is set to ADSL. The statistics table is as follows:

Transmit Statistics		Receive Statistics	
Transmit Frames	636	Receive Frames	949
Transmit Multicast Frames	16	Receive Multicast Frames	437
Transmit total Bytes	443401	Receive total Bytes	137259
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

A 'REFRESH' button is located at the bottom of the page.

[Ethernet]

Ekran Ethernet daje informacje o tym, jaką ilość danych przesłał i otrzymał Twój router poprzez połączenie Ethernet. Gdy chce się uaktualnić ekran, należy kliknąć REFRESH (Odświeżanie).

The screenshot shows the 'Traffic Statistics' page for the Ethernet interface. The 'Statistics' tab is selected under the 'Access Management' menu. The interface is set to Ethernet. The statistics table is as follows:

Transmit Statistics		Receive Statistics	
Transmit Frames	344	Receive Frames	237
Transmit Multicast Frames	16	Receive Multicast Frames	0
Transmit total Bytes	107747	Receive total Bytes	50877
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

A 'REFRESH' button is located at the bottom of the page.

[ADSL]

Ekran ADSL daje informacje o tym, jak wiele danych Twój router nadał lub przyjął poprzez połączenie ADSL. Gdy chce się uaktualnić ekran, należy kliknąć REFRESH (Odświeżanie).

The screenshot shows the 'Traffic Statistics' page for the ADSL interface. The 'Statistics' tab is selected under the 'Access Management' menu. The interface is set to ADSL. The statistics table is as follows:

Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

A 'REFRESH' button is located at the bottom of the page.

10. Rozwiązywanie problemów

Jeśli router nie funkcjonuje prawidłowo, należy najpierw przeprowadzić podane tutaj kontrole, pozwalające na proste wykrywanie usterek przed zwróceniem się do Twojego dostawcy usług internetowych (ISP) o pomoc.

10.1 Użycie diod świecących do problemów diagnostyki

Diody świecące pomagają znaleźć ewentualne przyczyny zaistniałych problemów.

10.1.1 Diody świecące zasilania

Dioda świecąca zasilania PWR LED znajdująca się na przedniej paneli nie zapala się.

KROKI	DZIAŁANIE NAPRAWCZE
1	Upewnij się, czy zasilacz jest przyłączony do routera i wetknięty do odpowiedniego źródła zasilania. Należy używać jedynie dostarczonych fabrycznych zasilaczy.
2	Sprawdź, czy router i źródło zasilania są włączone i czy router jest odpowiednio zasilany energią.
3	Włącz i wyłącz router.
4	Jeżeli błąd utrzymuje się, przyczyną nieprawidłowego działania może być usterka oprogramowania sprzętowego. Musisz się wówczas porozumieć z Twoim lokalnym dystrybutorem.

10.1.2 Dioda świecąca LAN

Dioda świecąca LAN, znajdująca się na przednim panelu, nie zapala się.

KROKI	DZIAŁANIE NAPRAWCZE
1	Sprawdź połączenia kabla Ethernet pomiędzy Twoim routerem i komputerem lub koncentratorom.
2	Sprawdź, czy kable Ethernet nie są uszkodzone.
3	Upewnij się, czy karta Ethernet Twojego komputera działa prawidłowo.
4	Jeśli powyższe czynności nie doprowadzą do rozwiązania problemu, musisz zwrócić się o pomoc do lokalnego dystrybutora.

10.1.3 Dioda świecąca ADSL

Dioda świecąca ADSL znajdująca się na panelu przednim nie zapala się.

KROKI	DZIAŁANIE NAPRAWCZE
1	Sprawdź przewód telefoniczny i połączenia pomiędzy portem routera ADSL i gniazdkiem ściennym.
2	Upewnij się, czy dostawca usługi telekomunikacyjnej sprawdził Wasz przewód telefoniczny i dostosował go do pracy ADSL.
3	Zresetuj linię ADSL, aby ponownie zainicjalizować łącze do DSLAM.
4	Jeśli powyższe czynności nie doprowadzą do rozwiązania problemu, zwróć się o pomoc do Twojego lokalnego dystrybutora.

10.2 Problemy z interfejsem sieciowym

Brak dostępu do interfejsu sieciowego.

KROKI	DZIAŁANIE NAPRAWCZE
1	Upewnij się, czy używasz prawidłowego adresu IP routera. Sprawdź adres IP routera.
2	Upewnij się, czy nie ma aktualnie sesji konsoli.
3	Sprawdź, czy włączyłeś dostęp do usług sieciowych. Jeśli skonfigurowałeś zabezpieczony adres Klienta IP, adres IP Twojego komputera musi pasować do niego. Patrz rozdział na temat zdalnego zarządzania, w którym zamieszczono szczegółowy opis.
4	W przypadku dostępu WAN musicie skonfigurować zdalne zarządzanie, aby umożliwić dostęp serwera z WAN (lub wszystkich).
5	Adresy Twojego komputera i adresy IP Twojego routera muszą znajdować się w tej samej podsieci dla dostępu LAN.
6	Jeśli zmieniłeś adres IP LAN routera, musisz wpisać nowy adres jako URL.
7	Usuń wszystkie filtry w LAN lub w WAN, które blokują dostęp do sieci.

