Nokia MW1122

ADSL/WLAN Router

T66520

USER MANUAL

NOKIA

MW1122

ADSL/WLAN Router

User Manual

05.07.2000
C33902.21 A0

1 Introduction to Nokia MW1122

Nokia MW1122 is an integrated ADSL (Asymmetric Digital Subscriber Line) bridge and router which enables high-speed Internet access from your wireless (WLAN) and Ethernet local area networks (LAN). It multiplies the capacity of the already installed telephone lines used traditionally for telephone and dial-up modem services. MW1122 brings high-speed connections available for home users, small offices and telecommuters.

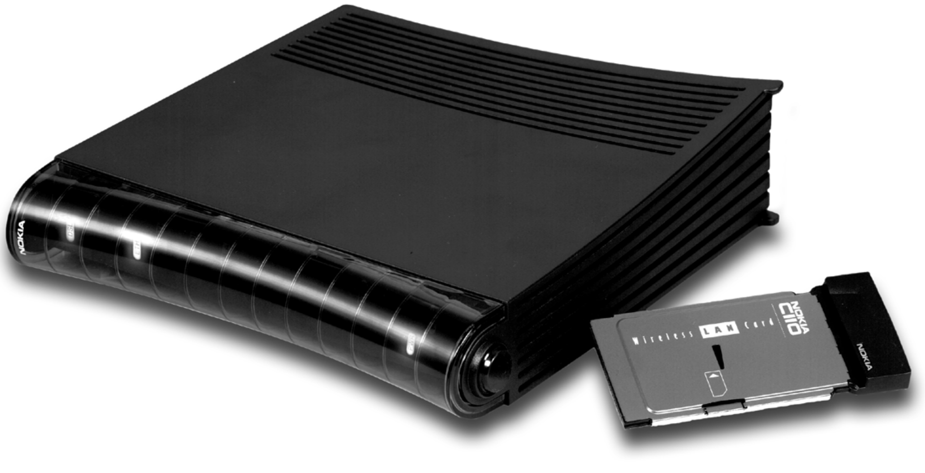


Figure 1 Nokia MW1122

2 Installing MW1122

Before you install MW1122 you may want to familiarise yourself with the interfaces and indicator lights of MW1122. From section 2.3 you will find a step-by-step installation procedure, which shows the physical installation of MW1122.

2.1 Interfaces

MW1122 has one ADSL line interface and two LAN interfaces: WLAN and ETH (wireless LAN and 10Base-T Ethernet). It also has a local management interface (CLI) for management purposes. The ADSL line interface is compatible with ITU-T G.992.1 specification. The wireless LAN port interface supports Nokia’s 11 Mbit/s IEEE 802.11b WLAN PC Card.

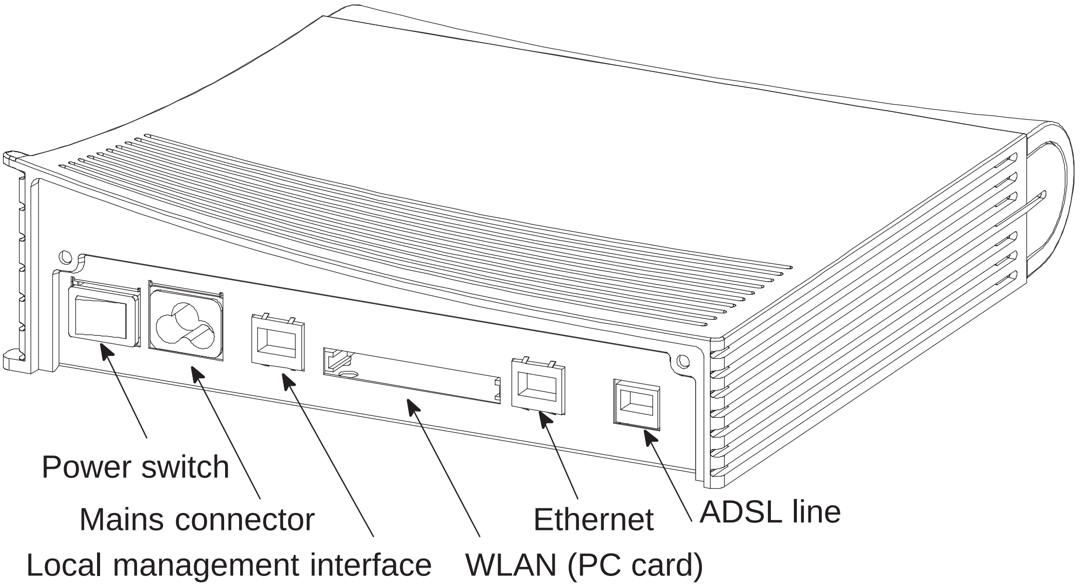


Figure 2 MW1122 back panel

2.2 Indicator lights

MW1122 has six indicator lights on the front panel: PWR, STA, WLAN, COL, ETH, and DSL. STA indicator is red. Other indicators are green.

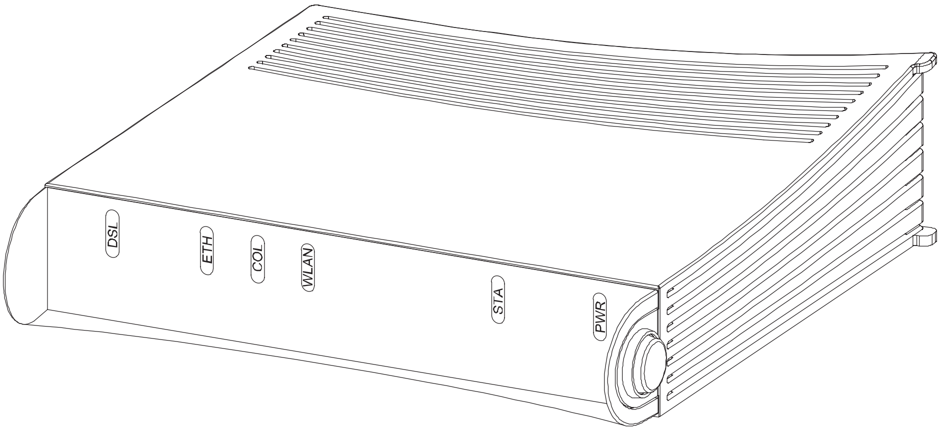


Figure 3 MW1122 front panel indicators

DSL	GREEN
Off	ADSL link is down.
Blinks	ADSL connection is being established.
On	ADSL link is up.

ETH	GREEN
Off	Ethernet is down.
On	10Base-T Ethernet is functional
Blinks	Receives traffic from Ethernet.

COL	GREEN
Blinks	Collisions on the Ethernet. Note, that it is normal that some collisions occur on the Ethernet.

WLAN	GREEN
Off	No stations on the WLAN or WLAN PC Card not inserted.
On	Stations on the WLAN but no traffic.
Blinks	Receives traffic through the WLAN interface.

STA	RED
Off	OK
On	Hardware malfunction during startup.

PWR	GREEN
Off	Power off.
On	Power on.

2.3 Step-by-step installation procedure

1. Plug the mains power cord to a mains outlet.
2. Plug the antenna into the antenna connector of the wireless LAN card, if included.
3. Insert the wireless LAN card, if included, gently into the MW1122 WLAN slot on the MW1122 back panel. Ensure that the card is aligned correctly.
4. Switch on MW1122. The PWR indicator lights up.
5. Ensure that wireless LAN clients (that is, the wireless devices you want to use in your network) have the same configuration as the wireless LAN card in the MW1122 modem and that they are in the Infrastructure mode. The default wireless LAN configuration of MW1122 is the following:

regulatory-domain	according to your location of use (Europe, Canada, USA, or Japan)
network name	MW-wxyz (case-sensitive), where wxyz are the last four numbers from your MW1122 serial number

   When you have set the network name to your wireless client, the wireless connection is established and the WLAN indicator on MW1122 fron panel will be lit.
6. Connect the 8-pin Ethernet cable between your PC and the Ethernet connector on the MW1122 back panel if you want use a PC equipped with a 10Base-T Ethernet card. Switch on your PC. The ETH indicator will be lit.

7. Connect the 6-pin ADSL line cable between the ADSL connector on the MW1122 back panel and your ADSL line wall socket. If you want to use telephone and data services simultaneously connect a splitter according to Figure 4. After a while, the DSL indicator starts blinking indicating that the ADSL connection is being established. After the connection has been established successfully the DSL indicator remains lit.

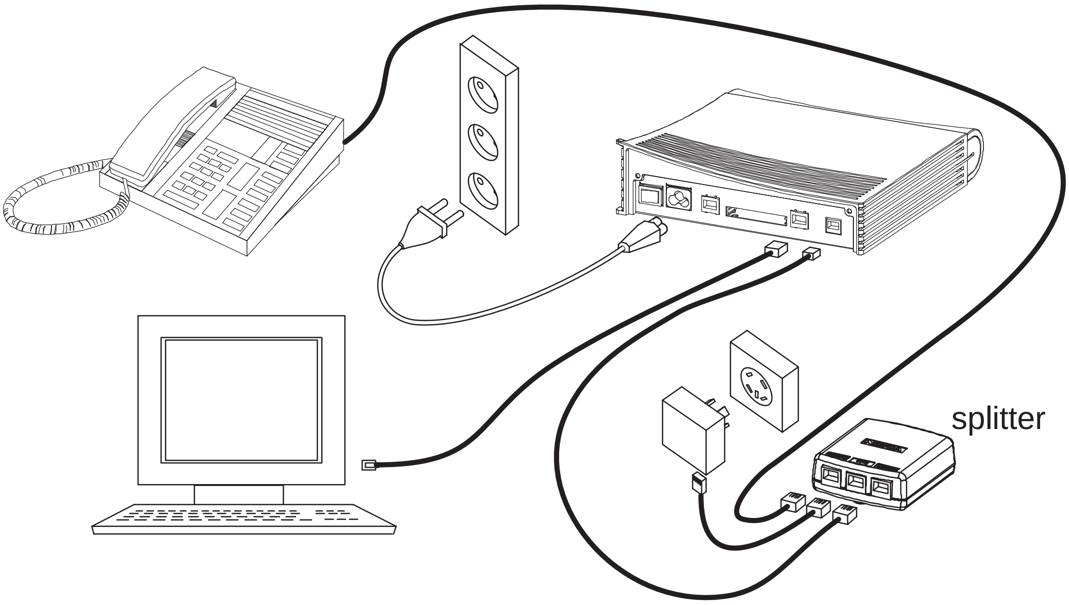


Figure 4 MW1122 and splitter connected

Now, your MW1122 has been connected and you can check the connections according to your service provider's instructions.

