DSL Gateway

HIGH-SPEED INTERNET CONNECTION

Administrator Manual

NOKIA

CONNECTING PEOPLE

NOKIA

Nokia M/MW Gateways M1112, M1122, MW1112, MW1122, MW1324 MW1352

Administrator Manual
C34300002ZE_00

Contents

Summary of changes

Document number	Date	Comment
DN0195869 Issue 1-0 en	8 Nov 2001	Valid for software version 2.3.0

1 Introduction to Nokia M/MW Gateways

The highly integrated Nokia M/MW Gateways can support wireless (MW series only) and Ethernet clients within your local network. In addition, MW1324 supports Phoneline (HPNA) clients.

Regardless of the LAN interface used for the clients, they all can belong to the same subnet for seamless networking. With your M/MW modem you can use a variety of applications on the already installed telephone lines used traditionally only for telephone and dial-up modem services.

M/MW Gateways bring high-speed connections available for home users, small offices and telecommuters.

Figure 1. Nokia M/MW and Nokia C111 Wireless LAN card & antenna (Optional)

2 Interfaces and indicator lights

This describes the external interfaces of M/MW and its front panel indicator lights. This manual uses MW1122 as Gateway example.

Refer to table below for supported features. More specific product information can be found in the Technical Specifications Chapter.

M/MW has six (MW1122: seven) indicator lights on the front panel: PWR, STA, WLAN, COL, ETH (MW1324 also HPNA) and DSL. The STA indicator is red. The other indicators are green.

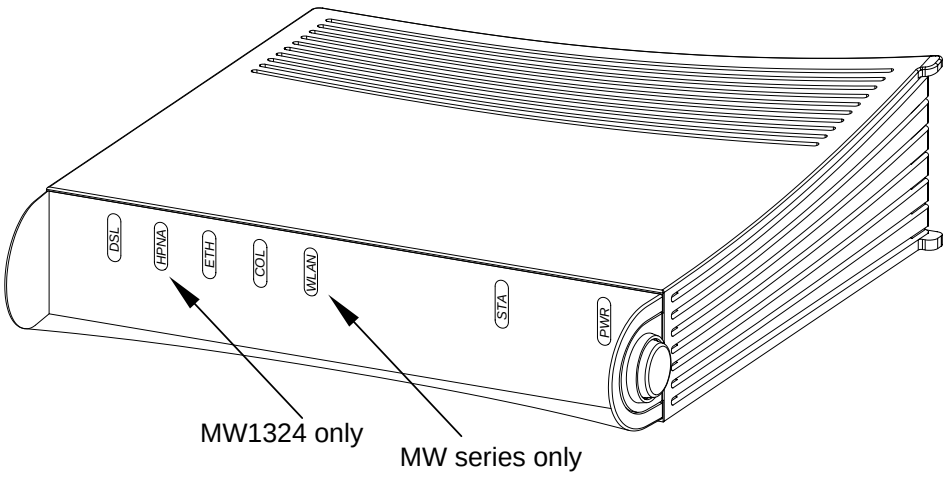

Figure 2. M/MW front panel indicators

DSL GREEN

Off	ADSL/SHDSL link is down.
Blinks	ADSL/SHDSL connection is being established.
On	ADSL/SHDSL link is up.

HPNA GREEN (MW1324 only)

Off	No stations detected.
On	Stations detected but no traffic.

Blinks Traffic detected at HPNA interface.

ETH GREEN

Off Ethernet is down.

On 10Base-T Ethernet is functional.

Blinks Traffic detected on Ethernet.

COL GREEN

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

WLAN GREEN (MW series only)

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.

Blinks The modem is booting.

PWR GREEN

Off Power off.

On Power on.

Table 1.

Interface	M1112	M1122	MW1112	MW1122	MW1122	MW 1352
ADSL (ITU-T and ANSI compatible)		X		X	X	
ADSL (ETSI TS 101 388 compatible)	X		X			
ADSL over ISDN	X		X			
SHDSL						X
CLI	X	X	X	X	X	X
WLAN			X	X	X	X
Ethernet	X	X	X	X	X	X
HPNA					X	

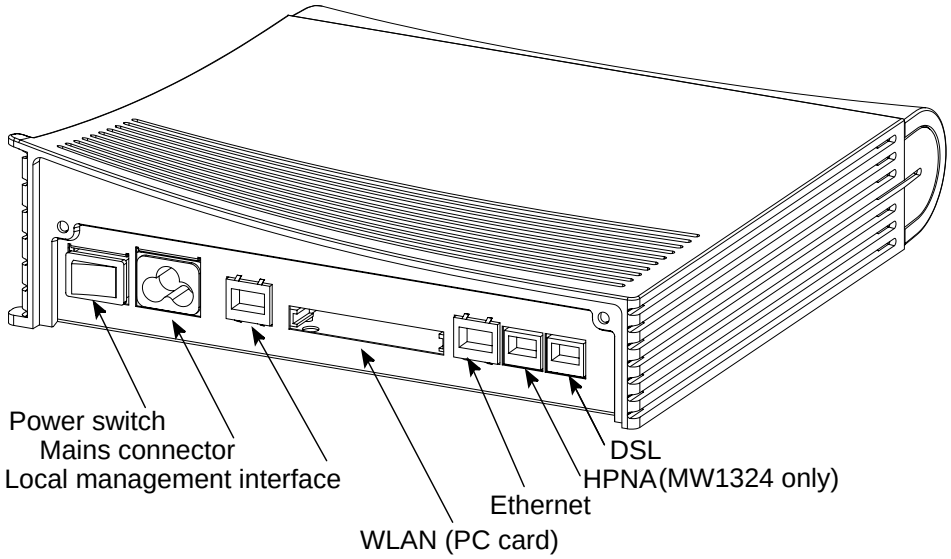

Figure 3. MW series back panel

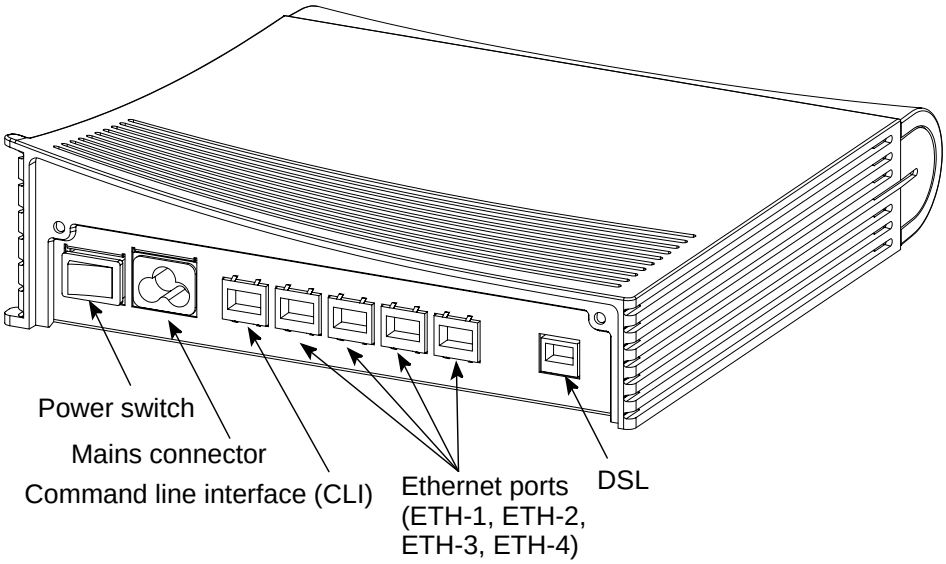

Figure 4. M series back panel

2.1 Ethernet interface

The Ethernet interface (ETH) is located on the back panel. The Ethernet interface is a standard 10 Mbit/s half-duplex 10Base-T interface. The mechanical connector is an 8-pin RJ-45. The pin-out numbering is shown in Table 2.

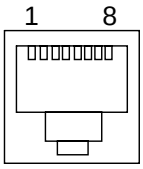

Figure 5. ETH connector

Table 2. Ethernet interface pin-out numbering MW series

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

Table 3. Ethernet interface pin-out numbering M-series

PIN	Signal	Direction M11x2 Ethernet	MDI signal
1	Rx+	<-	Receive data +
2	Rx-	<-	Receive data -
3	Tx+	->	Transmit data+
6	Tx-	->	Transmit data -

2.2 ADSL interface (all models except MW1352)

The ADSL interfaces of MW1122 and MW1122 are compatible with ITU-T G.992.1. The ADSL interface of MW1112 is compatible with ETSI TS 101 388 specification. The mechanical connector is a 6-pin RJ-12. The pin-out numbering is shown in Table 4.

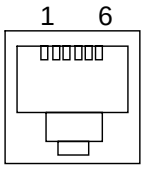

Figure 6. DSL/HPNA connector

Table 4. ADSL/SHDSL interface pin-out numbering

PIN	Signal
3	DSL1
4	DSL 2

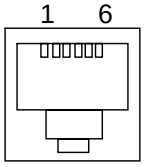

Figure 7. HPNA connector (MW1324 only)

Table 5. HPNA interface pin-out numbering (MW1324 only)

PIN	Signal
3	HPNA 1
4	HPNA 2

2.3 SHDSL interface (MW1352 only)

The SHDSL interface (DSL) is compatible with Nokia DSLAM. The mechanical connector is a 6-pin RJ-12 presented in Figure 6. The pin-out numbering is shown in Table 4.

3 M/MW default settings

Typically, M/MW has a customer-specific configuration. The default configuration of a general version is shown in Table 6.

Table 6. M/MW default settings

Config mode level	Parameter	Value
system	hostname	M/MW
eth	IP address	192.168.1.1 255.255.255.0
wlan	regulatory-domain	europe
	channel	varies
	network name	M/MW-wxyz, where wxyz are the last four numbers of the serial number which can be found on a sticker in on the bottom of M/MW.
	slave-to-eth	on
vcc1	pvc	0 (vpi) 100 (vci) ppp-vc (encaps)
	IP address	0.0.0.0 0.0.0.0, means that M/MW gets its IP address dynamically from the network.
	IP NAPT	on
	ppp authentication	both-chap-pap
	ppp username	none
	ppp password	none
common	ip route	0.0.0.0 0.0.0.0 0.0.0.0 vcc1
MW1352 only:	SHDSL region	Europe

Table 6. M/MW default settings (Continued)

Config mode level	Parameter	Value
MW1352 only:	SHDSL variant	CP-adaptive
MW1352 only:	SHDSL startup margin	6 dB
	DHCP mode	server

4 Browser management

M/MW Gateway can be managed with a web browser or command line interface (CLI). The web configuration pages of M/MW can be accessed through the Ethernet and wireless LAN ports or through the DSL/ATM channels of M/MW unless ip-admin is disabled. In order to access the web management feature, the IP function must be activated and an IP address must be given to the corresponding interface.

You can use your PC's web browser software to access the web configuration pages in M/MW. To access the web pages you must know the IP address of your M/MW or, alternatively, the name that your M/MW recognises.

In order to establish a connection through your web browser you need to use a cross over cable for MW series Gateways and a straight through cable for M series Gateways.

Note

Before using your web browser for configuration, you must know the IP address or the name assigned to your M/MW.

Note

On the following pages you find examples of web management windows. The modem presented in the examples is MW1122. The detailed contents of your pages may look different, depending on your modem model and its settings.

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

- Your service provider has given you an IP address for M/MW.
- Your M/MW uses Dynamic Host Configuration Protocol (DHCP) and Domain Name Server. In this case the name is *MW1122*, or you can run winipcfg.exe (Windows 95/98/Me) or ipconfig.exe (Windows 2000/NT). The IP address of M/MW is the Default Gateway address shown by the ipconfig program.

4.1 Opening a connection

To open a connection to the Nokia M/MW:

1. Start your web browser.
2. Enter the IP address or name of your Gateway in the **Address** (internet Explorer) or **Location/Go to** (Netscape Navigator) field of the browser.
3. Type in the username/password as requested. If no username/password is required, just click OK to proceed. The Nokia M/MW Main Page appears.

4.2 Main Page

The **Main Page** is shown first when you use a web browser to connect to M/MW. The currently shown page is shown highlighted on the list on the left. Clicking an item on the list (Wireless LAN, WLAN Clients, Service Providers, Local Network, Statistics, Restart, Save Config and Upgrades) takes you to the corresponding page.

Note

When you make modifications to the configuration, remember to save the configuration and restart your M/MW for your changes to take effect.

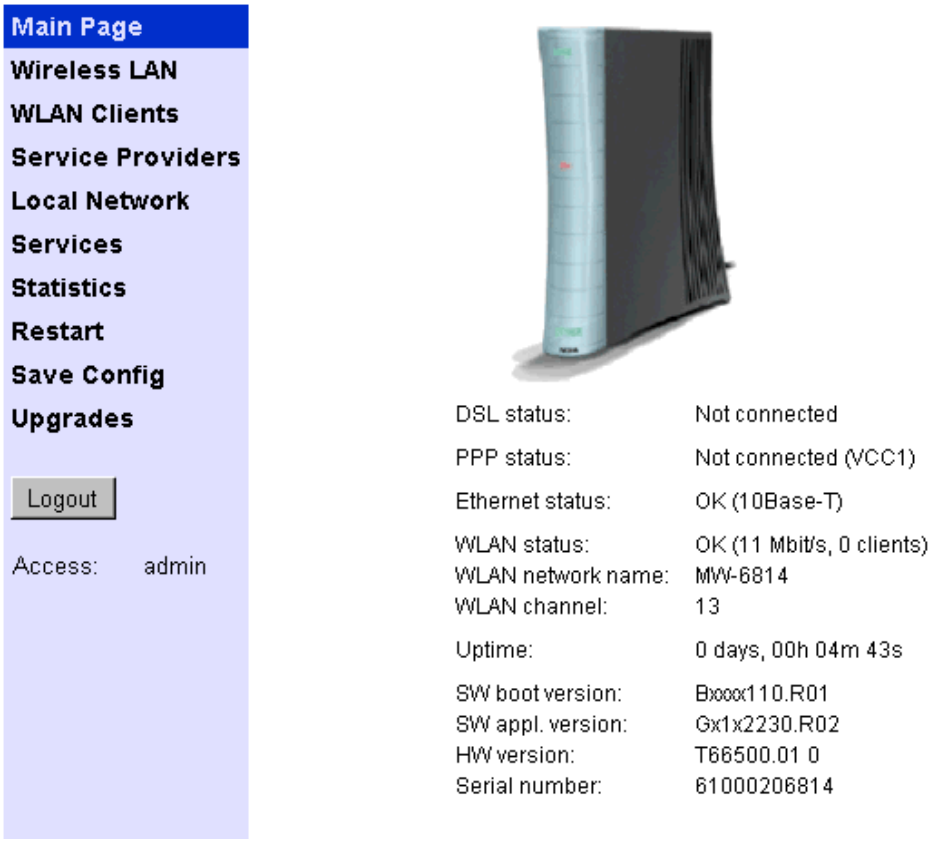

Figure 8. Main page

The **Main Page** shows you the statuses of the DSL line, Ethernet interface, HPNA (MW1324 only) 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 M/MW are shown at the bottom of the page.

4.3 Wireless LAN page

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

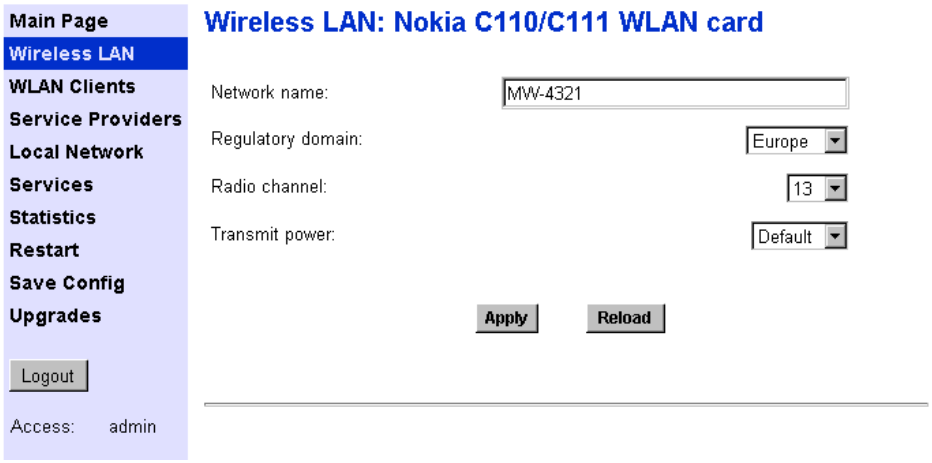

Figure 9. Wireless LAN page

Note

When you click the **Apply** button, the WLAN subsystem will be reset automatically. If you have changed the network name and you are accessing M/MW through the wireless connection, it will be disconnected. You must reconfigure the network name of the wireless LAN client to continue the 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.

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
France	10...13
Canada	1...11
USA	1...11
Japan	14

4.4 WLAN Clients page

On the **WLAN Clients** page you can enable access control based on the MAC addresses of the 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.

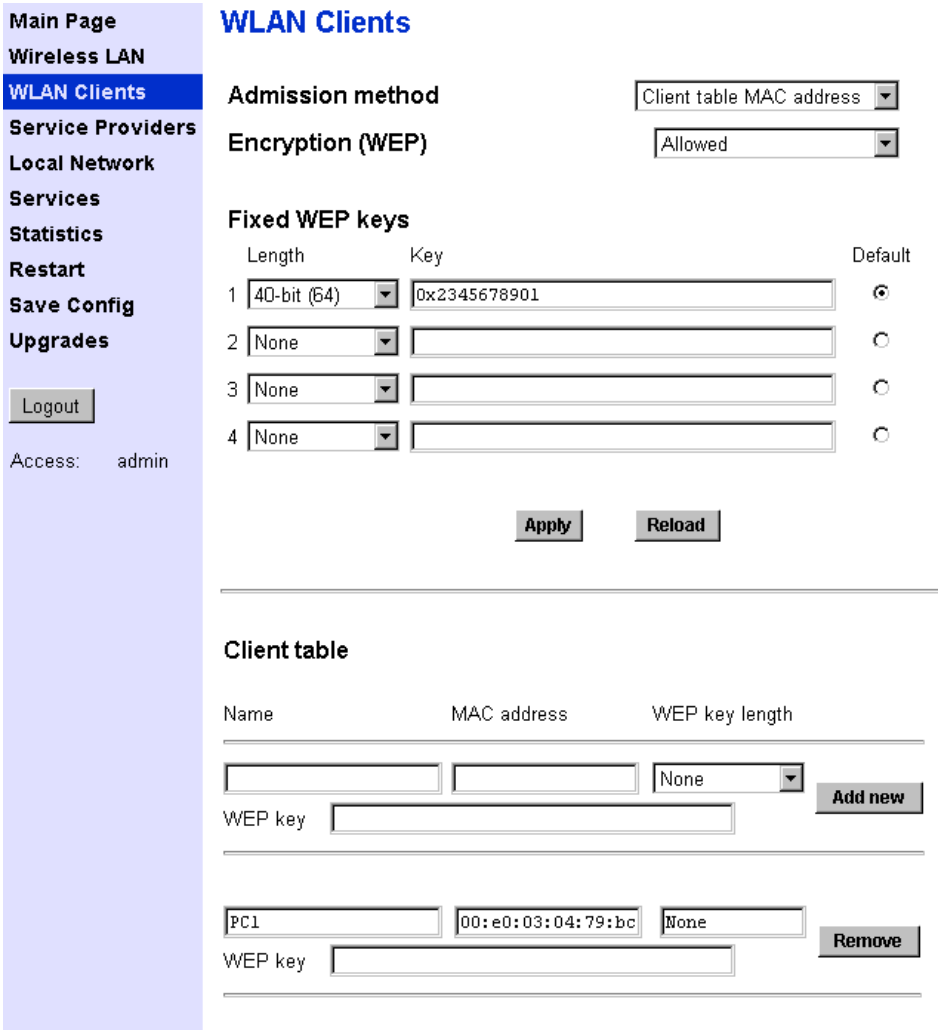

Figure 10. WLAN Clients page

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 in 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 the **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 and an additional station-specific key. Enter this key in the client table **Wep key** field.

You can enter the WEP keys in text or hexadecimal format. In text format, the allowed characters are: letters A–Z and a–z, numbers 0–9, and special characters , . ; : ! " # ¤ % & / ( ) = ?. In hexadecimal format, the allowed characters are: numbers 0–9 and letters a, b, c, d, e, and f. Note that the WEP key is case sensitive in text format. Table 7 shows the available key lengths. Give the hexadecimal keys in 0x1a3b5c7d9e format (i.e. insert *0x* in front of the key).

Table 7. WEP encryption keys

Key length	Format	Number of characters
40-bit	hexadecimal	10
104-bit	hexadecimal	26
128-bit	hexadecimal	32
40-bit	text	5
104-bit	text	13
128-bit	text	16

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 M/MW only, the wireless link will be disconnected until you have enabled encryption on both devices.

Note

Some WLAN client cards use 64 (40+24) bit keys. However, the actual key length of 40 bits must be used for M/MW.

There are five security modes which can be chosen from **Encryption (WEP)** 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, you must 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 key 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. A successful shared-key authentication results in an 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. 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 11 and 12 show the **WLAN Clients** page with default key and station-specific keys used, respectively. In Figure 11, 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 12, station PC1 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 and multicast.

Note

When you click the **Apply** button, the WLAN subsystem will be reset. If you have enabled the client table or changed the encryption mode and you are accessing M/MW through the wireless connection, the connection will be lost. You must reconfigure the wireless LAN client to continue the configuration.

