Nokia M11

ADSL Router

T66220

USER'S MANUAL

NOKIA

Nokia M11

ADSL ROUTER

User’s Manual

C33833.20 A0

The manufacturer has made every effort to ensure that the instructions contained in the documents are adequate and free of errors and omissions. The manufacturer will, if necessary, explain issues which may not be covered by the documents. The manufacturer’s liability for any errors in the documents is limited to the correction of errors and the aforementioned advisory services.

The documents have been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using them.The manufacturer welcomes customer comments as part of the process of continual development and improvement of the documentation in the best way possible from the user’s viewpoint. Please submit your comments to the nearest Nokia sales representative.

Document History

Document	Date	Comment
C33533001SE_00	30.12.1999	

Contents

Chapter 5

Chapter 1
Introduction to Nokia M11

Nokia M11 is an ADSL (Asymmetric Digital Subscriber Line) modem which enables high-speed Internet access and LAN (Local Area Network) interconnection. It increases the capacity of the already installed telephone lines used traditionally for telephone services. M11 enables high-speed connections for residential users, small offices and telecommuters.

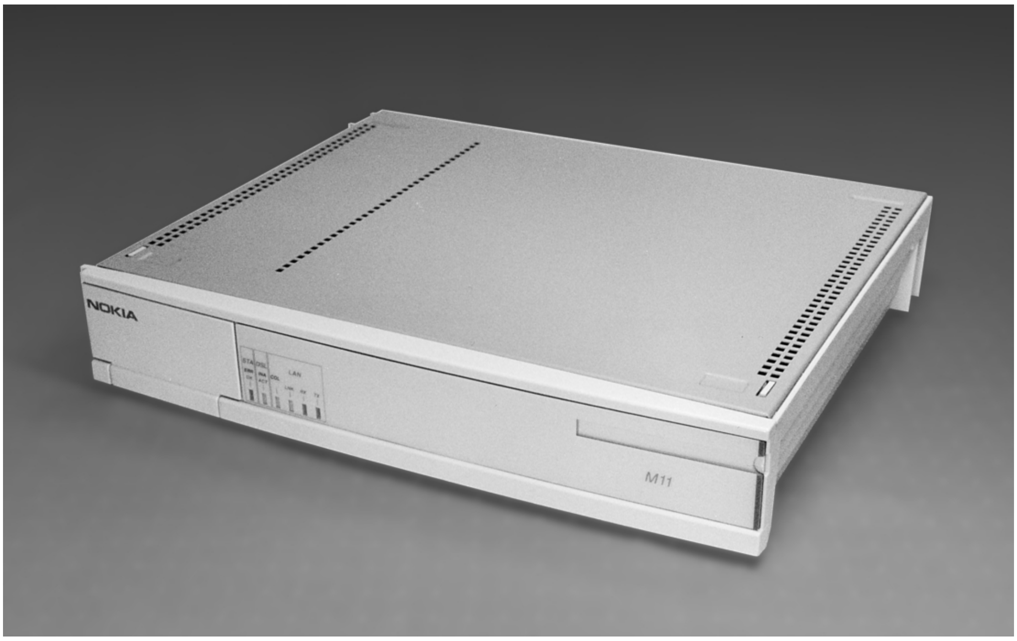


Figure 1-1 Nokia M11

Nokia M11 is a modem with an ADSL router and bridge. This allows a PC equipped with a 10Base-T Ethernet interface to be connected to a remote IP network via a Digital Subscriber Line Access Multiplexer (DSLAM) and an ATM access network. M11 can also act as a bridge between the Ethernet LAN and ADSL/ATM network interfaces. M11 is compatible with Nokia D DSLAM.

The ADSL transmission is based on a DMT (Discrete multitone) line code and it provides speeds up to 8 Mbit/s downstream (from the network) and 1 Mbit/s upstream (to the network). M11 can adjust its speed to the line conditions in steps of 32 kbit/s, maximising the data throughput over the given distance. Nokia M11 is compatible with the existing and emerging ADSL standards: ANSI T1.413 Issue 2 (ANSI ADSL), ITU-T G.992.1 (ITU-T ADSL), ITU-T G.992.2 (ITU-T ADSL Lite), and ITU-T G.996.1 (Handshake).

M11 provides optimised access to high-speed data services. It can be used to connect telecommuters to the corporate network or netsurfers to the Internet Service Provider’s (ISP) network, for example.

As a default, M11 supports plug-and-play operation for Internet access applications. The ADSL connection, data connection and Internet network addresses are set up automatically.

M11 has an integrated Web server which enables configuring the most frequently used parameters with an ordinary Web browser. M11 can also be managed through a command line interface via telnet protocol or via local console interface.

An external POTS (Plain Old Telephone System) filter enables the simultaneous use of the conventional telephone service and the ADSL data services.

Chapter 2
Applications and features

This chapter introduces the most common applications, features and management method options of M11.

2.1 Applications

M11 has three main applications:

- Internet access
- Remote work
- LAN interconnection

In these application examples M11 can act as a router, bridge or NAPT router. The selected mode for every single application depends on the access and service provider network architectures. Some basic application examples are described in this chapter. See Chapter 6 for more information on routing, bridging and Network Address Port Translation.

2.1.1 Internet access using M11 as a NAPT router

M11 can connect your PC via your operator’s Digital Subscriber Line Access Multiplexer (DSLAM) and ATM network to an Internet Service Provider (ISP). If you are connected to a single ISP, the network addresses (IP addresses) in your home can be part of the ISP’s IP address range. However, in many cases it is more practical that the home network is an independent network utilising private IP addresses which are not visible to outside and that M11 has only one external IP address received from the ISP. The external Internet services are accessed through this single IP address. This mode of operation is called the Network Port Address Translation (NAPT).

The benefits of NAPT are the minimum coupling of the ISP and the home network, the saving of public IP addresses, and in-built simple firewall functionality.

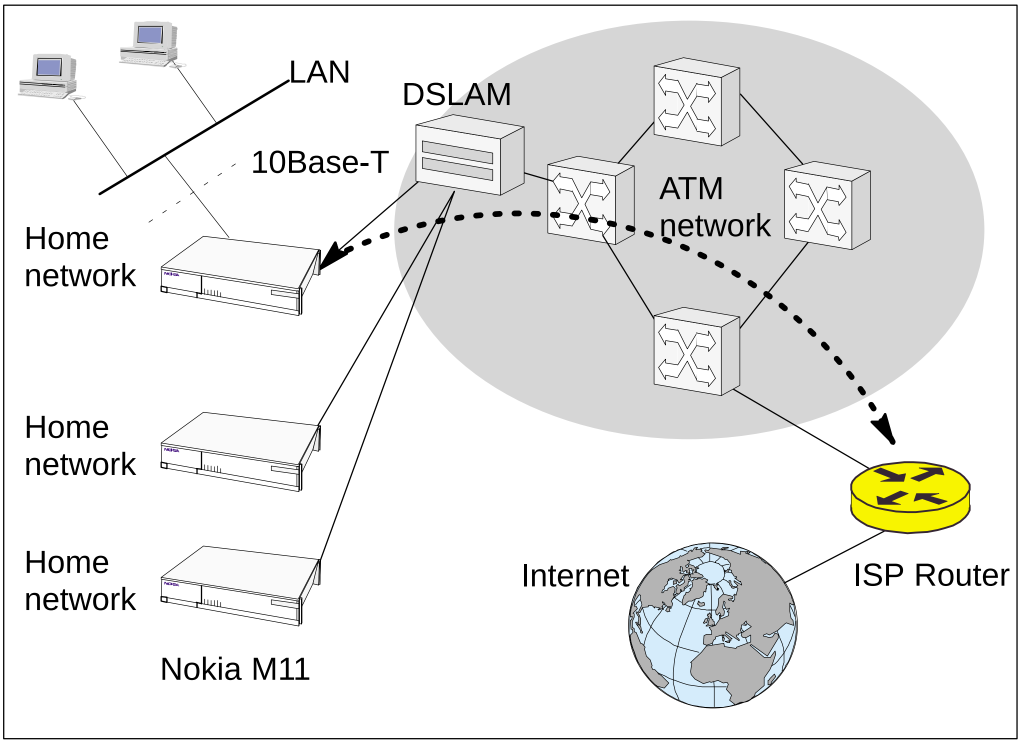


Figure 2-1 Internet access using M10 as a NAPT router

2.1.2 Remote work

In a typical remote work application M11 is used as an IP router to provide access to corporate Intranet services. Using routing between the home and the corporate networks prevents unnecessary broadcast traffic and non-IP protocol traffic from loading the access connection Still, it provides sufficient transparency for Intranet applications. The M11 routing table can be static or it can be updated dynamically using RIP version 1 and RIP version 2 routing protocols.

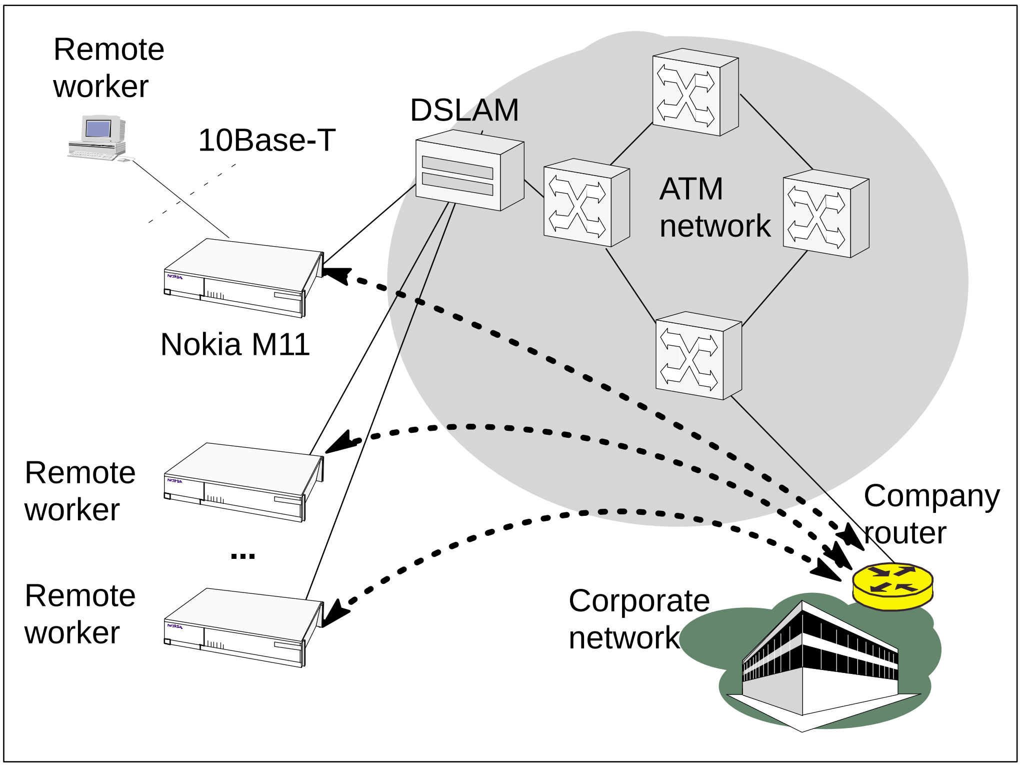


Figure 2-2 Remote work using M11 as a standard router

2.1.3 LAN interconnection using M11 as a bridge

LAN interconnection between corporate headquarters and its remote office is another typical M11 application. In the LAN interconnection application, M11 is typically used as an Ethernet bridge which relays all non-local Ethernet traffic between the corporate headquarters and remote sites through the ATM core network.

The benefit of bridging in this application example is the transparency for all network protocols in a multiprotocol data communications corporate network.

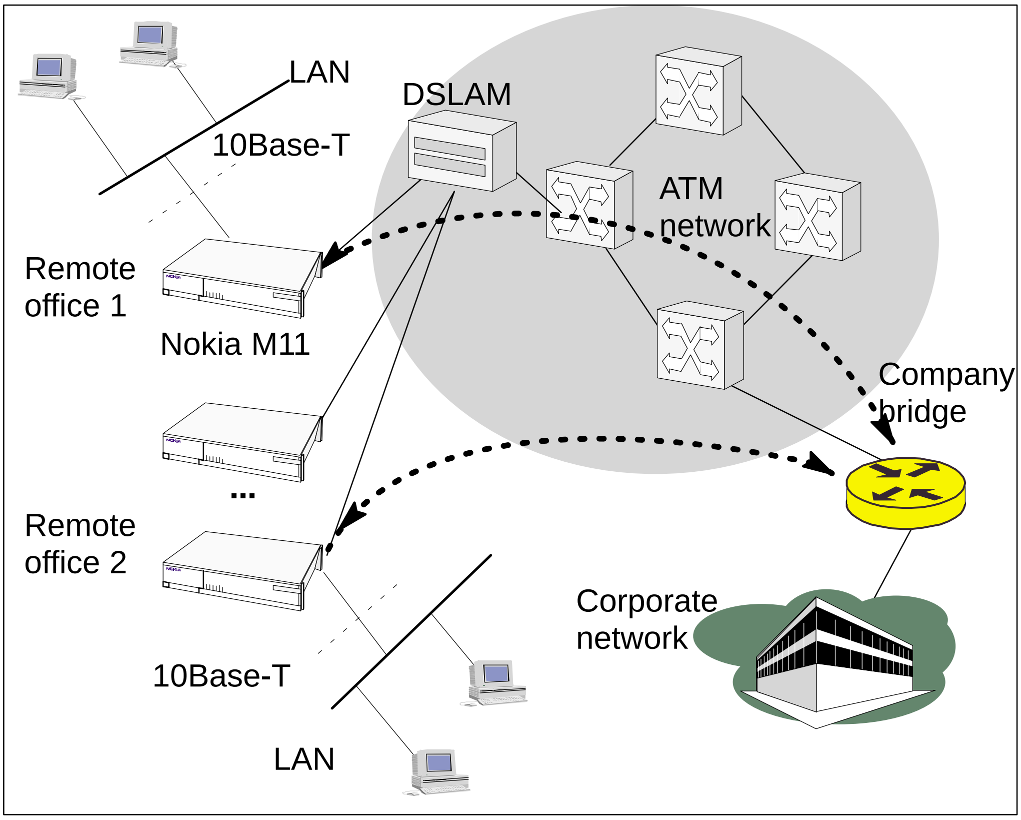


Figure 2-3 Internet access and LAN interconnection

2.2 Features

M11 can operate as an OSI layer 3 Internet Protocol (IP) router between the Ethernet interface and the virtual channels of ADSL/ATM interface. M11 supports both dynamic and static routing.

It can also operate as a self-learning bridge supporting up to 256 MAC addresses.

M11 supports IGMP (Internet Group Management Protocol) proxy function for IP multicast applications.

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 and the virtual channel connection (VCC) of the ATM/ADSL interface. Optionally, the routing between the VCCs can be disabled. M11 supports up to 8 simultaneous VCCs.

Bridging

Bridging is supported to provide full protocol transparency. Bridging can be used simultaneously with IP routing. M11 works as a self-learning bridge supporting up to 256 MAC addresses. Bridging is done between the Ethernet 10Base-T interface and each ATM VCC interface. Optionally, the bridging between the VCCs can be disabled. M11 supports up to 8 simultaneous VCCs.

Network Address Port Translation

M11 supports Network Address Port Translation (NAPT) for TCP/IP and UDP/IP protocols. When NAPT is used, a single IP address is allocated to a VCC which leads to the public IP network. The Ethernet subnet has private IP addressing and is not visible to the VCC. NAPT translates the IP source address and source port number dynamically to the VCC IP address and port number. Similarly, packets coming from the VCC are mapped back to the original destination addresses. NAPT allows up to 253 hosts to share a single VCC IP address to the public network. The Network Address Port Translation principle is presented in Figure 2-4.

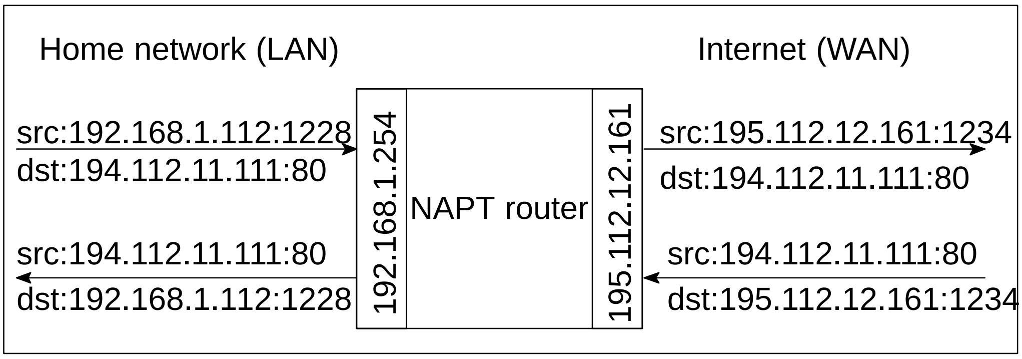


Figure 2-4 Principle of Network Address Port Translation

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 pinhole 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.

Dynamic Host Configuration

M11 can act as a Dynamic Host Configuration Protocol (DHCP) server for the PCs on the end-user home network. In this mode, M11 can assign up to 253 IP addresses to the PCs on the home network. M11 can also act as a DHCP relay agent and relay the DHCP requests to an external DHCP server.

ATM and ADSL

M11 supports up to 8 simultaneous VCCs and supports UBR (Unspecified bit rate) traffic shaping on all VCCs. The maximum transmit rate on each VCC is the ADSL upstream capacity. If more than one VCC is transmitting simultaneously, the ADSL upstream capacity is temporarily shared between these VCCs. When one VCC is idle, the bandwidth is used by another VCC. M11 also supports limited CBR on upstream (see Transmit priority selection in this chapter).