3 Configuring MW1122

Your service provider has configured your MW1122 for the service. However, you may want to change the settings regarding your wireless network. You will find these settings on the Wireless LAN and WLAN Clients web pages. **Do not change other settings unless specifically asked by your service provider.** You can change MW1122 settings with an ordinary web browser such as Microsoft Internet Explorer or Netscape Navigator.

If the WLAN indicator is lit on the MW1122 front panel, you can use your WLAN client for configuration. Of course, you can also use a PC connected to the ETH port of MW1122. In this case the ETH indicator should be lit.

3.1 Browser management

You can use your PC’s web browser software to access the web configuration pages in MW1122. To access the web pages you must know the IP address of your MW1122 or, alternatively, the “name” that your MW1122 recognises.

Note
Before using your web browser for configuration, you must know the IP address or the name assigned to your MW1122.

There are three ways to find out whether to use a name or an IP address:

- Your service provider has given you an IP address for MW1122.
- Your MW1122 uses Dynamic Host Configuration Protocol (DHCP) and Domain Name Server. In this case the name is *MW1122*.
- Your MW1122 uses DHCP. In this case run winipcfg.exe (Windows 95) or ipconfig.exe (Windows NT). The IP address of MW1122 is the Default Gateway address shown by the ipconfig program.

3.1.1 Opening a connection

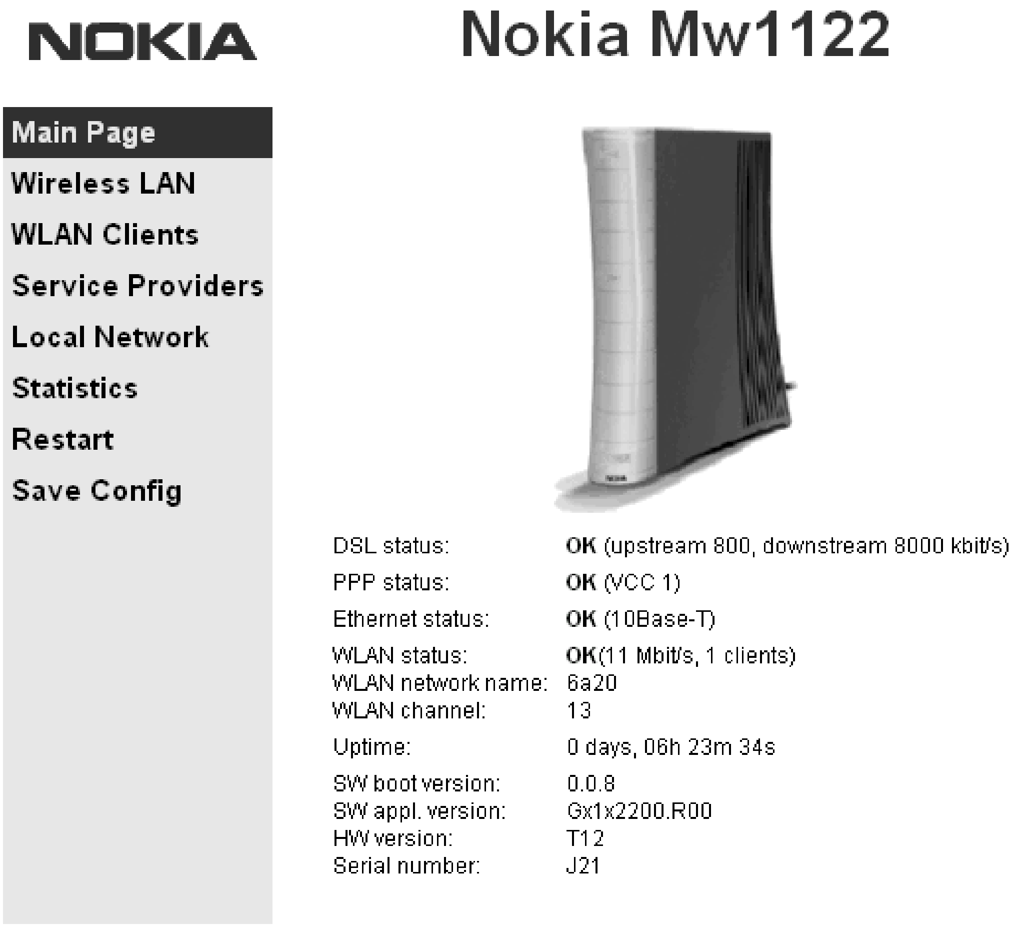
To open a connection to the Nokia MW1122:

1. Start your web browser.
2. Enter the name (’MW1122’) or IP address of your Nokia MW1122 in the browser’s Location or Address field and press Enter.
3. Type in the username/password as requested. If no username/password is required, just click OK to proceed. The Nokia MW1122 Main Page appears.

3.1.2 Main Page

Main Page is shown first when you use a web browser to connect to MW1122.The list on the left shows the current page highlighted. Clicking an item on the list (Wireless LAN, WLAN Clients, Service Providers, Local Network, Statistics, Restart, and Save Config) takes you to the corresponding page. Typically, you will only have to change the Wireless LAN and WLAN Clients settings.

Note
When you make modifications to the configuration, remember to save the configuration and restart your MW1122 for your changes to take effect.



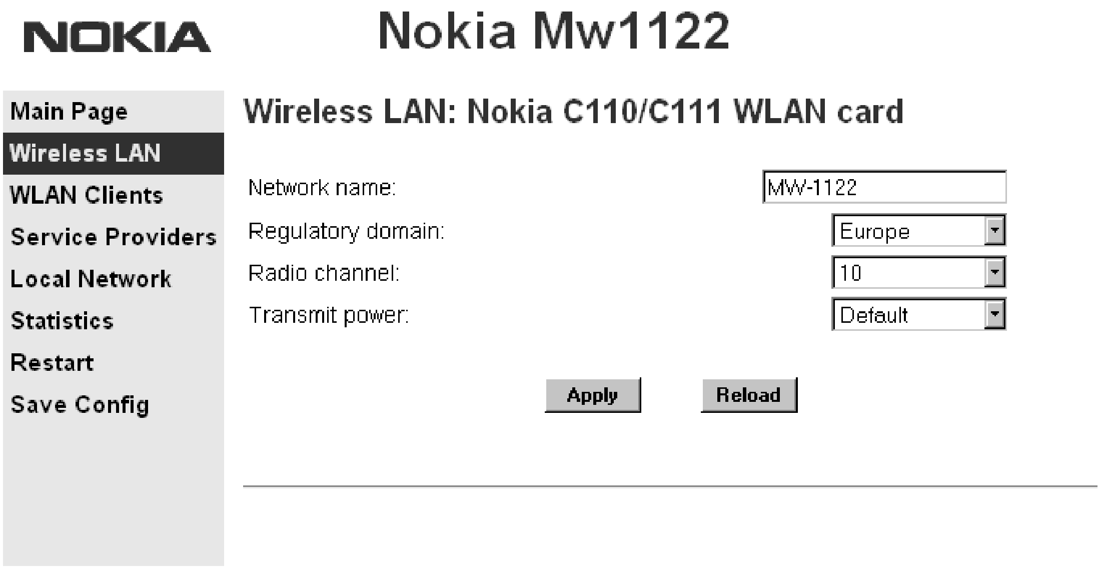
DSL status:	**OK** (upstream 800, downstream 8000 kbit/s)
PPP status:	**OK** (VCC 1)
Ethernet status:	**OK** (10Base-T)
WLAN status:	**OK**(11 Mbit/s, 1 clients)
WLAN network name:	6a20
WLAN channel:	13
Uptime:	0 days, 06h 23m 34s
SW boot version:	0.0.8
SW appl. version:	Gx1x2200.R00
HW version:	T12
Serial number:	J21

Figure 5 Main Page

The Main Page shows you the statuses of the DSL line, Ethernet interface, and wireless LAN interface. It also shows the number of wireless LAN clients on your network, wireless LAN network name and the channel in use. Software and hardware versions and the serial number of MW1122 are shown in the bottom of the page.

3.1.3 Wireless LAN page

You can change wireless LAN network settings on the Wireless LAN page.



Wireless LAN: Nokia C110/C111 WLAN card

Network name: MW-1122
Regulatory domain: Europe
Radio channel: 10
Transmit power: Default

Figure 6 Wireless LAN page

Note
When you click the Apply button, the WLAN subsystem will be reseted automatically. If you have changed the network name and you are accessing MW1122 through the wireless connection, the wireless link will be disconnected. You must reconfigure the network name to your wireless LAN client to continue configuration. The Reload button restores the settings if you have not saved the configuration yet.

Network name identifies your network and must be the same in all wireless LAN clients on your network. The default network name is MW-wxyz (case-sensitive), where wxyz are the last four numbers from your MW1122 serial number.