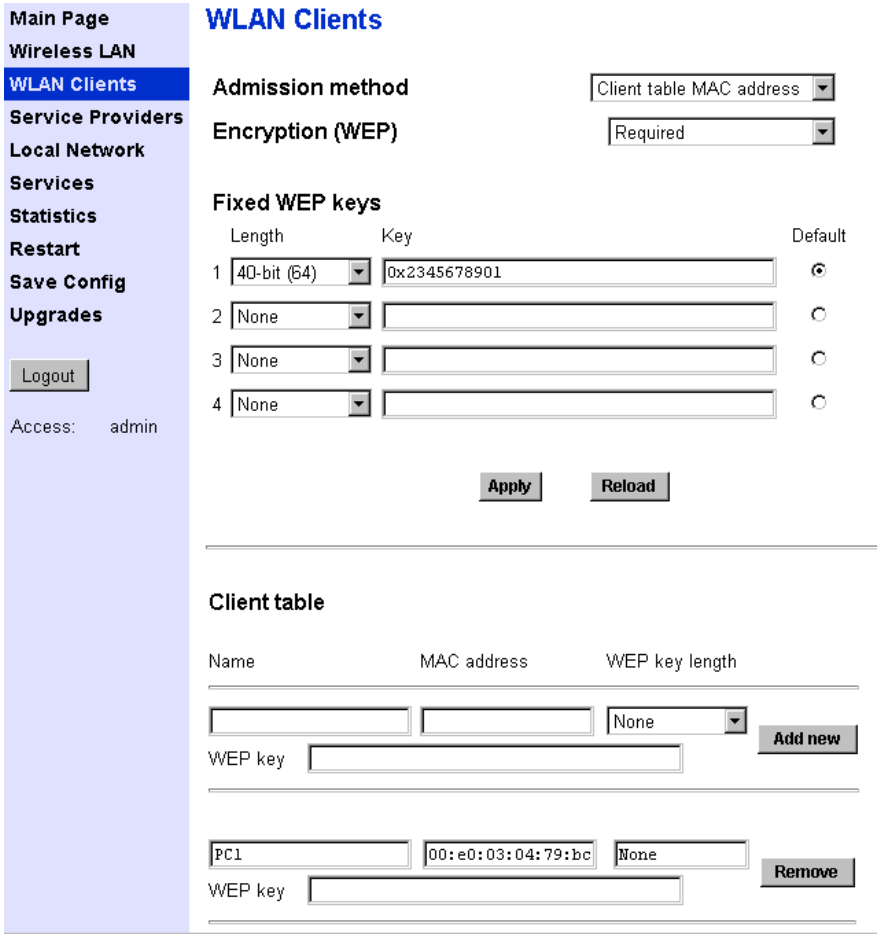

Figure 11. WLAN Clients page and default key encryption

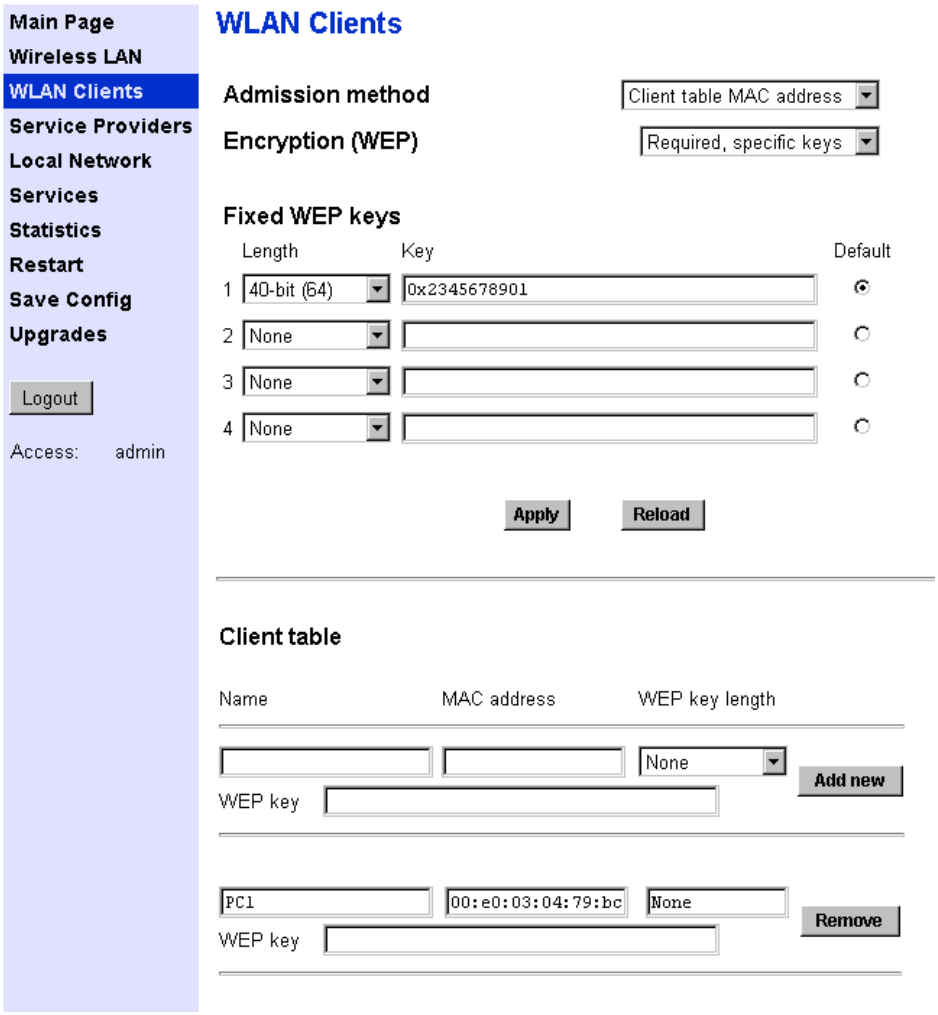

Figure 12. WLAN Clients page and station-specific key encryption

4.5 Service Providers pages

The **Service Providers** page can be used to set authentication for ATM VCCs with PPP encapsulation (Figure 13). 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 14). The name can be used in your PPTP client for tunnel configuration, see section *Point-to-Point Tunnelling Protocol*.

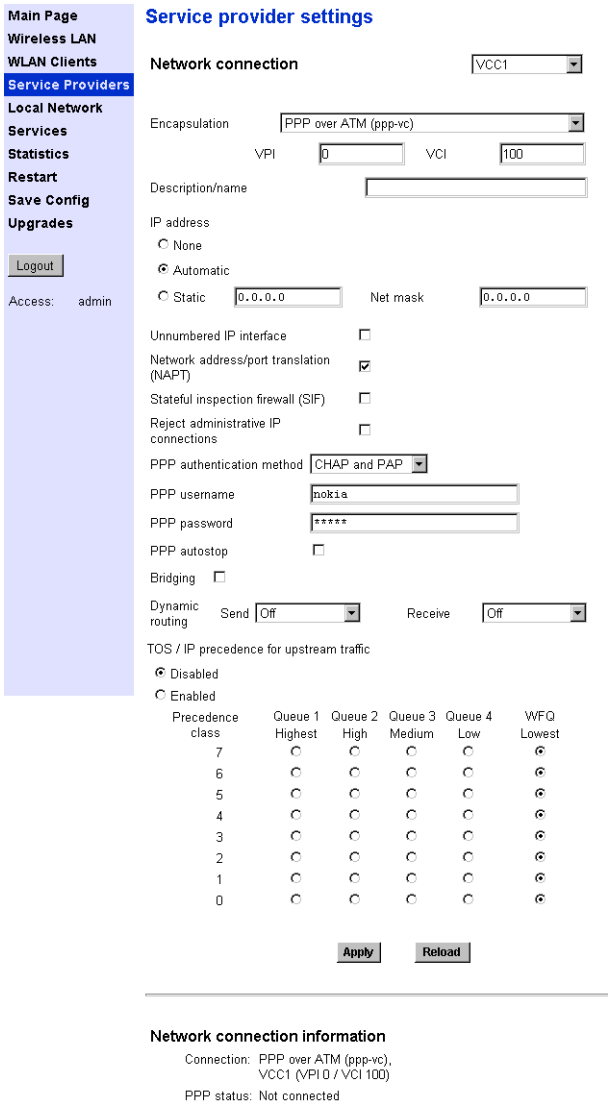

Figure 13. Service Providers page with PPP configuration

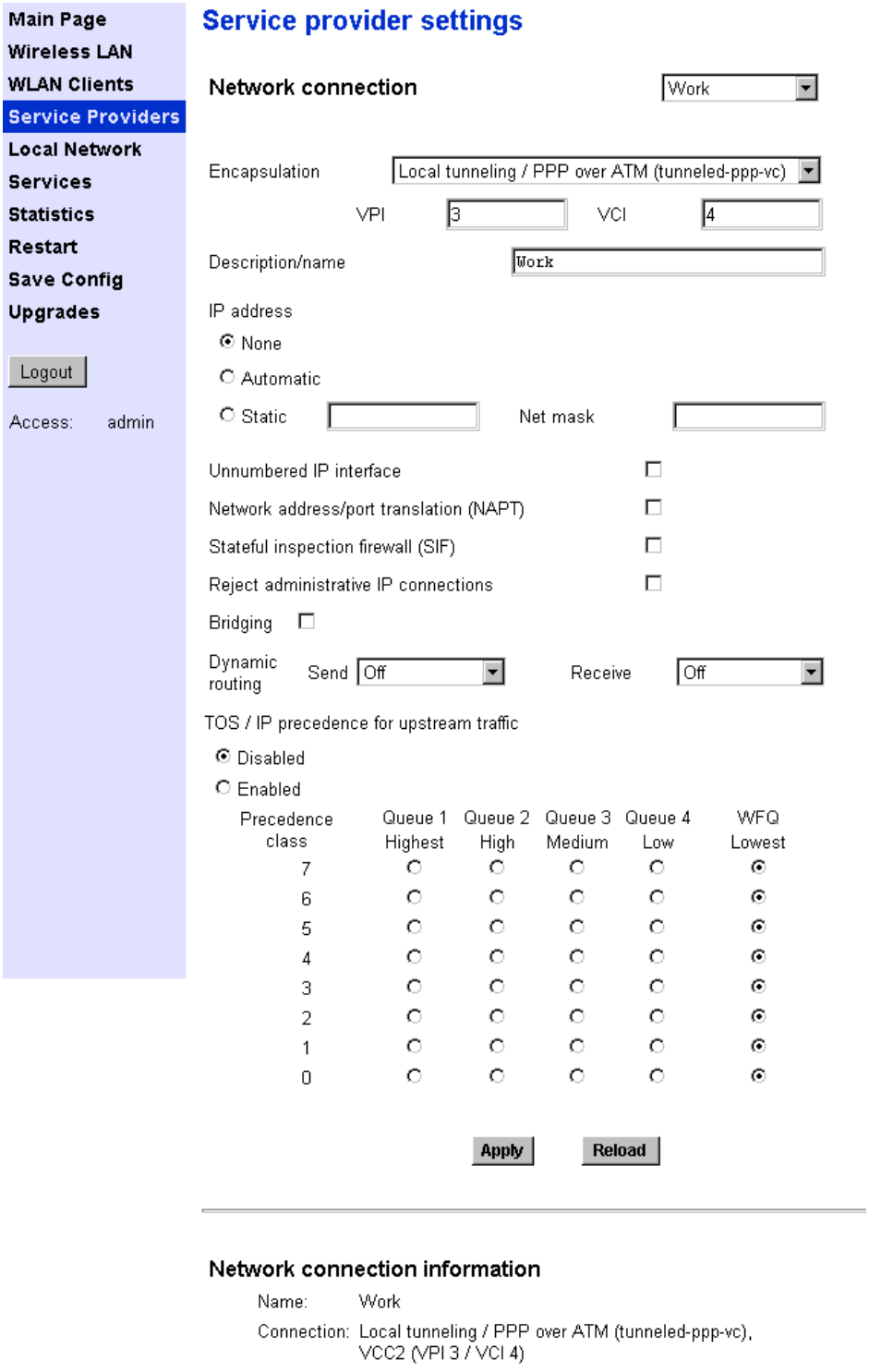

Figure 14. Service Providers page with PPTP configuration

4.6 Local Network pages

The **Local Network** page has three subpages: *Local ports*, *DHCP*, and *Routing*.

Local ports

On the *Local Network Local Ports* 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). HPNA interface is automatically slaved to the Ethernet. Hence, the Ethernet port configurations will apply to HPNA interface as well.

Note

When you click **Apply**, the IP addresses are changed immediately. If the IP address of the interface you are using change, 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. See below:

To request a new IP address in Win95/98

Click **Start**, and then click **Run**. In the **Open** box, type:

winipcfg	(IP dialogue box opens)
	Next, select
Release All	(IP address becomes 0.0.0.0)
	Then select
Renew All	(New IP address is assigned)

To request a new IP address in Windows NT and Windows 2000

Click **Start**, and then click **Run**. Type **cmd**. A DOS box opens.

In the DOS box, type **ipconfig/release**

Then type **ipconfig/renew**

Close the DOS box.

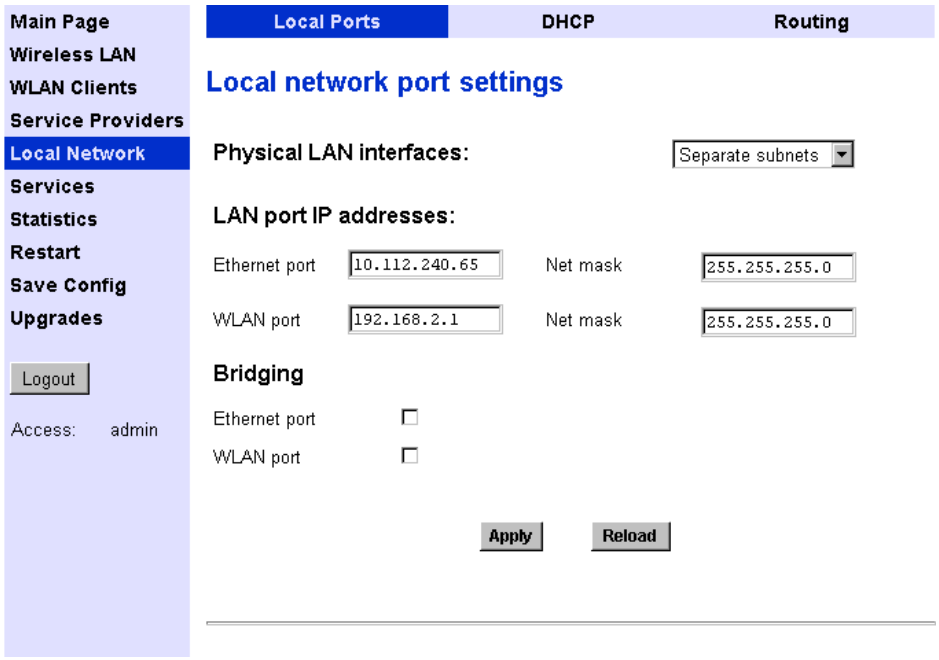

Figure 15. Local Network Local Ports page

DHCP

On the Local Network **DHCP** page 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. If a DHCP server is provided by the network (for example your service provider), the remote DHCP server can be supported through M/MW. In such a case local DHCP mode in your M/MW must be selected as DHCP Relay.

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 16, scope (a) has been bound to Ethernet interface and scope (b) to WLAN interface. When the address ranges are not defined, M/MW 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 is12 hours
- 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.

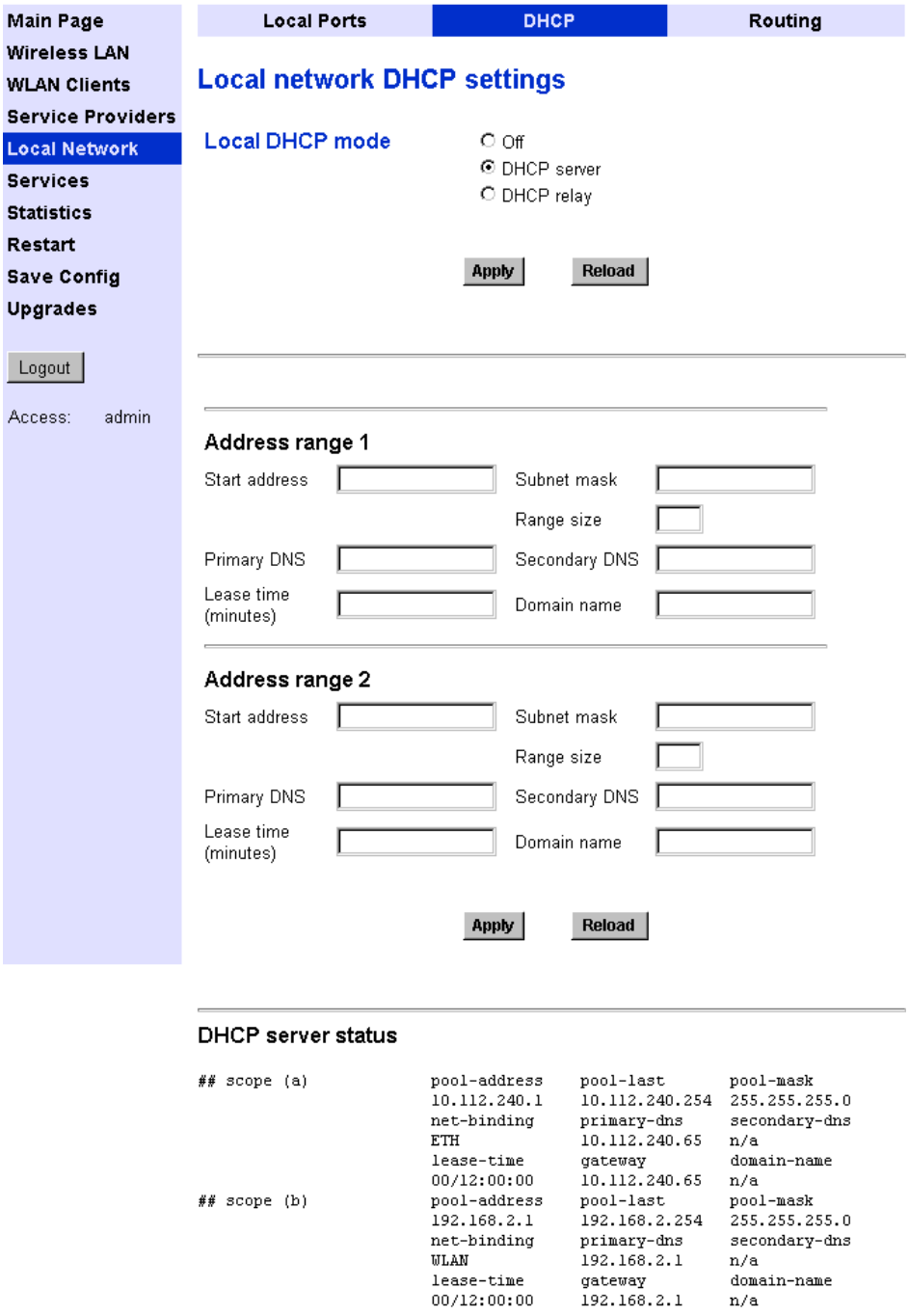

Figure 16. Local Network DHCP page with default values

Routing page

On the **Local Network Routing** 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 17.

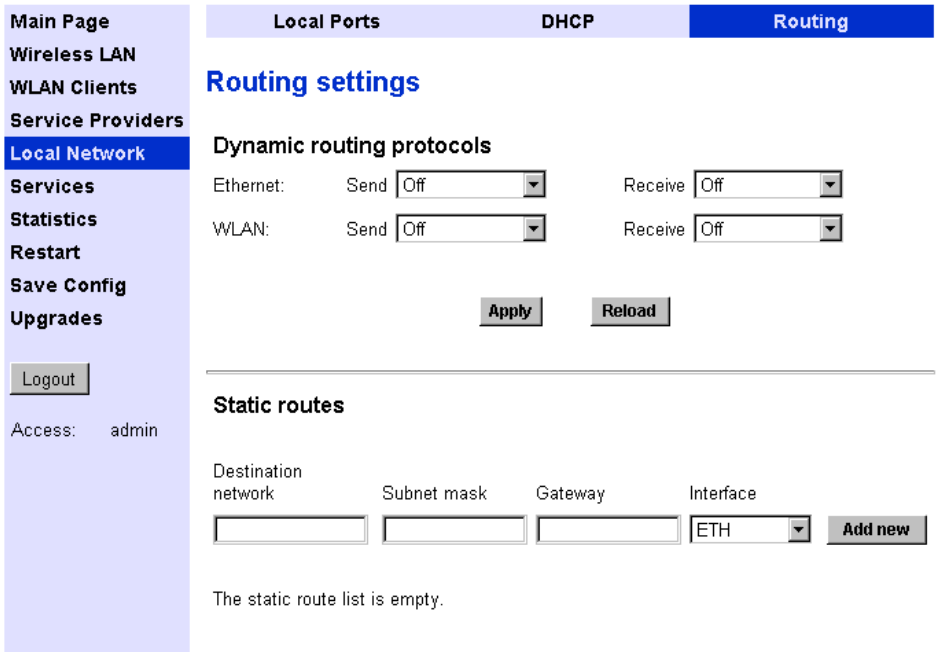

Figure 17. Local Network Routing page

4.7 Services

The Services are needed when Network Address and Port Translation (NAPT) or Firewalling (SIF) are in use and there are servers (for example a web server) inside LAN accessed from the WAN. By creating server entries into NAPT or SIF the defined servers become visible to the outside network. For a server, an entry is created by combining LAN IP address or subnet with the service name. M/MW has a number of predefined services from the most common applications. If the desired application is missing, the services pages allow the user to define new services

Names

Service name identifies a supported service. Each service needs to have a name, protocol and port number/range defined. New services can be added by filling in the above mentioned parameters next to the 'Add new' button clicking the button. The added service name is added to the service list. Existing service names can be removed by clicking the 'Remove' button next to the service which you want to remove. Predefined entries (listed below the user defined services) cannot be removed.

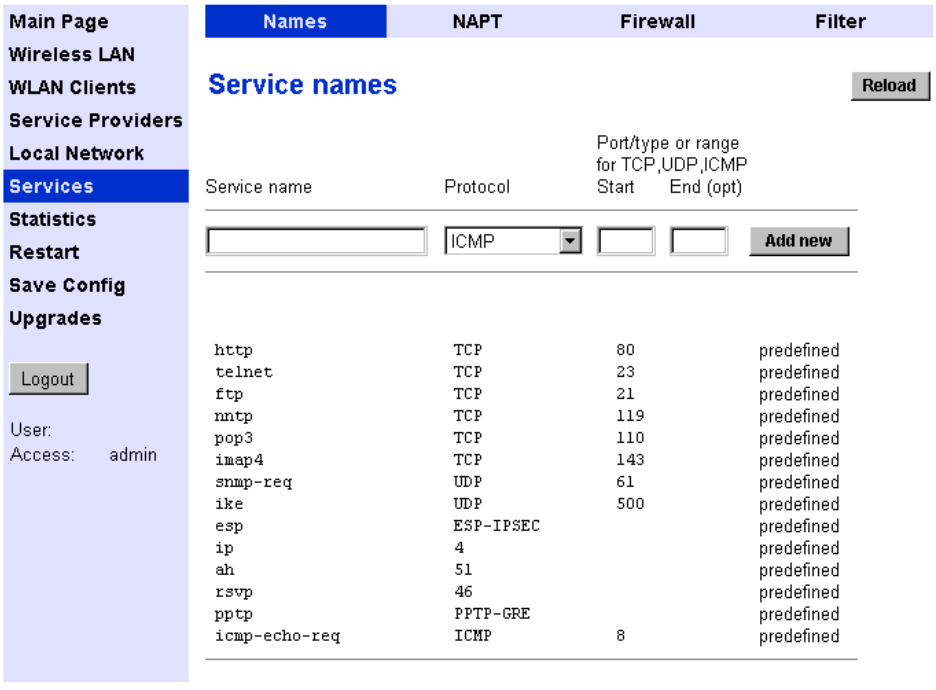

Figure 18. Services names page

NAPT

If Network Address Port Translation (NAPT) has been activated, the 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. The NAPT server support page has two main operational modes. The mode is selected by the 'Network Connection' pull down menu. The first selection is 'Global', which means that all server support configurations done are based on defined Service names and are used with all VCCs, Figure 19. By selecting a specific VCC (for example VCC 1), another page view is shown, where server support configurations can be defined for that selected ATM (VCC) connection. It is recommended that only Global configurations are to be used unless some specific need require otherwise.

In the example shown in Figure 20, a pinhole has been added on the **Server list**. This example means that all TCP traffic coming from the Internet through **Work** to ports 80...89 will be mapped to the IP address 192.168.1.2 ports 90...99 on your local network.