The ADSL transmission is based on the DMT line code. M11 provides a DMT line rate up to 8 Mbit/s downstream and up to 1 Mbit/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. M11 supports also ADSL Lite. In the ADSL Lite mode, the maximum line rates are 1536 kbit/s downstream and 512 kbit/s upstream.

The ATM over ADSL transmission is based on ITU-T G.992.1. ADSL Lite is based on ITU-T G.992.2.

Rate adaptation is done in steps of 32 kbit/s. The ADSL interface of M11 functions completely automatically and all configuration related to the ADSL connection is done at the access multiplexer in the operator’s premises. The network operator can set the data rates as a part of the network management functionality provided by Nokia D DSLAM.

Payload encapsulations

Both routed and bridged protocols are encapsulated in the ATM link by using either RFC 1483 LLC/SNAP encapsulation or VC multiplexing. M11 also supports PPP over AAL5 encapsulation, in which both bridged and 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.

See Chapter 6 for more information on the payload encapsulations.

Transmit priority selection

If you are using more than one upstream connections, you can set priorities to these connections. You can also set the maximum transmit rate to the connection. The following example explains the transmit priority selection:

Connection	Priority	Maximum transmit rate
VCC1	HIGH	400 kbit/s
VCC2	LOW	0 (no limit)

Table 2-1 Transmit priority selection example settings

The settings shown in Table 2-1 affect the connections in the following way:

- When VCC1 is not transmitting, VCC2 can use the whole bandwidth.
- When VCC2 is not transmitting, VCC1 gets only 400 kbit/s even if there was more bandwidth available on the upstream link.
- When VCC1 starts transmitting, it gets 400 kbit/s bandwidth and VCC2 gets the rest of the available bandwidth.
- If the upstream bandwidth is 400 kbit/s and VCC1 uses 400 kbit/s, VCC2 can not transmit anything until VCC1 starts to transmit less than 400 kbit/s.

IGMP proxy function

M11 can be used as an IGMP proxy which means that M11 can send IGMP queries and have IP hosts report their IP multicast host group memberships. See Chapter 6 for more information about IP multicast.

Management

There are four management methods in M11:

- Command line interface (CLI) through console serial port
- CLI via telnet
- SNMP
- Web browser management

The CLI allows complete configuration of the unit; the Web browser management allows the configuration of the most frequently used configuration parameters. SNMP can be used to read some equipment identity information and to provide traps for authentication failures.

2.2.1 Dedicated management channel

The operator or Internet Service Provider can establish a dedicated management channel to M11. This channel provides access to the M11 management (with telnet or Web browser) and it can be used to upload a new software to M11. When the management channel is in use it prevents data traffic between the management channel and the Ethernet as well as the traffic between the management channel and other active ATM channels. Figure 2-5 shows the principle of the dedicated management channel.

In Figure 2-5 VCC1 is used for customers data transmission. Administration through this channel has been disabled. The operator or the service provider uses the VCC2 for management purposes only.

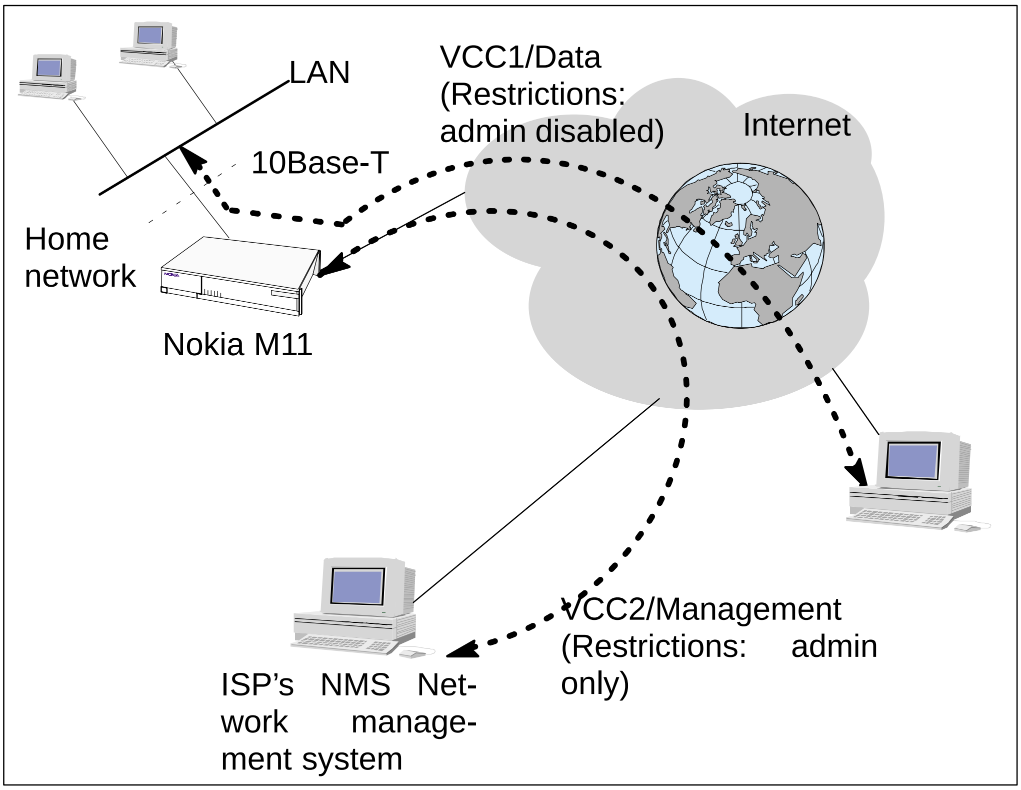

LAN
VCC1/Data (Restrictions: admin disabled)
Internet
10Base-T
Home network
Nokia M11
VCC2/Management (Restrictions: admin only)
ISP's NMS Network management system

Figure 2-5 Dedicated management channel

Chapter 3
Interfaces and indicator lights

M11 provides one Ethernet 10Base-T interface and one ADSL line interface. The ADSL line interface is based on ANSI ITU-T G.992.1.

3.1 10Base-T Ethernet interface

The Ethernet interface is a standard 10 Mbit/s half-duplex 10Base-T interface. The mechanical connector is an 8-pin RJ-45 connector.

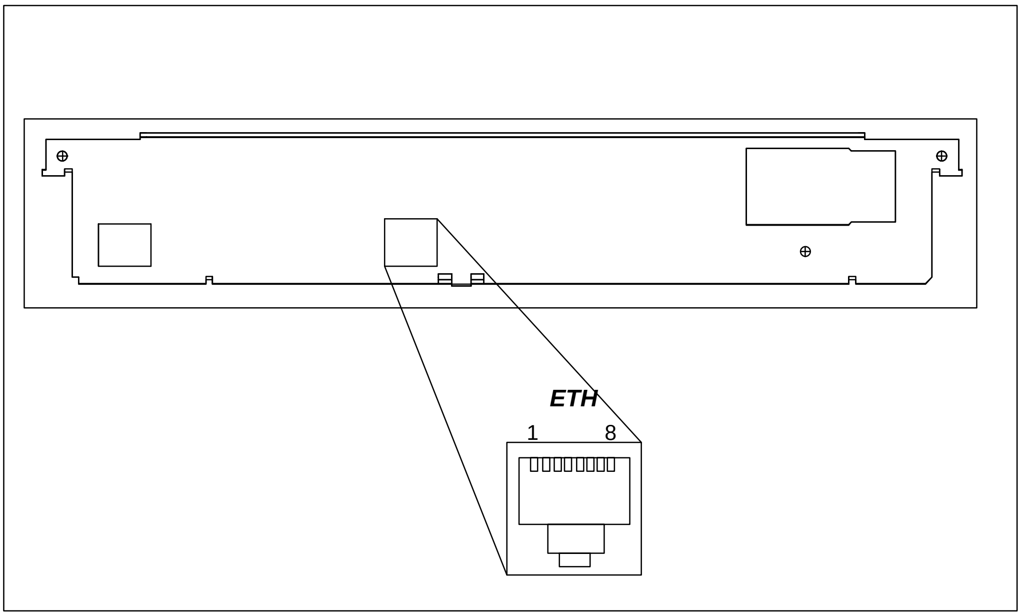


Figure 3-1 Ethernet connector location

PIN	Signal	Direction M11–Ethernet	MDI signal
1	Tx+	–>	Transmit data +
2	Tx–	–>	Transmit data –
3	Rx+	<–	Receive data +
6	Rx–	<–	Receive data –

3.2 ADSL line interface

The ADSL line interface is based on ITU-T G.992.1. The mechanical connector is a 6-pin RJ-11 connector.

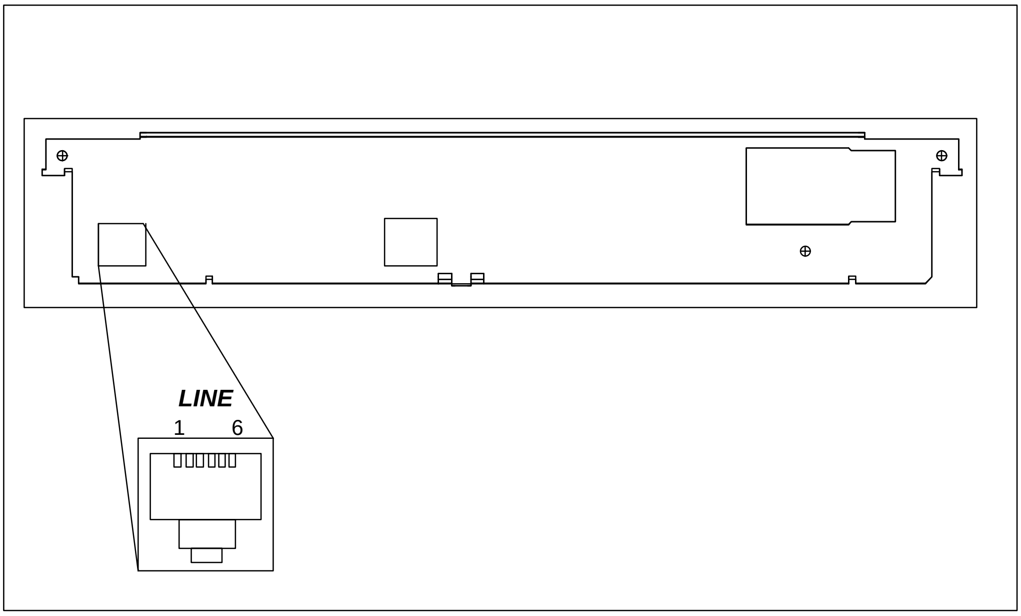


Figure 3-2 ADSL line connector location

PIN	Signal
3	DSL1
4	DSL2

3.3 Front panel indicator lights

Six indicator lights have been grouped into three groups on the front panel:

- STA
- DSL
- LAN

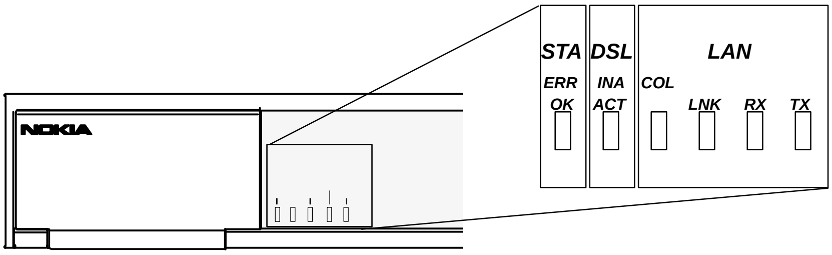


Figure 3-3 Front panel indicator lights

STA indicator (M11 status)

- ERR (red): There is a malfunction in the unit. Switch power off and on again. If this does not help send the unit for repair.
- OK (green): Unit is functional

DSL indicator (ADSL line status)

- INA (red): ADSL line is inactive (no connection). Blinking light indicates that the ADSL link is training.
- ACT (green): ADSL line is active (connection).

LAN indicators

- COL (red): Blinking light indicates collisions on the Ethernet.
- LNK (green): Lit if the Ethernet connection is OK.
- RX (green): Blinking light indicates that M11 is receiving Ethernet packets.
- TX (green): Blinking light indicates that M11 is transmitting Ethernet packets.

Chapter 4
Installing M11

This chapter presents step-by-step installation example procedures for three different application examples of Nokia M11:

- Internet access (NAPT router)
- Remote work (basic router)
- LAN interconnection (basic bridge)

These installation procedures are examples to guide you through some of the typical use cases.

In the installation examples, we assume that you have a new M11 with a factory default configuration. The complete default configuration is presented in the end of this chapter. The default settings are, briefly:

- Single ADSL/ATM channel (VPI = 0, VCI = 100)
- PPP over ATM/AAL5 encapsulation
- M11 retrieves IP address configuration from IP network using PPP-IPCP negotiation
- Network Address Port Translation activated
- Private IP addresses in use in LAN
- DHCP server for LAN interface activated

Before starting the installation, unpack the unit and check that it is physically undamaged.

4.1 Internet access (NAPT router)

This application is based on the default configuration of the Nokia M11. By default, Nokia M11 is an Internet access device that uses

Network Address Port Translation between the private home network and the public Internet.

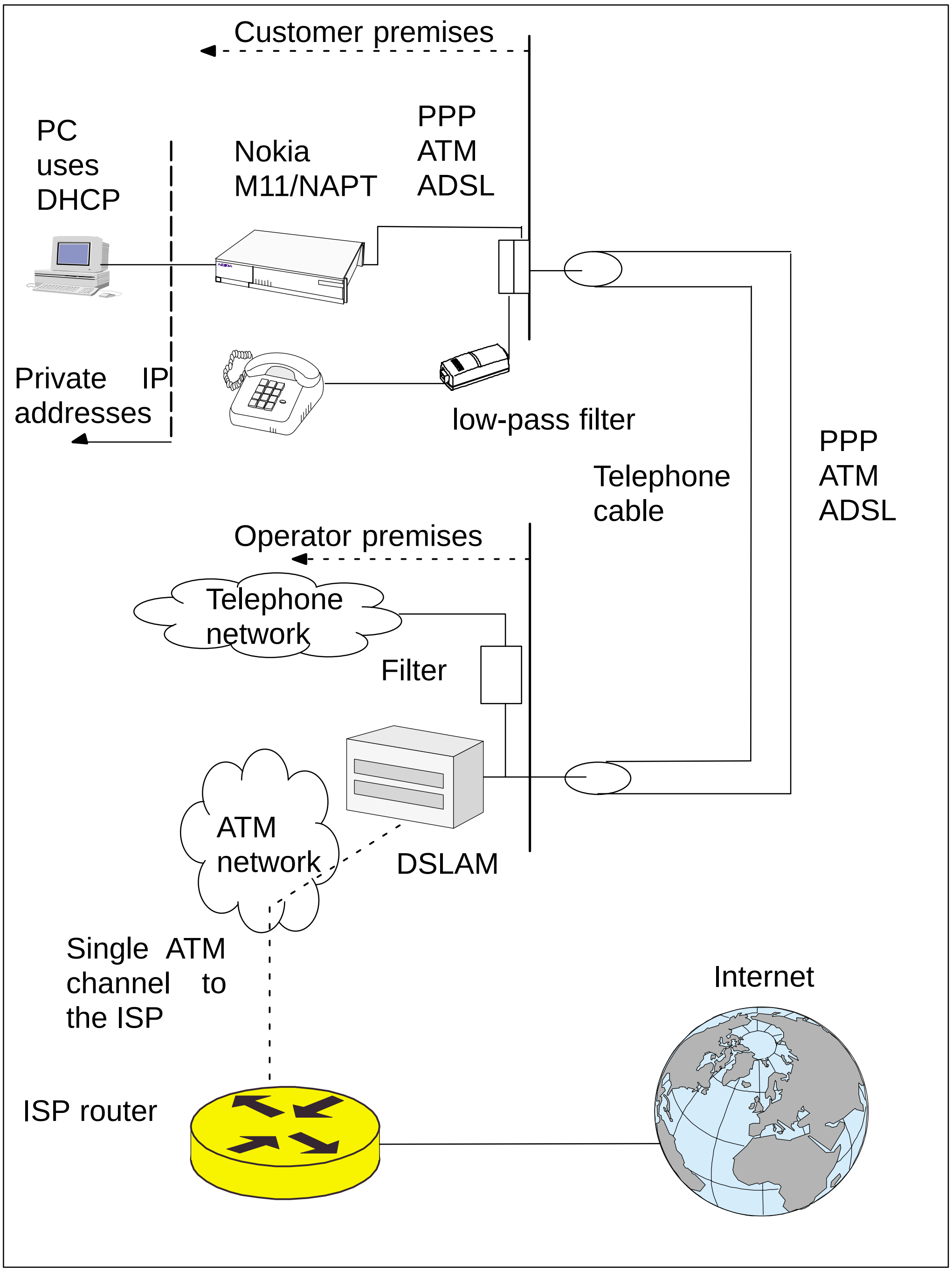


Figure 4-1 Internet access application

The Internet access application requires that your PC uses Dynamic Host Configuration Protocol (DHCP) to get its network address (IP address) from your Nokia M11.

The installation procedure depends on whether you want to use data services only or data and simultaneous telephone services. If you want data services only, start from Step 1a. If you want both data and telephone services, start from Step 1b .