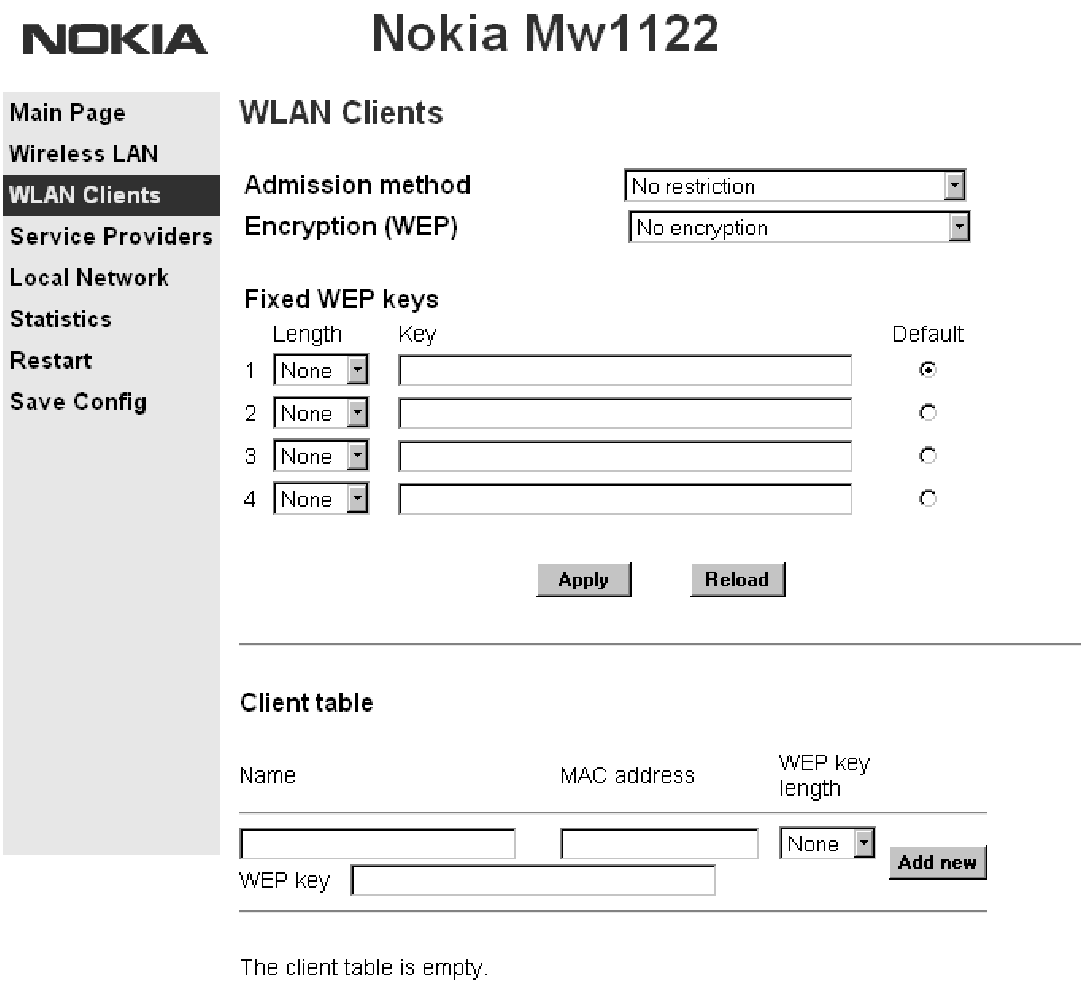
Set *Regulatory domain* according to your location of use. The *Regulatory domain* setting affects the available *Radio channels*. The radio channels corresponding to the regulatory domains are:

Europe	1...13
Canada	1...11
USA	1...11
Japan	14

Change *Transmit power* if your wireless network becomes weak on the edges.

3.1.4 WLAN Clients page

On the *WLAN Clients* page you can enable access control based on the MAC addresses of your wireless LAN clients. When access control is enabled, only the wireless stations on the Client table are allowed access to your wireless network. On this page, you can also activate Wired Equivalent Privacy (WEP) and set the encryption key parameters. Note, that unless you have encryption enabled other WLAN clients nearby have the possibility of monitoring the traffic on your wireless network



WLAN Clients

Admission method: No restriction

Encryption (WEP): No encryption

Fixed WEP keys

	Length	Key	Default
1	None		●
2	None		○
3	None		○
4	None		○

Client table

Name	MAC address	WEP key length
		None

WEP key

The client table is empty.

Figure 7 WLAN Clients page

Enabling access control

You can add a wireless station to the *Client table* by typing its MAC address to the *MAC address field* and clicking the *Add new* button. Use lower case characters only when typing the MAC address. You must identify the wireless station by filling the *Name* field. Activate the Client table by selecting *Client table MAC address* from the *Admission method* pull-down list and clicking the *Apply* button. Click *Remove* button if you want to remove a client from the Client table.

Encrypting wireless connection

If you want to activate WEP, you have two options:

- Use a fixed default key for all stations. There are four default keys available and the key is selected by clicking the corresponding radio button. Typically, there is no need to use any other key than number 1.
- Use a separate station-specific key. Enter this key in the Client table *Wep key* field.

Before you type the encryption key, select the key length from the pull-down list. Available lengths are 40 bits and 128 bits. If you select a 40-bit key, you must enter a key with 10 characters. If you select a 128-bit key, you must enter a key with 32 characters. The key is a hexadecimal string, so the available characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, a, b, c, d, e, and f.

Note

Remember to configure the same key to your wireless client. If you use your wireless client for web configuration, you can copy the key from the *Key* field and paste it to the wireless LAN client software. Then you can click the *Apply* to activate encryption. Note, that if you enable encryption on either client or MW1122 only, the wireless link will be disconnected until you have enabled encryption on both devices.

There are five security modes which can be chosen from *Encryption mode* pull-down list:

- No encryption; In this mode, encryption is always disabled. If a station tries shared-key authentication, a failed authentication will result.
- Allowed; In this mode, a station may use either open-key or shared-key authentication. If a station uses open-key authentication, encryption is disabled. If a station uses shared-key authentication, encryption is used.

- Required; In this mode, it is mandatory to use shared-key authentication. If open-key authentication is used, a failed authentication will result. When a station uses shared-key authentication, encryption is always used. Default keys are used if no station-specific key exists. Broadcast and multicast data will be encrypted using the default key.
- Required, Wifi; In this mode, a station may use either open-key or shared-key authentication and in both cases encryption is always used. Default keys are used if no station-specific keys exist. Broadcast and multicast data will be encrypted using the the default key.
- Required, specific keys; In this mode, a station must use shared-key authentication and station-specific key. If the station uses open-key authentication or station-specific key is not available, a failed authentication will result. Successful shared-key authentication results encryption using the station-specific keys. Broadcast and multicast data will be encrypted using the default key.

In most cases, it is acceptable to use default keys. Most modes also allow concurrent use of station-specific and/or user-specific keys at the same time. Wifi mode provides lower authentication support but it supports all certified WLAN clients. Wifi mode is recommended if other than Nokia wireless LAN cards are used.

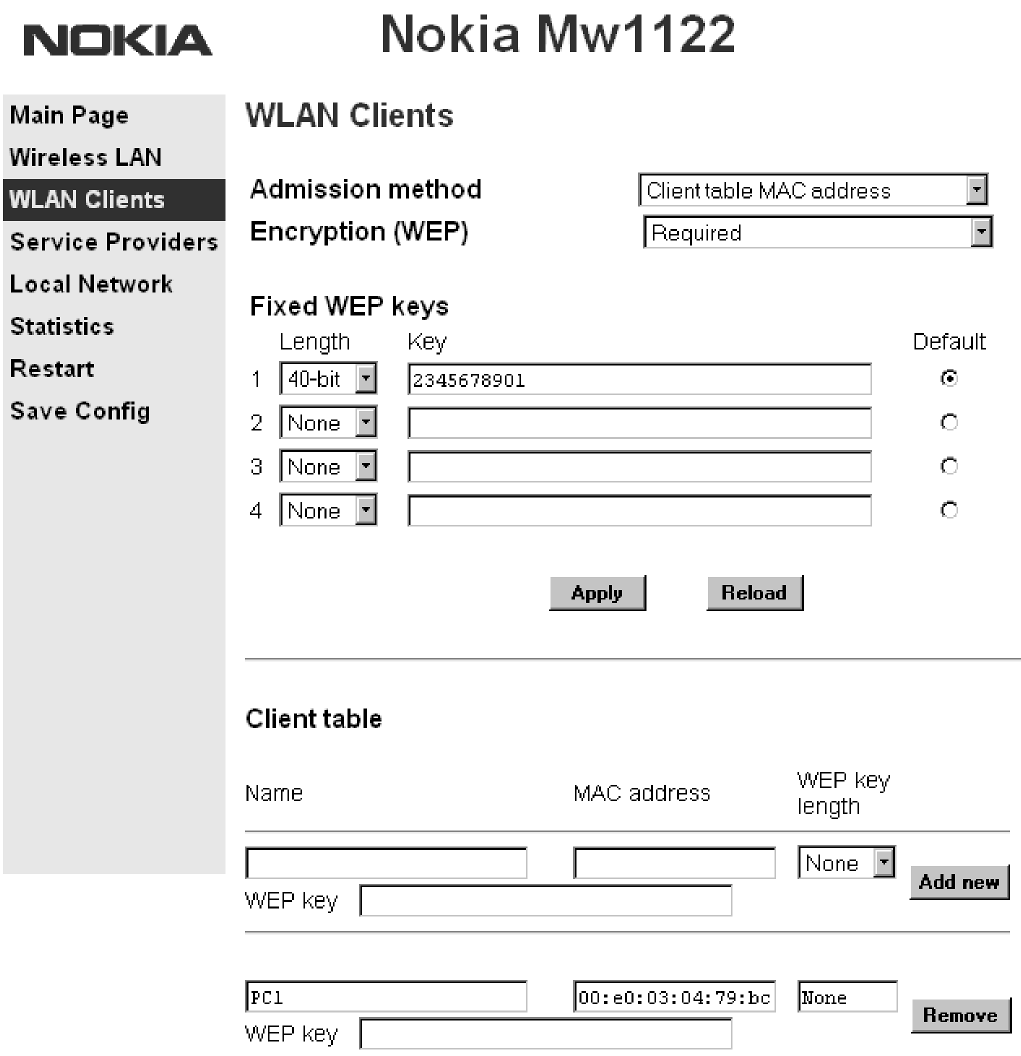
Figures 8 and 9 show Wlan Clients page with default key and station-specific keys used, respectively. In Figure 8, the station “PC1” on the Client table uses the default key 1. Additonally, the Client table is used as a MAC address -based access control list. In Figure 9, stations “PC1” and “PC2” use the station-specific key given in the *WEP key* field on the Client table. The MAC address -based access list is not needed, but the default key is used to encrypt the broadcast/multicast traffic.

Note

If you are using a station-specific key, you must also configure the default key because it is used for broadcast.

Note

When you click the Apply button, the WLAN settings become active. If you have enabled the access list or changed the encryption mode and you are accessing MW1122 through the wireless link, the connection will be lost. You must reconfigure the wireless LAN client to continue configuration.