Global NAPT entries are added by selecting “Global” from the Network connection menu and by filling in the appropriate service name (from the Names page), private LAN IP address and, optionally, WAN port number, if it is different from the port number set for the service. For example, selecting number 90 for http service adds a server entry that maps TCP port 90 to the LAN IP address port 80 as defined in predefined http service

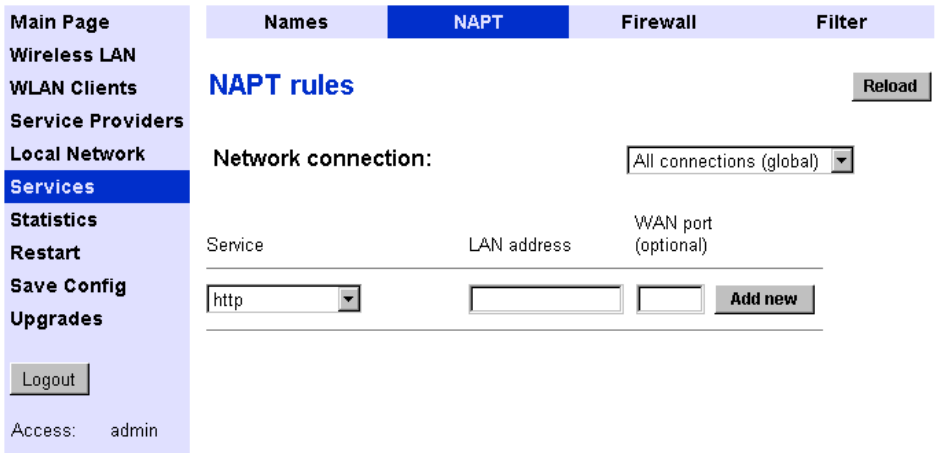

Figure 19. Services NAPT page (global)

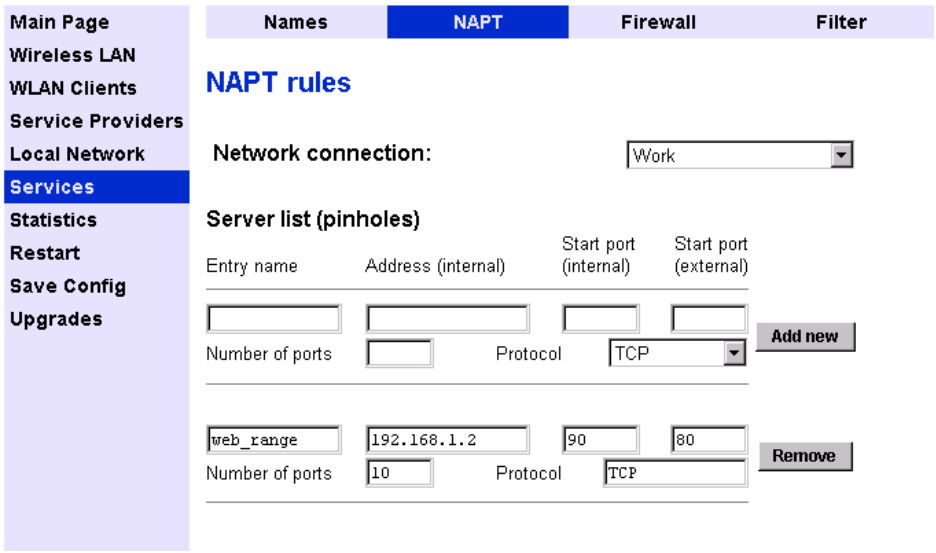

Figure 20. Services NAPT page (specific VCC)

Firewall

Firewall rules are used to set the server entries for Stateful Inspection Firewall (SIF). Entry is added by selecting service name and defining an IP address or address range. Entries can be removed by clicking **Remove** button next to the appropriate service entry line.

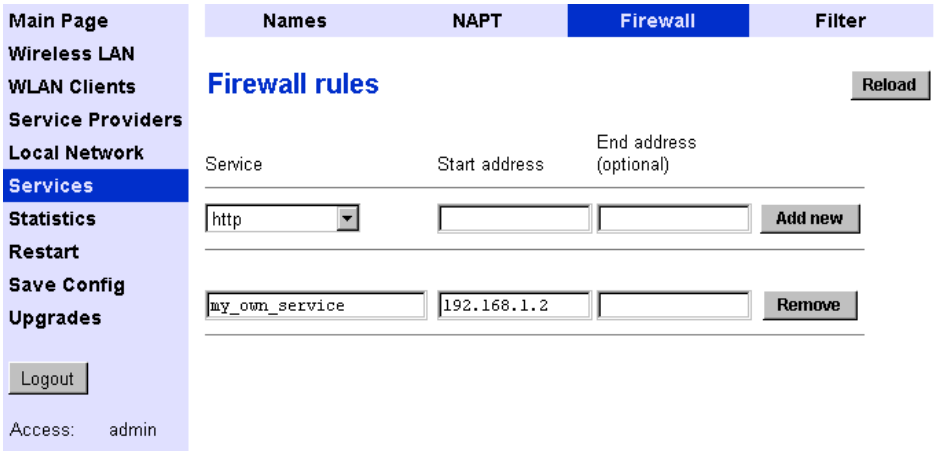

Figure 21. Firewall page

Filter

IP filter option filters ip packets originated from local are network towards wide area network (vcc). Filtering function depends on the service description, (service can be predefined like ftp, telnet, http or user defined) source address or addresses, destination address or addresses and filtering rule. In addition to filtering it is possible to set the diffserv field of ip header (for example the field originally defined as type-of-service or tos in rfc791 and redefined later when the concept of differiciated services has emerged) of packets subject to filtering with predefined values to indicate the level of precedence as desired. The predefind values account for compliant with the class selector (csc-0..csc-7), assured forwarding class (af-11..af-43) and expedited forwarding phb (ef).

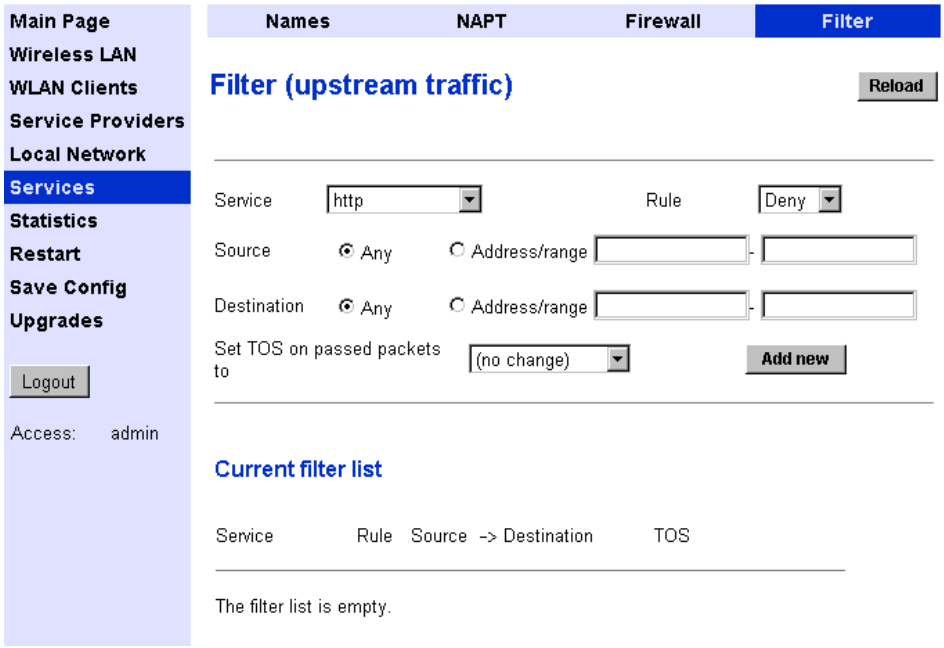

Figure 22. Filter page

4.8 Statistics page

The **Statistics** page lets you view a selection of M/MW statistics. To view the statistics of a particular function, click the corresponding button and the statistics view is opened in a separate window.

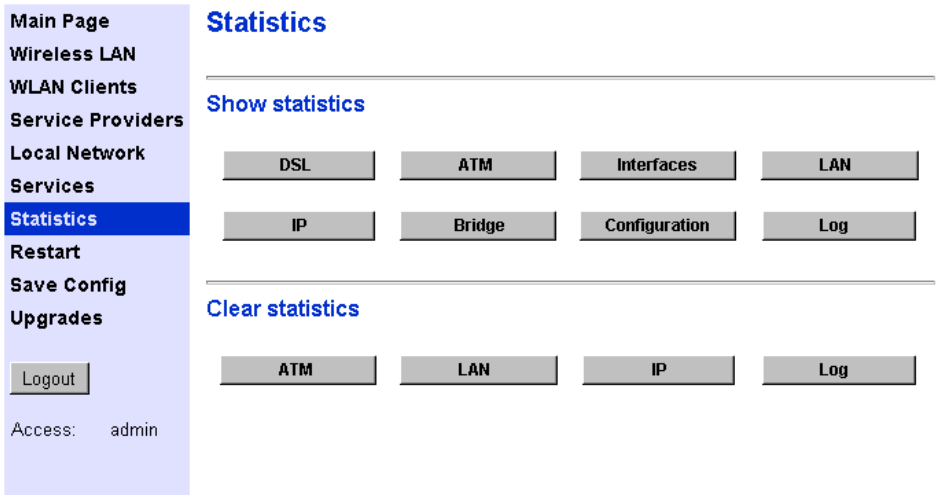

Figure 23. Statistics page

4.9 Restart page

On the **Restart** page, you can reset subsystems and restart M/MW.

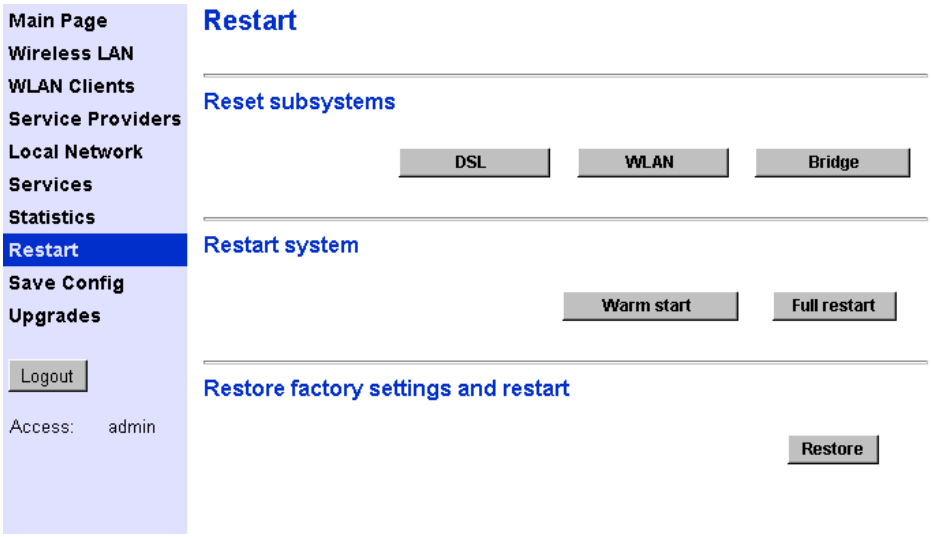

Figure 24. Restart page

4.10 Save Config page

When you change configuration, all configuration changes are activated immediately without restart/reload. However, the configuration will not be saved into the nonvolatile memory. If M/MW 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 after that the old configuration cannot be restored through the web interface.

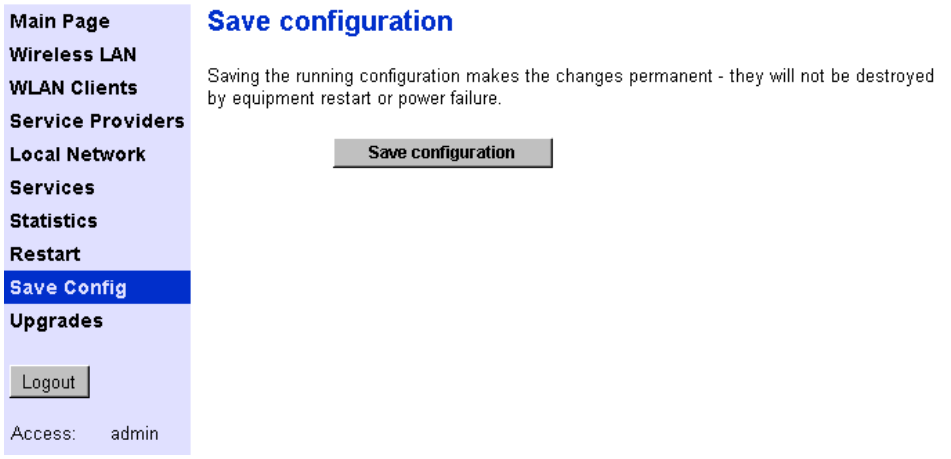

Figure 25. Save Config page

4.11 Upgrades

The Upgrade page is used to upgrade the application SW of M/MW. A new application is loaded by pressing **load new** button and selecting **new application file** (New file must be downloaded prior to the operation to PC/MAC local storage). By default, M/MW has an active application file and backup application file. Sometimes the application size might exceed the flash size resulting in that there is no additional space for a backup application. Should this happen there is a delete button which allows you to delete application files.

Caution

If delete is used and the application file and existing backup files are removed you must also load a new application. Otherwise when the system restarts, the application file is missing and a new application must be loaded through the CLI interface.

In Admin mode it is also possible to load a new configuration (or any) file in a similar way. Restart is required to activate the new configuration file (or local command from CLI).

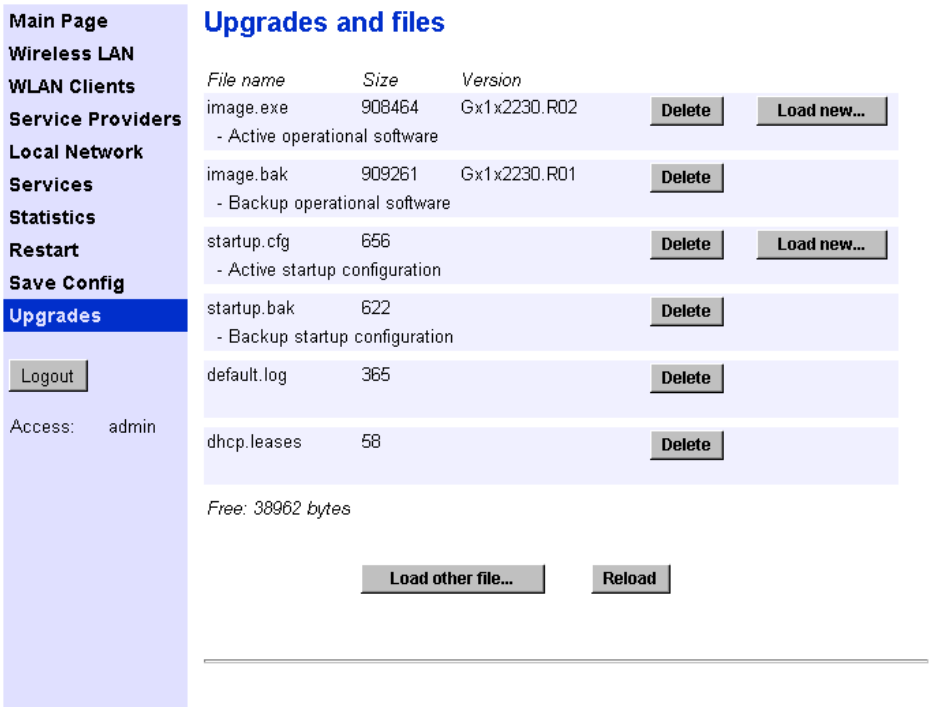

Figure 26. Upgrades page of M/MW in Admin mode

5 Features

M/MW 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. The HPNA interface of MW1324 is automatically slaved to the Ethernet.

5.1 Interfaces

M/MW has the following interfaces:

- Ethernet interface (ETH)
- MW1324 only: HomePNA 2.0 Interface (HPNA)
- Wireless LAN interface (MW series only)
- 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 M/MW web pages, the interface is called gateway or bridge IP interface.

M/MW can operate in four different main modes:

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

The mode in which M/MW operates depends on the configuration of the unit's interfaces.

Ethernet and WLAN interfaces

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

Slaved HPNA operation (MW1324 only)

The HPNA interface operation mode defaults to a mode where it operates as slaved to Ethernet. This mode is identical to WLAN slaved to Ethernet mode resulting that there is no need to change separate IP and/or Bridging configuration. Once active, HPNA client is connected to the Ethernet LAN network as M/MW, and the HPNA LED lights up. No additional configuration is needed.

Internal host/gateway interface

There is a special host/gateway logical IP interface within M/MW called VBRIDGE. This interface has a specific purpose in M/MW. 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 ETH/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

M/MW 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)
- RFC2516 PPPOE encapsulation using ETH-LLC (PPPOE-LLC)

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. 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).

5.2 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. M/MW supports up to 8 simultaneous VCCs.

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

5.3 Bridging

Bridging is supported to provide full protocol transparency. Bridging can be used simultaneously with IP routing. M/MW 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, bridging between the VCCs can be disabled.

5.4 Network Address Port Translation

M/MW 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 the 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 27.

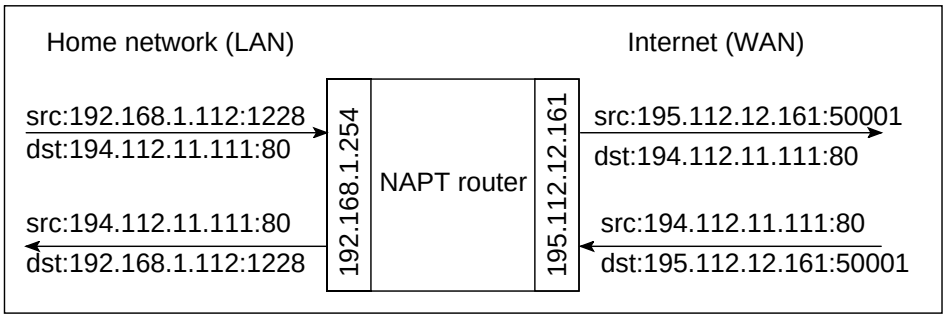

Figure 27. Principle of Network Address Port Translation

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 function (ALG). M/MW 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.

Global NAPT server entries are active for all possible ATM VCC that have NAPT enabled. In a typical application only one VCC exists resulting in that global and per VCC NAPT operates identically.

By default M/MW discards all packets received from the Internet that do not have a corresponding entry in the connection table or in the server entries except Telnet and HTTP. Answering the ICMP echo request can be enabled by defining server entry *"icmp-echo-request"* with IP address 0.0.0.0. Telnet and HTTP access can also be disabled on each VCC.

5.5 Stateful Inspection Firewall

Stateful Inspection Firewall (SIF) is used to filter the packets automatically in router mode when NAPT cannot be used. SIF creates, in the same way as NAPT, the connection entries for outgoing packets based on their IP source address, IP destination address, protocol, TCP/UDP source port (optional), TCP destination port, or ICMP type code. SIF allows only packets belonging to these connections to pass through M/MW from VCC. If server entries are needed, the Firewall page is used to define the entries.

When Firewall (SIF) is enabled, by default M/MW discards all packets received from the Internet that do not have a corresponding entry in the connection table or in the server entries except Telnet and HTTP. Answering the ICMP echo request can be enabled by defining server entry *"icmp-echo-request"* with IP address 0.0.0.0. Telnet and HTTP access can also be disabled on each VCC.

5.6 Dynamic Host Configuration Protocol

M/MW can act as a Dynamic Host Configuration Protocol (DHCP) server for the PCs on the user's home network. In this mode, M/MW 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. M/MW can also act as a DHCP relay agent and relay the DHCP requests to an external DHCP server.

DHCP client can be enabled on each interface (vcc, eth, vbridge). It is used to retrieve IP address, IP subnet, DNS and Default Gateway configurations automatically just like PPP is able to do. In general, DHCP is more flexible and allows more options than PPP. The only exception at the moment is the lack of authentication in DHCP. This means that if authentication is needed, PPP should be used.

5.7 DNS server and Relay

M/MW has a DNS server which is able to resolve its own name using DNS or netbios DNS. If M/MW is not able to resolve the requested DNS request, the message is forwarded to other DNS servers. The other DNS servers are learned dynamically (PPP or DHCP) or can be configured manually.

5.8 ATM and ADSL

M/MW 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 are 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. M/MW provides a DMT data transmission 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. M/MW supports also ADSL Lite. In the ADSL Lite mode, the maximum line rates are 1536 kbit/s downstream and 512 kbit/s upstream.

M/MW 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 M/MW functions automatically and all configurations related to the ADSL connection are 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 function provided by Nokia DSLAM.

5.9 Point-to-Point Tunnelling Protocol (PPTP)

When PPTP local tunnelling is used, a local network client initialises a PPTP-tunnelled PPP connection (VPN) to Nokia M/MW. 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 tunnelling is used when there is a need to have one or more computers connected independently to different networks. For example, in a remote work application, while the rest of the family may be using the common ISP services, one or two family members need to gain access to their corporate networks. With local tunnelling, these remote workers may be connected to a different network than the rest of the users.

Local tunnelling is activated using the PPTP client. In Windows, the Destination IP address must be M/MW LAN/WLAN/VBRIDGE IP address depending on the configuration. PPP packets within PPTP are mapped to the configured VCC. M/MW has three different ways to choose the ATM VCC that are used for tunnelling:

- Automatic, chooses the first free VCC
- Chooses the VCC number using C:number, where number is from 1 to 8. C:number is entered after the M/MW IP address (see Figure 28).
- Chooses the VCC number using N:name, where name is the VCCx description. N:name is entered after the M/MW IP address.

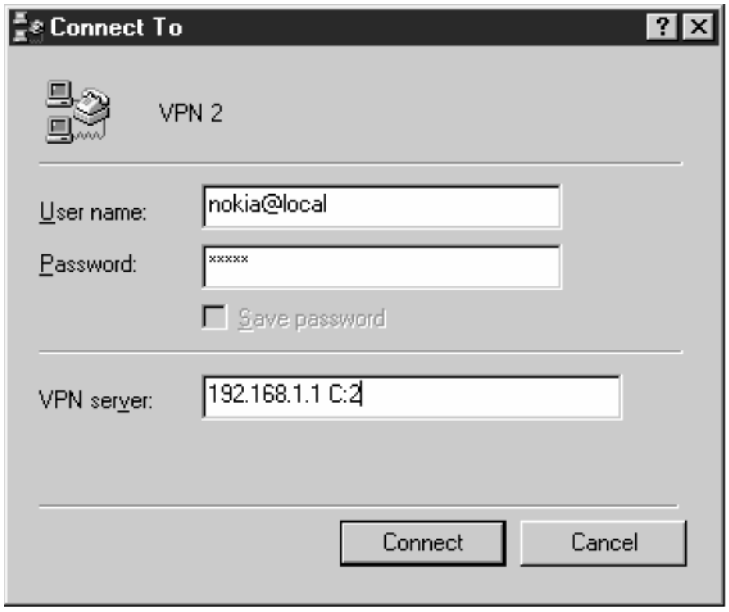

Figure 28. Choosing the VCC2 for tunnelling example

When PPPoE is used as encapsulation the PPTP session can also be directed to this VCC. Also up to 8 concurrent sessions will be supported.

5.10 Gateway operating as PPPoE router

The standard PPPoE mode is used when M/MW is operating as a bridge. The PPPoE protocol defines how PPP sessions are mapped into Ethernet packets. When M/MW operates as a bridge, this protocol is transparent to M/MW. In the bridge mode it is possible to define a specific “PPPoE-Bridging-only” mode that discards all other than PPPoE packets.

In **Router mode** the M/MW's PPPoE client mode allows the M/MW to transfer PPP packets over the Ethernet frames. This application is similar to the standard PPP but the packet capsulation is different. PPPoE packets are transmitted within the Ethernet frames. The extra PPPoE header requires an additional 8 Bytes of information resulting in that the maximum MTU for the PPPoE interface is 1492 instead of the standard MTU of 1500.

The PPPoE session begins with the Discovery phase which consists of 4 messages. During this phase the host selects which PPPoE server is to be used, and a session id is agreed. When M/MW's PPPoE client mode is active, the first PPPoE server from the network is always used.

5.11 Payload encapsulations

Both routed and bridged protocols are encapsulated in the ATM link by using either RFC 2684 LLC/SNAP encapsulation or VC multiplexing. M/MW 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.When PPPoE capsulation is used, the PPP packets are first encapsulated using RFC 2516 PPPoE framing and transported as defined in RFC 2684.