M11 has an optional three-level password (user, user-admin, and admin), which also affects the installation procedure. By default, the password is disabled but it can be enabled through the command line interface (see Chapter 5 Management). Steps 4b and 5b describe the actions when password is enabled.

Step 1a: Connect cables (data services only)

Connect the following cables:

- Connect the mains power cord first to Nokia M11 and then to a power outlet.
- Connect the Ethernet cross cable to the Nokia M11 ETH connector and the other end to your PC’s Ethernet port.
- Connect the ADSL cable to the telephone socket.
- Go to Step 2.

Step 1b: Connect cables (data and telephone services)

If you want to use your telephone line for both the high-speed ADSL service and normal telephone service, you must install a POTS filter. You can use Nokia POTS filter T66130 or T66150. See separate installation instructions for POTS filters.

Connect the following cables:

- Connect the mains power cord first to Nokia M11 and then to a power outlet.
- Connect the Ethernet cross cable to the Nokia M11 ETH connector and the other end to your PC’s Ethernet port.
- Connect the ADSL cable and the telephone according to the separate POTS filter installation instructions.
- Go to Step 2.

Step 2: Switch on M11

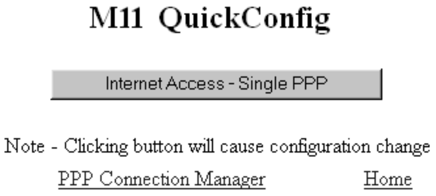
The green STA indicator and red DSL indicator light up. After a while the DSL light starts blinking, indicating that the connection is being established. Green DSL light indicates that the unit has a connection to the central office.

Step 3: Switch on PC

The LAN/LNK indicator lights up in the Nokia M11 front panel. Note that you must activate the DHCP functionality in your PC to make it retrieve an IP address from M11.

Step 4a: Connect to M11 with a Web browser (M11 password disabled)

Start the Web browser in your PC, write the IP address (192.168.1.254) or the default name (M11) of the M11 to the HTTP address field and press Enter. The M11 QuickConfig page is displayed. Note that the QuickConfig page is displayed first only when M11 has its factory default settings active. If M11 has been previously configured, the first page to appear is the M11 home page. Go to Step 5a.



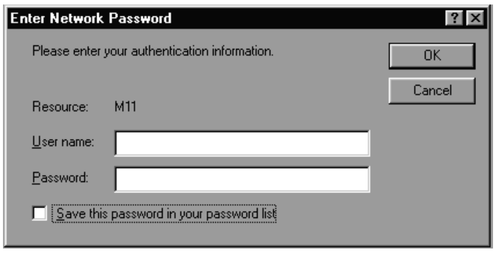
M11 QuickConfig

Note - Clicking button will cause configuration change

Figure 4-2 M11 QuickConfig page

Step 4b: Connect to M11 with a Web browser (M11 password enabled)

Start the Web browser in your PC, write the IP address (192.168.1.254) or the default name (M11) of the M11 to the HTTP address field and press Enter. Enter Network Password dialog is shown. Enter your M11 user name and password and click OK. Go to Step 5b.



Enter Network Password

Please enter your authentication information.

Resource: M11

User name:

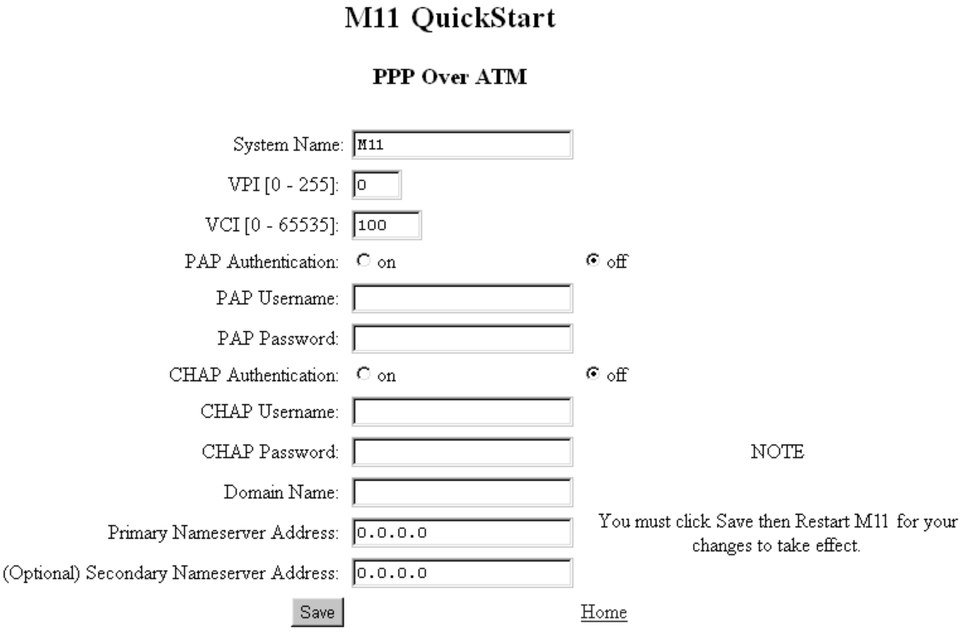
Password:

□ Save this password in your password list

Figure 4-3 M11 password page

Step 5a: Configure M11 (M11 password disabled)

Click Internet Access-Single PPP button to set your user name and password for the Internet service.



M11 QuickStart

PPP Over ATM

System Name:	M11	
VPI [0 - 255]:	0	
VCI [0 - 65535]:	100	
PAP Authentication:	○ on	● off
PAP Username:		
PAP Password:		
CHAP Authentication:	○ on	● off
CHAP Username:		
CHAP Password:		
Domain Name:		
Primary Nameserver Address:	0.0.0.0	
(Optional) Secondary Nameserver Address:	0.0.0.0	

NOTE

You must click Save then Restart M11 for your changes to take effect.

Figure 4-4 QuickStart page

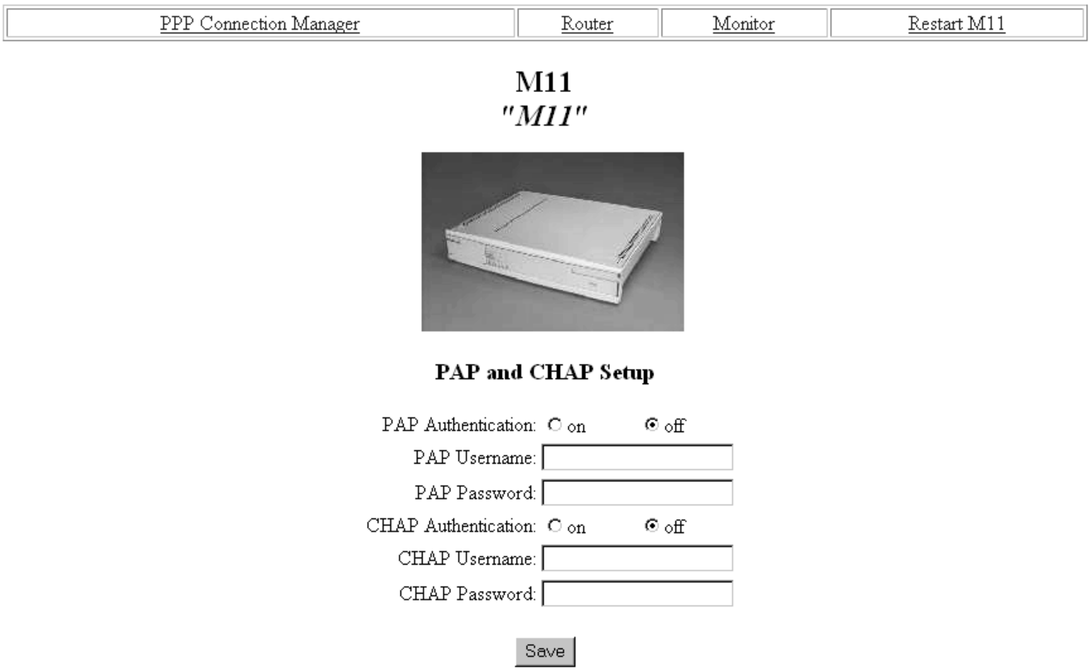
In this example we assume that the default settings of M11 are suitable for accessing Internet through your Internet Service Provider:

- Connection from M11 to ISP uses PPP over AAL5 protocol.
- ISP provides network address information to your M11 automatically.
- Default connection channel (VPI and VCI values) of M11 is correct.

This means that you only have to enable the needed authentication method (CHAP or PAP) by clicking the relevant radio button and to type in your username and password related to the authentication method. You will get the information which authentication method to use and your corresponding username and password from your Internet Service Provider. After entering the information, click Save and restart M11.

Step 5b: Configure M11 (M11 password enabled)

Enable PAP or CHAP authentication and type in your corresponding user name and password. You will get the information which authentication method to use and your corresponding username and password from your Internet Service Provider. After entering the information, click Save and restart M11.



PPP Connection Manager | Router | Monitor | Restart M11

M11

"M11"

PAP and CHAP Setup

PAP Authentication:	○ on	● off
PAP Username:		
PAP Password:		
CHAP Authentication:	○ on	● off
CHAP Username:		
CHAP Password:		

Save

Step 6: Surf

After the ADSL connection has been established, the installation is complete and you can use your Web browser normally.

4.2 Remote work (Basic router)

In the remote work application example, Nokia M11 routes you to your company’s LAN through an ATM network. In this example we assume that your PC belongs to your company’s IP network and has a fixed IP address. It is also assumed that static IP routing is used. An example is shown in Figure 4-5.

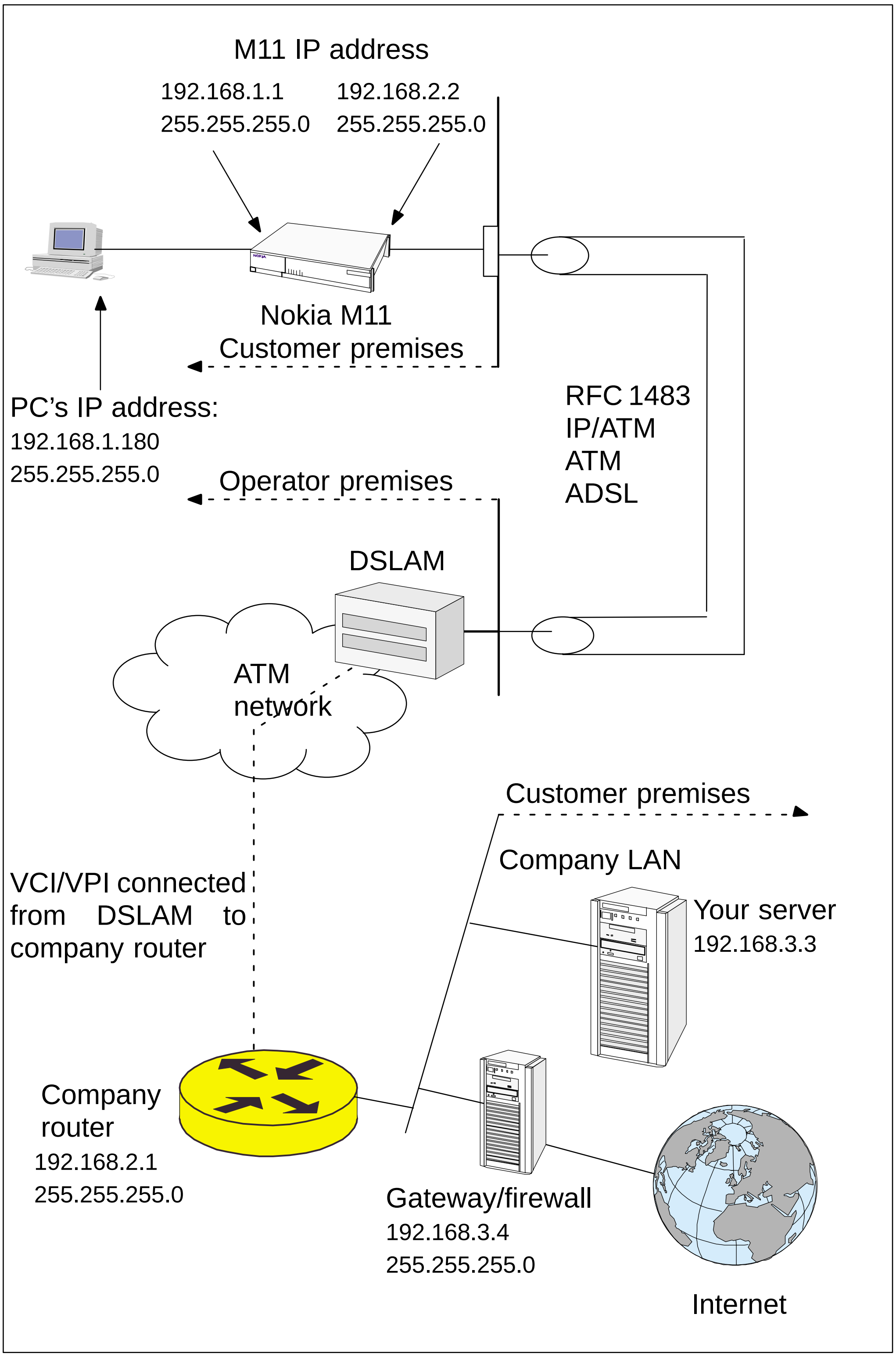


Figure 4-5 Remote work application

In this example the configuration is done using the command line interface (CLI) through the console port of Nokia M11. A special cable is needed, Product code E64320.01.

Step 1: Connect cables

- Connect the mains power cord to your M11 and the other end to the power outlet.
- Connect the M11 console cable to the console port behind the hatch in the front panel of your M11. Connect the other end of the cable to the serial port of your PC/terminal.

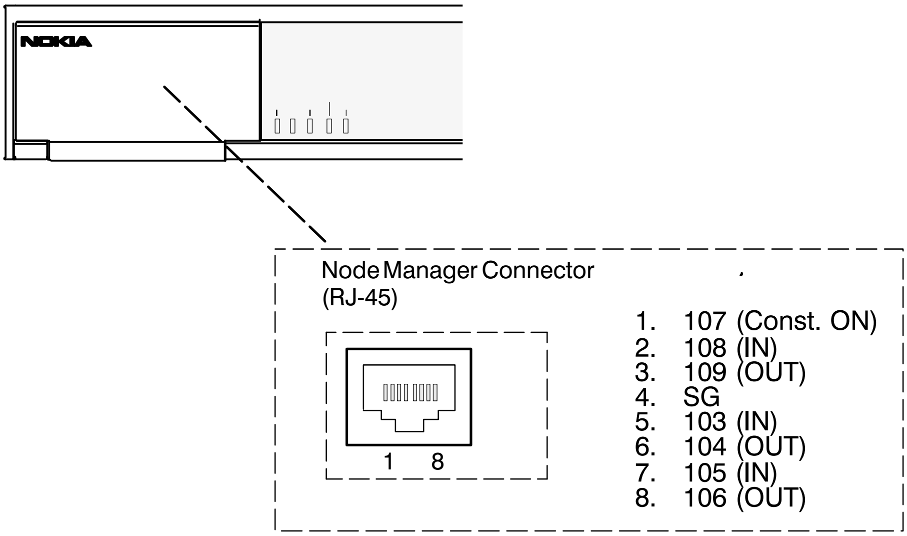


Figure 4-6 Location of the console port

- Switch on your Nokia M11. The green status (STA) indicator and the red DSL indicator light up.

Step 2: Switch on your PC and start its terminal software

Set the following terminal software parameters: 9600, 8 bits, no parity, 1 stop bit, no flow control.

Press enter in the terminal window. The Nokia command line interface prompt will be displayed. If a password has been assigned to your M11, you must enter the correct password.

Step 3: Configure M11

In configurations given here, we assume that the unit uses its default configurations and the changes are done on top of the default configuration of the M11 version T66220.01.

The Nokia M11 command line interface includes a step mode to automate the process of entering configuration settings. When you use the Config step mode, the CLI prompts you for all required and optional information. You can enter the configuration values appropriate for your site without having to enter complete CLI commands.

To enter the Config step, mode type `set` from the top node of the Config hierarchy. See Chapter 5 section *Stepping through M11 configuration* for more information on the step mode.

When you are in step mode, the CLI prompts you to enter the required and optional settings. If a setting has a default value or a current setting, the command line interface displays the default value for the command in parentheses. If a command has a limited number of acceptable values, those values are presented in brackets, with each value separated by a vertical line. For example, the following CLI step command indicates that the default value is off and that valid entries are limited to on and off.

```
option (off) [on|off]: on <Enter>
```

You can accept the default value for a field by pressing the ENTER key. To use a different value, type it in and press ENTER.