Interfejs sieciowy nie pokazuje prawidłowego obrazu.

KROKI	DZIAŁANIE NAPRAWCZE
1	Upewnij się, czy używasz Internet Explorer 5.0 lub późniejszych wersji.
2	Wykasuj pliki tymczasowe sieciowe i zaloguj się ponownie. W Internet Explorer kliknij <i>Tools, Internet Options</i> (Narzędzia, Opcje Internetu) a następnie kliknij przycisk (Wykasuj pliki) .Gdy pojawi się okno <i>Delete Files</i> (Wykasuj pliki) kliknijcie <i>Delete all offline content</i> (Wykasuj całą zawartość nie połączonych elementów), a następnie kliknijcie OK (czynności te mogą być różne w zależności od wersji Twojej przeglądarki internetowej).

10.3 Problemy z nazwą Użytkownika Login i hasłem

Zapomniałem mojej nazwy Użytkownika i/lub hasła podawanych przy logowaniu się.

KROKI	DZIAŁANIE NAPRAWCZE
1	Jeśli zmieniłeś hasło i zapomniałeś go, potrzebujesz załadować domyślny plik konfiguracji. Spowoduje to skasowanie wszystkich poprzednich konfiguracji i odtworzenie domyślnych fabrycznych wartości w tym także hasła.
2	Wciśnij przycisk DEFAULT (Domyślny) i przytrzymaj go przez 5 sekund, a następnie puść. Gdy dioda świecąca ADSL zacznie migać, oznacza to, że przywrócone zostały domyślne wartości i że router ponownie został uruchomiony.
3	Domyślną nazwą Użytkownika jest „admin”. Domyślnym hasłem jest „admin”. Pola Password (Hasło) i Username (Nazwa użytkownika) są czule na przypadki. Upewnij się, że wpisałeś prawidłowe hasło i nazwę Użytkownika, używając odpowiednio dużych liter lub małych liter.
4	Zaleca się usilnie zmianę domyślnej nazwy Użytkownika i domyślnego hasła. Upewnij się, czy przechowujesz nazwę Użytkownika i hasło w bezpiecznym miejscu.

10.4 Problemy z interfejsem LAN

Nie mogę uzyskać dostępu do routera z LAN ani też „pingować” żadnego komputera w LAN

KROKI	DZIAŁANIE NAPRAWCZE
1	Sprawdź diody świecące Ethernet, znajdujące się na przedniej paneli. Dioda świecąca LAN powinna być włączona dla portu, który został przyłączony do komputera osobistego. Jeśli jednak jest ona wyłączona, należy sprawdzić przewody pomiędzy Twoim routerem i komputerem osobistym. Upewnij się, czy odinstalowałeś wszystkie programowe zabezpieczenia firewall, przystępując do wykrywania usterek.
2	Upewnij się, czy adres IP i maska podsieci są zgodne pomiędzy routerem i stacją roboczą.

10.5 Problemy z interfejsem WAN

Inicjalizacja połączenia ADSL nie działa.

KROKI	DZIAŁANIE NAPRAWCZE
1	Sprawdź połączenia kabla pomiędzy portem ADSL i gniazdkiem ściennym. Dioda świecąca ADSL znajdująca się na przednim panelu routera powinna być włączona.
2	Sprawdź, czy VPI, VCI, typ odwzorowania i typ multipleksowania są takie same jak pobrane od Twojego operatora telefonicznego i ISP.
3	Włącz ponownie router. Jeśli będziesz miał nadal problemy, musisz sprawdzić VPI, VCI, typ odwzorowania i multipleksowania. Musisz to zweryfikować z operatorem telefonicznym i ISP.

Nie mogę otrzymać adresu WAN IP od ISP.

KROKI	DZIAŁANIE NAPRAWCZE
1	Dopilnuj, aby wszystkie urządzenia przyłączone do tego samego przewodu telefonicznego jak Twój router (na przykład telefony, faksy, modemy, telefony komórkowe) miały filtr włączony pomiędzy nimi, a gniazdkiem ściennym (chyba, że używasz centralny splitter lub centralny filtr, zainstalowany przez wykwalifikowanego elektryka, posiadającego odpowiednią licencję) i upewnij się, czy wszystkie filtry są prawidłowo zainstalowane i znajdują się w odpowiednich miejscach.
2	Brak filtrów przewodowych lub zainstalowanie filtrów przewodowych w złym miejscu może spowodować problemy z Twoimi połączeniami ADSL, w tym także częste rozłączenie.

Częsta utrata synchronizacji linii ADSL (rozłączenia).

KROKI	DZIAŁANIE NAPRAWCZE
1	ISP dostarcza adres WAN IP po uwierzytelnieniu. Uwierzytelnienie może nastąpić poprzez podanie nazwy użytkownika i hasła, adresu MAC lub nazwy komputera.
2	Nazwa Użytkownika i hasło mają zastosowanie tylko do PPPoE i PPPoA. Upewnij się, czy wpisałeś prawidłowy typ serwisu, nazwę Użytkownika i hasło.