5.12 Access list authorisation

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

5.13 Wireless LAN and radio interface

MW supports wireless LAN to be used as one of the interfaces. The wireless LAN utilises Nokia C110/C111 Wireless LAN PC card which must be inserted into the designated PC Card slot on the back panel of the modem. Only Nokia C110 or C111 Wireless LAN cards can be used. MW supports 64 WLAN clients. Without a wireless LAN card, MW operates as a normal ADSL terminal with one 10Base-T Ethernet interface. The wireless LAN card can be inserted into the PC Card slot while the modem is operating, and the wireless LAN connectivity is established without restarting the modem. Only the WLAN subsystem must be reset through the web interface or the command line interface (CLI).

Wireless LAN used in MW is based on IEEE802.11b standard operating at 2.4 GHz radio band. The band is 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 giving a typical indoor coverage of 20 to 50 metres. It is recommended that MW is located as centrally as possible within the area to be covered, because the indoor coverage is highly dependent on inner walls between the client and MW.

5.14 Wired Equivalent Privacy (WEP)

M/MW 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, M/MW supports both 104 and 128 bit RC4 WEP encryption

Some WLAN client cards on the market have only 64 bit encryption but is in reality 40 bit RC4 plus 24 bit Initialisation vector. Thus the mode is identical to M/MW 40 bit encryption because the IV is not part of the key length.

In M/MW the 128 bit key is really 128 bit and is therefore not compatible with some 128 bit keys which are in reality 104 bit because of the same interpretation.

5.15 Weighted Fair Queueing (Class of Service)

As a Class of Service (CoS) function, M/MW 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.

By using TOS-mapping it is possible to handle Class of Service. TOS-mapping allocates IP packets from the local area network with one of the five transmit queues implemented by the Gateway.

5.16 IGMP proxy support

M/MW can operate as an IGMP proxy. It can send IGMP Host Membership Queries to all hosts on its local network to learn about the host group members. The host group members respond by sending Host Membership Reports to the IGMP proxy. When the IGMP proxy receives a multicast transmission, it maps the host group address to the associated hardware address.

6 Main functions

6.1 M/MW operating as a NAPT router

In this mode M/MW has the following functions:

- Private IP addressing on the LAN side
- Single subnet for all LAN interface or separate subnets
- DHCP server on the LAN side, one or more address range/scope
- LAN interface acting as DNS server/relay and Default Gateway
- PPPoA-VCC, PPPoE-LLC or ETH-LLC with DHCP client on VCC side
- NAPT enabled
- The only active VCC is configured to act as the default gateway
- Dynamic IP address learned via PPP or DHCP

- DNS servers learned via PPP or DHCP
- Default gateway is the PPP peer or address learned via DHCP

M/MW distributes the LAN configuration using the built-in DHCP server. The DHCP server supplies the IP address, IP subnet mask, DNS-address (LAN port address) and Default Gateway Address (LAN port address).

When M/MW receives the DNS request, it forwards the request to all DNS servers learned by DHCP/PPP until one of the servers is chosen as the master server. M/MW then receives the DNS reply and forwards it to the requesting host. In addition to DNS relaying, the M/MW is able to resolve its own name/address using DNS or Netbios protocols.

Similarly, when normal data packets destined to VCC are received from LAN, they are transmitted to the default gateway. In NAPT operation, the source IP address and TCP/UDP source port or ICMP echo request identifier are changed to one taken from VCC interface pool and the entry is added/updated into the connection table. When packets are received, the connection table is scanned and the packet is forwarded to the original host. Connections initiated from the VCC side are dropped unless a server entry is found for that service. In this case, a temporary entry is created.

6.2 M/MW operating as a standard router

In this mode the M/MW requires some static configuration. When M/MW is acting as a standard router, the public IP addresses are used on LAN and VCC side and NAT/NAPT is not used. In this case LAN configurations must be made manually.

The WAN side can be configured manually or dynamically using the PPP/DHCP client on the VCC. The M/MW can act as DHCP relay forwarding the DHCP request to a predefined DHCP server. Thus, the service provided has full control of the LAN configuration.

Routing is based on static routes, or RIP v1/v2 is used to dynamically learn/ distribute the routing information. The Stateful Inspection Firewall (SIF) function can be enabled for each VCC. When enabled, the connection initiated from LAN saves the session data into the database and only responses to those sessions are routed through the M/MW back to LAN. Connections initiated from the VCC side are dropped unless a server entry is found for that service. In this case a temporary entry is created. All other packets are dropped.

6.3 M/MW operating as a standard bridge

In this mode the M/MW functions on a plug and play basis. A similar configuration can be used for all customers. M/MW maps the Ethernet packets to ATM VCC and vice versa. The DHCP server is located on your service provider's network and is used for allocating the IP configuration to the LAN.

If management access to M/MW is needed then

- DHCP client can be configured on VBRIDGE interface
- Management VCC can be configured to use static or Dynamic IP address allocation depending on the encapsulation model.

6.4 M/MW operating as a NAPT router and PPPoE bridge

It is possible to configure the M/MW to act as NAPT router using PPPoE VCC encapsulation and at the same time also Bridge the LAN host initiated PPPoE packets. The configuration is similar to the NAPT router configuration except that:

- PPPoE-LLC encapsulation must be used
- Bridging must be enabled on this VCC
- Bridging is enabled also on LAN

7 Configuration

This shows some configuration examples of M/MW. The examples can be used as a guide when you are planning your configuration. The command line interface (CLI) is presented in Chapter8. The command line interface section contains all CLI commands.

7.1 Configuration examples

This section presents some typical configuration examples. Figure 29 shows a general block diagram of the IP forwarding and bridging functions of M/MW. In the following configuration examples the outputs are not displayed in full.

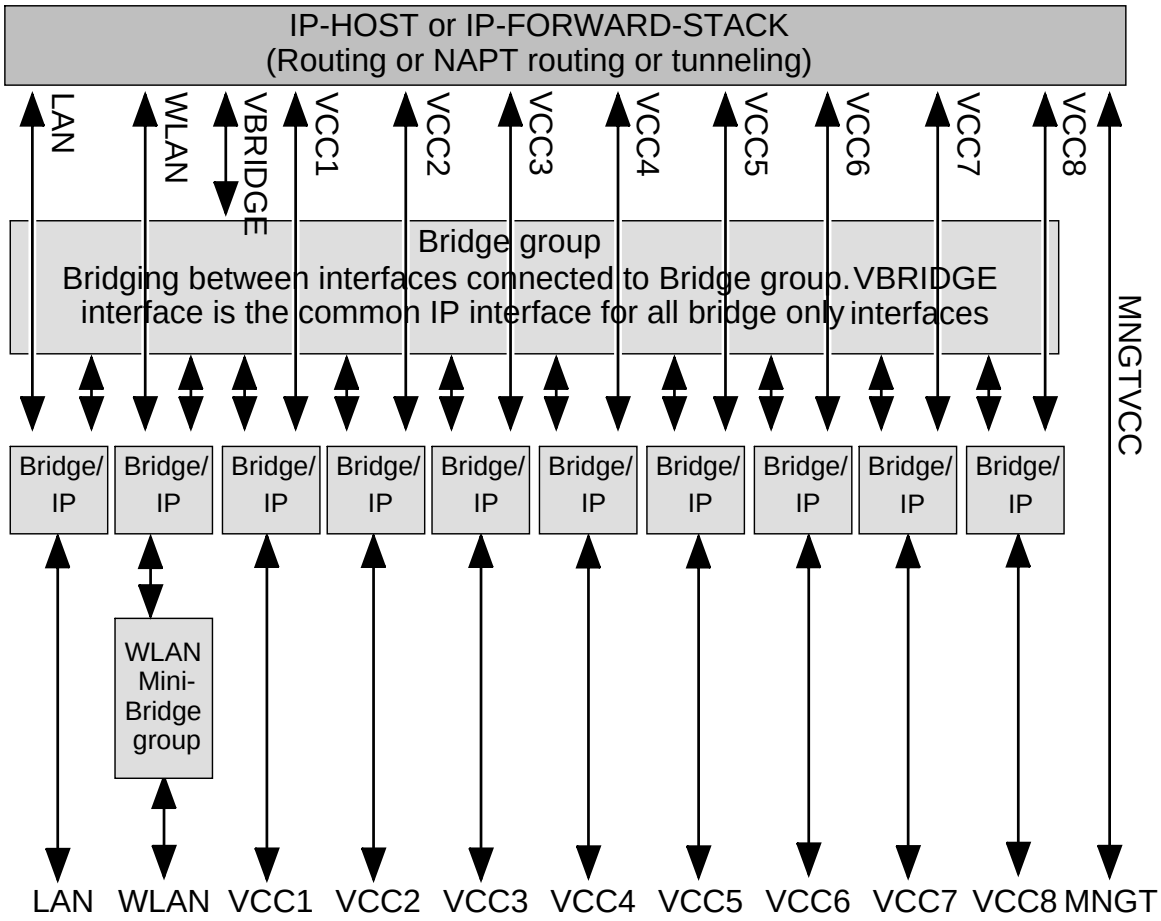

Figure 29. Block diagram

7.1.1 Routing/tunnelling IP only

If the application requires only routing of IP packets, an IP address should be configured for each interface in use. The example below shows a typical configuration in such a case.

```
MW1122> show conf running

eth

   ip address 192.168.1.1 255.255.255.0

wlan
```

```
   network-name nokia

   radio-channel europe 13

   ip address 192.168.2.1 255.255.255.0

vcc1

   pvc 0 101 ip-llc

   ip address 10.98.16.1 255.255.255.0

com

   ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1
```

7.1.2 Routing/tunnelling IP, bridging other protocols

When the application requires routing IP packets and bridging all other protocols, then IP address has to be configured and bridging enabled for all relevant interfaces. The result is that IP packets will be routed and all other packets will be bridged. In the configuration example below, Ethernet and WLAN interfaces route IP traffic and bridge all other protocols. ATM VCC1 routes IP traffic and ATM VCC2 interfaces bridges all traffic.

```
MW1122> show config running

eth

   ip address 192.168.1.1 255.255.255.0

   bridging

wlan

   network-name nokia

   radio-channel europe 13

   ip address 192.168.2.1 255.255.255.0

   bridging

vcc1

   pvc 0 101 ip-llc

   ip address 10.98.16.1 255.255.255.0

vcc2
```

```
   pvc 0 102 eth-llc

   bridging
```

7.1.3 Routing/tunnelling IP, bridging all protocols including IP

When IP packets that are received from LAN/WLAN must be routed/tunnelled to some ATM VCC and bridged to some other ATM VCC, then the VBRIDGE interface must be used as this common IP interface for all bridged interfaces. In this case, Ethernet and WLAN interfaces are configured as bridge only.

```
MW1122> show config running

eth

   bridging

wlan

   network-name nokia

   radio-channel europe 13

   bridging

vcc1

   pvc 0 101 ip-llc

   ip address 10.98.16.1 255.255.255.0

vcc2

   pvc 0 102 tunnelled-ppp-vc

vcc3

   pvc 0 103 eth-llc

   bridging

vbridge

     ip address 192.168.1.1 255.255.255.0
```

7.1.4 Bridging only

When only bridging is required, all ATM VCCs are configured as bridge. VBRIDGE IP address can be used as an optional management interface.

```
MW1122> show config running

eth

   bridging

wlan

   network-name nokia

   radio-channel europe 13

   bridging

vcc1

   pvc 0 101 eth-llc

   bridging

vcc2

   pvc 0 102 eth-llc

   bridging

vbridge

     ip address 192.168.1.1 255.255.255.0
```

7.1.5 Routing/tunnelling IP only using slaved WLAN

In all of the above examples slaved WLAN interface can be used instead of a dedicated configuration. When WLAN is slaved to LAN interface, all traffic will be bridged between the Ethernet and WLAN interfaces and treated like traffic received from the Ethernet interface only. Similarly, all traffic from ADSL/ SHDSL/ATM channels will be directed to the logical LAN interface where it is bridged internally and directed to the physical Ethernet and/or WLAN interface.

```
MW1122> show config running

eth

   ip address 192.168.1.1 255.255.255.0

wlan

   network-name nokia

   radio-channel europe 13
```

```
   slave-to-eth

vcc1

   pvc 0 100 ip-llc

   ip address 10.98.16.1 255.255.255.0

MW1122>
```

7.2 Typical configuration tasks

This section provides some typical configuration tasks. These configuration examples can be done through the command line interface.

Note

After you have made changes to the configuration, you must save the configuration if you want it to be active also after restarting M/MW.

7.2.1 Configuring null password

The null-password concept allows M/MW to be configured to request a password. If no password is entered, the user gets access to configured user/user-admin levels. The password is used only for admin levels and only one null password must be used. The configuration is done by entering a special command string **$null-password$** which allows to bypass the password request in a selected access mode. The password is still requested but not required.

```
MW1122(conf-password)#
MW1122(conf-password)#admin secret
MW1122(conf-password)#napt-user $null-password$
```

7.2.2 Configuring DHCP and DNS

The DHCP server can be enabled towards LAN, WLAN, and VBRIDGE ports. When the DHCP server is enabled, up to two address ranges (scopes) will be automatically generated and bound to LAN/WLAN/VBRIDGE interfaces, in this order if the interface has an IP address. Two address ranges will be required when LAN and WLAN interfaces separate IP addresses resulting that two different address spaces will be used, one for each interface.

The address range defines a pool of IP addresses and parameters like default gateway, DNS addresses and domain name (text). The generated default address range allows up to 253 IP addresses (C class). Automatically generated address ranges use LAN/WLAN/VBRIDGE IP address as gateway and DNS server addresses. If one address range is defined, then automatic binding will be disabled. If optional address range parameters like gateway or DNS addresses are not defined, LAN/WLAN/VBRIDGE IP addresses are used as in automatic binding.

Typically, when DHCP is used, the advertised DNS addresses point to LAN/WLAN/VBRIDGE interfaces. In such cases, the DNS proxy forwards the DNS request to statically configured DNS servers or to DNS servers learned dynamically via PPP/IPCP.

The following commands are used to configure DHCP and DNS settings:

```
MW1122(conf-common)#dhcp?

usage: dhcp mode

   dhcp address

   dhcp gateway

   dhcp dns

   dhcp lease-time

   dhcp domain-name

   dhcp relay-addr

MW1122(conf-common)#dhcp mode server ; this enables DHCP server
```

Normally, there is no need to configure the DNS addresses. If the service provider does not support automatic DNS address allocation, the DNS servers can be configured as shown by the following example:

```
MW1122(conf-common)# dns address primary 1.2.3.4

MW1122(conf-common)# dns address secondary 1.2.3.5

MW1122(conf-common)#
```

7.2.3 Configuring static and dynamic routing

Routing entries in the routing table are needed in order to forward the IP packets to the correct interface. M/MW has both static and dynamic routes. Static routes are configured manually and dynamic routes are learned automatically using RIP v1 and RIP v2 protocols. The following examples show how to configure static routes to M/MW.

Default gateway for an interface that learns the next hop automatically:

```
MW1122(conf-common)# ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1
```

Default gateway for an interface that requires static next hop:

```
MW1122(conf-common)# ip route 0.0.0.0 0.0.0.0 1.2.3.1 vcc1
```

Static route for an interface that learns the next hop automatically:

```
MW1122(conf-common)# ip route 131.132.133.0 255.255.255.0
0.0.0.0 vcc1
```

Static route for an interface that requires a static next hop:

```
MW1122(conf-common)# ip route 131.132.133.0 255.255.255.0
1.3.5.1 vcc1
```

M/MW can have only one default gateway. The interfaces that can learn gateway/ peer address dynamically can use value 0.0.0.0 instead of the next hop address.

7.2.4 Encrypting wireless connection (MW series only)

The minimal WEP encryption configuration is very simple. The WEP mode has to be selected, at least one key has to be configured, and the key has to be selected. In M/MW, the possible default keys are numbered from 1 to 4. In some WLAN products the numbering may be from 0 to 3. In those cases, the key 0 equals the key 1 in M/MW. Four keys are available to enable easy change of keys when the keys are changed at different times for different clients. A simple WEP configuration is shown in the following example:

```
MW1122(conf-wlan)# wep mode required

MW1122(conf-wlan)# wep key-entry 1 40-bit 0987654321

MW1122(conf-wlan)# wep default-key 1

MW1122(conf-wlan)#
```

If you want to use 104-bit keys, you must enter a key of 26 characters:

```
MW1122(conf-wlan)# wep key-entry 1 104-bit
```

```
1234567890abcdef1234567890

MW1122(conf-wep)#
```

If you want to use 128-bit keys, you must enter a key of 32 characters:

```
MW1122(conf-wlan)# wep key-entry 1 128-bit

1234567890abcdef1234567890abcdef

MW1122(conf-wlan)#
```

The client table and station-specific keys are configured in the following example:

```
MW1122(conf-wlan)wep mode specific key required

MW1122(conf-wlan)# sta pc_1 00:11:22:33:44:55

MW1122(conf-wlan)# sta pc_2 00:11:22:33:44:55 40-bit
1234567890

MW1122(conf-wlan)# sta pc_3 00:11:22:33:44:55 128-bit
1234567890abcdef1234567890abcdef
```

The first line is the client table entry only. The second and third lines configure the WEP key also.

7.2.5 Changing WLAN settings through the command line interface (MW series only)

Your Nokia MW is defined to have default settings as described in section. Sometimes you may have to modify these settings. In this section you can find instructions on when and how to change these settings.

Changing WLAN network name

By default, your MW has the WLAN network name *MW-wxyz*, where wxyz are four last numbers of the serial number of your MW. You can change this to suit your needs and make your network uniquely identifiable. To change the WLAN network name of MW:

1. Open a telnet or CLI session to MW as described earlier in this Chapter.
2. Start the configuration mode by typing `configure` ENTER.
3. Go to *wlan* configuration level by typing `wlan` ENTER.

4. Give new network name by typing `network-name` **new_network_name** ENTER where `new_network_name` is your new network name. Note, that network name is case-sensitive.

5. Remember to change the network names of your WLAN clients, also.

Changing WLAN channel

Sometimes, if there are other wireless LAN devices or devices using 2.4 GHz frequency nearby, it may be necessary to change the WLAN channel used by Nokia MW. The available channels depend on the regulatory domain. After selecting a new channel, remember to reset the WLAN subsystem of your Nokia MW as described below.

1. Open a telnet or CLI session to M/MW as described earlier in this Chapter.

2. Check your current channel by typing `show conf run` command. The channel is shown on top of the display, on `ap-station` line. The `ap-station` line contains the following information: MAC address/network name/channel/region.

3. Start the configuration mode by typing `configure` ENTER.

4. Go to *wlan* configuration level by typing `wlan` ENTER.

5. Set a new channel (13, for example) by typing `radio-channel europe 13` ENTER.

6. Reset wlan subsystem by going to the main mode by typing `quit` and giving `reset wlan` command.

7. Ensure that the channel has been changed by typing `show wlan stat` command.

You have now changed the WLAN channel of your Nokia MW and you can use the wireless LAN normally. You may need to restart your wireless LAN clients if they do not support automatic channel scanning. Consult the user manuals of each WLAN client for instructions on changing their WLAN channels.

Controlling the access to your network

You can control the access to your MW with a client table. By default, this feature is *off* in MW. This means that all WLAN clients are allowed to have access to your Nokia MW. Therefore it is important that you identify your WLAN clients, add them on the client table and activate the admission control function which prohibits other WLAN clients from entering your network. This is a major security issue protecting your wireless network from outsiders. To add clients to the client table:

1. Consult your computer's and WLAN clients' manuals on how to find out your WLAN clients' MAC addresses. For clients running Windows 95 and 98 operating systems, you can find out the MAC addresses by running `winipcfg.exe` and selecting WLAN card from the menu. The MAC address is shown in the `Adapter address` field.
2. Open a telnet or CLI session to MW as described earlier in this Chapter.
3. Start the configuration mode by typing `configure` ENTER.
4. Go to *wlan* configuration level by typing `wlan` ENTER.
5. Add an entry on the client table by giving the following command: `sta <name-string> <phys-address>`, where `name-string` identifies the client table entry (for example, a PC host name) and `phys-address` is the MAC address of the allowed wireless client.
6. Repeat the `sta` command if you want to add more clients on the client table.
7. If you want to remove WLAN clients from the client table, just type `no sta xx:xx:xx:xx:xx:xx`, where xx:xx:xx:xx:xx:xx is the MAC address of the wireless station you want to remove from the list.

Note

You must activate the admission control to prevent other WLAN clients from entering your network.

To activate the client table:

1. Open a telnet or CLI session to MW as described earlier in this Chapter. Start the configuration mode by typing `configure` ENTER.
2. Go to *wlan* configuration level by typing `wlan` ENTER.
3. Activate the client table by giving the `admission-control phys-address` ENTER command. You can deactivate admission control by typing `no admission-control` ENTER.
4. Type `show` on the *wlan* configuration level to view the activated client table entries.

7.2.6 File system and downloading new firmware using TFTP

M/MW has a flash file system. Some files in the file system have special meanings. These files are:

- image.exe; primary application file.
- image.bak; secondary application file used if image.exe has been corrupted or is missing. It is then renamed as image.exe automatically.
- startup.cfg; primary configuration file used during startup.
- dhcp.leases; contains DHCP lease table information.

M/MW has the following commands that can be used for file handling:

- copy
- rename
- delete
- dir

If you use image.exe as a destination filename with the copy command and the image.exe already exists, the existing image.exe will be automatically renamed as image.bak. This guarantees that the application file exists if M/MW loses power during SW download.

You can update the firmware of M/MW by downloading the new software from a TFTP server. To download and activate new M/MW firmware:

1. Use CLI to issue

   `install tftp:/<IP address>/<filename>` command, where `<IP address>` is the IP address of the TFTP server containing the new firmware and `<filename>` is the name of the file to be downloaded. The command `copy tftp:/<IP address>/filename image.exe` can be used alternatively.

2. After you will see `transfer status SUCCESSFUL` message, restart M/MW to activate the new firmware.

Downloading configuration or application from monitor

Monitor is a small application that is executed before the actual software image is started. Typically the Monitor automatically loads the application file image.exe. You can activate the Monitor by pressing m" followed by o" in the very beginning of the system startup (The CLI cable needs to be attached to the Gateway):

```
local MAC=00:40:43:02:36:72; Using M111/850 eth conf

Type 'm' (fast) followed by 'o' (in 10 sec) to activate
Monitor

Nokia Inc. (C) 1999-2001
```

```
Nokia Mboot

rel-Bxxxx110.R01 built on May  8 2001 @ 10:35:02

password:

mon-a>
```

The following commands are available for file handling in the Monitor:

- rename
- delete
- dir

M/MW has two methods of retrieving files:

- TFTP
- XMODEM

You can retrieve files from a TFTP server using the commands in the following example:

```
mon-a>ipa 192.168.1.1

   ip=192.168.1.1

ipserver=0.0.0.0

   ipgw=0.0.0.0

serverfile=

mon-a>ips 192.168.1.100

   ip=192.168.1.1

ipserver=192.168.1.100

   ipgw=0.0.0.0

serverfile=

mon-a>file startup.cfg

   ip=192.168.1.1

ipserver=192.168.1.100

   ipgw=0.0.0.0
```

```
serverfile=startup.cfg

mon-a>eget

tftp loader

   ip=192.168.1.1

ipserver=192.168.1.100

   ipgw=0.0.0.0

serverfile=startup.cfg

loading file...

file size=556

mon-a>wri startup.cfg

Writing successful

mon-a>
```

A file can also be transmitted from an XMODEM1K running in a PC, for example, as in the following example:

```
mon-a>xget

Start Xmodem1k sending...

mon-a>wri image.exe

Writing successful

mon-a>
```

7.2.7 Configuring tos-mapping

Tos-mapping allocates IP packets originated from the local area network with one of the five transmit queues implemented by the Gateway. When a transmission towards the wide area network takes place, the Gateway checks for each queue in a predefined priority order before actual packets are physically sent. First, packets allocated with the highest priority queue are transmitted, next packets allocated with the second highest priority queue are transmitted and so on. In case of excessive traffic load it is possible that lower priority queues will be blocked and very few packets belonging to these queues will be sent. If such a queue becomes full, packets allocated with the queue are to be dropped off. The four higher priority queues schedule packets on the first-come-first-served basis, the lowest priority queue schedules as incurred by the wight-fair-queing (wfq) algorithm.