In the following example the values changed by the user are in bold type. The default values have been accepted by pressing ENTER.

```
M11> config
Config Mode v1.0
(admin level privileges -- read/write)
M11 (top)>>set
Stepping set mode (press Control-X <Return/Enter> to
exit)...

   system
       name (”M11”): <Enter>
       Diagnostic Level List
           low
           medium
           high
```

```
        warnings
        failures
    diagnostic-level (high): <Enter>
dmt
    type (multi) [lite|dmt|ansi|multi]: <Enter>
atm
    option (on) [on|off]: <Enter>
    vcc 1
        option (on): <Enter>
        vpi (0) [0 - 255]: <Enter>
        vci (100) [0 - 65535]: <Enter>
        encap (ppp-vcmux)
            ppp-vcmux    :   PPP over ATM,
                             VC-muxed
            ppp-llc      :   PPP over ATM,
                             LLC-SNAP
            ether-vcmux  :   RFC-1483, bridged
                             Ethernet, VC-muxed
            ether-llc    :   RFC-1483, bridged
                             Ethernet, LLC-SNAP
            ip-vcmux     :   RFC-1483, routed IP,
                             VC-muxed
            ip-llc       :   RFC-1483, routed IP,
                             LLC-SNAP
            [ppp-vcmux|ppp-llc|ether-vcmux|
            ether-llc|ip-vcmux|ip-llc]: ip-llc
    vcc 2
        option (off): <Enter>
    vcc 3
        option (off): <Enter>
    vcc 4
        option (off): <Enter>
    vcc 5
        option (off): <Enter>
    vcc 6
        option (off): <Enter>
    vcc 7
        option (off): <Enter>
    vcc 8
        option (off): <Enter>
bncp
    option (off) [on|off]: <Enter>
ip
```

```
       option (on) [on|off]: <Enter>
       ethernet
           option (on) [on|off]: <Enter>
           address (192.168.1.254): 192.168.1.1
           broadcast (192.168.1.255): <Enter>
           netmask (255.255.255.0): <Enter>
           restrictions (none) [none|
           admin-disabled]: <Enter>
           proxy-arp (off) [on|off]: <Enter>
           rip-send (v1) [off | v1 | v2 |
           v1-compat]: <Enter>
           rip-receive (v1) [off | v1 | v2 |
           v1-compat]: <Enter>
       dsl vcc1
           option (off) [on|off]: on
           address (0.0.0.0): 192.168.2.2
           broadcast (0.0.0.255): 192.168.2.255
           netmask (255.255.255.0): <Enter>
           restrictions (none) [none|admin-disabled|
           admin-only]: <Enter>
           addr-mapping (on) [on|off]: off
           proxy-arp (off) [on|off]: <Enter>
       gateway
           option (on) [on|off]: <Enter>
           interface () [ip-address]: ip-address
           default (0.0.0.0): 192.168.2.1
       interwan-routing (off) [on|off]: <Enter>
       static routes

IP Static Route List

       destination-network (0.0.0.0) [enter a
       listed or new static route address]: <Enter>
       static-arp

IP Static ARP list

       ip-address (0.0.0.0) [enter a listed or new
       static route address]: <Enter>
   location
Location names: <Enter>

   name (””) [enter a listed or new location
   name]:<Enter>
   dhcp
       option (server) [off|server|relay-agent]: off
   dns
       domain-name (""): <Enter>
       primary-address (0.0.0.0): <Enter>
       secondary-address (0.0.0.0): <Enter>
   bridge
       option (off) [on|off]: <Enter>
       interwan-bridging (off) [on|off]: <Enter>
   snmp

Community Name List

   “public”

       community (""): <Enter>
       traps
           authentication-traps (off) [on|
           off]:<Enter>

IP Trap List

           ip-traps (0.0.0.0) [enter a listed or
           new IP address]: <Enter>
       sysgroup
           contact (""): <Enter>
           location (""): <Enter>
   ppp
       peer-database

Authentication User List

           peer-name ("") [enter a listed or new
           user name]: <Enter>
   pinhole

Pinhole Table

       name (“”) [enter a listed or new
       pinhole map entry]:
   servers
       web-http (80) [0 - 32767]: <Enter>
       telnet-tcp (23) [0 - 32767]: <Enter>

Stepping mode ended.

M11 (top)>> save
WARNING: ’dns domain-name’ is null, indicating no
domain name is available.
WARNING: ’dns primary-address [0.0.0.0]’ and ’dns
secondary-address [0.0.0.0]’ indicates no nameserver
is available.
Configuration data saved.

M11 (top)>> exit

M11> restart
REBOOT scheduled in 2 seconds

Goodbye.
```

The following changes were made in the above basic router example:

- Ip-llc encapsulation was selected for ATM channel 1. This encapsulation is used by your company’s main office router. Alternatively vc-mux encapsulation could be used. See Chapter 6 for more information on the payload encapsulations.
- IP address was assigned to the Ethernet port of your M11.
- IP and broadcast addresses were assigned to the ATM/ADSL interface of your M11.
- Address mapping was disabled because your PC and M11 belong to your company network.
- Default gateway was enabled and its IP address defines the IP gateway interface.
- IP address of the default gateway was given.
- DHCP was disabled.

The warnings in the end of the above example indicate that the addresses have not been specified. Messages given as Warnings are not fatal. If an actual error message occurs, the configuration has not been validated successfully and M11 does not save the configuration.

Step 4: Connect your M11 to the network

Connect the ADSL cable between a telephone socket and the LINE connector of the M11. Then connect the Ethernet cross cable between the Ethernet interface of your PC and the ETH connector of the M11.

The green LAN LNK indicator lights up when you connect the Ethernet cable. After a while the DSL light starts blinking, indicating that the connection is being established. The green DSL light indicates that the unit has a connection to the central office.

Step 5: Check that the connection works

Ping the company server or the gateway to check that the connection works.

4.3 LAN interconnection (Basic Ethernet bridge)

In this application example, Nokia M11 connects transparently to a remote office or company headquarters.

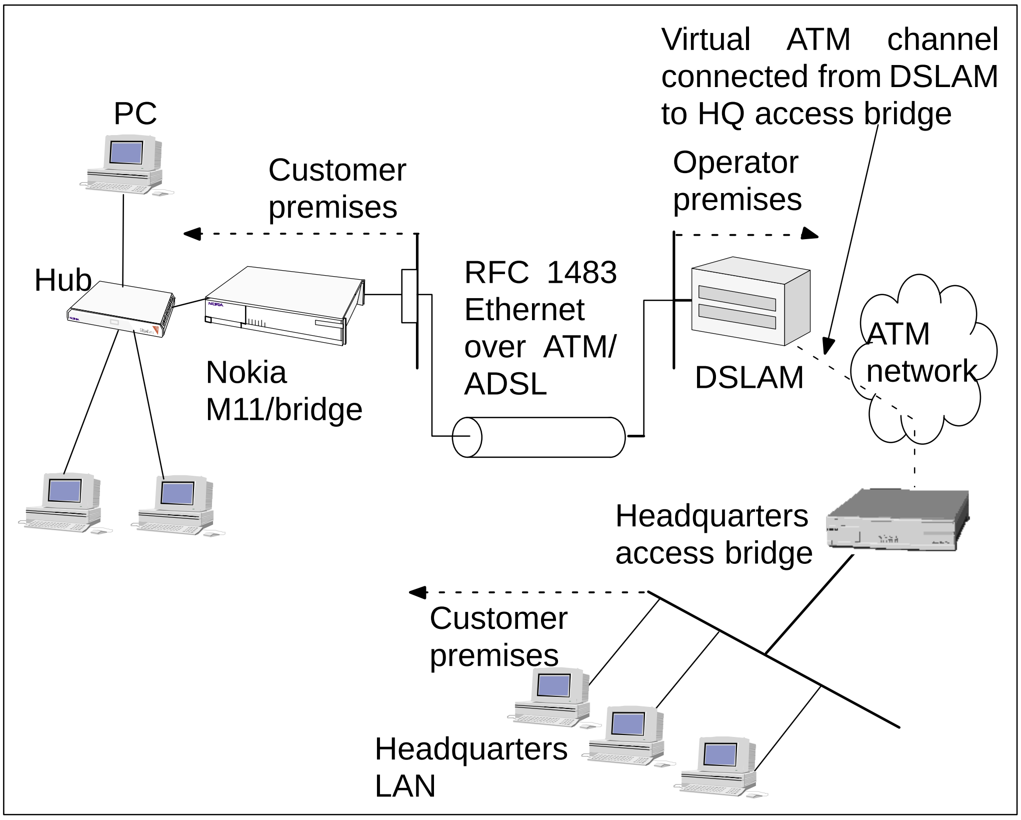

Virtual ATM channel connected from DSLAM to HQ access bridge
PC
Customer premises
Operator premises
Hub
RFC 1483 Ethernet over ATM/ ADSL
Nokia M11/bridge
DSLAM
ATM network
Headquarters access bridge
Customer premises
Headquarters LAN

Figure 4-7 LAN interconnection

Step 1: Connect cables

- Connect the mains power cord to your M11 and the other end to the power outlet.
- Connect the M11 console cable to the console port behind the hatch in the front panel of your M11. Connect the other end of the cable to the serial port of your PC/terminal. A special cable is needed, product code E64320.01.
- Switch on your Nokia M11. The green status (STA) indicator and the red DSL indicator light up.

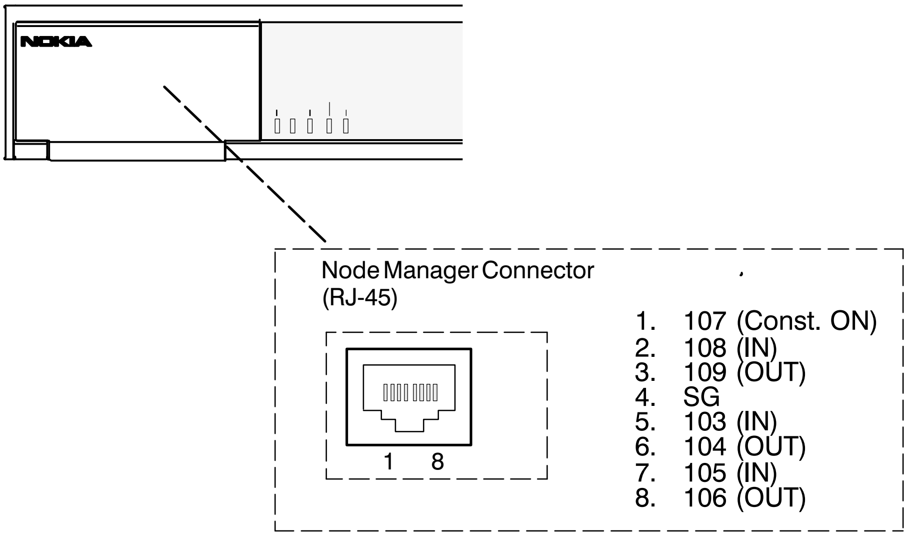


Figure 4-8 Location of the console port

Step 2: Switch on your PC and start the terminal software

Set the following terminal software parameters: 9600, 8, no parity, no flow control.

Step 3: Configure M11 using CLI commands

In configurations given here, we assume that the unit uses its default configurations and the changes are done on top of the default configuration.

The Nokia M11 command line interface includes a step mode to automate the process of entering configuration settings. When you use the Config step mode, the CLI prompts you for all required and optional information. You can enter the configuration values appropriate for your site without having to enter complete CLI commands.

To enter the Config step mode, type `set` from the top node of the Config hierarchy.

When you are in step mode, the CLI prompts you to enter the required and optional settings. If a setting has a default value or a current setting, the command line interface displays the default value for the command in parentheses. If a command has a limited number of acceptable values, those values are presented in brackets, with each value separated by a vertical line. For example, the following CLI step command indicates that the default value is off and that valid entries are limited to on and off.

```
option (off) [on|off]: on <Enter>
```

You can accept the default value for a field by pressing the ENTER key. To use a different value, type it in and press ENTER.

In the following example, the values changed by the user are in bold type. The default values have been accepted by pressing ENTER.

```
M11> config
Config Mode v1.0
(admin level privileges -- read/write
M11 (top)>>set
Stepping set mode (press Control-X <Return/Enter> to
exit)...

   system
       name (”M11”): <Enter>
       Diagnostic Level List
           low
           medium
           high
           warnings
           failures
       diagnostic-level (high): <Enter>
   dmt
       type (multi) [lite|dmt|ansi|multi]
   atm
       option (on) [on|off]: <Enter>
       vcc 1
           option (on): <Enter>
           vpi (0) [0 - 255]: <Enter>
           vci (100) [0 - 65535]: <Enter>
           encap (ppp-vcmux)
               ppp-vcmux    :   PPP over ATM,
                                VC-muxed
               ppp-llc      :   PPP over ATM,
                                LLC-SNAP
               ether-vcmux  :   RFC-1483, bridged
                                Ethernet, VC-muxed
               ether-llc    :   RFC-1483, bridged
                                Ethernet, LLC-SNAP
               ip-vcmux     :   RFC-1483, routed IP,
                                VC-muxed
               ip-llc      :    RFC-1483, routed IP,
                                LLC-SNAP
               [ppp-vcmux|ppp-llc|ether-vcmux|
               ether-llc|ip-vcmux|ip-llc]: ether-llc
       vcc 2
           option (off): <Enter>
       vcc 3
           option (off): <Enter>
       vcc 4
           option (off): <Enter>
       vcc 5
           option (off): <Enter>
       vcc 6
           option (off): <Enter>
       vcc 7
           option (off): <Enter>
       vcc 8
           option (off): <Enter>
   bncp
       option (off) [on|off]: <Enter>
   ip
       option (on) [on|off]: <Enter>
       ethernet
           option (on) [on|off]: off
       dsl vcc1
           option (off) [on|off]: <Enter>
       gateway
           option (on) [on|off]: off
       interwan-routing (off) [on|off]: <Enter>
       static routes

IP Static Route List

       destination-network (0.0.0.0) [enter a
       listed or new static route address]: <Enter>
       static-arp

IP Static ARP list

       ip-address (0.0.0.0) [enter a listed or new
       static route address]: <Enter>
   location
```

```
Location names: <Enter>

   name (””) [enter a listed or new
   location name]:<Enter>
   dhcp
       option (server) [off|server|relay-agent]: off
   dns
       domain-name (””): <Enter>
       primary-address (0.0.0.0): <Enter>
       secondary-address (0.0.0.0): <Enter>
   bridge
       option (off) [on|off]: on
       ethernet
           option (on) [on|off]: <Enter>
       dsl vcc1
           option (on) [on|off]: <Enter>
       interwan-bridging (on) [on|off]: <Enter>
   snmp

Community Name List

   “public”

       community (””): <Enter>
       traps
           authentication-traps (off) [on|
           off]: <Enter>

IP Trap List

           ip-traps (0.0.0.0) [enter a listed or
           new IP address]: <Enter>
       sysgroup
           contact (””): <Enter>
           location (””): <Enter>
   ppp
       peer-database

Authentication User List

           peer-name (””) [enter a listed or new
           user name]: <Enter>
   pinhole
```

```
Pinhole Table

       name ("") [enter a listed or new
       pinhole entry]:
   servers
       web-http (80) [0 - 32767]: <Enter>
       telnet-tcp (23) [0 - 32767]: <Enter>

Stepping mode ended.

M11 (top)>> ip
M11 (ip)>> set
Stepping set mode (press Control-X <Return/Enter> to
exit)...
   ip
       option (on) [on|off]: off
       interwan-routing (off) [on|off]: <Enter>
       static routes

IP Static Route List

           destination-network (0.0.0.0) [enter a
           listed or new static
           route address]: <Enter>
       static-arp

IP Static ARP list

       ip-address (0.0.0.0) [enter a listed or new
       static route address]: <Enter>

Stepping mode ended.
M11 (top)>> save
WARNING: 'dns domain-name' is null, indicating no
domain name is available.
WARNING: 'dns primary-address [0.0.0.0]' and 'dns
secondary-address [0.0.0.0]' indicates no nameserver
is available.
Configuration data saved.

M11 (ip)>> exit
```

```
M11> restart
REBOOT scheduled in 2 seconds

Goodbye.
```

The following changes were made in the above basic router example:

- Ether-llc encapsulation was selected for ATM channel 1. This encapsulation is used by your company’s main office bridge. Alternatively, ether-vcmux encapsulation could be used. See Chapter 6 for more information on the payload encapsulations.
- IP functionality, default gateway and interwan routing were disabled in the Ethernet. Note, that you have to go through the IP option twice: first to disable Ethernet and gateway options and then to disable the IP option.
- DHCP option was disabled.
- Bridge was enabled.

Warnings related to 0.0.0.0 settings of DNS servers are irrelevant in this configuration because the M11 is now a transparent bridge. Messages given as Warnings are not fatal. If an actual error message occurs the configuration has not been validated successfully and M11 does not save the configuration.

Step 4: Connect your M11 to the network

Connect the ADSL cable between the telephone socket and the LINE connector of the M11. Then connect the ETH connector of the M11 to your office hub with a direct cable. The green LAN LNK indicator lights up when you connect the Ethernet cable. After a while the DSL indicator starts blinking, indicating that the connection is being established. The green DSL light indicates that the unit has a connection to the central office.

Step 5: Check that the connection works

Establish a connection to the office server to check that the connection works.

4.4 Default settings

The table 4-1 indicates the default settings for Nokia M11. By default, Nokia M11 works as a plug and play unit in the Internet access application. In the table, the terms “Node” and “Subnode” refer to Config command hierarchy nodes (see Chapter 5).