WLAN Clients

Admission method: Client table MAC address

Encryption (WEP): Required

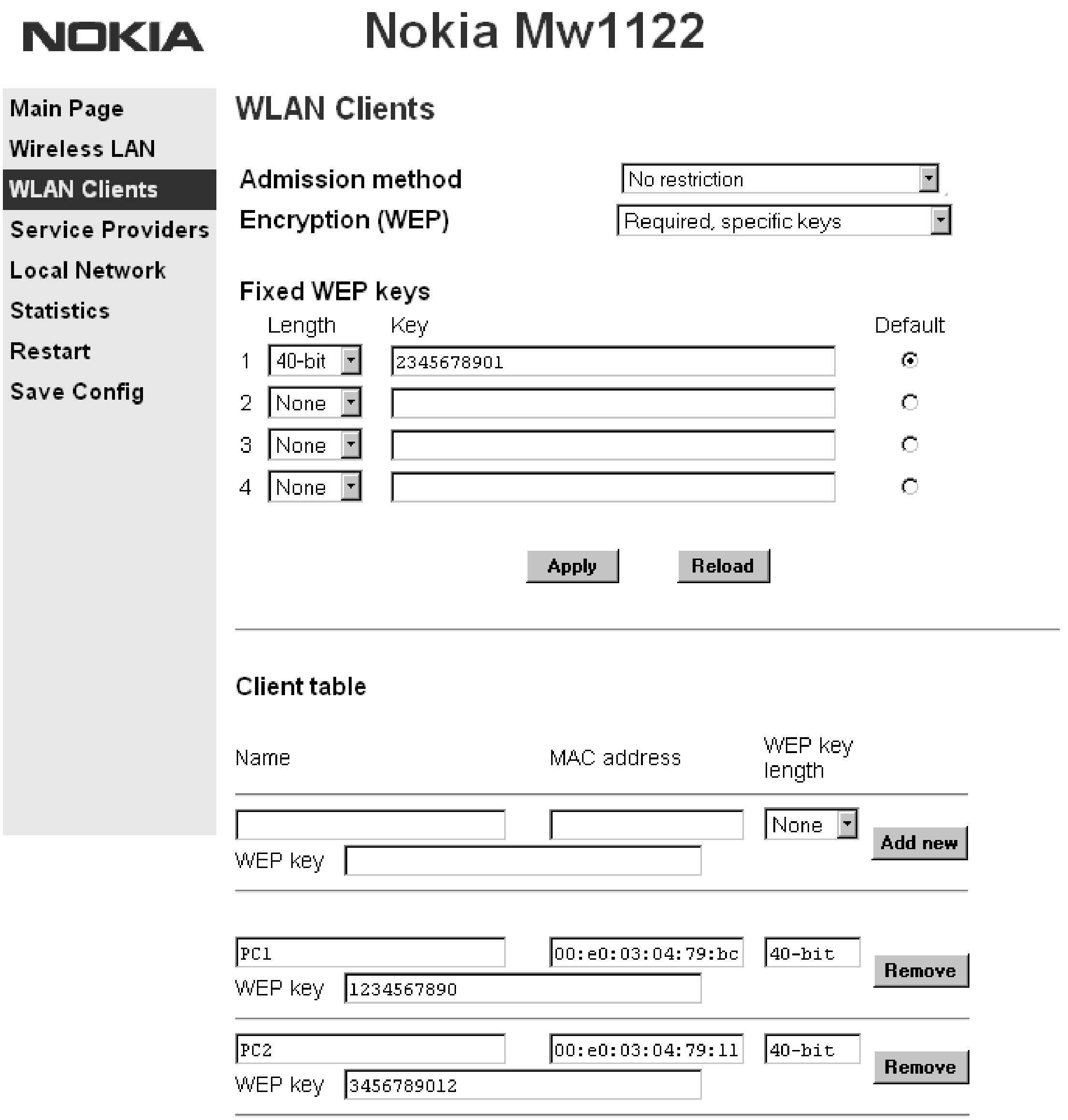
Fixed WEP keys

	Length	Key	Default
1	40-bit	2345678901	●
2	None		○
3	None		○
4	None		○

Client table

Name	MAC address	WEP key length
		None
WEP key:		
PC1	00:e0:03:04:79:bc	None
WEP key:		

Figure 8 WLAN Clients page and default key encryption



Nokia Mw1122

WLAN Clients

Admission method: No restriction

Encryption (WEP): Required, specific keys

Fixed WEP keys

	Length	Key	Default
1	40-bit	2345678901	●
2	None		○
3	None		○
4	None		○

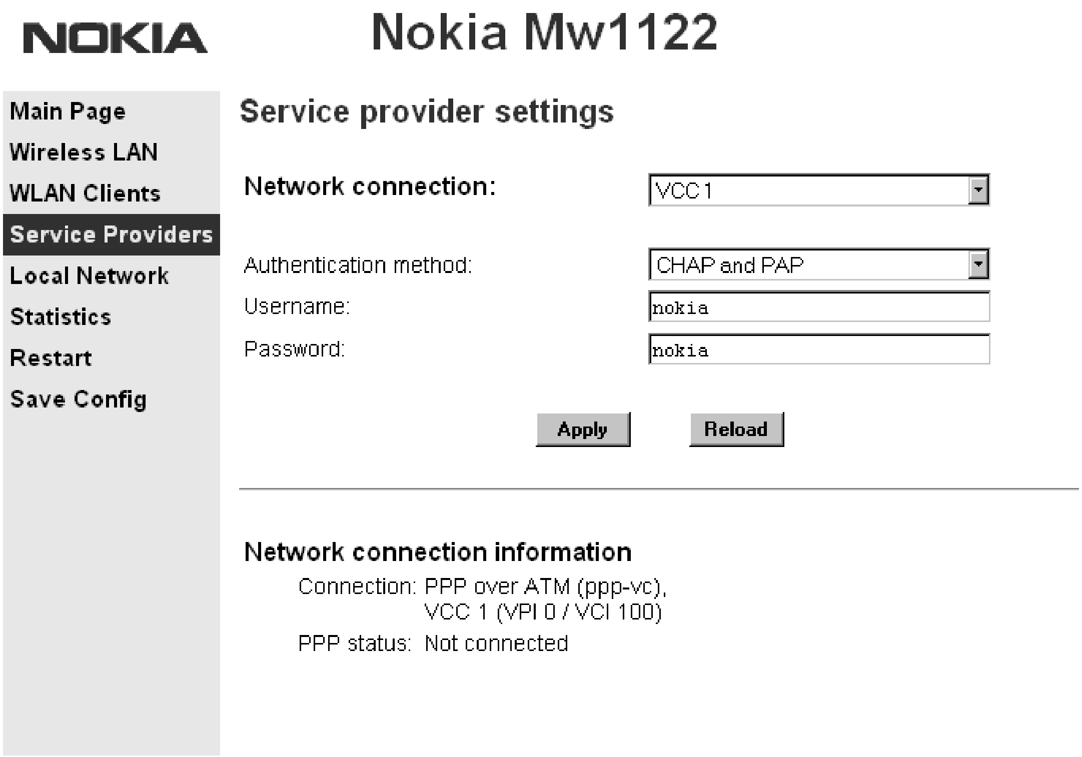
Client table

Name	MAC address	WEP key length	WEP key
		None	
PC1	00:e0:03:04:79:bc	40-bit	1234567890
PC2	00:e0:03:04:79:11	40-bit	3456789012

Figure 9 WLAN Clients page and station-specific key encryption

3.1.5 Service Providers pages

The *Service Providers* page can be used to set authentication for ATM VCCs with PPP encapsulation (Figure 10). You can set the *Authentication method* and the corresponding *Username* and *Password*. You can also view Network connection information in the bottom of the page. If you are using PPTP encapsulation, you can change the name of the connection through the Service Providers page (Figure 11).



Service provider settings

Network connection: VCC 1

Authentication method: CHAP and PAP

Username: nokia

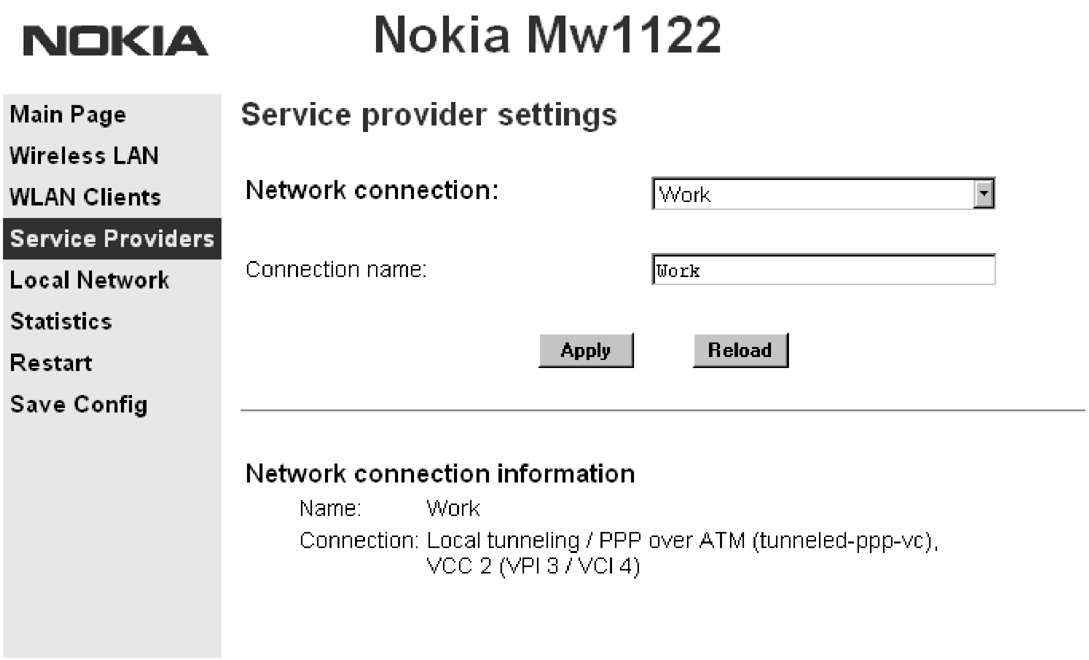
Password: nokia

Network connection information

Connection: PPP over ATM (ppp-vc),
VCC 1 (VPI 0 / VCI 100)

PPP status: Not connected

Figure 10 Service Provider page with PPP configuration



Service provider settings

Network connection: Work

Connection name: Work

Network connection information

Name: Work

Connection: Local tunneling / PPP over ATM (tunneled-ppp-vc), VCC 2 (VPI 3 / VCI 4)