The allocation process itself depends on the value of the diffserv field embedded in the IP header of each packet. The value discriminates among eight distinctive classes of service so that each class may be characterised with the level of precedence subject to investigation when packets traverse the network to allow for proper processing (packets of a higher precedence are to be processed faster in respect to packets of a lower precedence). The tos-mapping command syntax associates a single octet with each of the four higher priority queues, four octets altogether. Each bit of such an octet represents one particular level of precedence. When allocating packets that exhibit some level of presedence to be scheduled from the context of an arbitrary queue then the octet associated with that queue has to set the bit corresponding to the level of precedence considered. If the bit corresponding to a level of precedence is set in none of the four octets then such packets are to be allocated implicitely with the queue of the lowest priority. Any level of precedence may be allocated with only one priority queue at any given time.

8 Managing your M/MW

Management through the CLI console

M/MW can be managed locally through the command line interface (CLI). The local command line interface is accessed through the local management console (marked “CLI”) on the back panel of the modem. The local management console interface is an asynchronous V.24/V.28 character-based interface with the following configuration:

Table 8. CLI interface configuration

Setting	Value
Speed	9600
Parity	None
Data bits	8
Stop bits	1
Duplex	Full
Flow control	None

Use the 10Base-T Ethernet cable with the serial adapter to connect you PC's serial port to the local management console interface according to Figure 30.

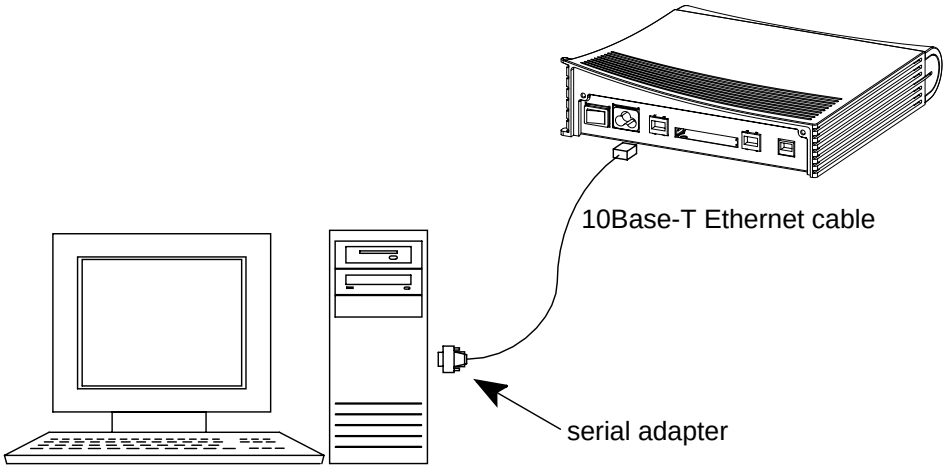

Figure 30. Local management cabling

Table 9. Command line interface pin-out numbering

PIN	Signal	Direction M/MW- terminal	MDI signal
1	107 DSR (const. ON)	->	Data set ready
2	108 DTR	<-	Data terminal ready
3	109 DCD (const. ON)	->	Data channel received line signal detector
4	102 SG		Signal ground
5	103 TxD	<-	Transmitted data
6	104 RxD	->	Received data
7	105 RTS (not in use)	<-	Request to send
8	106 CTS (const. ON)	->	Clear to send

Management through Telnet

The command line interface can also be accessed through the Ethernet and WLAN port of M/MW or through the ATM channels of M/MW on top of the Telnet protocol. In order to use the CLI through Telnet or the ATM channel, the IP address must be given to the corresponding interface.

Management through ATM virtual channel

M/MW can also be managed remotely through a separate ATM virtual channel. This channel is only used for management purposes. In order to use this management channel, it has to be activated first and given an IP address configuration. The management traffic to this interface is not routed to any other interfaces of M/MW.

Web browser management

This topic is described in detail in 4

9 CLI command modes and command syntax

Caution

Be careful when using CLI commands or web interface configuration options since they may change the configuration of M/MW and affect the operability of the modem. If you make changes to the CLI commands it is on your own responsibility.

The command line interface is divided into two modes: **main** and **configuration**.The CLI is case sensitive. All commands must be given in lower case characters. Only file names and strings can contain upper case characters.

You can recall your previous commands by pressing the up-arrow key on your keyboard.

CLI commands can also be given in a short format, for example the command **install** can be *i*, *in*, *ins* etc. The command **configure** can be entered as *con*, *conf* etc. If the CLI is unable to interpret your short-syntax command correctly, you receive an error message **"ambiguous command"** on the screen. When this happens, retype the command in longer format so that the CLI can interpret your command correctly. If you enter a wrong command you receive an error message **"invalid command"** on the screen. You can list all the available commands on the screen at any level by typing **?** or **help**.

The examples below represent typical command outputs; the outputs of your M/MW may differ from them, depending on the configuration of your modem. Note also that the modem presented in the examples is MW1122. In most cases, however, the examples are applicable to the other M/MW Gateways as well. All information which is applicable to certain modem(s) only is notified throughout the manual, for example *show HPNA (MW1324 only).*

9.1 Overview to main mode commands

The main mode lets you monitor the status and performance of M/MW. Note, however, that certain main mode commands change the configuration of your M/MW. The main mode commands and their functions are described in brief below. These commands are described in detail in Chapters 10 and 11.

- show — to display device entity status
- dhcp — to renew/release dynamic ip address
- ping — to check for the ip operability
- atmping — to check for the atm operability
- [no] debug — to enable/disable debug operations
- dir — to display file contents
- copy — to copy file system object
- rename — to rename file system object
- delete — to delete file system object
- install — to fetch new executable image
- configure — to enter custom configuration mode
- load — to load custom configuration
- script — to execute custom command batch
- save — to save log / custom configuration
- restore — to restore custom /default configuration
- clear — to clear statistics counters
- reset — to reset manageable device entity
- logout — to terminate administration session
- reaload — to force soft reset upon system
- restart — to force hard reset upon system

9.2 Overview to configuration mode commands

The configuration mode is divided into levels. You can enter the desired configuration level simply by typing the name of the level. By typing `quit` you will return to the main mode. The command `top` returns you to the root level of the configuration mode.

The configuration mode lets you change M/MW configuration. In the configuration mode, functions can be activated by entering the level name first and then by typing the corresponding command, for example `bridging`. The function can be deactivated by simply typing `no bridging`. In commands which require typing in parameter values, the default value can be restored by typing `de long-retry`, for example. `de` in front of the command means default. If you type in a value which is incorrect (for example, letters instead of numbers), the CLI prompts you to enter the value correctly and displays help. You can always get help on the command or display by typing `help` or `?` at the command prompt.

The configuration mode levels are listed below. The configuration mode commands are described in detail in Chapter 12 12.

- show — to display running configuration
- system — to enter system configuration level
- password — to enter password configuration level
- eth — to enter Ethernet configuration level
- wlan — (MW only) to enter wlan configuration level
- vcc1–vcc8 — to enter phy interface configuration level
- vbridge — to enter vbridge interface configuration level
- mngtvcc — to enter mgt interface configuration level
- common — to enter common params configuration level

10 "show" commands in main mode

10.1 show log

Description	Displays diagnostic log.
Syntax	show log
Arguments	all

Example

```
MW1122>show log
000/00:00:01 HI(1) IP    intf / ETH (eth) / admin.stat up
000/00:00:01 HI(1) ATM   chan / vcc1 / admin.stat up
000/00:00:01 HI(1) IP    intf / VCC1 (ppp) / admin.stat up
000/00:00:02 HI(1) DSL   line / oper.stat down
000/00:00:02 HI(1) WLAN  unit / mounted
000/00:01:06 HI(1) DSL   line / oper.stat down
000/00:02:05 HI(1) DSL   line / oper.stat up
000/00:02:35 HI(1) ATM   chan / vcc1 / admin.stat up
000/00:02:35 HI(1) IP    intf / VCC1 (ppp) / admin.stat down
000/00:02:35 HI(1) IP    intf / VCC1 (ppp) / admin.stat up
MW1122>
```

10.2 show dsl

Description	Displays DSL line status

Syntax	show dsl [all]
Arguments	all

Example

```
MW1122>show dsl
configured-mode          GlobeSpan /    G.DMT / CP
firmware-rev                41000
activity-status              OPER / G.DMT
                         near-end                              far-end
maximum-bitrate              8224 kbits                            n/a kbits
actual-bitrate               8064 kbits                            832 kbits
noise-margin                 11.0 dB                               n/a dB
output-power                 10.5 dBm                             19.8 dBm
attenuation                   3.0 dB                               4.0 dB
corr-intl-fec                   0                                   11
corr-fast-fec                   0                                    0
fail-intl-crc                   2                                    0
fail-fast-crc                   0                                    0
fail-intl-hec                   0                                    0
fail-fast-hec                   0                                    0
flaged-alarms                NONE                                 NONE
MW1122>
```

10.3 show eth

Description	Displays Ethernet interface status
Syntax	show eth [all]
Arguments	show eth command shows Ethernet interface state and status. all argument shows also additional information.

Example

```
MW1122> show eth
##eth(up)      type
               IEEE 802.3/DIX
                 pkt     oct     dis  err
stat-tx-payload  10964   672919  0    0
stat-rx-payload  10968   657690  0    0
MW1122>
```

10.4 show hpna (MW1324 only)

Description	Displays HPNA interface status
Syntax	show hpna [all | table]

Arguments	`show hpna`
	command shows HPNA interface state and status.
	`all`
	argument shows also interrupts.
	`table`
	
	shows the HPNA-clients phys-addresses and bit rates

Example	

```
MW1324> show hpna
## hpna(up)             type
                HOMEPNA 2.0
                  pkt     oct     dis  err
stat-tx-payload  1        28        0    0
stat-rx-payload  0         0        0    0
MW1324>
```

10.5 MW only: show wlan (all, stat, table)

Description	Displays WLAN interface status.

Syntax	show wlan [all | stat | table]

Arguments	`show wlan`
	command without arguments shows the state of the wlan interface and the payload statistics.
	`all`
	argument shows interrupts, state and payload statistics.
	`stat`
	argument shows detailed statistics.
	`table`
	argument shows the current stations on the wireless LAN.

Example

```
MW1122> show wlan
##wlan (up)        type
                   IEEE 802.11
                   pkt     oct      dis   err
stat-tx-payload    2218    926997   0     0
stat-rx-payload    2211    927009   12    0
MW1122>
```

10.6 show atm

Description	Displays ATM status.
Syntax	show atm [all]

Arguments	`show atm`
	command shows ATM channels and traffic statistics.
	`all`
	shows all ATM information.

Example

```
MW1122> show atm
##vcc1(up)  vpi    vci     type       encap
             0      35      DATA_PVC   ETH-LLC

                   pkt     oct        diserr
stat-tx-payload    223641  2568289    0     0
stat-rx-payload    18030   1440816    0     0
MW1122>
```

10.7 show bridge (if, stat, table)

Description	Displays interfaces which have bridging enabled.
Syntax	show bridge if
Arguments	None

Example
`MW1122> show bridge if`
`VBRI (up)  phys-address`
`  00:99:12:16:10:53`
`ETH (up)  phys-address`
`  00:00:00:00:00:00`
`WLAN (up)  phys-address`
`  00:00:00:00:00:00`
`VCC1 (up)  phys-address`
`  00:00:00:00:00:00`
`MW1122>`	

Description	Displays bridging statistics.
Syntax	show bridge stat
Arguments	None

Example
`MW1122> show bridge stat`
`in-packet  8518  out-packet  8494`
`discard  24`
`MW1122>`	

Description	Displays bridging table.

Syntax	show bridge table
Arguments	None

Example
`MW1122> show bridge table`
`if phys-address age type`
`VBRI 00:99:12:16:10:53 n/a forever`
`VCC1 00:60:08:94:da:a7 0 dynamic`
`WLAN 00:e0:03:04:0c:c9 15 dynamic`
`ETH 00:60:08:94:af:d7 0 dynamic`
`WLAN 00:e0:03:04:0c:e4 0 dynamic`
`nr-of-entries 5`
`MW1122>`	

10.8 show ppp (lcp, ipcp, pptp, pppoe)

Description	Shows PPP line connection protocol information
Syntax	show ppp lcp
Arguments	None
Example `MW1122>show ppp lcp`	

Description	shows IP control protocol information
Syntax	show ppp ipcp
Arguments	None
Example `MW1122>show ppp ipcp`	

Description	shows point-to-point tunnelling information

Syntax	show ppp pptp
Arguments	None
Example MW1122> MW1122>show ppp pptp VCC2 (pppoa-tunnel) net-address port status host-cid peer-cid 192.168.1.2 1060 ACTIVE 9 0 description pc2 MW1122>	

Description	shows point-to-point over ethernet
Syntax	show ppp pppoe
Arguments	None
Example MW1122>show ppp pppoe VCC1 padi-out pado-in padr-out pads-in status 1 1 1 1 ACTIVE padt-out padt-in ac-name 0 0 13011049810869-RAN-1 MW1122>	

10.9 show arp

Description	Displays ARP table.
Syntax	show arp
Arguments	None
Example MW1122>show arp VBRIDGE net-address phys-address age 10.98.20.140 00:00:0e:7c:15:d4 00.07 MW1122>	

10.10 show ip (if, stat, cache, route, icmp, udp, tcp, rip, igmp, snmp, service)

Description	Displays IP interfaces.
Syntax	show ip if
Arguments	None
Example	

```
MW1122> show ip if
VBRIDGE (up)
net-address     net-mask       mtu     phys-address
192.168.172.2   255.255.255.0  1500 00:99:12:16:10:53
as ETHERNET/RIP DISABLED
MW1122>
```

Description	Displays IP statistics.
Syntax	show ip stat
Arguments	None
Example	

```
MW1122> show ip stat
forwarding   NO FORWARD out-discards  0
default-ttl       255   out-no-routes 0
in-receives       2355  reasm-timeout 5
in-hdr-errors     0     reasm-reqds   0
in-addr-errors    1     reasm-OKs     0
forw-datagrams    0     reasm-fails   0
in-unknown-protos 0     frag-OKs      0
in-discards       2354  frag-fails    0
in-delivers       2354  frag-creates  0
out-requests      0     routing-discards0
MW1122>
```

Description	Displays IP cache table and statistics.

Syntax	show ip cache
Arguments	None

Example

```
MW1122> show ip cache
if    net-address  phys-header
ETH   192.168.1.3  005004b67d680040430236720800
ETH   192.168.1.2  005004b6697500404302367208 00
VCC2  10.98.16.250 0021
nr-of-entries      3
MW1122>
```

Description	Displays IP routing table.
Syntax	show ip route
Arguments	None

Example

```
MW1122>show ip route
VBRIDGE
route-dest  route-mask       netxthop       tag
10.98.20.255255.255.255.255  255.255.255.255BCAST
10.98.20.150255.255.255.255  10.98.20.150  IFACE
10.98.20.0  255.255.255.0    10.98.20.150  LOCAL
MNGTVCC
route-dest  route-mask       netxthop      tag
10.98.9.0   255.255.255.0    10.98.5.200   RIP
10.98.5.255 255.255.255.255  255.255.255.255BCAST
10.98.5.100 255.255.255.255  10.98.5.100   IFACE
10.98.5.0   255.255.255.0    10.98.5.100   LOCAL
ETH
route-dest  route-mask       netxthop      tag
10.98.0.255 255.255.255.255  255.255.255.255BCAST
10.98.0.254 255.255.255.255  10.98.0.254   IFACE
10.98.0.0   255.255.255.0    10.98.0.154   LOCAL
WLAN
route-dest  route-mask       netxthop      tag
10.98.1.255 255.255.255.255  255.255.255.255BCAST
10.98.1.254 255.255.255.255  10.98.1.254   IFACE
10.98.1.0   255.255.255.0    192.168.1.254 LOCAL
VCC3
route-dest  route-mask       netxthop      tag
11.22.20.255255.255.255.255  255.255.255.255BCAST
11.22.20.108255.255.255.255  11.22.20.108  IFACE
11.22.20.0  255.255.255.0    11.22.20.108  LOCAL
0.0.0.0     0.0.0.0          11.22.20.1    STAT
MW1122>
```

Description	Displays ICMP statistics.
Syntax	show ip icmp
Arguments	None
Example	

```
MW1122> show ip icmp
in-msgs           23 out-msgs               23
in-errors          0  out-errors             0
in-dest-unreachs   0  out-dest-unreachs      0
in-time-excds      0  out-time-excds         0
in-parm-probs      0  out-parm-probs         0
in-src-quenchs     0  out-src-quenchs        0
in-redirects       0  out-redirects          0
in-echos          23 out-echos              23
in-echo-reps       0  out-echo-reps          0
in-timestamps      0  out-timestamps         0
in-timestamp-reps  0  out-timestamp-reps     0
in-addr-masks      0  out-addr-masks         0
in-addr-mask-reps  0  out-addr-mask-reps     0
MW1122>
```

Description	Displays UDP statistics.
Syntax	show ip udp
Arguments	None
Example	

```
MW1122> show ip udp
in-datagrams       0 in-errors               0
no-ports           0 out-datagrams           0
MW1122>
```

Description	Displays TCP statistics.

Syntax	show ip tcp
Arguments	None

Example

```
MW1122> show ip tcp
rto-algorithm    VANJ        estab-resets     0
rto-min          0           curr-estab       0
rto-max          240000      in-segs          0
max-conn         16          out-segs         0
active-opens     0           retrans-segs     0
passive-opens    0           in-errs          0
attemp-fails     0           out-rsts         0
MW1122>
```

Description	Displays RIP statistics.
Syntax	show ip rip
Arguments	None

Example

```
MW1122> show ip rip
in-pkts        0       out-pkts      0
in-updates     0       out-updates   0
in-requests    0       out-requests  0
MW1122>
```

Description	shows internet group management protocol statistics
Syntax	show ip igmp
Arguments	None.

Example

```
MW1122>show ip igmp
forward-pkts              0              discard-pkts              0
lan-recv-reports          0              wan-send-reports          0
lan-send-queries          19             wan-recv-queries          0
lan-recv-leaves           0              wan-send-leaves           0
MW1122>
```

Description	Displays SNMP statistics.
Syntax	show ip snmp
Arguments	None.

Example

```
MW1122>show ip snmp
in-pkts                 0               in-get-nexts            0
out-pkts                0               in-set-requests         0
in-bad-versions         0               in-get-responses        0
in-bad-community-names  0               in-traps                0
in-bad-community-uses   0               out-too-bigs            0
in-asn-parse-errs       0               out-no-such-name        0
in-too-bigs             0               out-bad-values          0
in-no-such-name         0               out-gen-errs            0
in-bad-values           0               out-get-requests        0
in-read-onlys           0               out-get-nexts           0
in-gen-errs             0               out-set-requests        0
in-total-req-vars       0               out-get-responses       0
in-total-set-vars       0               out-traps               0
in-get-requests         0               enable-auth-traps       DISABLED
MW1122>
```

Description	shows ip service information
Syntax	show ip service
Arguments	None.

Example

```
MW1122>show ip ser
                        port-nr-sta     port-nr-end             tag prot
"http"                  80              80              PREDEFINED TCP
"telnet"                23              23              PREDEFINED TCP
"ftp"                   21              21              PREDEFINED TCP
"nntp"                  119             119             PREDEFINED TCP
"pop3"                  110             110             PREDEFINED TCP
"imap4"                 143             143             PREDEFINED TCP
"ike"                   200             200             PREDEFINED UDP
"esp"                   n/a             n/a             PREDEFINED ESP-IPSEC
"ip"                    n/a             n/a             PREDEFINED 4
"ah"                    n/a             n/a             PREDEFINED 51
"rsvp"                  n/a             n/a             PREDEFINED 46
"pptp"                  n/a             n/a             PREDEFINED PPTP-GRE
"icmp-echo-req"         8               8               PREDEFINED ICMP
MW1122>
```

10.11 show sif

Description	shows stateful inspection firewall
Syntax	show sif
Arguments	None.

Example

```
MW1122>show sif
                              in-use      total
norm-entries                       0      10000
h323-entries                       0         10

                             correct   no-match   errorous
wan-send-pkts                2325284          6          0
wan-recv-pkts                3948868          0        159
MW1122>
```

10.12 show sif table

Description	shows stateful inspection firewall table
Syntax	show sif table
Arguments	None.

Example

```
MW1122>show sif table
net-address      port publ-address     port peer-address     port prot  age type
192.168.1.2      1064 192.168.1.2      1064 192.168.4.1        80 TCP     1 FILT

MW1122>
```

10.13 show sif server

Description	shows stateful inspection firewall server
Syntax	show sif server
Arguments	None.

Example

```
MW1122>show sif se
VCC1                    dst-addr-sta    dst-addr-end     port  size prot
@telnet               $ 10.98.24.7      10.98.24.7         23     1 TCP
@http                 $ 10.98.24.7      10.98.24.7         80     1 TCP
```

10.14 show napt

Description	Displays used and available NAPT resources.
Syntax	show napt
Arguments	None.

Example

```
MW1122>show napt
                            in-use      total
norm-entries                     0      10000
h323-entries                     0         10
wan-ports-udp                    0      10000 (pool starts at 50000)
wan-ports-tcp                    0      10000 (pool starts at 50000)

                           correct   no-match   errorous
wan-send-pkts                    0          0          0
wan-recv-pkts                    0          0          0
MW1122>
```

10.15 show napt table

Description	Displays NAPT table entries.
Syntax	show napt table
Arguments	None.
Example	

```
MW1324>
MW1324> show napt table

net-address    port publ-address   port peer-address  port prot  age type
192.168.1.3    768  10.98.24.7     7502 10.98.16.250     0  ICMP   1 TRAN
192.168.1.2    1024 10.98.24.7     7503 10.98.16.250     0  ICMP   0 TRAN
MW1324>
```

10.16 show napt server

Description	Displays NAPT server support information.
Syntax	show napt server
Arguments	None.
Example	

```
MW1122>show napt se
VCC1                      dst-address     port-mappings          size prot
"ftp"                     192.168.1.2     21    <->    21           1 TCP
"meeting2"                192.168.1.2     1503  <->  1503           1 TCP
"meeting1"                192.168.1.2     1720  <->  1720           1 TCP
@telnet                 $ 10.98.24.71     23    <->    23           1 TCP
@http                   $ 10.98.24.71     80    <->    80           1 TCP
MW1122>
```

10.17 show dns

Description	Displays DNS entry table and statistics.
Syntax	show dns
Arguments	None.

Example
`MW1122> show dns`
`dns-proxy "MW1122"/"Nokia MW1122"/AUTOMATIC`
`MW1122>`	

10.18 show dhcp (client, server)

Description	Displays DHCP client
Syntax	show dhcp client
Arguments	None.
Example	

```
MW1122> show dhcp client
##scope (a)
  pool-address pool-last          pool-mask
  192.168.0.1  192.168.0.254      255.255.255.0
  net-binding  primary-dns        secondary-dns
  ETH          192.168.0.254      n/a
  lease-time   gateway            domain-name
  00/12:00:00  12.168.0.254       n/a
##scope (b)
  pool-address pool-last          pool-mask
  192.168.1.1  192.168.1.254      255.255.255.0
  net-binding  primary-dns        secondary-dns
  WLAN         192.168.1.254      n/a
  lease-time   gateway            domain-name
  00/12:00:00  192.168.1.254      n/a
MW1122>
```

Description	Displays DHCP server entry table and statistics. It also shows leased address and states
Syntax	show dhcp server
Arguments	None.