Node	Subnode	Parameter	M11 default
System		System name	M11
		System Diagnostic Level	3 (high)
		System Name Password/ User	<empty>
		System Name Password/ User-admin	<empty>
		System Name Password/ Admin	<empty>
		CLI Verbose	OFF
		CLI Lines	16
DMT		Type	multi
ATM Option			ON
	ATM VCC Options (8)		ON (VCC1), others OFF
		VCI (VCC1)	100
		VPI (VCCI1)	0
		Encapsulation (VCC1)	ppp-vcmux
		Tx-priority (VCC1)	HIGH
		TX–max–kbps	0 (no limit)
BNCP Option			OFF
PPP Option			ON
		PPP Maximum Receive Unit	1500
		LCP Magic Number Negotiation	ON
		Protocol Compression	OFF
		Address Compression	OFF
		LCP Echo Requests	ON
		Failures-max	10

Node	Subnode	Parameter	M11 default
PPP option (continued)		Configure-max	10
		Terminate-max	2
		Restart Timer	3
		Activity Timeout	0
	CHAP Option		OFF
		CHAP Name	<empty>
		CHAP Secret	<empty>
	PAP Option		OFF
		PAP Name	<empty>
		PAP Password	<empty>
	Chap Peer Option		OFF
	PAP Peer Option		OFF
		Peer Host Name(s)	<empty>
		Peer Host CHAP Secrets	<empty>
		Peer Host PAP Passwords	<empty>
IP Option			ON
	IP Gateway Option		ON
		IP Gateway Interface	ppp (VCC1)
		IP Gateway IP Address	<empty>
	IP Ethernet Option		ON
		IP Ethernet Address	192.168.1.254
		IP Ethernet Broadcast Address	192.168.1.255

Node	Subnode	Parameter	M11 default
	IP Ethernet option (continued)	IP Ethernet Netmask	255.255.255.0
		Restrictions	NONE
		IP Ethernet RIP send	RIP V1
		IP Ethernet RIP receive	RIP V1
	IP WAN Option		OFF
	IP DSL Option		OFF
	IP-ppp Option		ON (VCC1)
		IP-PPP IP Address	0.0.0.0 (VCC1)
		IP-PPP Peer IP Address	0.0.0.0 (VCC1)
		IP-PPP Address mapping	ON (VCC1)
		IP-PPP RIP Send	OFF
		IP-PPP RIP Receive	OFF
		IP-PPP Flush Routes	OFF
	Static Routes Tbl		<empty>
DHCP Option			ON
	DHCP Start IP address		192.168.1.1
DNS		Default Domain Name	<empty>
		Primary DNS Server Address	0.0.0.0 (The address will be retrieved from through the PPP link)
		Secondary DNS Server Address	0.0.0.0 (The address will be retrieved through the PPP link)
Bridge Option			OFF

Node	Subnode	Parameter	M11 default
SNMP		List of communities (table)	Public
		SNMP Authentication Traps	None
		Trap IP Address	<empty>
		Trap Community Name	Public
		SysGroup Contact Info	<empty>

Table 4-1 Nokia M11 default settings

4.5 Troubleshooting

If the data transmission does not work, you can check the following things:

Is the ADSL connection to the remote network working?

The front panel DSL indicator should be green if the ADSL link is functioning. You can also view the ADSL link status by giving the `show dsl` command line interface command. In case the ADSL link is not functioning, check that the cables connecting the unit to the telephone line/splitter are properly attached and then turn on the M11 again. If the ADSL link still does not work, contact your service provider.

Is the Ethernet connection working?

The front panel LAN LNK indicator is green if the Ethernet cable is properly attached. If not, ensure that the cables are properly connected. Ensure also that you are using a right kind of Ethernet cable. If you connect your M11 directly to a PC, you should use a cross-connect cable. If you connect your M11 to a hub, you should use a direct cable.

Is the ATM connection working?

You can check if the ATM connection is working by giving the `show atm` CLI command. The ADSL connection must be working before the

ATM connection can be established. If the ADSL connection is OK but the ATM connection is not, contact your service provider.

Is the PPP connection working?

If you are using PPP to connect to your service provider, you can also check that your PPP connection is working. You can do this by giving the `show ppp` CLI command. If the ADSL link and ATM link are working but the PPP link is not, you should first check that the user name and password you are using on the PPP link are correct. You can also try to restart the M11 (power-off and power-on) and check if the connection is established. If these do not work, contact your service provider for help.

Chapter 5
Management

M11 can be managed with a Web browser or command line interface (CLI). The Web configuration pages of M11 can be accessed through the Ethernet port or through the ADSL/ATM channels of M11. In order to access the Web management feature, the IP functionality must be activated and an IP address must be given to the corresponding interface.

The command line interface (CLI) can be accessed through the console port on the M11 front panel. The console interface is an asynchronous V.24/V.28 character-based interface with 9600 bit/s, 8 bits, no parity, 1 stop bit and no flow control. A special cable for connecting PC’s serial port to this interface is available from Nokia, product code E64320.01. The CLI contains an in-built step procedure which helps you to configure your M11 through the CLI. This procedure is presented in section *Stepping through M11 configuration* in this chapter.

The command line interface can also be accessed through the Ethernet port of M11 or through the ADSL/ATM channels of M11 on top of the telnet protocol. In order to use the CLI through telnet, the IP functionality must be activated and an IP address must be given to the corresponding interface.

5.1 Browser management

You can use your PC’s Web browser software to access the Web configuration pages in M11. To access the Web pages you must know the IP address of your M11 or, alternatively, the “name” that your M11 recognises.

5.1.1 Opening a connection

To open a connection to the Nokia M11:

1. Start your Web browser.
2. Enter the name or IP address of your Nokia M11 in the browser’s Open Location field and press enter.
   For example, you would enter http://192.168.1.254 if your Nokia M11 is using its default IP address. The default name is M11.

Note
If a user-admin password has been assigned to your Nokia M11, enter your username and password and click OK. Now PAP and CHAP Setup page appears, see Figure 5-4.

3. The Nokia M11 home page appears. If you connect to your M11 for the first time the QuickConfig page appears.

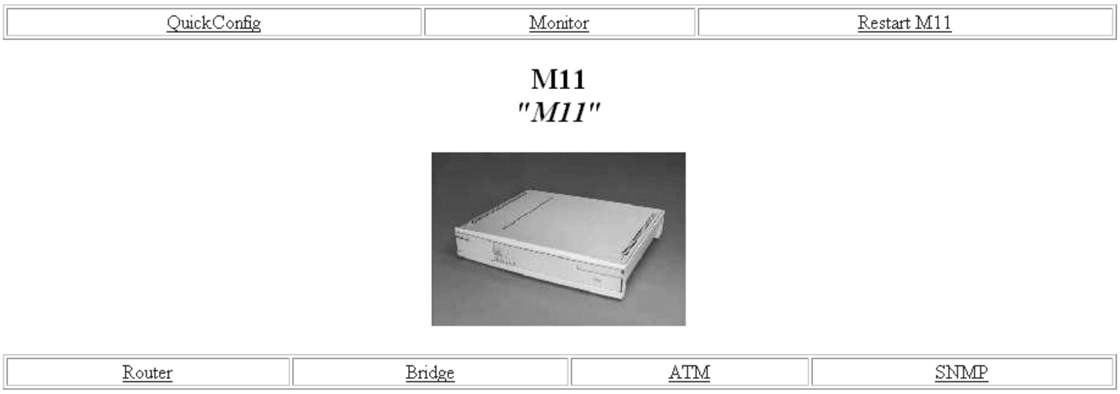


Figure 5-1 M11 home page

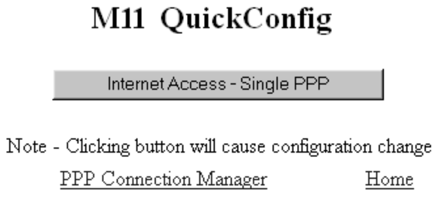
4. Use the links on the Nokia M11 home page to issue a command or open a page.

- “QuickConfig” link opens the QuickConfig page which lets you enter basic Internet access application settings for your Nokia M11.
- “Monitor” link opens the Monitor page which displays operating statistics for your Nokia M11.

- “Router” link is used to configure some generic routing/IP address management parameters and Ethernet interface IP parameters if M11 is used as a router.
- “Bridge” link is used to enable bridging and attach interfaces to the bridge function.
- “ATM” link is used to activate ATM channels, select payload encapsulations to ATM and configure important ATM channel parameters.
- “Restart” M11 link restarts your M11 causing it to activate any updated configuration information.
- “SNMP” link is used to configure the SNMP parameters of M11.

5.1.2 QuickConfig page

The QuickConfig page lets you enter basic configuration information for your Nokia M11. To display the QuickConfig page, click QuickConfig on the M11 homepage. The QuickConfig page also opens when you connect to your M11 for the first time.



M11 QuickConfig

Note - Clicking button will cause configuration change

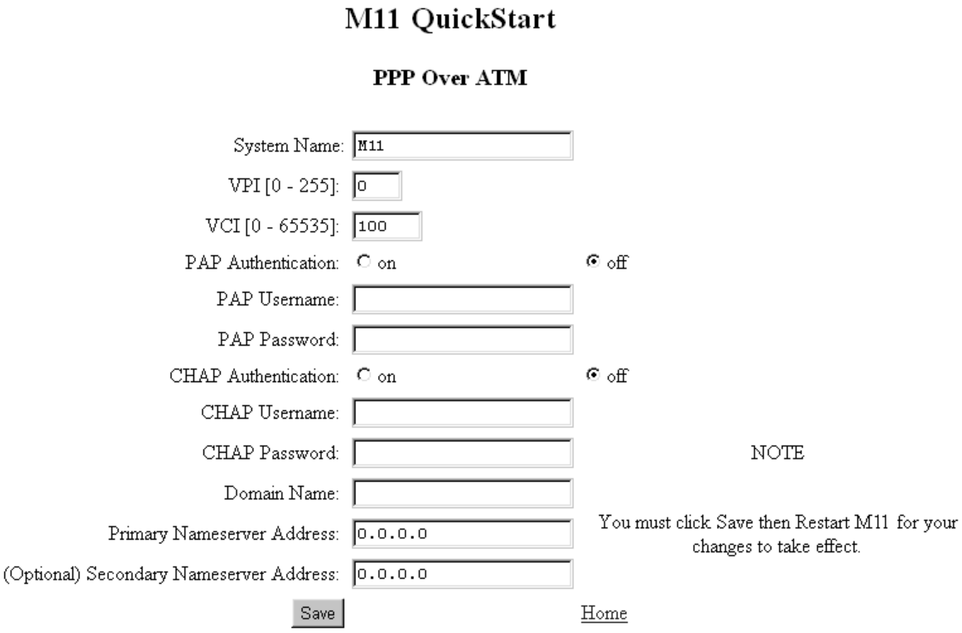
Figure 5-2 QuickConfig page

By clicking the Internet Access-Single PPP button you can enter basic Nokia M11 settings for an Internet access application. Clicking the Internet Access-Single PPP opens the QuickStart page. Normally you only need to enter your username and password for the Internet service.

If you have configured multiple PPP channels into use, you can manage them through the PPP Connection Manager.

Note
If a user-admin password has been assigned to your M11, the PAP and CHAP Setup page will be displayed instead of the QuickConfig page.

QuickStart page



M11 QuickStart

PPP Over ATM

System Name: M11

VPI [0 - 255]: 0

VCI [0 - 65535]: 100

PAP Authentication: ○ on ● off

PAP Username:

PAP Password:

CHAP Authentication: ○ on ● off

CHAP Username:

CHAP Password:

Domain Name:

Primary Nameserver Address: 0.0.0.0

(Optional) Secondary Nameserver Address: 0.0.0.0

NOTE

You must click Save then Restart M11 for your changes to take effect.

Figure 5-3 QuickStart page

1. Change virtual path (VPI) and channel (VCI) identifiers if needed.

   VPI and VCI are used to select the connection channel that is used between M11 and the Internet service provider (ISP). Normally you do not have to change these values.

2. Enable PAP or CHAP if needed. Enter the respective username and password.
3. Enter local LAN Domain Name if required.
4. Enter Domain Name Server addresses if required. Normally these are assigned automatically and user should not fill these fields.
5. Save the configuration and restart M11.

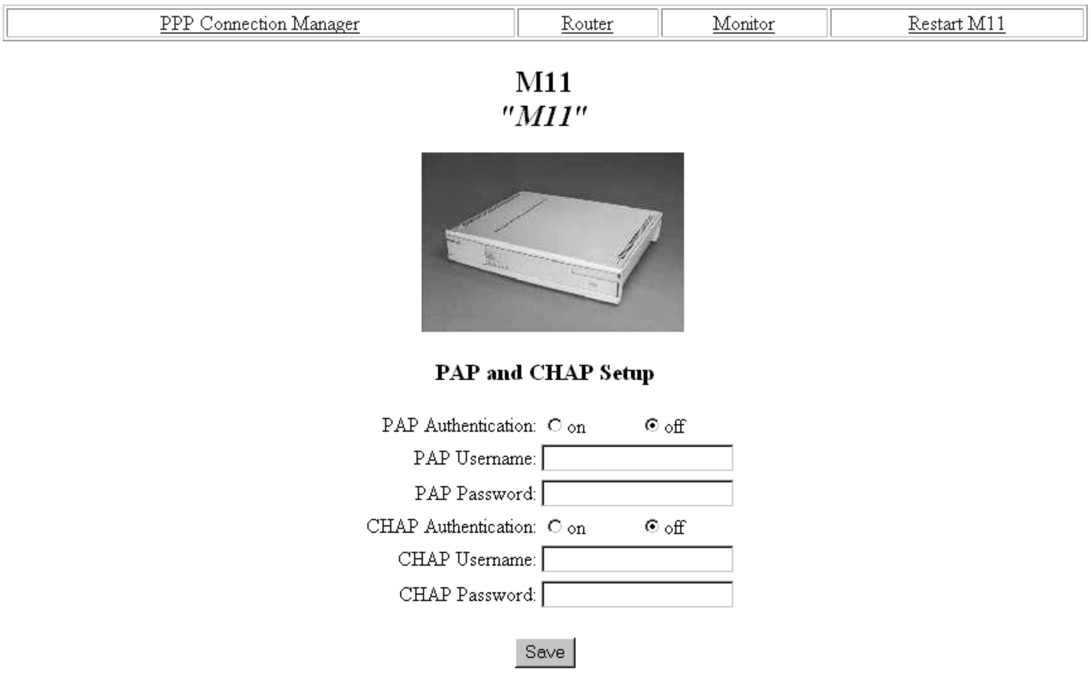
Note

You must save the new configuration and restart your M11 for your changes to take effect.

PAP and CHAP Setup page

If a user-admin password has been assigned to your M11, the PAP and CHAP Setup page will appear when you enter your M11 user name and password and click OK.

On this page you can enable/disable PAP/CHAP and enter the corresponding usernames and passwords. By clicking the “Pinhole” link, you can go to the NAT Pinhole page and configure pinhole settings. The “Monitor” link takes you to the Monitor page, where you can monitor the performance of your M11.



M11

"M11"

PAP and CHAP Setup

PAP Authentication: ○ on ● off

PAP Username:

PAP Password:

CHAP Authentication: ○ on ● off

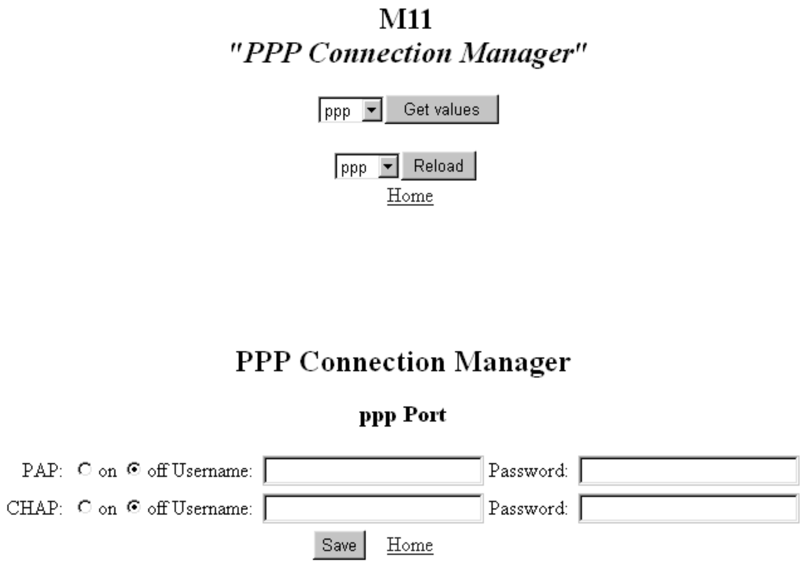
CHAP Username:

CHAP Password:

Figure 5-4 PAP and CHAP Setup page

PPP Connection Manager pages

You can set the user name and password for each PPP connection you have configured. Select the PPP connection you want to modify from the list. Click “Get values” to modify username and password of the connection. Click “Reload” to restart the PPP connection of the selected channel. The PPP connection will be restarted and new CHAP or PAP settings will be used.