10.6 Problemy z dostępem do Internetu

Nie mogę uzyskać dostępu do Internetu.

KROKI	DZIAŁANIE NAPRAWCZE
1	Upewnij się, czy router jest włączony i przyłączony do sieci.
2	Jeśli dioda świecąca ADSL jest wyłączona, należy postąpić tak, jak to opisano w rozdziale 11.1.3 (strona 71).
3	Sprawdź ustawienia Twojego WAN
4	Upewnij się, czy wpisałeś prawidłową nazwę Użytkownika i hasło.
5	W przypadku stacji bezprzewodowych sprawdź, czy zarówno router, jak i stacja (stacje) bezprzewodowa używają takiego samego ESSID, kanału i kluczy (klawiszy) WEP (jeśli włączone zostało zaszyfrowane WEP).

Połączenia z internetem są rozłączane.

KROKI	DZIAŁANIE NAPRAWCZE
1	Sprawdź zasady harmonogramu
2	Jeśli używasz PPPoA lub PPPoE, musisz sprawdzić ustawienie czasu aktywności.
3	Skontaktuj się ze swoim ISP.

Jeśli będziesz miał jakiegokolwiek problemy z konfigurowaniem lub ustawieniem Twojego routera Ethernet ADSL, nie bój się skontaktować z nami.

Przed skontaktowaniem się z nami upewnijcie się, czy zebrałeś wszystkie niżej podane informacje. Podanie kompletnych szczegółowych informacji dotyczących Twojego problemu pomoże nam w znalezieniu właściwej odpowiedzi.

Nazwa modelu:

Numer fabryczny:

Ustawienia PC:

Inne:

ENVIRONMENT PROTECTION:



This symbol on our product nameplates proves its compatibility with the EU Directive 2002/96 concerning proper disposal of waste electric and electronic equipment (WEEE). By using the appropriate disposal systems you prevent the potential negative consequences of wrong product take-back that can pose risks to the environment and human health. The symbol indicates that this product must not be disposed of with your other waste. You must hand it over to a designated collection point for the recycling of electrical and electronic equipment waste. The disposal of the product should obey all the specific Community waste management legislations. Contact your local city office, your waste disposal service or the place of purchase for more information on the collection.

Weight of the device: 945,6g

This is declared by MODECOM S.A., that the product MC-420 meets indispensable requirements and other applicable provisions of Directive 1999/5/WE. For declaration of conformity see Internet MODECOM web site under www.modecom.pl, „Certificates”. The product is designed for use within EU territory.

DECLARATION

This instruction manual was designed to provide the users with practical hints and basic information on the usage of the router MC-420. Hence, MODE COM S.A. exempts from legal duty of possible printing errors and misunderstanding of the instruction that may occur in this manual. MODE COM S.A. does not guarantee the completeness and relevance of the instruction. Therefore, we will not be held responsible for any accidental damage caused by the faulty usage.

OCHRONA ŚRODOWISKA:



Niniejsze urządzenie oznakowane jest zgodnie z dyrektywą Unii Europejskiej 2002/96/UE dotyczącą utylizacji urządzeń elektrycznych i elektronicznych (WEEE). Zapewniając prawidłowe usuwanie tego produktu, zapobiegasz potencjalnym negatywnym konsekwencjom dla środowiska naturalnego i zdrowia ludzkiego, które mogą zostać zagrożone z powodu niewłaściwego sposobu usuwania tego produktu. Symbol umieszczony na produkcie wskazuje, że nie można traktować go na równi z innymi odpadami z gospodarstwa domowego. Należy oddać go do punktu zbiórki zajmującego się recyklingiem urządzeń elektrycznych i elektronicznych. Usuwanie urządzenia musi odbywać się zgodnie z lokalnie obowiązującymi przepisami ochrony środowiska dotyczącymi usuwania odpadów. Szczegółowe informacje dotyczące usuwania, odzysku i recyklingu niniejszego produktu można uzyskać w urzędzie miejskim, zakładzie oczyszczania lub sklepie, w którym nabyłeś niniejszy produkt.

Masa sprzętu: 945,6g

Niniejszym MODECOM S.A. oświadcza, że produkt MC-420 jest zgodny z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami dyrektywy 1999/5/WE. Deklaracja zgodności dostępna jest na stronie internetowej MODECOM, pod adresem www.modecom.pl w dziale „certyfikaty”. Produkt przeznaczony do wykorzystania na terenie UE.

DEKLARACJA

Poniższa instrukcja zawiera podstawowe dane i praktyczne wskazówki dotyczące użytkowania MC-420. MODECOM S.A. nie bierze jednak odpowiedzialności za błędy w druku oraz wszelkie błędy wynikające z niezrozumienia informacji zawartych w tej instrukcji. MODECOM S.A. nie gwarantuje dokładności i ważności informacji zawartych w niniejszej instrukcji. Dlatego też nie odpowiadamy za uszkodzenia wywołane niewłaściwym użytkowaniem.

Notes:

MODECOM S.A. 00-124 Warsaw, Poland, Rondo ONZ 1.