Example

```
MW1122> show dhcp server
##scope (a)
  pool-address pool-last           pool-mask
  192.168.0.1  192.168.0.254       255.255.255.0
  net-binding  primary-dns         secondary-dns
  ETH          192.168.0.254       n/a
  lease-time   gateway             domain-name
  00/12:00:00  12.168.0.254        n/a
##scope (b)
  pool-address pool-last           pool-mask
  192.168.1.1  192.168.1.254       255.255.255.0
  net-binding  primary-dns         secondary-dns
  WLAN         192.168.1.254       n/a
  lease-time   gateway             domain-name
  00/12:00:00  192.168.1.254       n/a
MW1122>
```

10.19 show status (session, password, performance)

Description	Displays MW1122 hardware and software information.

Syntax	show status [session | password | performance]

Arguments	Optional arguments
	`session`
	`password`
	and
	`performance.`
	`session`
	shows information of the active configuration sessions. If login-id is used, it is shown on the screen.
	`performance`
	shows error counters.

Example

```
MW1122>show stat
product-id              T66580.01  0
serial-num              61011403338
cpu-type                XPC850SR / B
flash-type              2 M
sdram-type              8 M
phys-address-lan        00:40:43:04:fc:9b
phys-address-wan        00:40:43:04:fc:9c
short-desc              MW1122
long-desc               NOKIA MW1122 ADSL Router
boot-version            Bxxxx110.R01
appl-version            CHECKEDOUT
log-severity            HIGH
start-uptime            000/02:36:06
MW1122>
```

10.20 show config running

Description	Displays currently active configuration. If you have made changes in the configuration and you want them to be active after restart, save the current configuration to startup.cfg file using `save config` command.

Syntax	show config running
Arguments	None

Example

```
MW1122>show config running
system
 hostname MW1122
eth
 ip address 192.168.1.1 255.255.255.0
wlan
 network-name M/MW-3338
 radio-channel europe 13
 slave-to-eth
vcc1
 pvc 0 100 ppp-vc
 ip address 0.0.0.0 0.0.0.0
 ip napt
vcc2
vcc3
vcc4
vcc5
vcc6
vcc7
vcc8
vbridge
mngtvcc
common
 ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1
 dhcp mode server
MW1122>
```

10.21 show config startup

Description	Displays the startup configuration of your MW1122. This is the configuration saved in the startup.cfg file. Startup.cfg file is activated when MW1122 is switched on. If the startup.cfg file is missing, the default configuration is used.

Syntax	show config startup
Arguments	None

Example

```
MW1122> show config startup
system
     hostname MW1122
eth
     ip address 192.168.172.148
     255.255.255.128
wlan
     network name nokia
     radio channel europe 13
     ip address 192.168.172.21
     255.255.255.128
vcc1
     pvc 0 155 tunnelled-ppp-vc
     bridging
vbridge
mngtvcc
common
MW1122>
```

10.22 show config default

Description	Displays the default configuration of M/MW. M/MW uses this configuration if the startup.cfg file is missing.

Syntax	show config default
Arguments	None

Example
`MW1122>show config default`
`system`
`  hostname MW1122`
`eth`
`  ip address 192.168.1.1 255.255.255.0`
`wlan`
`  network-name M/MW-3338`
`  radio-channel europe 13`
`  slave-to-eth`
`vcc1`
`  pvc 0 100 ppp-vc`
`  ip address 0.0.0.0 0.0.0.0`
`  ip napt`
`vcc2`
`vcc3`
`vcc4`
`vcc5`
`vcc6`
`vcc7`
`vcc8`
`vbridge`
`mngtvcc`
`common`
`  ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1`
`  dhcp mode server`
`MW1122>`	

10.23 show config user

Description	shows user configuration
Syntax	show config user
Arguments	None
Example `MW1122> show config user`	

10.24 show config file

Description	Displays the local configuration file
Syntax	show config file <filename>
Arguments	`filename` is the name of the local configuration file.

Example

```
MW1122>show config file startup.cfg
system
 hostname MW1122
eth
 ip address 192.168.1.1 255.255.255.0
wlan
 network-name M/MW-3338
 radio-channel europe 13
 slave-to-eth
vcc1
 pvc 0 100 ppp-vc
 ip address 0.0.0.0 0.0.0.0
 ip napt
vcc2
vcc3
vcc4
vcc5
vcc6
vcc7
vcc8
vbridge
mngtvcc
common
 ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1
 dhcp mode server
MW1122>
```

10.25 show debug

Description	Displays the status (ON/OFF) of the debug functions.

Syntax	show debug
Arguments	None.

Example

```
MW1122> show debug
log             OFF  dsl               OFF
eth             OFF  wlan-header       OFF
wlan-packet     OFF  wlan-mngt         OFF
wlan-ctrl       OFF  wlan-table        OFF
atm-aal0        OFF  atm-aal5          OFF
ppp             OFF  pptp              OFF
arp             OFF  ip-host           OFF
ip-forward      OFF  ip-icmp           OFF
napt-map        OFF  napt-entry        OFF
napt-internal   OFF  napt-h323         OFF
dhcp            OFF  dns               OFF
MW1122>
```

10.26 show crash

Description	displays crash statistics

Syntax	show crash
Arguments	none

Example

```
MW1122>show crash
boot-version             rel-Bxxxx110.R01 built on May  8 2001 @ 10:35:02
appl-version
exception-id             DATA ACCESS ERROR (0x300) taken at 00/00:00:01
gpr0                     0x00000000      gpr1                      0x0046d9d0
gpr2                     0x002449d8      gpr3                      0x0075eb30
gpr4                     0x00000000      gpr5                      0xffffffff
gpr6                     0x0000290c      gpr7                      0x00000000
gpr8                     0x0076098c      gpr9                      0x05000000
gpr10                    0x00000000      gpr11                     0x00000000
gpr12                    0x00000000      gpr13                     0x0040d5fc
gpr14                    0x00000000      gpr15                     0x00000000
gpr16                    0x00000000      gpr17                     0x00000000
gpr18                    0x00000000      gpr19                     0x00000000
gpr20                    0x00000000      gpr21                     0x00000000
gpr22                    0x00000000      gpr23                     0x00000000
gpr24                    0x00000000      gpr25                     0x00000000
gpr26                    0x00000000      gpr27                     0x00000000
gpr28                    0x00000000      gpr29                     0x00000000
gpr30                    0x0075eb30      gpr31                     0x0075eb30
srr0                     0x0012e204      srr1                      0x00009902
msr                      0x00000000      dsisr                     0x00001009
lr                       0x0012e1f8      dar                       0x05000180
st1                      0x0012e7d4      st1                       0x00002908
st3                      0x00000000      st3                       0x00000000
MW1122>
```

11 Other main mode commands

11.1 dhcp renew

Description	Renews the IP address of the provided interface
Syntax	dhcp renew

Arguments	`if-id`
	`identifier of`
	`interface to renew`

Example `MW1122> dhcp renew`	

11.2 dhcp release

Description	releases ip address
Syntax	dhcp release

Arguments	`if-id`
	`identifier of interface to`
	`release`

Example `MW1122> dhcp release`	

11.3 ping

Description	Send an ICMP echo request to an IP address to test the IP function.
Syntax	ping <IP address>
Arguments	`IP address` is the IP address of the ping destination in dotted decimal format.

Example
`MW1122> ping 198.168.172.23`
`Reply from 198.168.172.23: bytes 32 time <10ms TTL=128`
`MW1122>`	

11.4 atmping

Description	Sends five OAM F5 loopback cells to the specified VPI/VCI destination with a 5 second total timeout interval. You can use atmping to test the ATM connection.

Syntax	atmping <vpi> <vci> <range>

Arguments	`vpi`
	is the Virtual Path Identifier and
	`vci`
	is the Virtual Channel Identifier of the ATM channel you want to test.
	`vpi`
	values are integers (0...255).
	`vci`
	values are integers (0...65535)
	`range`
	values are
	`segment`
	and
	`end-to-end`
	depending whether you want to test the first segment of the ATM connection or the end-to-end connection.

Example
`MW1122> atmping 0 23 segment`
`reply asserted roundtrip time = 4.20 ms`	

11.5 [no] debug

Description	Switches all debug operations off. To quit debugging, write no debug all on the screen regardless of what is being printed on the screen.
Syntax	no debug all
Arguments	`no` switches debugging off.

Example
`MW1122> no debug all`
`MW1122>`	

11.6 dir

Description	Displays the contents of M/MW file directory.
Syntax	dir
Arguments	None

Example

```
MW1122>dir
                        file-name       bytes-size      appl-vers
                        startup.bak            329
                        image.exe           722928      CHECKEDOUT
                        startup.cfg            327
                        dhcp.leases             60
nr-of-files             4
bytes-avail             1135970
MW1122>
```

11.7 copy

Description	Copies files within M/MW or over a TFTP (Trivial File Transfer Protocol) connection. With this command you can, for example, download configuration files.
Syntax	copy [file:/] <src-filename> [file:/] <dst-filename> copy [file:/] <src-filename> tftp:/<IP address>/<../dst-filename> copy tftp:/<IP address>/<../src-filename> [file:/] <dst-filename>

Arguments	`src-filename`
	is the name of the file you want to copy.
	`dst-filename`
	is its destination filename.
	`IP address`
	is the IP address of the TFTP server.

Example

```
MW1122>copy tftp:/191.111.111.1/file.txt file.new
MW1122>
```

11.8 rename

Description	Renames a file
Syntax	rename <old-filename> <new-filename>

Arguments	`old-filename`
	is the name of the file you want to rename.
	`new-filename`
	is the new filename.

Example
`MW1122> rename newconfig oldconfig`
`MW1122>`	

11.9 delete

Description	Deletes a file
Syntax	delete <del-filename>
Arguments	`del-filename` is the name of the file you want to delete.

Example
`MW1122> delete oldfile`
`MW1122>`	

11.10 install

Description	Downloads a new firmware from a TFTP server. Remember to restart M/MW after downloading to activate the new firmware.
Syntax	install tftp:/<IP address>/<../src-filename>

Arguments	`IP address`
	is the IP address of the TFTP server.
	`src-filename`
	is the name of the file which contains the new software.

Example
`MW1122> install tftp:/10.98.20.6/appl-A0.4.2`
`blocks received transfer status SUCCESSFUL`	

11.11 conf

Description	Enters the configuration mode
Syntax	conf
Arguments	`none`

Example
`MW1122> conf`
`MW1122(conf)#`	

11.12 load

Description	Loads a custom configuration

Syntax	load <cfg-file name>
Arguments	none
Example MW1122>load startup.cfg MW1122>	

11.13 script

Description	Executes a custom command batch.
Syntax	script <batch-filename>
Arguments	batch-filename is the name of the file in which you want to execute.
Example MW1122>script swap.bat MW1122>	

11.14 save log file

Description	Saves log to a file.
Syntax	save log file<log-filename>
Arguments	log-filename is the name of the file in which you want to save the log.
Example MW1122>save log file log.txt MW1122>	

11.15 save log default

Description	Saves log with a default file name (default.log).
Syntax	save log default
Arguments	None

Example
`MW1122>save log default`
`MW1122>`	

11.16 save config

Description	Saves the configuration to a file.
Syntax	save config {file<filename> | startup | user}

Arguments	`filename`
	is the name of the file in which you want to save the configuration.
	`startup-config`
	argument saves the configuration into a startup.cfg file.
	`user`
	saves the user configuration into user cfg.

Example
`MW1122>save config startup-config`
`MW1122>`	

11.17 restore config

Description	Restores the default or user configuration. You must have the admin privileges to issue this command. Restart your M/MW after you have issued this command.
Syntax	restore config <default | user>

Arguments	`default`
	argument restores the default configuration of M/MW.
	`user`
	argument restores the user configuration. The user configuration can be made with admin rights only.

Example
`MW1122>restore config default`
`MW1122>`	

11.18 clear (log, eth, hpna, wlan, atm, bridge, ppp, ip, crash)

Description	Clears the statistics counters.
Syntax	clear <log | eth | hpna | wlan | atm | bridge | ppp | ip | crash>

Arguments	`log`
	argument rewinds the diagnostic log to the beginning of the log file.
	`eth`
	argument clears the Ethernet statistics counters.
	`hpna (M/MW1324 only)`
	argument clears the HPNA statistic counters
	`wlan`
	argument clears the WLAN statistics counters.
	`atm`
	argument clears the ATM statistics counters.
	`bridge`
	argument clears the bridging counters.
	`ppp`
	argument clears the PPP counters.
	`ip`
	argument clears the IP statistics counters.
	`crash`
	argument clears the crash statistics counters

Example
`MW1122> clear log`
`MW1122>`	

11.19 reset (log, dsl, wlan, bridge, ppp, arp, cache, sif, napt, dhcp)

Description	Resets subsystems.
Syntax	reset <log | dsl | wlan | bridge | ppp [vcc-id] | arp | cache | sif | napt | dhcp>

Arguments	`log`
	resets the diagnostic log subsystem.
	`dsl`
	resets the DSL subsystem. The DSL connection will be re-established.
	`wlan`
	resets the WLAN subsystem. The subsystem reset is required for loading the WLAN configuration parameters to the WLAN subsystem.
	`bridge`
	clears the bridge table
	`ppp`
	resets the whole PPP subsystem. The PPP connection will be re-established. If you provide a VCC number (vcc-id), only that connection will be reseted.
	`arp`
	clears the ARP table.
	`cache`
	resets the cache.
	`sif`
	resets the SIF subsystem
	`napt`
	resets the NAPT subsystem.
	`dhcp`
	resets the DHCP subsystem

Example
`MW1122> reset wlan`
`MW1122>`	

11.20 logout

Description	Logs out from the command line interface.
Syntax	logout
Arguments	None
Example MW1122>logout goodbye...	

11.21 reload

Description	Restarts M/MW software.
Syntax	reload
Arguments	None
Example MW1122>reload MW1122>reload in progress...	

11.22 restart

Description	Restarts M/MW. This command is equivalent to switching the power first off and then on.
Syntax	restart
Arguments	None
Example MW1122> restart MW1122> restart in progress...	

12 Configuration mode commands

12.1 Multilevel commands

12.1.1 top

Description	Returns you to the configuration root level from a higher configuration level.
Syntax	top
Arguments	None.

Example
`MW1122(conf-system)#top`
`MW1122(conf)#`	

12.1.2 quit

Description	Exits the configuration mode and returns you to the main mode
Syntax	quit
Arguments	None.

Example
`MW1122(conf)#quit`
`MW1122>`	

12.1.3 show

Description	Displays the current running configuration.
Syntax	show
Arguments	None

Example

```
MW1122(conf)#show
system
 hostname MW1122
eth
 ip address 192.168.1.1 255.255.255.0
wlan
 network-name M/MW-3338
 radio-channel europe 13
 slave-to-eth
vcc1
 pvc 0 100 ppp-vc
 ip address 0.0.0.0 0.0.0.0
 ip napt
vcc2
vcc3
vcc4
vcc5
vcc6
vcc7
vcc8
vbridge
mngtvcc
common
 ip route 0.0.0.0 0.0.0.0 0.0.0.0 vcc1
 dhcp mode server
MW1122(conf)#
```

`show` command given on different configuration levels displays the current configuration of that particular configuration level.

Use the following commands to enter different configuration levels:

`system`

`password`

`eth`

`wlan`

```
vcc1 ... vcc8

vbridge

mngtvcc

common
```

12.2 System level commands (conf)#system

12.2.1 conf-system-hostname

Description	Assigns a hostname to M/MW.
Syntax	hostname <name-string>
Arguments	`name-string` is an ASCII string of maximum of 32 characters.

Example
`MW1122(conf-system)#hostname nokia`
`MW1122(conf-system)#`	

12.2.2 conf-system-log level

Description	Assigns log severity level
Syntax	log level <low-medium-high>
Arguments	`low, medium, high`
Example `MW1122(conf-system)#log level medium`	

12.2.3 conf-system-timeout

Description	Sets a timeout for a management session.
Syntax	[de] timeout <value>
Arguments	`value` is a time from 1 to 255 minutes. The default value is 60.

Example
`MW1122(conf-system)#timeout 10`
`MW1122(conf-system)#`	

12.3 Password level commands (conf)#password

12.3.1 conf-system-password (user, bridge-user, router-user, pptp-user, napt-user, admin)

Description	Switches password on/off and sets a new password for different user levels. Note, that you must assign admin password before you can assign other passwords. When removing passwords, admin password must be removed last.
Syntax	[no] <user | bridge-user | router-user | pptp-user | napt-user | admin> <passwd-string>

Arguments	`no`
	switches off user password.
	`user`
	argument sets the user privilege level password. User password gives no access to the configuration mode. Also, firmware download is not allowed on the user privilege level.
	`bridge-user`
	sets the bridge-user privilege level password. Bridge user can set static routes and enable VBRIDGE IP address.
	`router-user`
	sets the router-user privilege level password. Router user can change log levels and hostname.
	`pptp-user`
	sets the PPTP-user privilege level password. PPTP user can change VCCx description, DHCP, DNS and LAN/VBRIDGE configurations.
	`napt-user`
	sets the NAPT-user privilege level password. NAPT user can change VCCx description, LAN/VBRIDGE, NAPT servers (pinholes), PPP username/password/mode/autostop, DHCP, DNS configurations, and set static routes.
	`admin`
	sets the administrator privilege level password. Administrator can change all configuration parameters. Only the administrator is allowed to use file handling commands (copy, rename, etc.).
	`passwd-string`
	is the new password.

Example `MW1122(conf-password)# admin nokia`	

12.4 Eth level commands (conf)#eth

12.4.1 conf-eth-[no] bridging

Description	Switches on/off bridging.
Syntax	[no] bridging
Arguments	`no` switches bridging off.

Example
`MW1122(conf-eth)#bridging`
`MW1122(conf-eth)#`	

12.4.2 conf-eth-[no] ip address

Description	Switches on/off routing in the Ethernet interface.
Syntax	[no] ip address <IP address> <ip-mask>

Arguments	`no`
	switches routing off.
	`IP address`
	is the IP address you want to assign to the Ethernet interface.
	`ip-mask`
	is the subnet mask.

Example
`MW1122(conf-eth)#ip address 192.168.132.11 255.255.255.0`
`MW1122(conf-eth)#`	

12.4.3 conf-eth-ip rip-send

Description	Switches on/off RIP send function. When enabled M/MW sends Routing Information Protocol messages to other routers.
Syntax	[no] ip rip-send <rip-send-mode>

Arguments	`no`
	switches rip-send function off.
	`v1`
	send-mode selects RIP version 1.
	`v2`
	send-mode selects RIP version 2.
	`compatible-v1`
	send-mode selects the sending of RIPv2 packets using broadcast.

Example
`MW1122(conf-eth)#ip rip-send v1`
`MW1122(conf-eth)#`	

12.4.4 conf-eth-ip rip-receive

Description	Switches on/off RIP send function. When enabled M/MW receives Routing Information Protocol messages from other routers.
Syntax	[no] ip rip-receive <rip-receive-mode>

Arguments	`no`
	switches RIP receive function off.
	`v1`
	receive-mode selects RIP version 1.
	`v2`
	receive-mode selects RIP version 2.
	`both-v1v2`
	receive-mode selects both RIP version 1 and version 2.

Example
`MW1122(conf-eth)#ip rip-receive v1`
`MW1122(conf-eth)#`	

12.4.5 conf-eth-ip admin-disabled

Description	Enables/disables the management of M/MW through the Ethernet interface.
Syntax	[no] ip admin-disabled
Arguments	`no` enables management through the Ethernet interface.

Example
`MW1122(conf-eth)#ip admin-disabled`
`MW1122(conf-eth)#`	

12.5 Wlan level commands (conf)#wlan (MW only)

12.5.1 conf-wlan-network-name

Description	Assign a logical name to the wireless station. This name defines a logical group of wireless stations. Network name ensures that the wireless stations connect to the correct logical network. You must issue `reset wlan` command to activate the new network name. If you use the web interface, the new value will be activated automatically.
Syntax	network-name <name-string>
Arguments	`name-string` is your logical network name. The maximum length of the name is 32 characters. Note that this argument IS case-sensitive.

Example
`MW1122(conf-wlan)#network-name Home`
`MW1122(conf-wlan)#`	

12.5.2 radio-channel

Description	Sets the region appropriate for the area where you are using your WLAN. This command also sets the radio channel. Note that the region affects the number of channels available. You must issue `reset wlan` command to activate the new regulatory domain and radio channel. If you use the web interface, the new value will be activated automatically.
Syntax	[no] radio-channel <regulatory-domain> <ch-number>

Arguments	Select the regulatory domain
	`(europe, france, canada, usa`
	or
	`japan)`
	according to your location of use.
	The available channels depend on the region setting. Channel numbers
	`ch-number`
	for different regions are:
	Europe: 1...13
	France: 10...13
	Canada: 1...11
	USA 1...11
	Japan: 14

Example
`MW1122(conf-wlan)#radio-channel europe 13`
`MW1122(conf-wlan)#`	

12.5.3 rts-threshold

Description	Determines whether RTS/CTS frames should be sent on the wireless link and what size frames they should be used for. Frames larger than the parameter value will be preceded by an RTS/CTS exchange. You must issue `reset wlan` command to activate the new RTS/CTS frame size threshold.
Syntax	[de] rts-threshold <limit>

Arguments	`de`
	sets the default value 2312.
	`The limit`
	values are integers 256...65535.

Example
`MW1122(conf-wlan)#rts-threshold 2000`
`MW1122(conf-wlan)#`	

12.5.4 fragment-threshold

Description	Sets the fragmentation threshold. Decreasing the fragmentation threshold will reduce the probability of packet errors due to interference from other devices. You must issue `reset wlan` command to activate the new fragment threshold limit.
Syntax	[de] fragment-threshold <limit>

Arguments	`de`
	sets the default value 2312.
	`The limit`
	values are integers 0...3000

Example
`MW1122(conf-wlan)#fragment-threshold 2000`
`MW1122(conf-wlan)#`	

12.5.5 beacon-interval

Description	Sets the time interval in milliseconds for beacons sent by the wireless station. A beacon is a short message containing the network name. If the wireless station receives a beacon with a network name matching its own, it knows that it is on the correct channel and can communicate with other stations in its group. You must issue `reset wlan` command to activate the new beacon interval.
Syntax	[de] beacon-interval <value>

Arguments	`de`
	sets the default beacon interval 200.
	`value`
	is the time interval in milliseconds, 1...65535.

Example
`MW1122(conf-wlan)#beacon-interval 3000`
`MW1122(conf-wlan)#`	

12.5.6 dtim-interval

Description	Sets the DTIM (Delivery Traffic Indication Message) time interval at which M/MW will send its broadcast traffic. You must issue `reset wlan` command to activate the new DTIM interval.
Syntax	[de] dtim-interval <value>

Arguments	`de`
	sets the default interval 2.
	`value`
	is an integer 1...255.

Example
`MW1122(conf-wlan)#dtim-interval 10`
`MW1122(conf-wlan)#`	

12.5.7 short-retry

Description	Specifies the number of retries the radio will do during an RTS/CTS attempt before aborting. You must issue `reset wlan` command to activate the new number of retries.
Syntax	[de] short-retry <value>

Arguments	`de`
	sets the default value 15.
	`value`
	is the number of retries, 7...255.

Example
`MW1122(conf-wlan)#short-retry 20`
`MW1122(conf-wlan)#`	

12.5.8 long-retry

Description	Specifies the number of retries the radio will do during data transmission attempt before aborting. You must issue `reset wlan` command to activate the new number of retries.
Syntax	[de] long-retry <value>

Arguments	`de`
	sets the default value 15.
	`value`
	is the number of retries, 4...255.