Figure 11 Service Providers page with PPTP configuration

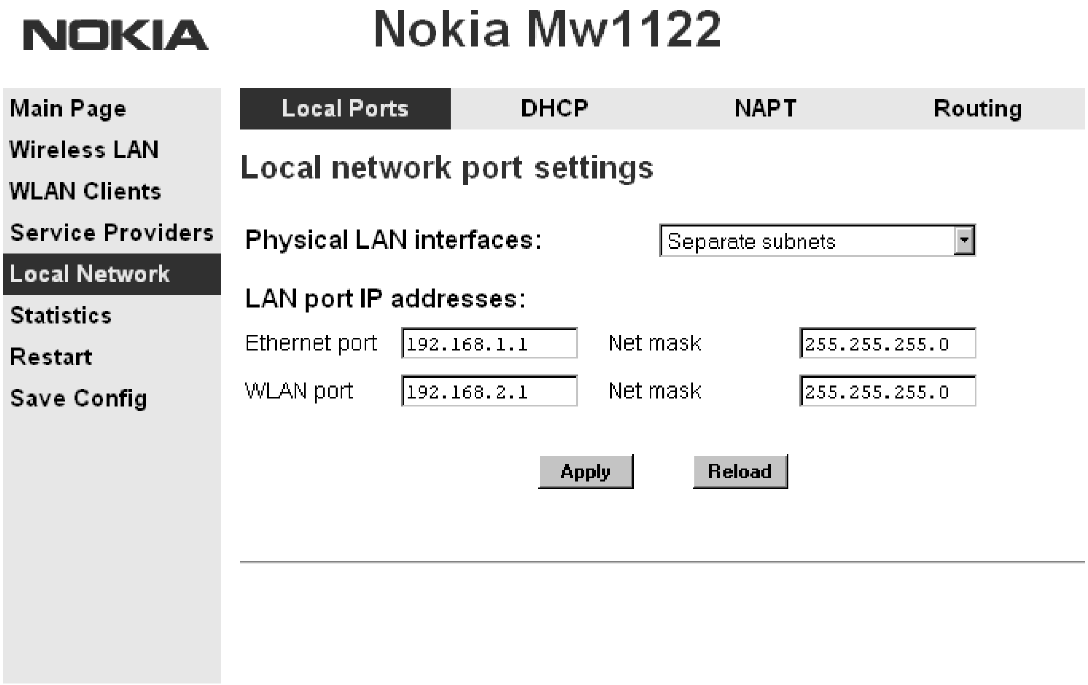
3.1.6 Local Network pages

The *Local Network* page as four sub pages: *Local ports*, *DHCP*, *NAPT*, and *Routing*.

Local ports

On the *Local Network Local Ports* sub page you can assign IP addresses to Ethernet and wireless LAN ports. If you set *Physical LAN interfaces* as *Single subnet*, you don't have to set the IP address and subnet mask to the WLAN port. Instead, the Ethernet IP address is used for both LAN ports (WLAN slaved to LAN).

Note
When you click Apply, the IP addresses are changed immediately. If the IP address of the interface you are using changes the connection will be lost. You have to reconfigure the IP address of the accessing host. For example, in Windows programs winipcfg.exe or ipconfig.exe must be used first to release the old address and then to renew to request new address.



Local network port settings

Physical LAN interfaces: Separate subnets

LAN port IP addresses:

Ethernet port 192.168.1.1 Net mask 255.255.255.0

WLAN port 192.168.2.1 Net mask 255.255.255.0

Figure 12 Local Network Local Ports page

DHCP

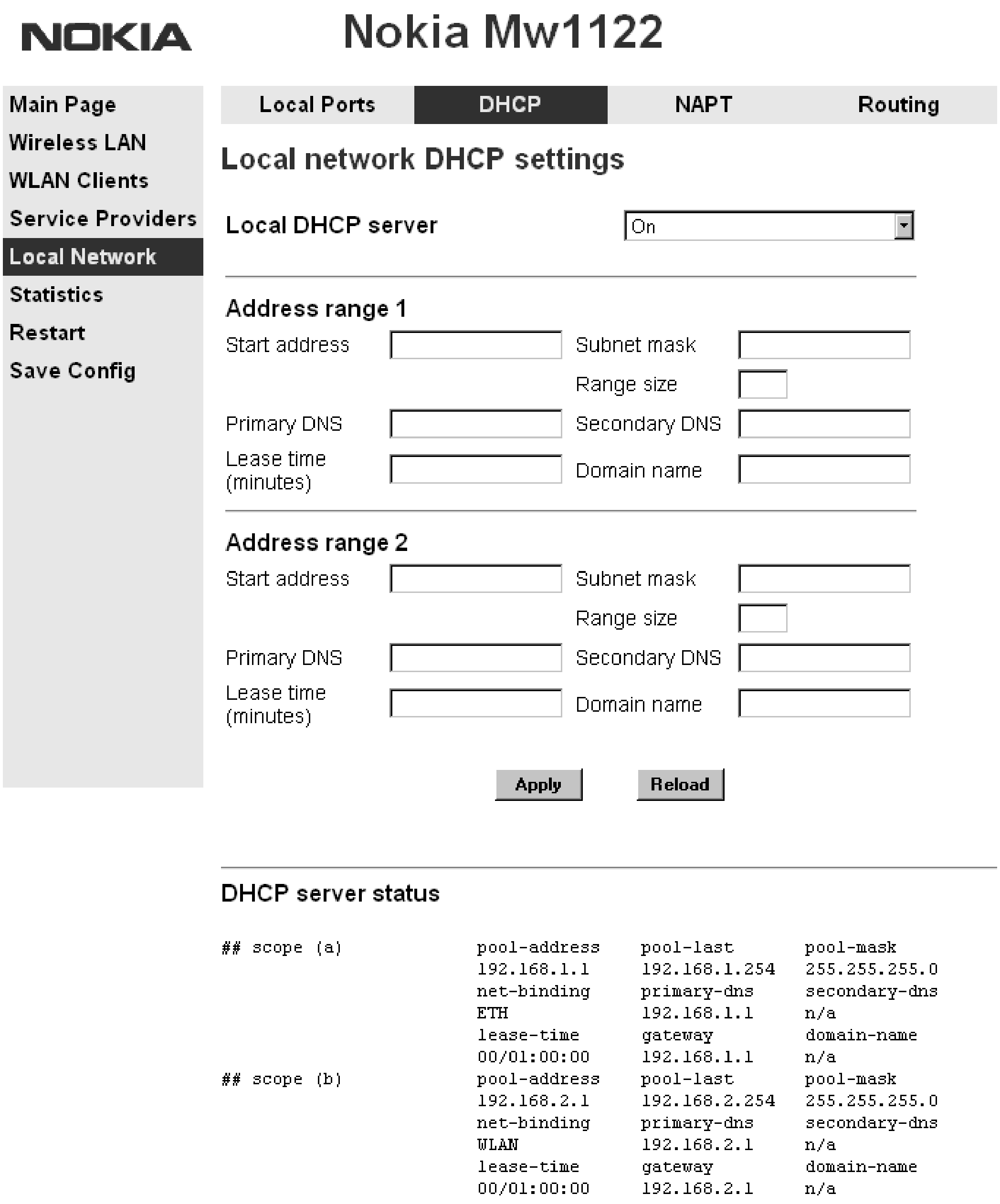
On the *Local Network DHCP* subpage you can enable/disable Dynamic Host Control Protocol and set the Address ranges from which the addresses are distributed to the DHCP clients on your network. You can also set the Domain Name Server addresses here.

Start address is the first address in the address range. The *Range size* defines how many addresses the range contains. *Subnet mask* is the subnet mask of the addresses in the range. *Primary* and *Secondary DNS*s set the domain name servers for the corresponding address range. *Lease time* defines how often the DHCP client must renew its lease. *Domain name* defines the domain name for the range.

The DHCP server can be enabled towards LAN, WLAN and VBRIDGE (gateway interface) ports. When the DHCP server is enabled, up to two scopes (address ranges) are automatically generated and bound to LAN/WLAN/VBRIDGE interfaces, in this order if the interface has an IP address. If your LAN and WLAN interfaces have separate IP addresses you must configure two address ranges, one for each interface. In Figure 13, scope (a) is has been bound to Ethernet interface and scope (b) to WLAN interface. When the address ranges are not defined, MW1122 uses the default values for all DHCP parameters. The default values are:

- Start address is the interface IP address
- Subnet mask 255.255.255.0
- Range size of up to 253 addresses starting from the interface IP address.
- DNS address is the interface IP address
- Lease time is 60 minutes
- Domain name is null string

If at least one address range has been defined, then IP address, DNS, domain name and lease time, if defined, override the default values.



Local network DHCP settings

Local DHCP server: On

Address range 1

Start address | Subnet mask
Range size
Primary DNS | Secondary DNS
Lease time (minutes) | Domain name

Address range 2

Start address | Subnet mask
Range size
Primary DNS | Secondary DNS
Lease time (minutes) | Domain name

DHCP server status

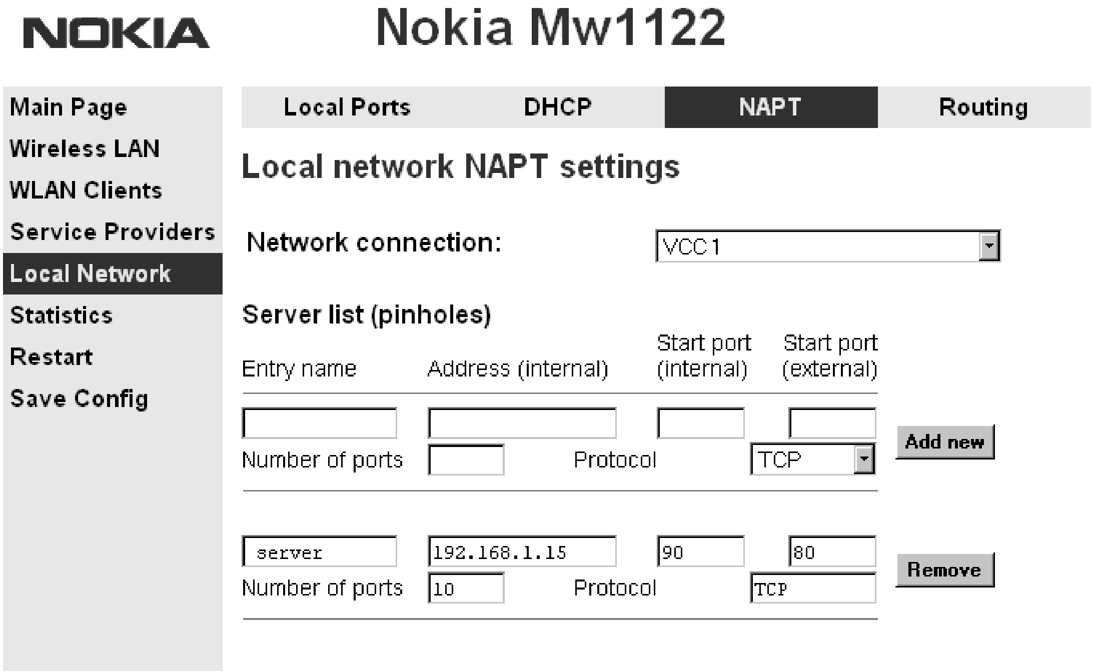
```
## scope (a)            pool-address   pool-last      pool-mask
                        192.168.1.1    192.168.1.254  255.255.255.0
                        net-binding    primary-dns    secondary-dns
                        ETH            192.168.1.1    n/a
                        lease-time     gateway        domain-name
                        00/01:00:00    192.168.1.1    n/a
## scope (b)            pool-address   pool-last      pool-mask
                        192.168.2.1    192.168.2.254  255.255.255.0
                        net-binding    primary-dns    secondary-dns
                        WLAN           192.168.2.1    n/a
                        lease-time     gateway        domain-name
                        00/01:00:00    192.168.2.1    n/a
```

Figure 13 Local Network DHCP page

NAPT

If Network Address Port Translation (NAPT) has been activated, servers on your local network are not visible outside your network. On NAPT page, you can configure pinholes through which you can provide outside access to your web server from the Internet, for example.