M11

"PPP Connection Manager"

ppp ▾ Get values

ppp ▾ Reload

Home

PPP Connection Manager

ppp Port

PAP: ○ on ● off Username: Password:

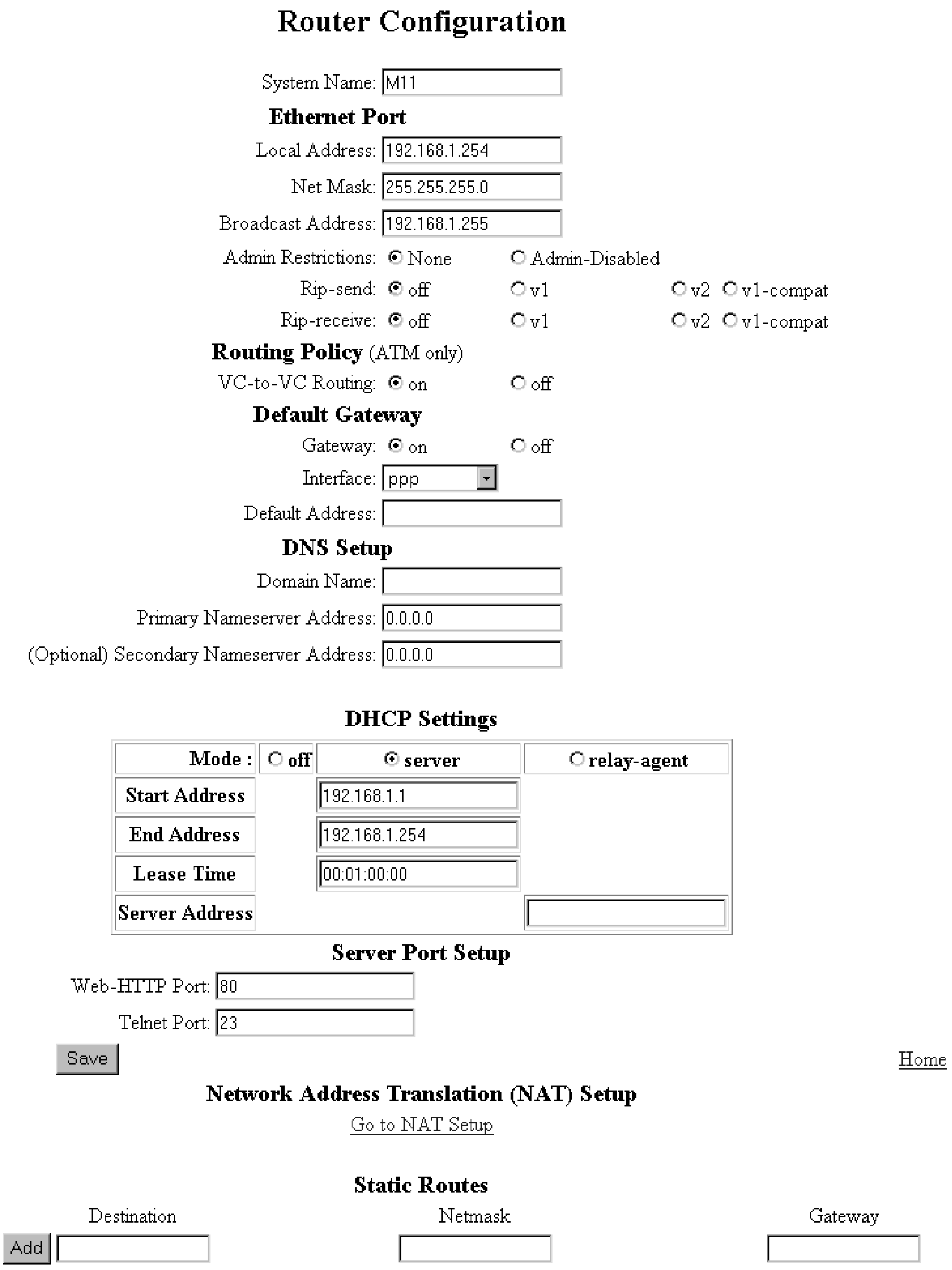
CHAP: ○ on ● off Username: Password:

Save Home

Figure 5-5 PPP Connection Manager pages

5.1.3 Router page

The Router page is used to configure global parameters of the IP routing functionality for M11 and IP parameters for the Ethernet interface.



Router Configuration

System Name: M11

Ethernet Port

Local Address: 192.168.1.254

Net Mask: 255.255.255.0

Broadcast Address: 192.168.1.255

Admin Restrictions: ● None ○ Admin-Disabled

Rip-send: ● off ○ v1 ○ v2 ○ v1-compat

Rip-receive: ● off ○ v1 ○ v2 ○ v1-compat

Routing Policy (ATM only)

VC-to-VC Routing: ● on ○ off

Default Gateway

Gateway: ● on ○ off

Interface: ppp

Default Address:

DNS Setup

Domain Name:

Primary Nameserver Address: 0.0.0.0

(Optional) Secondary Nameserver Address: 0.0.0.0

DHCP Settings

Mode :	○ **off**	● **server**	○ **relay-agent**
Start Address		192.168.1.1	
End Address		192.168.1.254	
Lease Time		00:01:00:00	
Server Address			

Server Port Setup

Web-HTTP Port: 80

Telnet Port: 23

Network Address Translation (NAT) Setup

Go to NAT Setup

Static Routes

Destination	Netmask	Gateway

Figure 5-6 Router page

Filling in router settings

1. Enter the name of your M11 in the System Name field.

   Each M11 is assigned a name as a part of its factory initialisation. The default name is M11. A system name can be 1-64 characters long and cannot contain any special characters. If you want to use a space character in the system name, you must use quotes, for example “Nokia M11”. The name can be later used to access the M11 through a telnet connection or a Web page from the Ethernet interface.

2. Enter the IP address of your M11.

   Local address is the IP address of your M11’s Ethernet interface.

3. Enter the *subnet mask*.

   Net mask is used to identify the network portion of an IP address. The net mask specifies which bits of the 32-bit binary IP address represent the network information. Most sites should use 255.255.255.0 for their net mask.

4. Enter the broadcast address.

   The *Broadcast address* is used to send messages to all computers on your network. Most sites should use xxx.yyy.zzz.255 as their broadcast address, where xxx.yyy.zzz is the network portion of the IP address.

5. Enable/disable management through the Ethernet port (*Admin Restrictions*).

   You can disable management through the Ethernet port by clicking *Admin-Disabled.* You must have admin rights to set admin restrictions.

Note

If you disable management through the Ethernet port and restart M11, you can no longer manage M11 with your local telnet or Web browser.

6. Enter RIP settings for the Ethernet interface.

   Rip-send and Rip-receive radio buttons are used to enable dynamic routing using Routing Information Protocol (RIP). *RIP* and *RIP version 2* can be used. RIP-send with *V1-compat* option enables the sending of RIPv2 packets using broadcast. RIP-receive with *V1-compat* option accepts both RIPv1 and RIPv2 packets.

7. Enable/disable routing between ATM VCCs (*Routing Policy*).

   IP forwarding and dynamic route distribution between ATM VCC routing can be switched off when multiple VCCs are used.

8. Enable/disable default gateway.

   The default gateway is the host to which your M11 will send a packet when it does not know how to reach the packet's destination host.

9. Select the default gateway port from the Interface list.

   The default gateway port can be one of the active PPP channels or a specified IP address defined in *Default Address* field (see step 10.).

10. Set an IP address (*Default Address*) for your default gateway if you selected “ip-address“ in step 9.

11. Enter domain name server settings.

    A domain name server is a network computer responsible for matching host names to numeric IP addresses so that network traffic can be routed correctly. These fields are set if DNS addresses are not allocated dynamically. Consult your service provider for further assistance.

    Domain names identify organisations on the Internet. The domain name is usually the domain name of your company or your ISP.

    If a secondary name server address is configured, M11 relays the name service request to that server whenever the primary name server is unavailable.

12. Enable/disable DHCP server.

    As a Dynamic Host Control Protocol (DHCP) server, your M11 can assign IP addresses to other devices on your LAN. If you want your M11 to assign IP addresses, enter the first number of the IP address range in the Start Address field and the last number of the IP address range to the End Address field. Lease Time indicates how often the PC will renew the DHCP lease.

    If you want your M11 to relay the DHCP request to an external server, you can do this by enabling the *relay-agent* and writing the server’s IP address to the Server Address field.

Note

If you use M11 as a DHCP server, you must assign IP addresses outside the M11’s DHCP address range to devices requiring static IP addresses. Before M11 assigns an IP address to a DHCP client, it verifies that no other device is using that address. However, network conflicts can result when the M11 assigns an address in its DHCP range to one device and another device configured to use that address is turned on.

13. Change M11 Web-HTTP port number if needed.

    You must change the M11 internal Web server port number default value 80 if the same port number is used for pinhole functionality. See Pinhole configuration example in Figure 5-12.

14. Change M11 telnet port number if needed.

    You must change M11 internal telnet server port number default value 23 if the same number is used for pinhole functionality.

15. Click *Go to NAT Setup* to configure the pinhole functionality if needed.

16. Enter static routes

    Static route identifies a manually configured route to a remote network. Unlike dynamic routes, which are acquired and confirmed periodically from other routers, static routes do not time out.

    You can specify static routes by filling in the remote router’s destination address, net mask and gateway address. After you have filled in the required information, click *Add.*

17. Save the configuration.

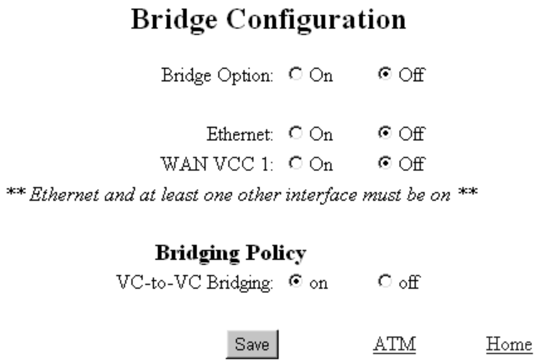
    You must save the new configuration. *Save* command takes you to the M11 home page.

18. Restart your M11.

    You must restart your M11 by clicking *Restart M11* for your changes to take effect.

5.1.4 Bridge page

Bridge page is used to enable/disable bridging. When bridging is enabled the page is used to select the interfaces that are included in the bridging function.



Bridge Configuration

Bridge Option: ○ On ● Off

Ethernet: ○ On ● Off

WAN VCC 1: ○ On ● Off

*** Ethernet and at least one other interface must be on ***

Bridging Policy

VC-to-VC Bridging: ● on ○ off

Figure 5-7 Bridge page

Only those ATM interfaces that support ’ether-llc’ or ’ether-vcmux’ encapsulation or ’ppp-vcmux’ encapsulation with BNCP support can be used in bridging operation.

Filling in bridge settings

1. Turn on bridge
2. Click ATM to configure ATM channels, if needed (see Section 5.1.5).
3. Select the interfaces you want to use for bridging.

   Ethernet indicates the Ethernet interface of M11. DSL VCC radio buttons indicate ATM channels using ’ether-llc’ or ’ether-vcmux’ encapsulation. WAN VCC radio buttons indicate ATM channels using ’ppp-vcmux’ encapsulation with BNCP support.
4. Enable/disable bridging between ATM VCCs.

   This option can be used when multiple M11s are connected together using bridged connection. Disabling the bridging between the VCCs eliminates the loops from the bridged network.

5. Save the configuration.

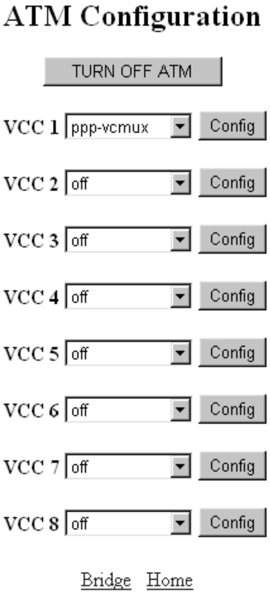
   You must save the new configuration. Save command takes you to the M11 home page.

6. Restart your M11.

   You must restart your M11 by clicking *Restart M11* for your changes to take effect.

5.1.5 ATM page

ATM page is used to enable/disable ATM channels and select the payload encapsulation method for a particular channel. After enabling an ATM channel, you can configure the channel in more detail through the ATM-channel-specific *Config* buttons.



ATM Configuration

VCC 1 ppp-vcmux

VCC 2 off

VCC 3 off

VCC 4 off

VCC 5 off

VCC 6 off

VCC 7 off

VCC 8 off

Figure 5-8 ATM page

Filling in ATM settings

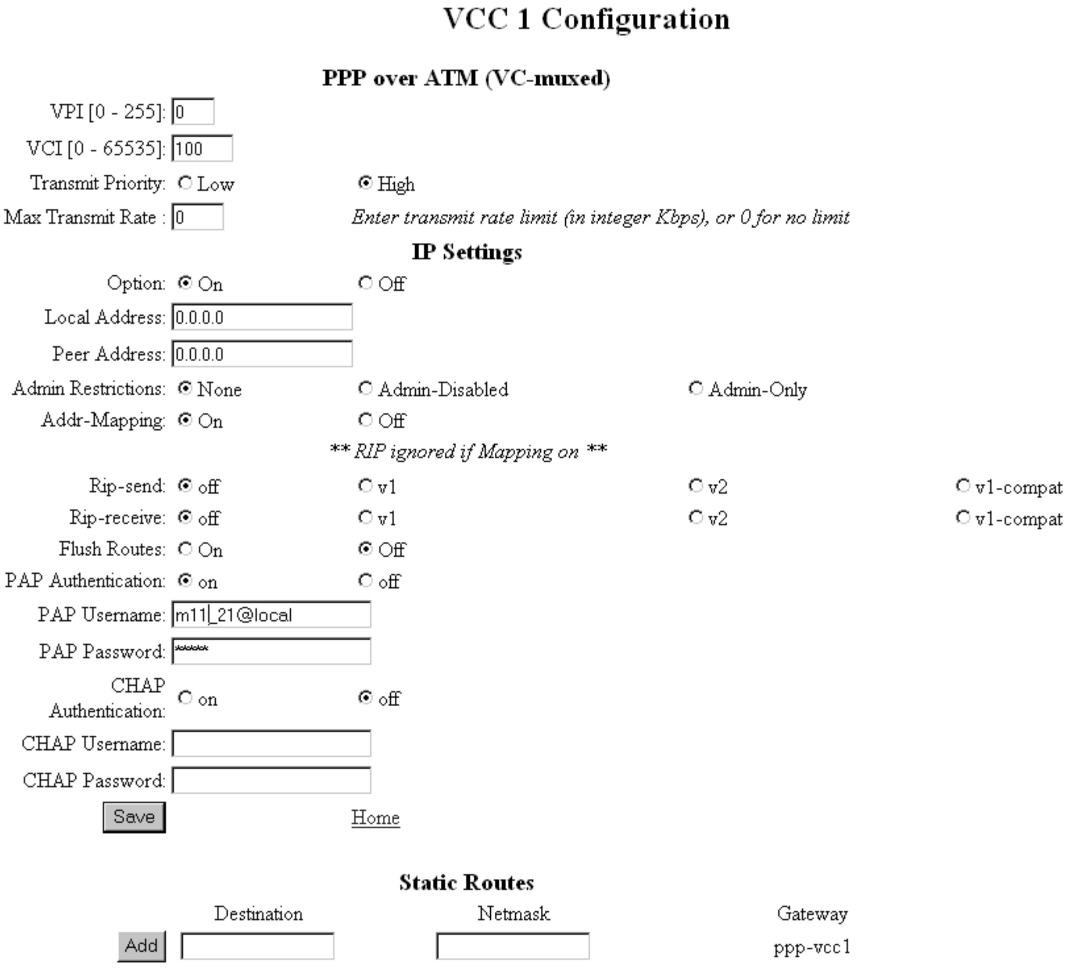
1. Enable a channel by selecting the encapsulation from the list. Up to eight ATM channels can be used.

2. Configure the ATM channels.

   Click Config button for the channel you want to configure.

Configuring ATM channels

PPP over ATM (VC-muxed)



VCC 1 Configuration

PPP over ATM (VC-muxed)

VPI [0 - 255]:	0			
VCI [0 - 65535]:	100			
Transmit Priority:	○ Low	● High		
Max Transmit Rate :	0	*Enter transmit rate limit (in integer Kbps), or 0 for no limit*		

IP Settings

Option:	● On	○ Off		
Local Address:	0.0.0.0			
Peer Address:	0.0.0.0			
Admin Restrictions:	● None	○ Admin-Disabled	○ Admin-Only	
Addr-Mapping:	● On	○ Off		

*** RIP ignored if Mapping on ***

Rip-send:	● off	○ v1	○ v2	○ v1-compat
Rip-receive:	● off	○ v1	○ v2	○ v1-compat
Flush Routes:	○ On	● Off		
PAP Authentication:	● on	○ off		
PAP Username:	m11_21@local			
PAP Password:	*****			
CHAP Authentication:	○ on	● off		
CHAP Username:				
CHAP Password:				

Static Routes

	Destination	Netmask	Gateway
Add			ppp-vcc1

Figure 5-9 ATM channel configuration page (VC-muxed)

1. Set the virtual path and virtual channel identifications.
2. Enable/disable Transmit priority function and set the maximum transmit rate.

   Transmit priority function allows you to set priorities to the upstream direction of ATM channels.

Note
You must have admin rights to set transmit priorities.

3. Enable/disable IP.

   IP Settings allow you to activate the IP layer function of the ATM channel. *Local address* and *peer address* specify the basic IP address parameters of the ATM channel interface (PPP over ATM). If you write 0.0.0.0 in these fields, M11 will try to get them from the network using either IPCP protocol (ATM channel using PPP) or DHCP (ATM channel not using PPP).

   Admin Restrictions is used to apply management restrictions to the channel. If you select *Admin-Disabled*, you cannot manage M11 through this channel. If you select *Admin-Only*, this channel will be used as a dedicated management channel.

   Address mapping radio button activates/deactivates the Network Address Port Translation (NAPT).

4. Configure Routing Information Protocol (RIP) settings.

   Enable/disable dynamic routing for the active IP interface on the ATM channel by selecting the corresponding radio buttons. If *RIP-send* is selected, M11 sends RIP messages (version 1, 2 or both) to the network. If *RIP-receive* is selected, M11 listens to RIP messages from the network. RIP-send with *V1-compat* option enables the sending of RIPv2 packets using broadcast. RIP-receive with *V1-compat* option accepts both RIPv1 and RIPv2 packets. If you enable *Flush Routes*, the learned routes are deleted when the PPP connection is disconnected.

5. Enable/disable PAP/CHAP authentication and fill in the corresponding usernames and passwords if authentication is needed. Ask your service provider which authentication to use.

6. Add static routes to the routing table of the interface.

   Enter *destination address*, *net mask* and *gateway* and click Add.