Example
`MW1122(conf-wlan)#long-retry 10`
`MW1122(conf-wlan)#`	

12.5.9 tx-power-level

Description	Changes transmit level to low or default.
Syntax	[de] tx-power-level <ident>

Arguments	`de`
	sets the default transmit level.
	Power level identifier
	`low`
	changes the transmit level to low.
	You must issue
	`reset wlan`
	command to activate the new transmit power level. If you use the web interface, the new value will be activated automatically.

Example
`MW1122(conf-wlan)#tx-power-level low`
`MW1122(conf-wlan)#`	

12.5.10 [no] wep mode

Description	Selects wireless encryption mode
Syntax	[no] wep mode <encrypt-scheme>

Arguments	`no`
	switches wireless encryption scheme off.
	`encrypt-scheme`
	argument can be
	`allowed`
	In this mode, the station may use either open-key or shared-key authentication. If the station uses the open-key authentication, encryption is disabled. If the station uses shared-key authentication, encryption is enabled.
	`required`
	In this mode, it is mandatory to use shared-key authentication. If open-key authentication is used, a failed authentication will result. When the station uses shared-key authentication, encryption is always used. Default keys are used if no station-specific key exists. Broadcast/multicast data is encrypted using the default key.
	`specific-key-required`
	In this mode, the station must use shared-key authentication and station-specific keys. 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 stattion-specific keys. Broadcast and multicast data is encrypted using the default key.
	`wifi-required`
	In this mode, the station may use either open-key or shared-key authentication and in both cases encryption is always used.. Broadcast and multicast data is encrypted using the default key.
	You must issue
	`reset wlan`
	command to activate the changes. If you use the web interface, the new values will be activated automatically.

Example
`MW1122(conf-wlan)#wep mode allowed`
`MW1122(conf-wlan)#`	

12.5.11 wep default-key

Description	Selects which default key is used.
Syntax	[no] wep default-key <id>

Arguments	`no`
	switches default key off.
	`id`
	argument can be
	`1, 2, 3`
	or
	`4.`
	You must issue
	`reset wlan`
	command to activate the changes. If you use the web interface, the new values will be activated automatically.

Example
`MW1122(conf-wlan)#wep default-key 1`
`MW1122(conf-wlan)#`	

12.5.12 wep key-entry

Description	Sets the wireless encryption keys 1, 2, 3, and 4.
Syntax	[no] wep key-entry <id> <key-length> <key-value>

Arguments	`no`
	switches the key off.
	`id`
	argument can be
	`1, 2, 3`
	or
	`4.`
	`key-length`
	can be
	`40-bit`
	`104–bit`
	or
	`128-bit.`
	`key-value`
	is a string of 10 (hexadecimal format) or 5 (text format) characters (40-bit key), or 26 (hexadecimal format) or 13 (text format)characters (104-bit key), 32 (hexadecimal format) or 16 (text format) characters (128-bit key). You can enter the WEP keys in text or hexadecimal format. In text format, the allowed characters are: letters A-Z and a-z, numbers 0-9, and special characters , . ; : ! " # ¤ % & / ( ) = ?. In hexadecimal format, the allowed characters are: numbers 0-9 and letters a, b, c, d, e, and f. Note that the WEP key is case sensitive in text format. Give the hexadecimal keys in 0x1a3b5c7d9e format (i.e. insert *0x* in front of the key).
	You must issue
	`reset wlan`
	command to activate the changes. If you use the web interface, the new values will be activated automatically.

Example
`MW1122(conf-wlan)#wep key-entry 1 40-bit 12345`
`MW1122(conf-wlan)#`	

12.5.13 max-client-number

Description	Sets the maximum number of WLAN clients.
Syntax	[de] max-client -number<limit>
Arguments	`limit` is an integer between 1 and 64. The default value is 64.

Example
`MW1122(conf-wlan)#max-client-number 5`
`MW1122(conf-wlan)#`	

12.5.14 admission-control

Description	Switches admission control on/off. Admission control lets only designated wireless stations join the wireless LAN.
Syntax	[no] admission-control <mode>

Arguments	`no`
	switches admission control off.
	`mode`
	argument is
	`phys-address`
	when you want to restrict access by defining a list of permitted addresses.
	You must issue
	`reset wlan`
	command to activate the changes. If you use the web interface, the new values will be activated automatically.

Example
`MW1122(conf-wlan)#admission-control phys-address`
`MW1122(conf-wlan)#`	

12.5.15 sta

Description	Defines a list of addresses (client table) which are permitted to join the wireless LAN. There are two commands here. You can use the default encryption key by only entering the name string and the physical address (MAC address) if a default key has been activated (See *Select default encryption key* command). If the default key has not been activated, the connection will not be encrypted. You can also set a specific encryption key for this station by entering the the key length and key value after the physical address argument. You must issue `reset wlan` command to activate the changes. If you use the web interface, the new values will be activated automatically.
Syntax	[no] sta<name-string><phys-address> [no] sta <name-string><phys-address> <key-length> <key-value>

Arguments	`no`
	switches off access control list.
	`name-string`
	is a name given to this station.
	`phys-address`
	is the physical address (MAC address) of the permitted wireless station.
	`key-length`
	is the key length of the wireless encryption key. The length can be
	`40, 104 or 128`
	bits.
	
	key-value
	is a hexadecimal string of 10 (40-bit), 26 (104-bit) or 32 (128-bit) characters. Give the hexadecimal keys in 0x1a3b5c7d9e format (i.e. insert *0x* in front of the key). The key can also be entered in text format. The key lengths in text format are 5 characters (40-bit key), 13 characters (104-bit) and 16 characters (128-bit key). In text format, the allowed characters are: letters A-Z and a-z, numbers 0-9, and special characters , . ; : ! " # ¤ % & / ( ) = ?.

Example	`MW1122(conf-wlan)#sta Home 00:e0:03:04:79:bc 40-bit 1234567890` `MW1122(conf-wlan)#`

12.5.16 wlan slave-to-eth

Description	This command makes the wireless LAN interface slave to Ethernet interface. In this case you do not have to assign an IP address to the wireless LAN interface. The IP address of the Ethernet interface serves also as an IP address to the wireless LAN interface. Note that you must issue this command on the root level of the configuration mode.
Syntax	[no] wlan slave-to-eth
Arguments	`None.`

Example
`MW1122(conf)#wlan slave-to-eth`
`MW1122(conf)#`	

12.5.17 bridging

Description	Switches on/off bridging at the WLAN interface.
Syntax	[no] bridging
Arguments	`no` switches bridging off.

Example
`MW1122(conf-wlan)#bridging`
`MW1122(conf-wlan)#`	

12.5.18 [no] ip address

Description	Switches on/off routing in the WLAN interface.
Syntax	[no] ip address <IP address> <ip-mask>

Arguments	`no`
	switches routing off.
	`IP address`
	is the IP address you want to assign to the wireless LAN interface.
	`ip-mask`
	is the subnet mask.

Example
`MW1122(conf-wlan)#ip address 192.168.132.12 255.255.255.0`
`MW1122(conf-wlan)#`	

12.5.19 [no] ip rip-send

Description	Switches on/off RIP send function. When enabled, M/MW sends Routing Information Protocol messages to other routers.
Syntax	[no] ip rip-send <rip-send-mode>

Arguments	`no`
	switches rip-send function off.
	`v1`
	send-mode selects RIP version 1.
	`v2`
	send-mode selects RIP version 2.
	`compatible-v1`
	send-mode selects the sending of RIPv2 packets using broadcast.

Example
`MW1122(conf-wlan)#ip rip-send v1`
`MW1122(conf-wlan)#`	

12.5.20 [no] ip rip-receive

Description	Switches on/off RIP receive function. When enabled, M/MW receives Routing Information Protocol messages from other routers.
Syntax	[no] ip rip-receive <rip-receive-mode>

Arguments	`no`
	switches RIP receive function off.
	`v1`
	receive-mode selects RIP version 1.
	`v2`
	receive-mode selects RIP version 2.
	`both-v1v2`
	receive-mode selects both RIP version 1 and version 2.

Example
`MW1122(conf-wlan)#ip rip-receive v1`
`MW1122(conf-wlan)#`	

12.5.21 [no] ip admin-disabled

Description	Enables/disables the management of M/MW through the wireless LAN interface.
Syntax	[no] ip admin-disabled
Arguments	`no` enables management through the wireless LAN interface.

Example
`MW1122(conf-wlan)#ip admin-disabled`
`MW1122(conf-wlan)#`	

12.6 VCC level commands (conf)#vccx

12.6.1 [no] desc

Description	Assigns a name to the ATM channel. The name can be 31 characters long.
Syntax	[no] desc <desc-string>

Arguments	`no`
	deletes the name.
	`<desc-string>`
	is an ASCII string of maximum of 31 characters.

Example
`MW1122(conf-vccx)#desc Work`
`MW1122(conf-vccx)#`	

12.6.2 [no] pvc

Description	Activates an ATM channel and sets the encapsulation for that channel.
Syntax	[no] pvc <vpi> <vci> <encap>

Arguments	`no`
	deactivates the ATM channel.
	`vpi`
	is the Virtual Path Identifier of the ATM channel. Possible values are 0...255.
	`vci`
	is the Virtual Channel Identifier of the ATM channel. Possible values are 0...65535.
	`encap`
	is the encapsulation of the ATM channel. The encapsulations are
	`eth-llc,ip-llc, ppp-vc, pppoe-llc, tunnelled-ppp-vc`

Example
`MW1122(conf-vccx)#pvc 0 100 ip-llc`
`MW1122(conf-vccx)#`	

12.6.3 [no] bridging

Description	Switches bridging on/off on the specified ATM channel.
Syntax	[no] bridging
Arguments	`no` switches off bridging.

Example
`MW1122(conf-vccx)#bridging`
`MW1122(conf-vccx)#`	

12.6.4 ppp pppoe service

Description	Assigns a logical name for pppoe service. Service name for pppoe is required for some ppoe applications.
Syntax	ppp pppoe-service <name-string>

Arguments	`<name-string>`
	assigns a name for ppp pppoe service
	`no`
	ppp pppoe service switches off ppp pppoe service.

Example
`MW1122(conf-vccx)#ppp pppoe—service isp1`
`MW1122(conf-vccx)#`	

12.6.5 [no] ppp authentication

Description	Switches PPP authentication on/off on the specified ATM channel.
Syntax	[no] ppp authentication <mode>

Arguments	`no`
	switches off PPP authentication.
	`chap`
	mode selects Challenge Handshake Authentication Protocol.
	`pap`
	mode selects Password Authentication Protocol.
	`both-chap-pap`
	mode selects both authentication protocols.

Example
`MW1122(conf-vccx)#ppp authentication chap`
`MW1122(conf-vccx)#`	

12.6.6 [no] ppp username

Description	Sets the username used in PPP authentication.
Syntax	[no] ppp username <name-string>

Arguments	`no`
	deletes PPP username.
	`name-string`
	is your PPP username. The maximum length of the username is 64 characters.

Example
`MW1122(conf-vccx)#ppp username ut32aj`
`MW1122(conf-vccx)#`	

12.6.7 [no] ppp password

Description	Sets the password used in PPP authentication.
Syntax	[no] ppp password <passwd-string>

Arguments	`no`
	deletes PPP password.
	`passwd-string`
	is the PPP password. The password must be 4...15 characters long.

Example
`MW1122(conf-vccx)#ppp password jfddslfj`
`MW1122(conf-vccx)#`	

12.6.8 [no] ppp autostop

Description	When enabled, the authentication failure causes the PPP negotiation to stop. The command `reset ppp vccx` is required to restart the PPP negotiation.
Syntax	[no] ppp autostop
Arguments	`no` disables PPP autostop.

Example
`MW1122(conf-vccx)#ppp autostop`
`MW1122(conf-vccx)#`	

12.6.9 [no] ip address

Description	Switches on/off routing on the ATM channel.
Syntax	[no] ip address <IP address> <ip-mask>

Arguments	`no`
	switches routing off.
	`IP address`
	is the IP address you want to assign to the ATM channel. IP address 0.0.0.0 with subnet mask 0.0.0.0 can be used with ppp-vc encapsulation if the dynamic IP address negotiation is required.
	`ip-mask`
	is the subnet mask.

Example
`MW1122(conf-vccx)#ip address 192.168.132.13 255.255.255.0`
`MW1122(conf-vccx)#`	

12.6.10 ip unnumbered

Description	Configures ip unnumbered option for vcc. Unnumbered option will be bound to the Ethernet interface.
Syntax	ip unnumbered <binding>

Arguments	`<to-eth>`
	binds Ethernet to unnumbered interface
	`[no]`
	ip unnumbered disables unnumbered interface in the vcc

Example
`MW1122(conf-vccx)#ip unnumbered to-eth`
`MW1122(conf-vccx)#`	

12.6.11 [no] ip rip-send

Description	Switches on/off RIP send function. When enabled, M/MW sends Routing Information Protocol messages to other routers.
Syntax	[no] ip rip-send <rip-send-mode>

Arguments	`no`
	switches rip-send function off.
	
	v1
	send-mode selects RIP version 1.
	`v2`
	send-mode selects RIP version 2.
	`compatible-v1`
	send-mode selects the sending of RIPv2 packets using broadcast.

Example
`MW1122(conf-vccx)#ip rip-send v1`
`MW1122(conf-vccx)#`	

12.6.12 [no] ip rip-receive

Description	Switches on/off RIP receive function. When enabled, M/MW receives Routing Information Protocol messages from other routers.

Syntax	[no] ip rip-receive <rip-receive-mode>

Arguments	`no`
	switches RIP receive function off.
	
	v1
	receive-mode selects RIP version 1.
	`v2`
	receive-mode selects RIP version 2.
	`both-v1v2`
	receive-mode selects both RIP version 1 and version 2.

Example
`MW1122(conf-vccx)#ip rip-receive v1`
`MW1122(conf-vccx)#`	

12.6.13 [no] ip sif

Description	Enables SIF function
Syntax	[no] ip sif
Arguments	`no` switches the SIFfunction off

Example
`MW1122(conf-vccx)#ip sif`
`MW1122(conf-vccx)#`	

12.6.14 [no] ip napt

Description	Enables Network Address Port Translation.
Syntax	[no] ip napt
Arguments	`no` switches NAPT function off.

Example
`MW1122(conf-vccx)#ip napt`
`MW1122(conf-vccx)#`	

12.6.15 [no] ip server-napt

Description	Sets a NAPT server support entry.
Syntax	[no] ip server-napt <pool-string><hidden-address> <hidden-port-base> <public-port-base> <port-pool-size> <protocol-id>

Arguments	`no`
	deletes pinhole entry.
	`pool-string`
	identifies the server entry.
	
	hidden-address
	is the address of the local server for which the pinhole is made.
	`hidden-port-base`
	is the start of the local port range.
	`public-port-base`
	is the start of the external port range.
	`port-size`
	is the size of the port range.
	`protocol-id`
	is the protocol allowed through the pinhole. Available protocols are: UDP, TCP, PPTP-GRE, and ESP-IPSEC
	Example:
	When
	`hidden-port-base`
	is 80,
	`public-port-base`
	is 80 and
	`port-size`
	is 1, traffic coming to external port (WAN port) 80 will be mapped to internal port 80.

Example
`MW1122(conf-vccx)#ip server-napt web_server 192.168.1.100 80 80 1 tcp`
`MW1122(conf-vccx)#`	

12.6.16 [no] ip admin-disabled

Description	Enables/disables the management of M/MW through the ATM channel.
Syntax	[no] ip admin-disabled
Arguments	`no` enables management through the ATM channel.

Example
`MW1122(conf-vccx)#ip admin-disabled`
`MW1122(conf-vccx)#`	

12.6.17 tos-mapping

Description	Tos-mapping allocates ip packets originated from the local area network with one of the five transmit queues implemented by the modem.
Syntax	tos-mapping <1st-privilege-qmask> <2nd-privilege-qmask> <3rd -privilege-qmask> <4th-privilege-qmask>

Arguments	`<1st-privilege-qmask>`
	bit mask for 1st privilege queue
	`<2nd-privilege-qmask>`
	bit mask for 2nd privilege queue
	`<3rd-privilege-qmask>`
	bit mask for 3rd privilge queue
	`<4th-privilege-qmask>`
	bit mask for 4th privilege queue
	`[no]`
	tos-mapping removes all bit masks

Example
`MW1122(conf-vccx)#tos—mapping 80 40 20 10`
`MW1122(conf-vccx)#`	

12.7 Vbridge level commands (conf)#vbridge

12.7.1 [no] ip address

Description	Switches on/off routing.
Syntax	[no] ip <IP address> <ip-mask>

Arguments	`no`
	switches off routing.
	`IP address`
	is the IP address of the Vbridge in dotted decimal notation.
	`ip-mask`
	is the subnet mask in dotted decimal notation.

Example
`MW1122(conf-vbridge)#ip address xxx.xxx.xxx.xxx 255.255.255.0`
`MW1122(conf-vbridge)#`	

12.7.2 [no] ip rip-send

Description	Switches on/off RIP send function. When enabled, M/MW sends Routing Information Protocol messages to other routers.
Syntax	[no] ip rip-send <version>

Arguments	`no`
	switches rip-send function off.
	`v1`
	version selects RIP version 1.
	`v2`
	version selects RIP version 2.
	`compatible-v1`
	version selects the sending of RIPv2 packets using broadcast.

Example
`MW1122(conf-vbridge)#ip rip-send v1`
`MW1122(conf-vbridge)#`	

12.7.3 [no] ip rip-receive

Description	Switches on/off RIP receive function. When enabled, M/MW receives Routing Information Protocol messages from other routers.
Syntax	[no] ip rip-receive <rip-receive-mode>

Arguments	`no`
	switches RIP receive function off.
	`v1`
	receive-mode selects RIP version 1.
	`v2`
	receive-mode selects RIP version 2.
	`both-v1v2`
	receive-mode selects both RIP version 1 and version 2.

Example
`MW1122(conf-vbridge)#ip rip-receive v1`
`MW1122(conf-vbridge)#`	

12.7.4 [no] ip admin-disabled

Description	Enables/disables the management of M/MW through the vbridge.
Syntax	[no] ip admin-disabled
Arguments	`no` enables management through the ATM channel.

Example
`MW1122(conf-vbridge)#ip admin-disabled`
`MW1122(conf-vbridge)#`	

12.8 Mngtvcc level commands (conf)#mngtvcc

12.8.1 [no] pvc

Description	Activates a dedicated management channel and sets the encapsulation for that channel.
Syntax	[no] pvc <vpi> <vci> <encap>

Arguments	`no`
	deactivates the ATM channel.
	`vpi`
	is the Virtual Path Identifier of the ATM channel. Possible values are 0...255.
	`vci`
	is the Virtual Channel Identifier of the ATM channel. Possible values are 0...65535.
	`encap`
	is the encapsulation of the ATM channel. Encapsulations are
	`ppp-vc, eth-llc, pppoe-llc`
	and
	`ip-llc.`

Example
`MW1122(conf-mngtvcc)#pvc 0 100 eth-llc`
`MW1122(conf-mngtvcc)#`	

12.8.2 ppp pppoe-service

Description	Assigns a logical name for pppoe service. Service name for pppoe is required for some ppoe applications.

Syntax	ppp pppoe-service <name-string>

Arguments	`<name-string>`
	asigns a name for ppp pppoe service
	`[no]`
	ppp pppoe service disables pppoe service

Example
`MW1122(conf-mngtvcc)#ppp pppoe service manager`
`MW1122(conf-mngtvcc)#`	

12.8.3 [no] ppp authentication

Description	Switches PPP authentication on/off on the specified ATM channel.
Syntax	[no] ppp authentication <mode>

Arguments	`no`
	switches off PPP authentication.
	`chap`
	mode selects Challenge Handshake Authentication Protocol.
	`pap`
	mode selects Password Authentication Protocol.
	`both-chap-pap`
	mode selects both authentication protocols.

Example
`MW1122(conf-mngtvcc)#ppp authentication chap`
`MW1122(conf-mngtvcc)#`	

12.8.4 [no] ppp username

Description	Sets the username used in PPP authentication.
Syntax	[no] ppp username <name-string>

Arguments	`no`
	deletes PPP username.
	`name-string`
	is your PPP username. The maximum length of the username is 64 characters.

Example
`MW1122(conf-mngtvcc)#ppp username ut32aj`
`MW1122(conf-mngtvcc)#`	

12.8.5 [no] ppp password

Description	Sets the password used in PPP authentication.
Syntax	[no] ppp password <passwd-string>

Arguments	`no`
	deletes PPP password.
	`passwd-string`
	is the PPP password. The password must be 4...15 characters long.

Example
`MW1122(conf-mngtvcc)#ppp password jfddslfj`
`MW1122(conf-mngtvcc)#`	

12.8.6 [no] ppp autostop

Description	When enabled, the authentication failure causes the PPP negotiation to stop. The command `reset ppp vccx` is required to restart the PPP negotiation.
Syntax	[no] ppp autostop
Arguments	`no` disables PPP autostop.

Example
`MW1122(conf-mngtvcc)#ppp autostop`
`MW1122(conf-mngtvcc)#`	

12.8.7 [no] ip address

Description	Switches on/off routing.
Syntax	[no] ip address <IP address> <ip-mask>

Arguments	`no`
	switches off routing.
	`IP address`
	is the IP address of the Vbridge in dotted decimal notation. IP address 0.0.0.0 with subnet mask 0.0.0.0 can be used with ppp-vc encapsulation if the dynamic IP address negotiation is required.
	`ip-mask`
	is the subnet mask in dotted decimal notation.

Example
`MW1122(conf-mngtvcc)#ip address xxx.xxx.xxx.xxx 255.255.255.0`
`MW1122(conf-mngtvcc)#`	

12.8.8 [no] ip rip-receive

Description	Switches on/off RIP receive function.
Syntax	[no] ip rip-receive <rip-receive-mode>

Arguments	`no`
	switches rip-send function off.
	`v1`
	receive-mode selects RIP version 1.
	`v2`
	receive-mode selects RIP version 2.
	`both-v1v2`
	receive-mode selects both RIP version 1 and version 2.

Example
`MW1122(conf-mngtvcc)#ip rip-receive v1`
`MW1122(conf-mngtvcc)#`	

12.9 Common level commands(conf)#common

12.9.1 ppp mru

Description	Sets the maximum size of the received PPP packets.
Syntax	[de] ppp mru <size>
Arguments	`size` is the size of a PPP packet. Default size is 1500.

Example
`MW1122(conf-common)#ppp mru 1000`
`MW1122(conf-common)#`	

12.9.2 ppp restart

Description	Defines how long M/MW waits for the configure-request packet.
Syntax	[de] ppp restart <time>
Arguments	`time` in seconds (1-30)

Example
`MW1122(conf-common)#ppp restart 5`
`MW1122(conf-common)#`	

12.9.3 ppp max-config

Description	Defines how many times the configure-request packet will be sent.
Syntax	[de] ppp max-config <pkt-count>
Arguments	`pkt-count` is the number of configure request packets, values 1...30.

Example
`MW1122(conf-common)#ppp max-config 10`
`MW1122(conf-common)#`	

12.9.4 ppp max-terminate

Description	Defines how many terminate-request packets will be sent before M/MW decides that the connection is down.

Syntax	[de] ppp max-terminate <pkt-count>
Arguments	`pkt-count` is the number of configure request packets, values 1...30.

Example
`MW1122(conf-common)#ppp max-terminate 10`
`MW1122(conf-common)#`	

12.9.5 ppp max-failure

Description	Defines how many times PPP options will be offered before the negotiation fails.
Syntax	[de] ppp max-failure <pkt-count>
Arguments	`pkt-count` is the number of packets, values 1...30.