In the example shown in Figure 14, a pinhole has been added on the Server list. This example means that all TCP traffic coming from the Internet through VCC1 to ports 80...89 will be mapped to the IP address 192.168.1.15 ports 90...99 on your local network.



Local network NAPT settings

Network connection: VCC1

Server list (pinholes)

Entry name	Address (internal)	Start port (internal)	Start port (external)
Number of ports		Protocol	TCP
server	192.168.1.15	90	80
Number of ports	10	Protocol	TCP

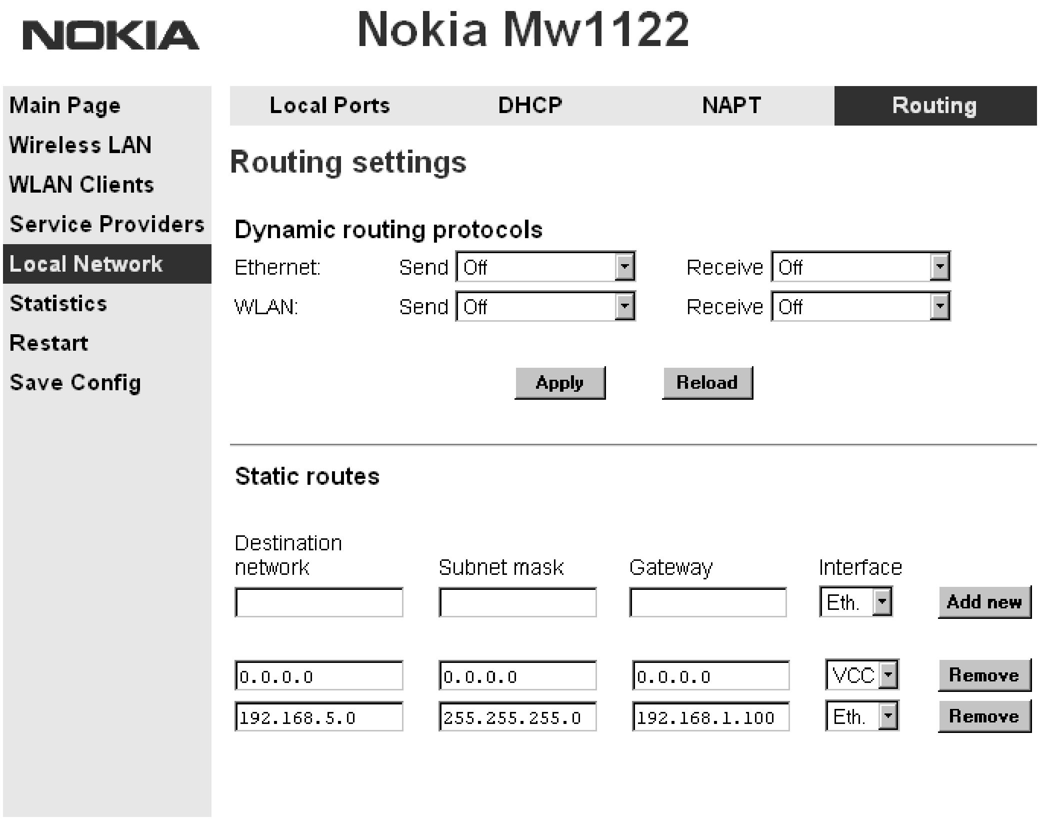
Figure 14 Local Network NAPT page

Routing page

On the *Local Network Routing* sub page you can set static routes and enable/disable dynamic routing protocols (Routing Information Protocol version 1 and 2).

To enable dynamic routing to a particular interface select the Routing protocol version from the pull-down list and click the Apply button. RIP versions 1 and 2 are supported. Send *v1-compat. v2* option enables the sending of RIPv2 packets using broadcast. Receive *v1-compat. v2* option enables the receiving of both RIPv1 and RIPv2 packets.

To add a static route, type in the *Destination network* IP address, the *Subnet mask* of the destination network, and the *Gateway* and the *Interface* through which the destination network can be reached. Then click the *Add new* button. There are two static routes in Figure 15.



Nokia Mw1122

Routing settings

Dynamic routing protocols

Ethernet: Send Off Receive Off

WLAN: Send Off Receive Off

Static routes

Destination network	Subnet mask	Gateway	Interface	
			Eth.	Add new
0.0.0.0	0.0.0.0	0.0.0.0	VCC	Remove
192.168.5.0	255.255.255.0	192.168.1.100	Eth.	Remove

Figure 15 Local Network Routing page

3.1.7 Statistics page

The Statistics page lets you view a selection of MW1122 statistics. to view statistics of a particular function, click the corresponding button and the statistics view is opened on a separate window.

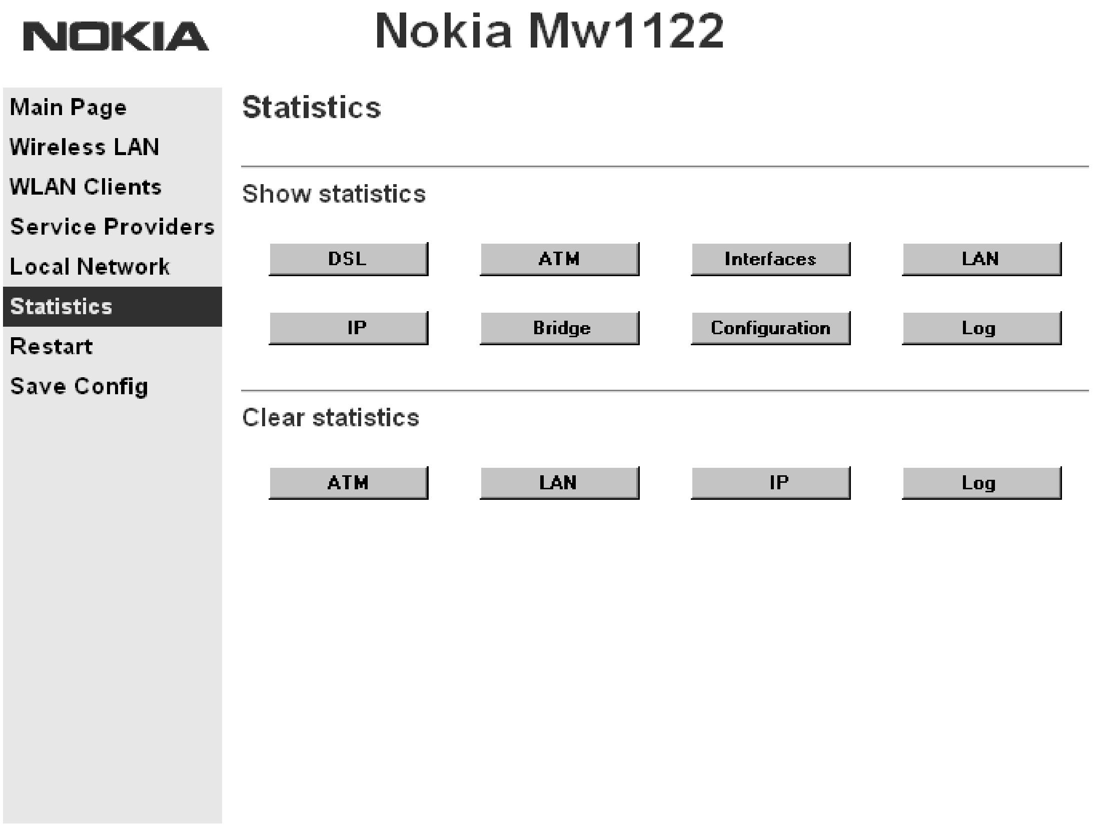


Figure 16 Statistics page

3.1.8 Restart page

On the Restart page, you can reset subsystems and restart MW1122.