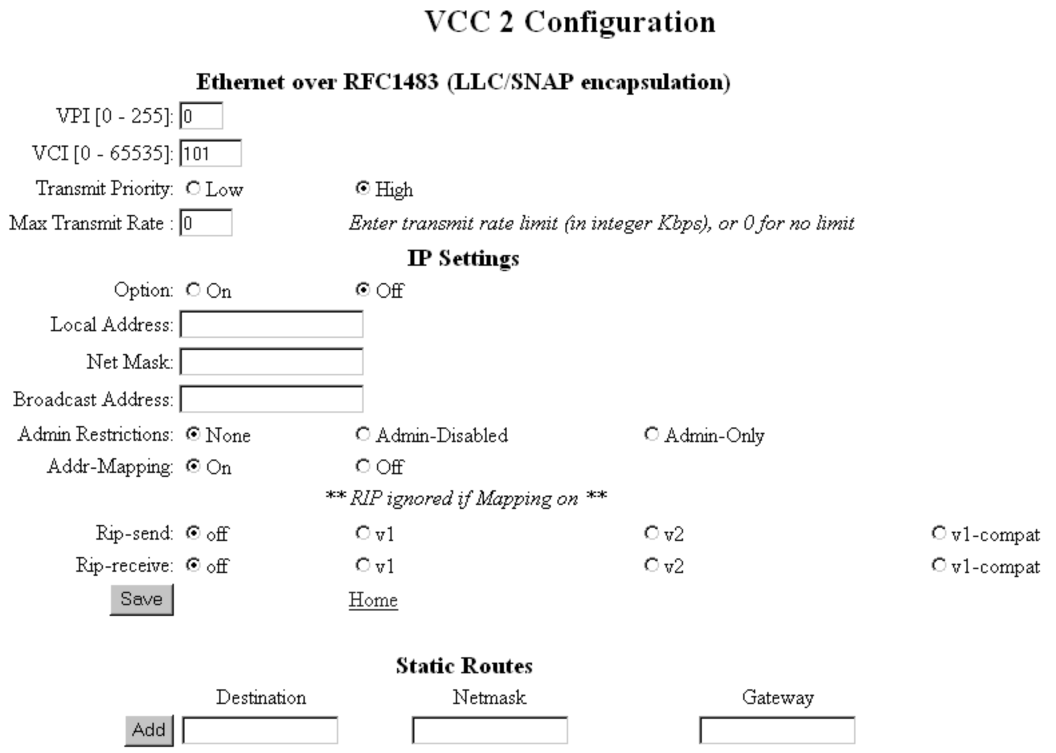
7. Save the configuration.

   You must save the new configuration. *Save* command takes you to the M11 home page.

8. Restart your M11.

   You must restart your M11 by clicking *Restart M11* for your changes to take effect.

Other encapsulations



VCC 2 Configuration

Ethernet over RFC1483 (LLC/SNAP encapsulation)

VPI [0 - 255]: 0

VCI [0 - 65535]: 101

Transmit Priority: ○ Low ● High

Max Transmit Rate : 0 *Enter transmit rate limit (in integer Kbps), or 0 for no limit*

IP Settings

Option: ○ On ● Off

Local Address:

Net Mask:

Broadcast Address:

Admin Restrictions: ● None ○ Admin-Disabled ○ Admin-Only

Addr-Mapping: ● On ○ Off

*** RIP ignored if Mapping on ***

Rip-send: ● off ○ v1 ○ v2 ○ v1-compat

Rip-receive: ● off ○ v1 ○ v2 ○ v1-compat

Static Routes

Figure 5-10 ATM channel configuration page (other encaps.)

1. Set the virtual path and virtual channel identifications.

2. Enable/disable IP.

   IP setting allows you to activate the IP layer function of the ATM channel. *Local address*, *net mask* and *broadcast address* specify the basic IP address parameters of the ATM channel interface (IP over RFC1483). If you enter 0.0.0.0 in these fields, M11 will try to get them from the network using either IPCP protocol (ATM channel using PPP) or DHCP (ATM channel not using PPP).

   Address mapping radio button activates/deactivates the Network Address Port Translation (NAPT).

3. Configure Routing Information Protocol (*RIP*) settings.

   Enable/disable dynamic routing for the active IP interface on the ATM channel by selecting the corresponding radio buttons. If *RIP-send,* is selected M11 sends RIP messages (version 1, 2 or both) to the network. If *RIP-receive* is selected, M11 listens to RIP messages from the network. RIP-send with *V1-compat* option enables the sending of RIPv2 packets using broadcast. RIP-receive with *V1-compat* option accepts both RIPv1 and RIPv2 packets.

4. Add static routes to the routing table of the interface.

   Enter *destination address*, *net mask* and *gateway* and click Add.

5. Save the configuration.

   You must save the new configuration. *Save* command takes you to the M11 home page.

6. Restart your M11.

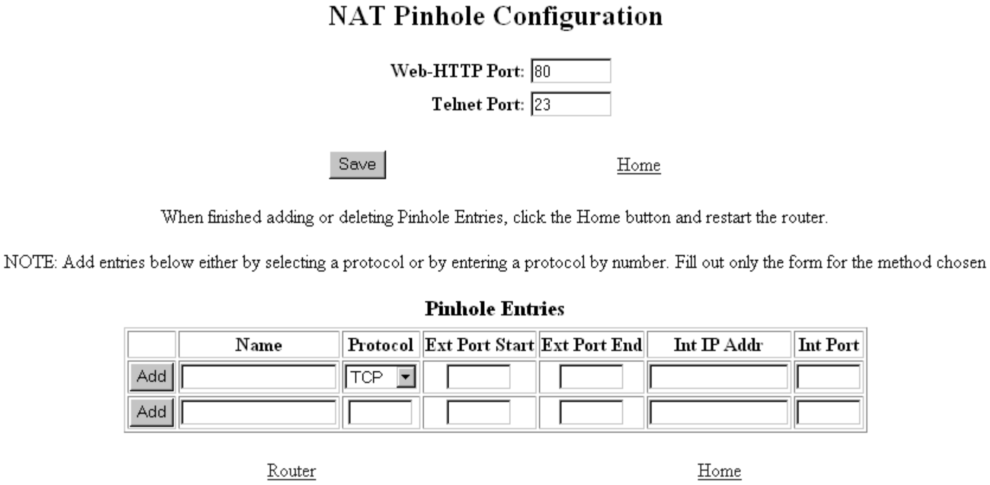
   You must restart your M11 by clicking *Restart M11* for your changes to take effect.

5.1.6 NAT pinhole page

The NAT pinhole page is used to make servers located in a LAN visible to the WAN through a VCC. It allows fixed NAPT mapping between a WAN/VCC IP address/port number and an internal LAN IP address/port number. Separate entries must be created for TCP and UDP ports.

The standard port numbers for the most common protocols are:

- HTTP (Hypertext Transfer Protocol) is TCP port 80
- FTP (File Transfer Protocol) is TCP port 21
- SMTP (Simple Mail Transfer Protocol) is TCP port 25
- NNTP (Network News Transfer Protocol) is TCP port 119



NAT Pinhole Configuration

Web-HTTP Port: 80

Telnet Port: 23

When finished adding or deleting Pinhole Entries, click the Home button and restart the router.

NOTE: Add entries below either by selecting a protocol or by entering a protocol by number. Fill out only the form for the method chosen

Pinhole Entries

	Name	Protocol	Ext Port Start	Ext Port End	Int IP Addr	Int Port
Add		TCP ▾				
Add						

Figure 5-11 NAT pinhole page

1. Enter a *name* for the pinhole entry. Select the *protocol*. Enter the *External Port Start* and *External Port End* numbers. These define the available range of allowed external ports (port number in WAN interface). Enter *Internal IP address* (server IP address in LAN) and *Internal Port* number (server port number in LAN). The Internal Port number is the start of the internal port range.
2. Click *Add*.
3. Repeat until each server’s information is filled.
4. To remove an entry, click *delete*.

5. Change the integrated Web and telnet servers' *port numbers* if needed.

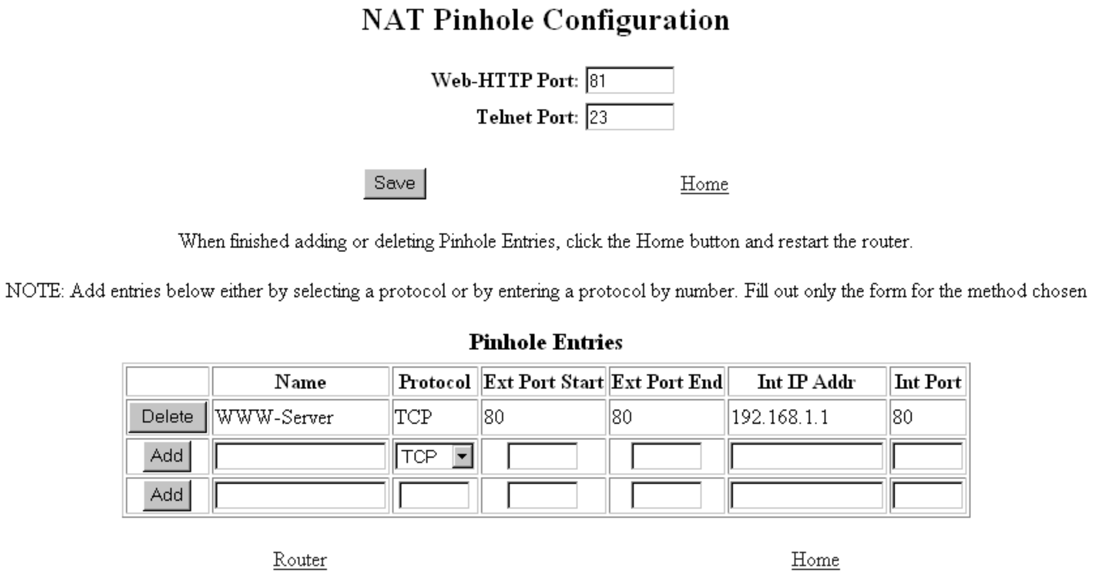
   If you have servers (Web or telnet servers) on your home network which must be accessible from outside your home network, you must change the default port numbers (80 and 23, respectively) of the integrated Web and telnet servers of your M11.
6. Save new port numbers and restart M11.

Pinhole configuration example

The pinhole configuration example in Figure 5-12 can be used to allow access from WAN to a Web server on the LAN. The example configuration relays the traffic coming from the M11 WAN TCP port 80 to the LAN IP address 192.168.1.1 port 80. Port 80 is a standard TCP port for HTTP. The port number of the M11's integral Web server has been changed to 81.

Note

M11's integral Web server used for monitoring and configuration uses also port 80 by default. You must change the server port by typing the new port number in the Web HTTP Port field or else the TCP traffic to this port is directed to the M11 Web server instead of the Web server on your LAN.



NAT Pinhole Configuration

Web-HTTP Port: 81

Telnet Port: 23

When finished adding or deleting Pinhole Entries, click the Home button and restart the router.

NOTE: Add entries below either by selecting a protocol or by entering a protocol by number. Fill out only the form for the method chosen

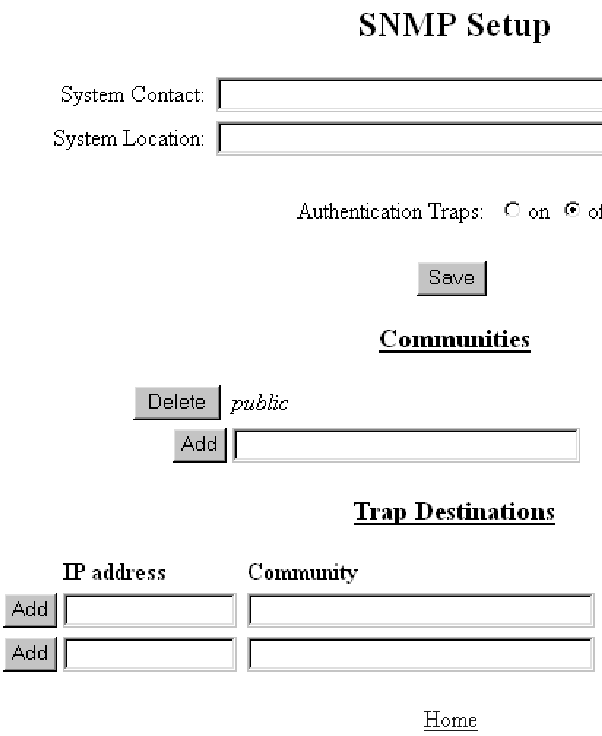
Pinhole Entries

	Name	Protocol	Ext Port Start	Ext Port End	Int IP Addr	Int Port
Delete	WWW-Server	TCP	80	80	192.168.1.1	80
Add		TCP ▾				
Add						

Figure 5-12 Pinhole configuration example

5.1.7 SNMP page

The SNMP page is used to configure the SNMP-related parameters of M11. In M11, the SNMP can be used only for writing/reading system contact information and trap addresses. Trap address is an address to which a trap is sent in case of an authentication violation.



SNMP Setup

System Contact:

System Location:

Authentication Traps: ○ on ● off

Communities

public

Trap Destinations

IP address | Community

Figure 5-13 SNMP page

Filling in SNMP settings

1. Enter *contact information* and *system location* information in the corresponding fields.
2. Enable/disable *authentication traps*.
3. Add/delete user *communities* if needed.

   Enter the name of the new user community into the field.
4. Enter *trap destination* addresses.

   Enter the *IP addresses* of the hosts to which the traps are sent. Enter also the *community* string related to this address.

5. Save the configuration.

   You must save the new configuration. Save command takes you to the M11 home page.

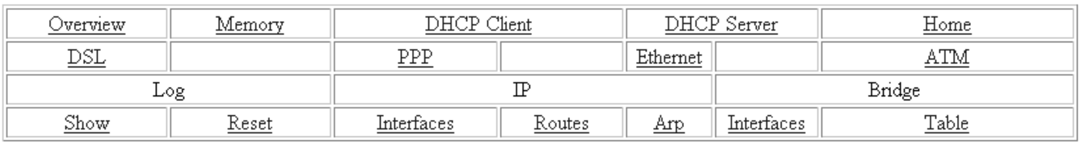
6. Restart your M11.

   You must restart your M11 by clicking Restart M11 for your changes to take effect.

5.1.8 Monitor page

You can get information about the status and statistics of the M11 through the Monitor page. The following links are available on the Monitor page.

- **Overview** displays the basic identification information of M11.
- **Memory** displays the memory usage of M11.
- **DHCP Client** displays the IP address settings M11 has received from the network.
- **DHCP Server** displays the DHCP server lease table.
- **Home** returns to home page.
- **DSL** displays the the status of the ADSL connection and statistics about the connection.
- **PPP** displays status information about the IP/PPP interfaces.
- **Ethernet** displays status information of the Ethernet interface.
- **ATM** displays status information of the ATM channels.
- **Show** displays the Diagnostic log of M11.
- **Reset** scrolls the Diagnostic log window back to the first message.
- **Interfaces** displays status information of the active interfaces.
- **Routes** displays the routing table.
- **ARP** displays the ARP cache table.
- **Table** displays the bridge table



Overview	Memory	DHCP Client		DHCP Server		Home
DSL		PPP		Ethernet		ATM
Log		IP			Bridge	
Show	Reset	Interfaces	Routes	Arp	Interfaces	Table

Figure 5-14 Monitor page

5.2 Command line interface

The Nokia M11 operating software includes a command line interface (CLI) that lets you monitor and configure your M11 over a telnet or a local serial console connection. You can use the CLI to enter and update configuration settings in M11, monitor its performance, and restart it. Some CLI commands are not available until certain conditions are met. For example, you must turn a function on before you can enter settings for that function.

The commands of the CLI are divided into two hierarchies: Root and Config. The Root command hierarchy lets you monitor the performance of your M11, display and reset M11 statistics, and issue administrative commands to restart M11 functions. The Config command hierarchy lets you configure the settings of your M11.

5.2.1 Starting and ending a CLI session

You can open a command line interface session by opening a telnet connection from a workstation on your network to an M11 Ethernet or ADSL port or by connecting a terminal to the console port on Nokia M11.

Connecting with telnet

You initiate a telnet connection by issuing the following command from an IP host that supports telnet (or a personal computer running a telnet application such as Microsoft or NCSA Telnet).

```
telnet ADSL_ip_address
```

You must know the IP address of your Nokia M11 before you can connect to it via a telnet connection to it. You can use the command line interface to configure the IP address of your M11.

Connecting through console port

You can connect a terminal or a terminal emulator to the console port on the Nokia M11 front panel to configure, administer, and monitor your Nokia M11. To use the Nokia M11 console, you need a special cable (E64320.01) and either a terminal or a terminal emulator (such as a personal computer with a terminal emulation application that supports 9600-baud communication).

To connect your Nokia M11 to a terminal or terminal emulators:

1. Plug the special cable E64320.01 into the console port behind the hatch on the Nokia M11 front panel.
2. Connect the other end of the serial cable to the serial port on your terminal (or terminal emulator) or the serial port of your computer.
3. Turn on the terminal or run the terminal emulator program on your computer.

Use the following settings to configure your terminal emulation session:

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

The console interface uses the same command line interface as the telnet interface.

Logging in

The command line interface login process emulates the login process for a Unix host. If your Nokia M11 has been assigned a system password, you must enter a username (up to 64 characters) and your administrator, user-administrator or user password.