Example
`MW1122(conf-common)#ppp max-failure 10`
`MW1122(conf-common)#`	

12.9.6 [no] ip cache

Description	Switches IP cache on/off. Enabled IP cache increases the speed of the IP packet forwarding.
Syntax	[no] ip cache
Arguments	`no` switches IP cache off.
Example `MW1122(conf-common)#` `MW1122(conf-common)#`	

12.9.7 [no] ip route

Description	Adds/deletes an IP route
Syntax	[no] ip route <dest-net> <net-mask> <gateway> <if>

Arguments	`no`
	deletes an IP route.
	`dest-net`
	is the IP address of the destination in the dotted decimal notation.
	`net-mask`
	is the subnet mask of the destination in dotted decimal notation.
	`gateway`
	is the default gateway for the route.
	`if`
	is the interface through which the destination can be reached,
	`vbridge`
	or
	`mngtvcc`.

Example
`MW1122(conf-common)#ip route 131.112.11.0 255.255.255.0 131.2.111.2 mngtvcc`
`MW1122(conf-common)#`	

12.9.8 [no] ip host-acl

Description	You can define up to four networks from which M/MW1122 can be accessed using telnet or http. If you define one or more addresses, M/MW can be accessed from the specified addresses only.

Syntax	[no] ip host-acl <access-net> <net-mask>

Arguments	`no`
	switches host access list off.
	`access-net`
	is the allowed host network and
	`net-mask`
	is its subnet mask.

Example
`MW1122(conf-common)#ip host-acl 192.168.1.0 255.255.255.0`
`MW1122(conf-common)#`	

12.9.9 [no] ip service

Description	Adds/deletes an IP service
Syntax	[no] ip service <dest-name> <port-id> <port-nr-start>[<port-nr-end>]

Arguments	`service-name`
	`dest-net`
	is the IP address of the destination in the dotted decimal notation.
	`net-mask`
	is the subnet mask of the destination in dotted decimal notation.
	`gateway`
	is the default gateway for the route.
	`if`
	is the interface through which the destination can be reached,
	`vbridge`
	or
	`mngtvcc`.

Example
`MW1122(conf-common)#ip service 131.112.11.1 255.255.255.0 131.2.111.2 mngtvcc`
`MW1122(conf-common)#`	

12.9.10 ip filter

Description	IP filter option filters ip packets originated from the local area network towards wide area network (vcc).
Syntax	ip filter <service-name> <src-addr-pool> <dst-addr-pool> <filtering-rule> [<tos>]

Arguments	`<service-name>`
	given as symbolic name as defined by the ip service list
	`<src-addr-pool>`
	defines source address pool subject to the filtering
	`<dst-addr-pool>`
	defines address pool subject to the destination filtering
	`all`
	includes all addresses
	`<filtering-rule`
	pass, deny or drop
	`[<tos>]`
	optionally provide value of tos precedence
	<csc-1, csc-2, csc-3, csc-4, csc-5, csc-6, csc-7, af-11, af-12, af-13, af-21, af-22, af-23, af-31, af-32, af-33, af-41, af-42, af-43, ef>

Example
`MW1122(conf-common)#ip filter My_Filter 192.168.1.1 192.168.1.3 deny`
`MW1122(conf-common)#`	

12.9.11 [no] ip sif-server

Description	switches on the SIF server function

Syntax	ip sif-server <service name> <dst-addr-pool>

Arguments	`service name`
	assigns a name for the SIF server
	`dst-addr-pool`
	defines the destination address range for the SIF server

Example `MW1122(conf-common)# ip sif-server webserver 192.168.1.3-192.168.1.3`	

12.9.12 [no] ip napt-server

Description	switches the NAPT server function on/off
Syntax	[no] ip napt-server <service name> <dst-addr> [<src-port>]

Arguments	`[no]`
	switches the NAPT server function off
	`service-name`
	assigns a name for the NAPT server
	`dst-addr`
	defines the destination address for the NAPT server
	`src-port`
	defines the source port

Example
`MW1122(conf-common)# ip napt-server`
`MW1122(conf-common)#`	

12.9.13 [no] dhcp mode

Description	Switches on/off dynamic host configuration protocol.
Syntax	[no] dhcp mode <service>

Arguments	`no`
	switches off DHCP.
	`service`
	parameter value is
	`server`
	when you want to use M/MW as a DHCP server.
	or
	`relay`
	when you want to use M/MW as a.....

Example
`MW1122(conf-common)#dhcp mode server`
`MW1122(conf-common)#`	

12.9.14 [no] dhcp address

Description	You can define two DHCP address ranges with this command. The default pool is the IP address of the interface with a subnet mask 255.255.255.0. If you use DHCP, you must set both ranges, one for the Ethernet interface and the other for the wireless LAN interface. (1 and 2). The only exeption is when you use wireless LAN interface as a slave to Ethernet interface. If you don't define an address range, up to two ranges will be defined automatically for ETH/WLAN/ VBRIDGE interfaces, in this order, if the interface has an IP address.
Syntax	[no] dhcp address <scope> <pool-base> <pool-mask> <pool-size>

Arguments	`no`
	switches off address pool.
	`scope`
	defines the pool. Values are
	`1`
	and
	`2.`
	`pool-base`
	is the first IP address in the pool in dotted decimal format.
	`pool-mask`
	is the subnet mask of the pool addresses.
	`pool-size`
	is the size of the address pool, 0...254.

Example	`MW1122(conf-common)#dhcp address 1 168.190.1.1 255.255.255.0 100` `MW1122(conf-common)#`

12.9.15 [no] dhcp gateway

Description	Defines a gateway address for DHCP clients
Syntax	dhcp gateway <scope><gw-server>

Arguments	`scope`
	Defines the DHCP pool (1 or 2)
	`gw-server`
	defines an address for the gateway server

Example
`MW1122(conf-common)# dhcp gateway`
`MW1122(conf-common)#`	

12.9.16 [no] dhcp dns

Description	Defines a DNS address for the DHCP clients.
Syntax	[de | no] dhcp dns <scope> <class> <dns-server>

Arguments	`scope`
	defines the DHCP pool (1 or 2).
	`class`
	defines whether the server is a
	`primary`
	or a
	`secondary`
	server.
	`dns-server`
	is the IP address of the DNS server.

Example
`MW1122(conf-common)#dhcp dns 1 primary 190.168.2.1`
`MW1122(conf-common)#`	

12.9.17 [no] dhcp lease-time

Description	Defines the time how often the PC has to renew its DHCP lease.
Syntax	[de] dhcp lease-time <scope> <time-count>

Arguments	`scope`
	defines the DHCP pool (1 or 2).
	`time-count`
	is the renewal interval in minutes, 1...65535.

Example
`MW1122(conf-common)#dhcp lease-time 1 360`
`MW1122(conf-common)#`	

12.9.18 [no] dhcp domain-name

Description	Set the domain name for the DHCP pool. The domain name is used to show the client in which network the client is in.
Syntax	[no] dhcp domain-name <scope> <name-string>

Arguments	`scope`
	defines the DHCP pool (1 or 2).
	`name-string`
	set the domain name.

Example
`MW1122(conf-common)#dhcp domain-name 1 nokia.com`
`MW1122(conf-common)#`	

12.9.19 [no] dhcp relay-addr

Description	Defines the IP address of the DHCP server when M/MW is used as DHCP relay.
Syntax	[no] dhcp relay-addr <dhcp-server><auto-server> <if>

Arguments	`no`
	switches off DHCP relay server address.
	`<dhcp-server>`
	parameter value is the IP address of the external DHCP server when you want to use M/MW as a DHCP server and
	`<auto-server>`
	`<if>`

Example
`MW1122(conf-common)#dhcp relay-addr 192.168.123.1`
`MW1122(conf-common)#`	

12.9.20 [no] dns

Description	Defines the address of the domain name server used by M/MW.
Syntax	[no] dns address <class> <dns-server>

Arguments	`no`
	deletes domain name server address.
	`class`
	defines whether the server is a
	`primary`
	or a
	`secondary`
	name server.
	`dns-server`
	is the IP address of the DNS server.

Example
`MW1122(conf-common)#dns address primary 190.168.12.1`
`MW1122(conf-common)#`	

12.9.21 snmp name

Description	Assigns a logical name of the snmp managed object for snmp protocol.
Syntax	snmp <name-string>

Arguments	`<name-string>`
	assigns a name for the snmp managed object
	`[de]`
	snmp name removes snmp name

Example
`MW1122(conf-common)#snmp name gateway1`
`MW1122(conf-common)#`	

12.9.22 snmp contact

Description	Assigns a logical name of the snmp managed object for snmp protocol. This may be a telephone number, e-mail address, person's name etc.
Syntax	snmp <contact-string>

Arguments	`<contact-string>`
	assigns snmp contact information for snmp protocol
	`[no]`
	disables contact information

Example
`MW1122(conf-common)#snmp contact help.desk@nokia.com`
`MW1122(conf-common)#`	

12.9.23 snmp location

Description	Assigns location information of the snmp managed object for snmp protocol
Syntax	snmp <location-string>

Arguments	`<location-string>`
	assigns snmp location information
	`[no]`
	disables snmp location information

Example
`MW1122(conf-common)#snmp location 10thfloor`
`MW1122(conf-common)#`	

12.9.24 snmp getr-community

Description	Assigns a community name for snmp protocol (read) requests
Syntax	snmp <getr-community-string>

Arguments	`<gtr—communitystring>`
	assigns a community name for snmp get (read) requests.
	`[de]`
	sets default community name (public)

Example
`MW1122(conf-common)#snmp getr-community public`
`MW1122(conf-common)#`	

12.9.25 snmp trap-community

Description	Assigns a community name used for snmp traps.
Syntax	snmp > <trap-community-string>
Arguments	<community-string> assigns a community name for snmp traps. [de] sets default community name for snmp traps (public)
Example MW1122(conf-common)#snmp trap-community name public MW1122(conf-common)#	

12.9.26 snmp dest-trap-addr

Description	Assigns an ip address of the snmp management workstation where the snmp traps will be sent.
Syntax	snmp <ip-address>
Arguments	<ip-address> ip address where snmp traps will be sent [no] deletes trap destination address.
Example MW1122(conf-common)#snmp dest-trap-addr 131.228.121.1 MW1122(conf-common)#	

12.9.27 [no] misc adsl-variant (MW1324 only)

Description	Switches between full-rate ADSL (G.992.1) and ADSL lite (G.992.2).
Syntax	[no] misc adsl-variant <specifier>

Arguments	`specifier`
	argument
	`no`
	sets default ADSL mode.
	`lite`
	switches to ADSL lite.
	argument
	`g_dmt`
	switches to G.DMT mode.
	`multimode`
	switches to multimode.
	`ansi`
	switches to ANSI mode.

Example
`MW1324(conf-common)#misc adsl-variant lite`
`MW1324(conf-common)#`	

12.9.28 [no] misc adsl-variant (MW1112, MW1122, M1112 and M1122)

Description	Switches between full-rate ADSL (G.992.1) and ADSL lite (G.992.2).
Syntax	[no] misc adsl-variant <specifier>

Arguments	`specifier`
	argument
	`no`
	sets default ADSL mode.
	`lite`
	switches to ADSL lite.
	argument
	`t001`
	allows the use of the old Alcatel datapump software (2.5.8). Note, that this command will restart the DSL line
	`no misc adsl-variant`
	sets full rate ADSL mode

Example
`M1122(conf-common)#misc adsl-variant lite`
`M1122(conf-common)#`	

12.9.29 [no] misc shdsl-region (MW1352 only)

Description	europe: This option enables ITU-T G991.2 Annex B operation for European networks. north-america: this option enables ITU-T G991.2 Annex A operation for North American networks.
Syntax	shdsl - region
Arguments	`europe` `north america`

Example
`MW1352(conf-common)#misc shdsl-region europe`
`MW1352(conf-common)#`	

12.9.30 [no] misc shdsl-variant (MW1352 only)

Description	Sets the SHDSL mode and data rate. By default, MW1352 is in CP-adaptive mode.
Syntax	[no] misc shdsl-variant <specifier> <bitrate>

Arguments	`<specifier>`
	selects the SHDSL mode. Allowed specifiers are:
	`cp-fixed`
	sets the CP (customer premises) mode and fixed data rate.
	`co-fixed`
	sets the CO (central office) mode and fixed data rate.
	`co-adaptive`
	sets the CO mode and adpative data rate mode
	`<bitrate>`
	sets the bitrate. The fixed mode bitrates are: 64kbit/s-2304 kbit/s with 64 kbit/ granularity.
	`no misc shdsl-variant`
	sets the default CP-adaptive mode.

Example
`MW1352(conf-common)#misc SHDSL-variant cp-fixed 2304`
`MW1352(conf-common)#`	

12.9.31 [no] misc shdsl-startup-margin (MW1352 only)

Description	Startup Margin is the difference in dB between noise at which the MW1352 will operate at an error rate of 10^{-7} BER and the set noise margin in dB (default 6dB)
Syntax	shdsl-startup-margin<value>
Arguments	`value` `0–15`

Example
`MW1352(conf-common)#misc shdsl–startup-margin 3`
`MW1352(conf-common)#`	

12.9.32 misc shdsl-backoff-disabled (MW1352 only)

Description	Select this option to enable/disable transmit power reduction on short loops
Syntax	misc shdsl-backoff-disabled
Arguments	[no] switches off transmit power
Example MW1352(conf-common)#misc shdsl-backoff-disabled MW1352(conf-common)#	

12.9.33 [no] misc shdsl-power-scale (MW1352 only)

Description	Provides a power scale parameter
Syntax	shdsl -power-scale <value>
Arguments	values <-3.0...2.0> – given as decimal number
Example MW1352(conf-common)#misc shdsl–power-scale 2 MW1352(conf-common)#	

12.9.34 [no] misc pptp-to-pppoe

Description	switches on/off pptp to pppoe tunnelling
Syntax	[no] pptp-to-pppoe <if-id>
Arguments	if-id interface identifier VCC1...VCC8
Example MW1122(conf-common)# misc pptp-to-pppoe	

12.9.35 misc alg-h323-disabled

Description	Disables application level gateway for h323 protocol. This option is needed because some video conference softwares do not work properly when alg-h323 is used.
Syntax	misc alg-h323-disabled
Arguments	[no] activates alg-h323

Example
`MW1122(conf-common)# misc alg-h323-disabled`
`MW1122(conf-common)#`	

12.9.36 [no] misc interwan-routing

Description	Switches on/off routing between ATM channels.
Syntax	[no] interwan-routing
Arguments	no switches off routing between ATM channels.

Example
`MW1122(conf-common)#misc interwan-routing`
`MW1122(conf-common)#`	

12.9.37 [no] misc interwan-bridging

Description	Switches on/off bridging between ATM channels.
Syntax	[no] interwan-bridging
Arguments	no switches off bridging between ATM channels.

Example
`MW1122(conf-common)#misc interwan-bridging`
`MW1122(conf-common)#`	

Appendix A. Technical specifications

A.1 Technical specifications

Features	
ADSL (MW1122, MW1324)	
Physical layer	ANSI T1.413 Issue 2 (ANSI ADSL), ITU-T G.992.1 (ITU-T ADSL), ITU-T G.992.2 (G.lite), and ITU-T G.994.1 (Handshake) compatible
ADSL (M1112, MW1112)	
Physical layer	ETSI TS 101 388 compatible
ADSL line connector(all models)	RJ-12
ATM over ADSL (all models except MW1352)	
ATM connections	PVC, up to 8 virtual circuits for data
Service categories	UBR
Encapsulations	RFC2684 ETH-LLC, RFC2684 IP-LLC, RFC2364 PPP-VC, RFC2364 TUNNELLED-PPP-VC, RFC2516 PPPoE-LLC
SHDSL (MW1352 only)	
Physical layer	ITU-T G.991.2 (ITU-T SHDSL)
SHDSL line connector	RJ-12
ATM over SHDSL (MW1352 only)	
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, PPPoE-LLC
Ethernet interface	
Ethernet	10Base-T, half duplex
Encapsulation	DIXv2 (transmit), IEEE 802.3 and DIXv2 (receive)
Ethernet connectors	RJ-45
HomePNA 2.0 interface (MW1324 only)	
HPNA	Half duplex, 4 - 16 Mbit/s
Modes	HPNA 1.0, 1.1 and 2.0 specifications data rates up to 16 Mbit/s

Encapsulation	Ethernet compatible
Connector	RJ-12
Wireless LAN interface (MW models only)	
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, DHCP relay, DHCP client, DNS relay, PPTP local tunnelling, PPPoE client
Class of Service	Weighted fair queueing
Firewall	Stateful inspection firewall
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 + 1 stop bit (8-N-1)
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
HPNA (MW1324 only)	HomePNA activity and status
ETH	Ethernet activity and status
COL	Ethernet collision
WLAN	WLAN activity and status
STA	M/MW startup
PWR	Power on
Mechanical construction and power supply	
Width	255 mm
Height	65 mm
Depth	230 mm
Weight	1 kg
Mains connection	
Voltage	100 Vrms-240 Vrms AC (nominal values)
Frequency	50/60 Hz
Power consumption	10 W
Ambient confitions, EMC and safety	
Operating temperature	5 to 45°C
Humidity	10% to 90%, non-condensing
EMC	
M/MW 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	EN300286–2: 1997, FCC part 15 class B
Overvoltage	ITU-T K.21, FCC PART 68
Safety	
Safety	EN 60950, UL 1950, 3rd edition

Glossary

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
AAL	ATM Adaptation Layer
AH	Authentication Header
ALG	Application Layer Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CO	Central Office
COL	Collision
CoS	Class of Service
CP	Customer Premises
CTS	Clear-To-Send
DHCP	Dynamic Host Configuration Protocol
DMT	Discrete Multitone
DNS	Domain Name Server
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTIM	Delivery Traffic Indication Message
EMC	Electromagnetic Compatibility
ESP	Encapsulation Security Payload

ETH	Ethernet
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HPNA	Home Phone Line Network Alliance
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
If	Interface
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPSEC	Internet Protocol Security
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Media Access Control
MNGT	Management

MNGTVCC	Management Virtual Channel Connection
MTU	Maximum Transmission Unit
NAPT	Network Address and Port Translation
NNTP	Network News Transfer Protocol
PAP	Password Authentication Protocol
PHY	Physical Layer
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
PVC	Permanent Virtual Circuit
PWR	Power
RAN	Remote Access Node
RFC	Request For Comments
RIP	Routing Information Protocol
RTS	Request-To-Send
SHDSL	Single pair High bit rate Digital Subscriber Line
SIF	Stateful Inspection Firewall
SNMP	Simple Network Management Protocol
STA	Status
TCP	Transmission Control Protocol
TC-PAM	Trellis Coded Pulse Amplitude Modulation.
TFTP	Trivial File Transfer Protocol
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
VCC	Virtual Channel Connection

VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WFQ	Weighted Fair Queueing
WLAN	Wireless Local Area Network
WWW	World Wide Web

Terms

10Base-T	10 Mbit/s Ethernet LAN specification using two pairs of twisted cabling. 10Base-T is a part of the IEEE 802.3 specification.
Authentication	Determining the identity of a user that is attempting to access a network.
Asymmetric digital subscriber line, ADSL	High-speed transmission technology using existing copper telephone lines. Data is transmitted in general from a server to a user.
Bridge	Device or software that transmits data from a source network to a destination network. These two networks use normally the same protocol.
Broadcast	Transmitting data to everyone on the network. Rf. multicast.
Command line interface, CLI	Character-based man-machine interface for configuring a device.
Digital subscriber line, xDSL	Generic abbreviation for various different DSL types, for example ADSL, HDSL, SDSL, and VDSL.
Domain name server, DNS	Server used on the Internet for translating names of network nodes into IP addresses. A name server lets users access networks nodes by name instead of having to remember IP address numbers.
Domain name system, DNS	System containing domain name servers.
Encapsulation	Method for using multiple protocols within the same network. This is done by enclosing a data unit of one protocol into a data unit of another protocol.
Encryption	For data security, transforming data into an unreadable form to prevent any but the intended receiver from reading it.

Encryption key	Character or bit sequence which is used for encryption, decryption or authentication of data.
Ethernet	Local area network that connects devices like computers, printers, and terminals. Ethernet operates over twisted-pair or coaxial cable.
Gateway	Device or software in an information network which links two networks that use differents communications protocols.
HomePNA, HPNA	Technology for the home network based on Ethernet and using existing phone lines. Voice and data travel on the same wires without interfering with each others.
Internet protocol security, IPSEC	Protocol that enhances data security by providing secure exchange of packets at the IP layer.
IP address	Numerical identification individualising a device connected to the Internet or a network for example 192.168.1.2.
Local area network, LAN	Data transmission network covering a small area for example a flat or a house. Usually based on Ethernet technology.
MAC address	Unique fixed address of a piece of hardware, normally set at the time of manufacture and used in LAN protocols.
Multicast	Transmitting data to a select group of recipients at the same time for example sending an e-mail message to a mailing list. Rf. broadcast.
Network address port translation, NAPT	Method by which IP addresses and translating transport identifiers (for example TCP and UDP port numbers, ICMP query identifiers) are mapped from one address realm to another, providing transparent routing to end hosts.
Packet Internet Groper, ping	Program used to test whether a particular network destination is accessible, by sending an ICMP (Internet control message protocol) echo request and waiting for a response. Ping is used primarily to troubleshoot Internet connections.
Ping	See Packet Internet Groper.
Proxy server	Server which retrieves information from the Internet and stores the information that users frequently use to speed up the retrieval. For example, in using the web the proxy server speeds up the downloading of those web pages located behind slow or congested network connections.
Request for comments, RFC	Document series which describes the Internet suite of protocols and related experiments.
Router	Device or software which transmits data from a source network to a destination network in accordance with an address.

Single pair high bit rate digital subscriber line, SHDSL	High-speed transmission technology using existing copper telephone lines.
Stateful Inspection Firewall, SIF	Firewall which provides access control at the network layer by inspecting the contents of incoming packets and accepting or rejecting them depending upon their content.
Subnet mask	Numerical indentification used to determine what subnetwork an IP address belongs to for example 255.255.255.0.
Tunnelling	Technique to improve the rate, reliability, and security of transmission in a network by creating for transmission a permanent connection, called tunnel, which is often secured by encryption.
Unspecified bit rate, UBR	Quality of service QoS where there are no guarantees in terms of data loss rate and delay. UBR is very efficient, but not used for critical data.
VBRIDGE vai Vbridge	Gateway/bridge management interface used as a bridge host interface or gateway interface depending on the operation mode On the M/MW web pages, the VBRIDGE is called gateway or bridge IP interface.
Virtual private network, VPN	Network which is constructed by using a public information network and which uses encryption. The terminal equipment can be situated all over the world but they function as if they were connected to a local area network LAN.
Weighted fair queueing, WFQ	Traffic management technique that controls transmission bandwidth allocation determined by the bandwidth needed for the traffic flow.
Wide area network, WAN	Data communications network that serves users across a broad geographic area.
Wi-Fi, Wireless Fidelity	Wireless LAN standard (IEEE 802.11b) developed to maximise multi-vendor interoperability as well as to introduce a variety of performance improvements and benefits to the wireless networking technology.
Wired equivalent privacy, WEP	Security protocol used to provide data security by encrypting data over radio waves. The WEP is defined in IEEE 802.11 standard and it is designed to provide the same level of security as that of a wired LAN.
Wireless LAN Card, Nokia C111	Card which enables to wirelessly connect compatible laptop computers, hand-held devices, desktop PCs, and other devices with a type II or II PC card slot to a wired local area network through an access point.
Wireless local area network, WLAN	Local area network using wireless connections as transmission path.

NOKIA

CONNECTING PEOPLE