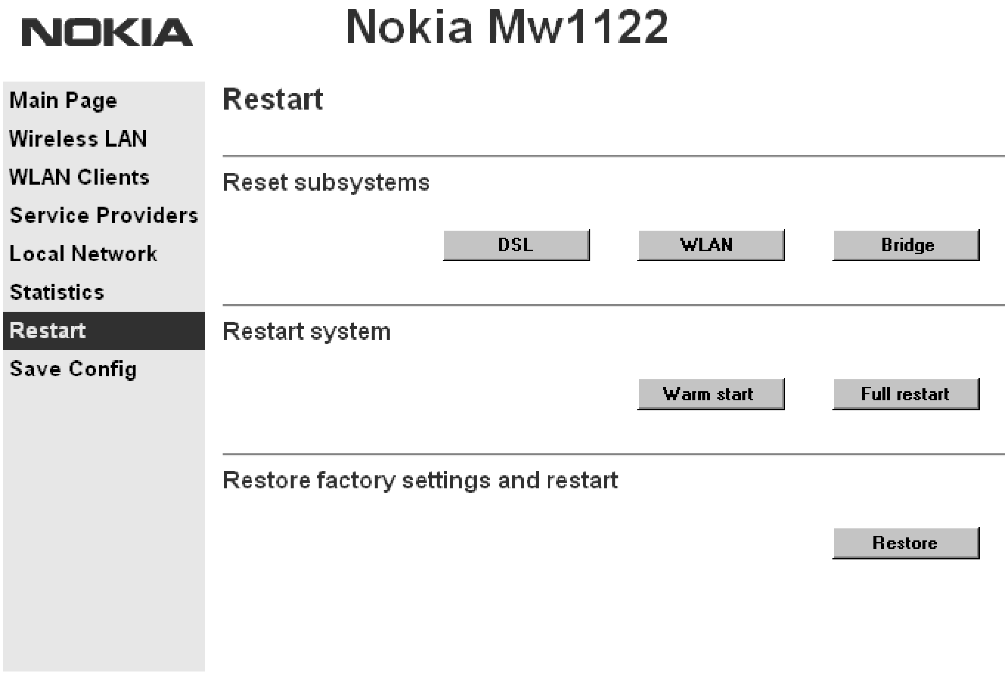
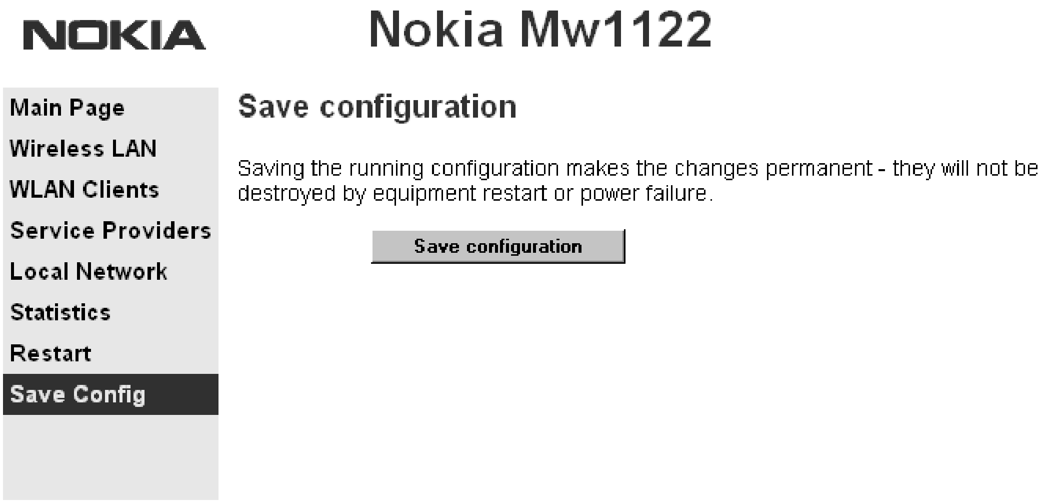


Figure 17 Restart page

3.1.9 Save Config page

When you change the configuration, all configuration changes are activated immediately without restart/reload. However, the configuration will not be saved into the nonvolatile memory. If MW1122 is restarted or powered down without saving the configuration, the old configuration will be restored. Clicking the Save configuration button saves the configuration into the nonvolatile memory and the old configuration cannot be restored through the web interface.



Save configuration

Saving the running configuration makes the changes permanent - they will not be destroyed by equipment restart or power failure.

Figure 18 Save Config page

4 Features

MW1122 can operate as a bridge and/or Internet Protocol (IP) router between Ethernet, wireless LAN and the virtual channels of ADSL/ATM interfaces supporting both dynamic and static routing.

4.1 Interfaces

MW1122 has the following interfaces:

- Ethernet interface (LAN)
- Wireless LAN interface (WLAN)
- 8 ATM VCC interfaces
- ATM VCC management interface

- Gateway/bridge management interface. This interface is used as a bridge host interface or gateway interface depending on the operation mode. In this manual it is called VBRIDGE. On the MW1122 web pages, the interface is called gateway or bridge IP interface.

MW1122 can operate in four different main modes:

- Bridging only
- Routing/tunneling IP only
- Routing/tunneling IP, bridging all but IP
- Routing/tunneling IP and bridging all, including IP

The mode in which MW1122 operates depends on the configuration of the unit's interfaces.

LAN and WLAN interfaces

LAN and WLAN interfaces can be configured individually to bridge and route packets. There are three different operational modes in both LAN and WLAN interfaces:

- Bridging only; only bridging is activated in the interface. In this case the interface bridges all protocols.
- Routing only; only IP address is configured in the interface. In this case, the interface routes IP packets.
- Bridging and routing; Bridging is activated in the interface and IP address is configured in the interface. In this case, the interface routes IP packets and bridges all other packets.

Slaved WLAN operation

The wireless LAN interface can be configured to operate as a slave to the Ethernet interface. In this case, there is no need to configure the IP address or bridging to the wireless LAN interface. The Ethernet and the wireless LAN interface are bridged together internally and both interfaces are treated as a single LAN interface. All LAN configuration parameters defining bridging and IP-related parameters, such as IP address, admin-disabled and RIP configuration address, are used for both LAN and WLAN interfaces.

Internal host/gateway interface

There is a special host/gateway logical IP interface within MW1122 called VBRIDGE. This interface has a specific purpose in MW1122. In applications where some ATM virtual channel connections are used for bridging IP traffic and some other ATM virtual channel connections are used for routing IP traffic, the VBRIDGE interface must be used instead of LAN/WLAN IP addresses. Alternatively, this interface is used in bridge only application when the IP address is required for remote management purposes.

Data VCC operation

MW1122 supports the following encapsulations in each ATM data virtual channel individually:

- RFC2684 LLC encapsulation for bridged IP (ETH-LLC)
- RFC2684 LLC encapsulation for routed IP (IP-LLC)
- RFC2364 Virtual circuit multiplexed PPP over AAL5 (PPP-VC)
- RFC2364 Virtual circuit multiplexed PPP over AAL5 used to tunnel LAN/WLAN/VBRIDGE PPTP packets (TUNNELED-PPP-VC)

If an IP address is given to a virtual channel interface and bridging is enabled at that interface, then IP data at that interface is routed and all other protocols are bridged. The only encapsulation which allows both bridging and routing simultaneously is ETH-LLC. For example, it is possible to route ETH-LLC encapsulated packets and at the same time bridge, for example, PPPoE packets (PPPoE packets are transported directly over Ethernet frame, not within IP packets).

4.2 Routing

Routing is based on routing entries in a routing table. Static routes are added via the management interface and dynamic routing is done using RIP and RIPv2. Routing is done between the Ethernet 10Base-T interface, the wireless LAN interface and the virtual channel connection (VCC) of the ATM/ADSL interface. MW1122 supports up to 8 simultaneous VCCs.

MW1122 supports IGMP (Internet Group Management Protocol) proxy receive function for IP multicast applications.

4.3 Bridging

Bridging is supported to provide full protocol transparency. Bridging can be used simultaneously with IP routing. MW1122 works as a self-learning bridge supporting up to 1024 MAC addresses. Bridging is done between the Ethernet 10Base-T interface, the wireless LAN interface and each ATM VCC interface. Optionally, the bridging between the VCCs can be disabled.

4.4 Network Address Port Translation

MW1122 supports Network Address Port Translation (NAPT) for TCP/IP, UDP/IP and ICMP/IP protocols. When NAPT is used, a single IP address is allocated to a VCC which leads to the public IP network. The Ethernet subnet has private IP addressing and is not visible to the VCC. NAPT translates the IP source address and source port number dynamically to the VCC IP address and port number. Similarly, packets coming from the VCC are mapped back to the original destination addresses. NAPT allows up to hundreds of hosts to share a single VCC IP address to the public network. The principle of Network Address Port Translation is presented in Figure 19.

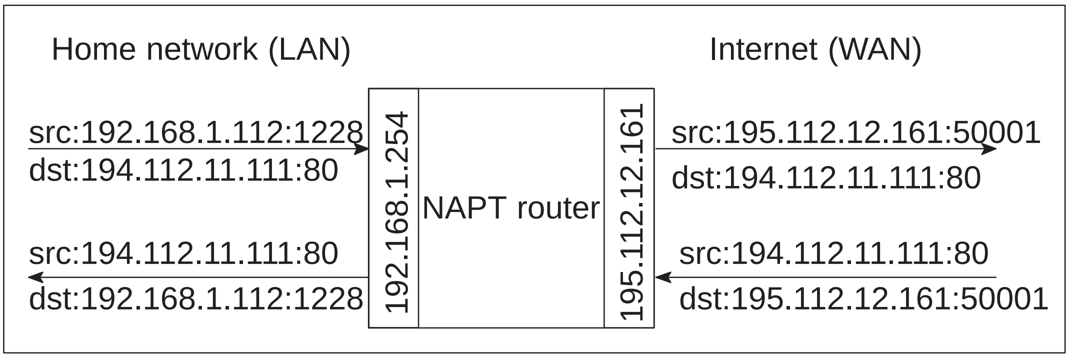


Figure 19 Principle of Network Address Port Translation

NAPT may restrict the operation of some IP applications. NAPT also operates as a simple IP firewall because translation is only allowed when the first packet is transmitted from the LAN. This means that the NAPT table entry is created only when a packet is sent from the home network to the Internet. With server support capability, the user can add static entries to the NAPT table allowing the translation always in both directions. This capability is used to add servers (HTTP, NNTP, and FTP), which are visible to the public IP network via the VCC, on the LAN subnet.

NAPT supports most IP-based protocols. Because NAPT operates on the IP and transport layer, the application that includes IP address and port within the payload will not work properly through NAPT. In many cases, these applications can be passed through the NAPT using

Application Layer Gateway functionality (ALG). MW1122 has ALG for the following protocols/applications:

- ICMP
- FTP
- H.323 including NetMeeting
- CUSeeMe
- PPTP
- IRC
- IPSEC ESP tunnel mode and IKE

Note, that most IPSEC implementations will fail when passed through NAPT. A typical reason is that the identification may fail if the identification is based on IP address. Also, only tunnel mode without Authentication Header (AH) works.

4.5 Dynamic Host Configuration Protocol

MW1122 can act as a Dynamic Host Configuration Protocol (DHCP) server for the PCs on the end-user home network. In this mode, MW1122 can assign up to 253+253 consecutive addresses from two separate address ranges (that is, 253 consecutive addresses per address range) to the PCs on the home network. Two separate address ranges are used when LAN and WLAN are operating as separate subnets. MW1122 can also act as a DHCP relay agent and relay the DHCP requests to an external DHCP server.

4.6 ATM and ADSL

MW1122 supports up to 8 simultaneous VCCs and supports UBR (Unspecified bit rate) traffic shaping on all VCCs. The maximum transmit rate on each VCC is the ADSL upstream capacity. If more than one VCC is transmitting simultaneously, the ADSL upstream capacity is temporarily shared between these VCCs. When one VCC is idle, the bandwidth is used by another VCC.

The ADSL transmission is based on the DMT line code. MW1122 provides a DMT line rate up to 8 Mbit/s downstream and up to 800 kbit/s upstream. The DMT transceiver is rate adaptive and capable of providing faster rates over short distances or slower rates over long distances. The transceiver adapts itself to the line conditions. MW1122 supports also ADSL Lite. In the ADSL Lite mode, the maximum line rates are 1536 kbit/s downstream and 512 kbit/s upstream.

MW1122 supports both G.992.1 and G.992.2 ADSL recommendations defined by ITU-T.

Rate adaptation is done in steps of 32 kbit/s. The ADSL interface of MW1122 functions completely automatically and all configuration related to the ADSL connection is done at the access multiplexer in the operator's premises. The network operator can set the data rates as a part of the network management functionality provided by Nokia DSLAM.

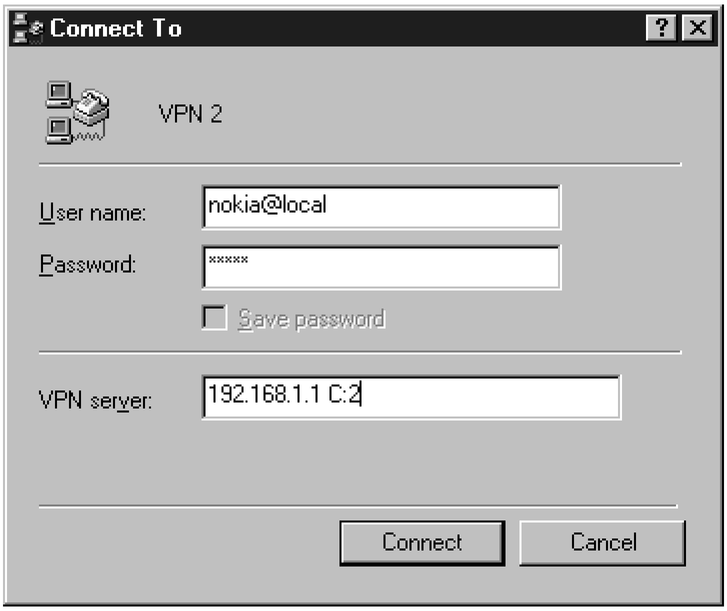
4.7 Point-to-Point Tunneling Protocol (PPTP)

When PPTP local tunneling is used, a local network client initialises a PPTP-tunneled PPP connection (VPN) to Nokia MW1122. The modem terminates the tunnel and all data from that terminated local PPTP tunnel will be forwarded to an assigned ATM VCC by using PPP over AAL5 encapsulation. Thus, each local PPTP tunnel requires an equivalent ATM VCC assigned to it restricting the total number of local PPTP hosts to 8.

Local tunneling is used when there is a need to have one or more computers connected independently to different networks. For example, in remote work application, the rest of the family may be using the common ISP services and one or two family members need to gain access to their corporate networks. With local tunneling, these remote workers may be connected to a different network than the rest of the users.

Local tunneling is activated using the PPTP client running, for example, in Windows The destination IP address must be MW1122 LAN/WLAN/VBRIDGE IP address depending on the configuration. PPP packets within PPTP are mapped to the configured VCC. MW1122 has three different ways to choose the ATM VCC that will be used for tunneling:

- Automatic, chooses the first free VCC
- Chooses the VCC number using C:number, where number is from 1 to 8. C:number is fed after the MW1122 IP address (see Figure 20).
- Chooses the VCC number using N:name, where name is the VCCx description. N:name is fed after the MW1122 IP address.



VPN 2

User name: nokia@local

Password: *****

□ Save password

VPN server: 192.168.1.1 C:2

Figure 20 Choosing the VCC2 for tunneling example

4.8 Point-to-Point Protocol over Ethernet (PPPoE)

Standard PPPoE mode is used when MW1122 is operating as a bridge. PPPoE protocol defines how PPP sessions are mapped into Ethernet packets. When MW1122 operates as a bridge, this protocol is transparent to MW1122.

4.9 Payload encapsulations

Both routed and bridged protocols are encapsulated in the ATM link by using either RFC 2684 LLC/SNAP encapsulation or VC multiplexing. MW1122 also supports PPP over AAL5 encapsulation, in which routed protocols are first encapsulated in PPP (RFC 1661). PPP is then encapsulated in ATM according to the IETF PPP over AAL5 using RFC 2364 VC multiplexing or LLC/NLPID encapsulation.

4.10 Access list authorisation

When a wireless LAN is used, it is important to be able to control the clients accessing to MW1122. Therefore, MAC-address-based access control may be used. It prevents all communications to a such client whose MAC address does not appear on the access list. When a new client is brought to the network, its MAC address needs to be added to the access list. This can be done manually through the local command line interface (CLI) or with a Web browser management.

4.11 Wireless LAN and radio interface

MW1122 supports wireless LAN to be used as one of the interfaces. The wireless LAN utilises Nokia C110/C111 Wireless LAN PC card which needs to be inserted to the designated PC Card slot on the back panel of the modem. Only Nokia C110 or C111 Wireless LAN cards can be used. Without a wireless LAN card, MW1122 operates as a normal ADSL terminal with one 10Base-T Ethernet interface. The wireless LAN card can be inserted to the PC Card slot while the modem is operating and the wireless LAN connectivity will be achieved without restarting the modem. Only the WLAN subsytem must be reseted through the web interface or the command line interface.

Wireless LAN used in MW1122 is based on IEEE802.11 standard operating at 2.4 GHz radio band. The band has been divided into subchannels which are dependent on local regulations. Typically, in Europe, there are 13 and, in USA, 11 channels. The transmission power is limited to 100 mW/MHz giving typical indoor coverage of 20 to 50 metres.

4.12 Wired Encryption Privacy (WEP)

MW1122 supports full-speed WEP encryption and both authentication methods defined in IEEE 802.11b: Open-key and shared-key authentication. The encryption is 40-bit RC4 WEP encryption. Additionally, MW1122 supports 128-bit RC4 WEP encryption.

4.13 Weighted Fair Queueing (Class of Service)

As a Class of Service (CoS) function, MW1122 supports Weighted Fair Queueing (WFQ) for each ATM VCC. The CoS function ensures that different IP traffic flows are treated fairly in the upstream (towards the Internet) direction. This may be necessary, in some cases, because the upstream capacity of the ADSL line is somewhat limited compared to the Ethernet bandwidth on the office or home LAN. The WFQ CoS function classifies IP traffic flows based on IP address, protocol and port fields. It is capable of identifying the IP flow from all supported payload encapsulation formats. WFQ works properly only with IP-based protocols. If the flow is IP-based but is encrypted using IPSec or PPP encryption, then WFQ cannot identify the flows correctly. In this case, the default flow is used and the default flow is treated as a single flow.

5 Technical specifications

Features	
ADSL	
Physical layer	ANSI T1.413 Issue 2 (ANSI ADSL), ITU-T G.992.1 (ITU-T ADSL), and ITU-T G.994.1 (Handshake) compatible.
ADSL line connector	RJ-11
ATM over ADSL	
ATM connections	PVC, up to 8 virtual circuits
Service categories	UBR
Encapsulations	RFC2684 ETH-LLC, RFC2684 IP-LLC, RFC2364 PPP-VC, RFC2364 TUNNELED-PPP-VC
Ethernet interface	
Ethernet	10Base-T, half duplex
Encapsulation	DIXv2 (transmit), IEEE 802.3 and DIXv2 (receive)
Ethernet connectors	RJ-45
Wireless LAN interface	
Wireless LAN	IEEE 802.11b DSSS
Data connector	PC Card slot type 2
Routing	
Routing protocols	RIPv1, RIPv2, and static routes
Other	NAPT, IGMP proxy, DHCP server, DNS relay, PPTP local tunneling
Class of Service	Weighted fair queueing

Bridging	
Bridging	Self-learning bridge, bridges between all interfaces. Possibility to disable bridging between WAN interfaces.
MAC table	1024 entries
Class of Service	Weighted fair queueing
Command line interface (CLI) for local management	
Physical layer	Electrically RS-232, TxD, RxD and GND signals
Data format	Asynchronous, 8+no parity
Bit rate	9600 bps
Flow control	None
CLI connector	RJ-45
Dedicated ATM management channel	
Service categories	UBR
Encapsulations	RFC2684 ETH-LLC, RFC2684 IP-LLC, RFC2364 PPP-VC
IP addressing	Statically configured Through IPCP when PPP over ATM is used
Routing	Static routes RIPv1, RIPv2
Management protocols	Telnet/TCP/IP for command line interface, TFTP/UDP/IP for software and configuration download, HTTP/web server
Management through payload	
Management protocols	Telnet/TCP/IP for command line interface, TFTP/UDP/IP for software and configuration download, HTTP/web server
Indicator lights	
DSL	ADSL line status
ETH	Ethernet activity and status
WLAN	Wlan activity and status
COL	Ethernet collision
STA	MW1122 startup error
PWR	Power on

5.1 Connectors and pin numbering

The pin numberings are given here if you want to obtain longer cables for your MW1122.

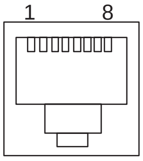


Figure 21 ETH connector

PIN	Signal	Direction MW1122-Ethernet	MDI signal
1	Tx+	–>	Transmit data +
2	Tx–	–>	Transmit data –
3	Rx+	<–	Receive data +
6	Rx–	<–	Receive data –

Table 1 Ethernet interface pin-out numbering

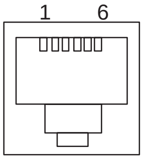


Figure 22 DSL connector

PIN	Signal
3	DSL1
4	DSL2

Table 2 ADSL interface pin-out numbering

5.2 Ambient conditions, EMC and safety

Ambient conditions

Operating temperature range	5 to 45°C
Humidity	10% to 90%, non-condensing

EMC

MW1122 complies with the following specifications provided that the device is connected to an earthed socket outlet:

Emission	EN55022: 1998 class B
Immunity	EN55024: 1998
EMC	EN300386-2: 1997
Overvoltage	ITU-T K.21

Safety

Safety	EN60950