Entering your username lets Nokia M11 record your access; your username is not used to validate your authorisation. The passwords give you the following rights:

● User password	view (but not change) M11 settings and monitor statistics
● User-administrator	change CHAP and PAP settings, configure pinhole, Ethernet and router settings as well as monitor M11 statistics
● Administrator	change M11 settings and view statistics

When you have logged in successfully, the command line interface lists the username and the security level (admin, user-admin or user) associated with the password you entered in the diagnostic log.

Issuing CLI commands

CLI commands consist of *keywords* and *arguments*. Keywords in a Config command specify the action you want to take or the entity on which you want to act. Arguments in a Config command specify the values appropriate to your site. For example, the Config command `set ip ip-ppp address` *`ip_address`* consists of three keywords (`ip`, `ip-ppp`, and `address`) and one argument (*`ip_address`*). When you configure your M11, you replace command arguments with values appropriate to your site. For example, `set ip ip-ppp address 192.31.222.57`

The optional arguments are marked with braces {argument} and the mandatory arguments with square brackets [argument].

Table 5-1 provides guidelines for formatting CLI commands.

Command component	Rules for entering CLI commands
Command word	CLI commands must start with a command word (`set`, `show`, `delete`). You can truncate CLI commands to three characters (`set`, `sho`, `del`). CLI commands are not case-sensitive: you can enter “`SET`“, “`Set`“ or “`set`“.
Keywords	Keywords are not case-sensitive. You can enter “`SYSTEM`, “`System`“ or “`system`“ as a keyword without changing its meaning. Keywords can be abbreviated to the length that they are differentiated from other keywords. For example, you can reduce the command “`set ip ip-ppp option on`“ to “`set i i o on`“.
Argument text	Text strings can be as many as 32 characters long, unless otherwise specified. Special characters are represented using backslash notation. Text strings may be enclosed in double (”) or single (’) quote marks. If the text string includes an embedded space, it must be enclosed in quotes.
Numbers	Type numbers as integers.
IP addresses	Type IP addresses in dotted decimal notation (nnn.nnn.nnn.nnn, where nnn = 0 to 255).

Table 5-1 CLI syntax

If a command is ambiguous or miskeyed, Nokia CLI prompts you to enter additional information.

Ending a CLI session

You end a command line interface session by typing `quit` in the Root mode. Entering `quit` in the Config mode switches the session into the Root mode.

Using the CLI help facility

The help command lets you display on-line help for Root and Config commands. To display a list of the commands available to you from your current location in the command line interface hierarchy, type `help`. To display help related to a particular command, type the command followed by a question mark, for example `show ?`.

Saving settings

The `save` command saves the working copy of the settings to restart values. You can save the changes you have made for a specific function or for all functions in your Nokia M11. The Nokia M11 automatically validates its settings when you save and displays a warning message if the configuration is not correct.

5.2.2 Root command hierarchy

When you start a CLI session you begin in Root mode. The Root mode lets you monitor the performance of your M11, display and reset M11 statistics, and issue M11 commands.

Root prompt

When you are in Root mode, the CLI prompt is the name of the M11 followed by a right angle bracket (>). For example, if you open a command line interface to the M11 named “Kilo” you would see `Kilo>` as your CLI prompt.

Root command shortcuts

You can truncate most commands in the command line interface to their shortest unique string. For example, you can use the truncated command `q` in place of the full `quit` command to exit the command line interface.

The only command you cannot truncate is `restart`. To prevent accidental interruption of communications, you must enter the `restart` command in its entirety.

You can use the `!!` command to repeat the last command you entered. You can press the CTRL+P or ESC+K key sequences to obtain the same result.

Root commands

You can get a list of the Root commands by typing `?` at the Root prompt.

●	`help`	to get help
●	`configure`	to configure unit’s options
●	`netstat`	to show IP information

● `ping`	to send ICMP Echo request
● `atmping`	to send ATM OAM loopback
● `arp`	to send ARP request
● `quit`	to quit shell
● `reset`	to reset subsystems
● `restart`	to restart unit
● `show`	to show system information
● `start`	to start subsystem
● `status`	to show basic status of unit
● `telnet`	to telnet to a remote host
● `who`	to show who is using the shell
● `log`	to add a message to the diagnostic log
● `loglevel`	to report or change diagnostic log level
● `install`	to download and program an image into flash
● `download`	to download a config file
● `upload`	to upload a config file
● `clear`	to erase all stored configuration information

The following tables present the Root commands, their detailed descriptions, syntax and usage examples.

Command	**Send ARP request**
Description	Sends an Address Resolution Protocol request to match the nnn.nnn.nnn.nnn IP address to an Ethernet hardware address.
Syntax	arp [nnn.nnn.nnn.nnn]
Arguments	The argument is an IP string which consists of four decimal numbers with values between 0 and 255 separated by dots.
Example	`M11> arp 192.221.11.11`

Command	**Clear configuration settings**
Description	Clears the configuration settings of your M11. Issuing the `restart` command after the `clear` command restores the default configuration. `clear` command alone clears the configuration and brings M11 into an undefined state.
Syntax	clear {yes}
Arguments	If you do not use the optional `yes` argument, CLI prompts you to confirm the clear command.
Example	`M11> clear yes`

Command	**Download software update**
Description	Downloads a new version of the Nokia M11 operating software from a TFTP (Trivial File Transfer Protocol) server, validates the software image, and programs the image into the Nokia M11 memory. After you install new operating software, you must restart Nokia M11.
Syntax	install [server_address] [filename] {confirm}
Arguments	The TFTP server must be accessible on your Ethernet network or through one of the active ATM virtual channels and a route to the server must exist. The `server address` argument identifies the IP address of the TFTP server on which your Nokia M11 operating software is stored. The `filename` argument identifies the path and name of the operating software file on the TFTP server. If you include the optional `confirm` keyword, you will not be prompted to identify a TFTP server or file name. Your Nokia M11 begins the software installation using its default boot settings.

Example	`M11> install 192.168.1.1 M11c_500.d39`
	`*** WARNING *** YOU ARE ABOUT TO ERASE`
	`AND REPROGRAM THE NOKIA M11’S PERMANENT`
	`SOFTWARE STORAGE WITH A NEW SOFTWARE VER-`
	`SION OBTAINED VIA THE TFTP PROTOCOL.`
	`About to install new Flash EPROM software`
	`image:`
	`     server: 192.168.1.1`
	`     file: “M11c_500.d39”`
	`Do you wish to proceed? (type ’yes’ to`
	`confirm): yes`
	`Installing`
	`M11>`

Command	Add message to log
Description	Adds the message in the *message_string* argument to the Nokia M11 diagnostic log.
Syntax	log [message_string]
Arguments	`message_string` argument is the message you want to add to the log.
Example	`M11> log 05/05/99`

Command	Define log level
Description	Displays or modifies the types of log messages you want Nokia M11 to record. You can enter the `loglevel` command with the `level` argument to specify the types of diagnostic messages you want to record. All messages with a level number equal to or greater than the level you specify are recorded.
Syntax	loglevel {level}
Arguments	If you enter the `loglevel` command without the optional *level* argument, the Nokia CLI displays the current log level setting. The values for the argument are: 1 or low — Trivial status messages. 2 or medium — Messages that can help monitor the network traffic. 3 or high — Status messages that may be significant but do not constitute errors. 4 or warning — Recoverable error conditions and useful operator information 5 or failure — Messages describing error conditions that may not be recoverable
Example	`M11> loglevel 3`

Command	**Ping**
Description	Causes the Nokia M11 to send a series of ICMP Echo requests for the device with the specified IP address. You can use the `ping` command to determine whether an IP address is already in use on your network. You cannot use the `ping` command to ping the Nokia M11’s own IP address. If a host using the specified IP address is active, it returns one or more ICMP Echo replies, confirming that it is accessible from your network.
Syntax	ping [ip_address]
Arguments	`ip_address` argument is the IP address, in dotted decimal notation, of the device you want to locate.
Example	`M11> ping 192.122.12.11`

Command	**ATM ping**
Description	Sends 5 OAM F5 loopback cells to the specified VPI/VCI destination with a 5 second total timeout interval.
Syntax	atmping [vpi] [vci] [segment | end-to-end]
Arguments	`vpi` and `vci` specify the channel and the third argument specifies segment or end-to-end loopback.
Example	`M11> atmping 0 100 segment`

Command	**Exit**
Description	Exits the Nokia M11 command line interface.
Syntax	quit
Arguments	None.
Example	`M11> quit`

Command	**Reset ATM statistics**
Description	Resets ATM statistics to zero.
Syntax	reset atm
Arguments	None
Example	`M11> reset atm`

Command	Clear crash information
Description	Clears crash-dump information which identifies the contents of M11 registers at the point of system malfunction.
Syntax	reset crash
Arguments	None.
Example	`M11> reset crash`

Command	Reset DHCP server leases
Description	Resets DHCP server leases.
Syntax	reset dhcp server
Arguments	None
Example	`M11> reset dhcp server`

Command	Release DHCP client lease
Description	Resets DHCP client lease of the WAN port.
Syntax	reset dhcp client lease
Arguments	None
Example	`M11> reset dhcp client lease`

Command	Retrieve DHCP client configuration
Description	Retrieves the DHCP client configuration for the WAN port.
Syntax	reset dhcp client retrieve
Arguments	None
Example	`M11> reset dhcp client retrieve`

Command	Reset ADSL connection
Description	Resets the ADSL connection.
Syntax	reset dsl
Arguments	None.
Example	`M11> reset dsl`

Command	Reset Ethernet statistics
Description	Resets the Ethernet statistics to zero.
Syntax	reset enet
Arguments	None.
Example	`M11> reset enet`

Command	Rewind log
Description	Rewinds the diagnostic log display to the top of the existing M11 diagnostic log. The `reset log` command does not clear the diagnostic log. The next `show log` command will display information from the beginning of the log file.
Syntax	reset log
Arguments	None.
Example	`M11> reset log`

Command	Reset PPP connection
Description	Resets and restarts the PPP connection of the specified ATM logical channel. When you issue the `reset ppp` command, Nokia M11 closes the PPP session on the specified ATM channel and restarts the connection. You can use also `start ppp` command to reset and restart PPP connection.
Syntax	reset ppp [vccx]
Arguments	vccx indicates the ATM channel, x = 1 – 8.
Example	`M11> reset ppp vcc1`

Command	Reset packet statistics
Description	Resets packet statistics to zero.
Syntax	reset xdsl
Arguments	None
Example	`M11> reset xdsl`

Command	Restart M11
Description	Restarts M11. You must enter the the complete restart command to initiate a restart.
Syntax	restart {seconds}
Arguments	If you include the optional `seconds` arguments, your Nokia M11 will restart when the specified number of seconds has elapsed.
Example	`M11> restart 5`

Command	Show crash information
Description	Displays the most recent crash information.
Syntax	show crash
Arguments	None.
Example	`M11> show crash`

Command	Show DHCP server leases in RAM
Description	Displays the DHCP leases stored in RAM.
Syntax	show dhcp server leases
Arguments	None.
Example	`M11> show dhcp server leases`

Command	**Show DHCP server leases in NVRAM**
Description	Displays the DHCP leases stored in NVRAM
Syntax	show dhcp server store
Arguments	None.
Example	`M11> show dhcp server store`

Command	**Show DHCP client parameters**
Description	Displays the DHCP client parameters of the WAN port.
Syntax	show dhcp client
Arguments	None.
Example	`M11> show dhcp client`

Command	**Show Ethernet statistics**
Description	Displays the Ethernet statistics of your M11.
Syntax	show enet {all}
Arguments	Optional argument `all` displays more detailed information.

Example	`M11> show enet`
	`Ethernet driver statistics, device 0:`
	`Packets out:   16578`
	`Packets in:    11`
	`Xmit errors:   0`
	`Recv errors:   0`
	`CRC errors:    0`
	`Frame errors:  0`
	`No buffers:    0`
	`No handler:    0`
	`No message:    0`
	`M11>`

<table>
<tr><th>Command</th><th>Show ADSL information</th></tr>
<tr><td>Description</td><td>Displays the current status and some statistics about the ADSL connection, for example upstream and downstream data rates.</td></tr>
<tr><td>Syntax</td><td>show dsl</td></tr>
<tr><td>Arguments</td><td>None.</td></tr>
<tr><td>Example</td><td><pre>
M11> show dsl
DSL Statistics:
Type: ALC DMT CP
Datapump HW Rev: f
Datapump FW Rev: 2.5.8
Datapump Vendor ID: 1f9
Current Status: LINK UP
Data Path: Fast

               Downstream   Upstream
Current rate   8000 Kbps   800 Kbps
Maximum rate   10000 Kbps   963 Kbps

Noise Margin   11.5 db   12.0 dB
Attenuation   0.0 db   3.0 dB
Out Power   10.0 dB   12.0 dB

               Near   Far
FEC Counts Fast 0   0
CRC Counts Fast 0   0
HEC Counts Fast 0   0
M11>
</pre></td></tr>
</table>

Command	**Show ATM information**
Description	Displays the current status and some statistics of the active ATM channels.
Syntax	show atm {all}
Arguments	Optional argument `all` displays more detailed information.

Example	`M11> show atm`
	`ATM port status: Cell delineation achieved`
	`Rx data rate (bps): 8192000`
	`Tx data rate (bps): 819200`
	
	`ATM Virtual Circuits:`
	
	`VCC# Type VPI VCI Bound Encapsulation`
	`-------------------------------------`
	`1    PVC   0  100  Yes  PPP over ATM (VC-muxed)`
	
	`ATM Traffic Parameters:`
	
	`VCC# Tx Priority Tx Rate Limit`
	`------------------------------`
	`1      High         None`
	
	`M11>`

Command	**Show ARP table**
Description	Displays the Ethernet address resolution table stored in M11.
Syntax	show ip arp
Arguments	None.
Example	`M11> show ip arp`

<table>
<tr><th>Command</th><th>Show IP interfaces</th></tr>
<tr><td>Description</td><td>Displays the IP interfaces of your M11. You can also use <code>netstat -i</code> command for this purpose.</td></tr>
<tr><td>Syntax</td><td>show ip interfaces</td></tr>
<tr><td>Arguments</td><td>None.</td></tr>
<tr><td>Example</td><td><pre>
M11> show ip interfaces
IP Interfaces:
ENET (lan): (up broadcast default rip-
send v1 rip-receive v1)
     inet 192.168.1.254
     netmask ffffff00
     broadcast 192.168.1.255
physical address 00.40.43.08.ff.ff
mtu 1500
PPP (vcc1): (up point-to-point rip-send
v2 rip-receive v2)
     inet 10.98.20.21
     netmask 0
     peer address 10.98.20.1
     physical address
     00.00.00.00.00.00
     mtu 1500
M11>
</pre></td></tr>
</table>

<table>
<tr><th>Command</th><th>Show IP routes</th></tr>
<tr><td>Description</td><td>Displays the IP routes stored in your M11. You can also use <code>netstat -r</code> command for this purpose.</td></tr>
<tr><td>Syntax</td><td>show ip routes</td></tr>
<tr><td>Arguments</td><td>None.</td></tr>
<tr><td>Example</td><td><pre>
M11> show ip routes
IP gateway (route) table:
0. Default Gateway -> PPP (vcc1), D 2, T
0, (configured) UP DEFAULT

IP route cache
Net 192.168.1.1, gateway 192.168.1.1,
metric 0, timeout 0, via ENET (lan)
Net 192.168.1.255, broadcast, via ENET
(lan)
M11>
</pre></td></tr>
</table>

Command	Show diagnostic log
Description	Displays blocks of information from the Nokia M11 diagnostic log.
Syntax	show log {all}
Arguments	To see the entire log, you can repeat the show log command or you can use the argument `all` and scroll through the complete log.
Example	`M11> show log all`

Command	Show memory usage
Description	Displays the memory usage of your M11.
Syntax	show memory {all}
Arguments	Optional argument `all` displays more detailed information.
Example	`M11> show memory all`

Command	Show PPP information
Description	Displays information about open PPP links.
Syntax	show ppp {stats | lcp | ipcp | bncp | lastconnect}
Arguments	You can display a subset of the PPP statistics by including optional `stats`, `lcp`, `ipcp`, `bncp`, or `lastconnect` argument.
Example	`M11> show ppp`

Command	Show M11 information
Description	Displays current status of a Nokia M11, the device’s hardware and software revision levels, a summary of errors encountered, and the length of time the Nokia M11 has been running since it was last restarted.
Syntax	show status
Arguments	None.

Example	`M11> show status`
	
	`Terminal shell v1.0`
	`Nokia M11 multiport ADSL router/bridge`
	`Running Nokia M11 software version 5.3.0 (build R2)`
	`(completed login: administrator level)`
	`Serial number 61992701988, CPU MPC860SAR, firmware 2.6`
	`Product ID`
	`Error logger message counts:`
	`Low 0, Medium 0, High 25, Warning 35, Lost 0, Total 60`
	`Boot state: unknown`
	`Uptime 00:00:00:35`
	`M11>`

Command	Open telnet session
Description	Opens a telnet session to a remote host
Syntax	telnet [host] {port}
Arguments	`host` is the IP address of the remote host. Optional argument indicates the port of the remote host.
Example	`M11> telnet 1.12.123.123`

Command	Show users
Description	Displays the names and hostnames of the current shell users.
Syntax	who
Arguments	None
Example	`M11> who`

Command	**Download configuration file**
Description	Downloads a configuration file from a TFTP server.
Syntax	download [server-ipaddress] [filename] {confirm}
Arguments	`server-ipaddress` is the IP address of the TFTP server. `filename` is the name of the configuration file. If invoked as `download` with no arguments, you will be prompted for information. If the optional `confirm` keyword is added, the transfer will proceed without further questions.

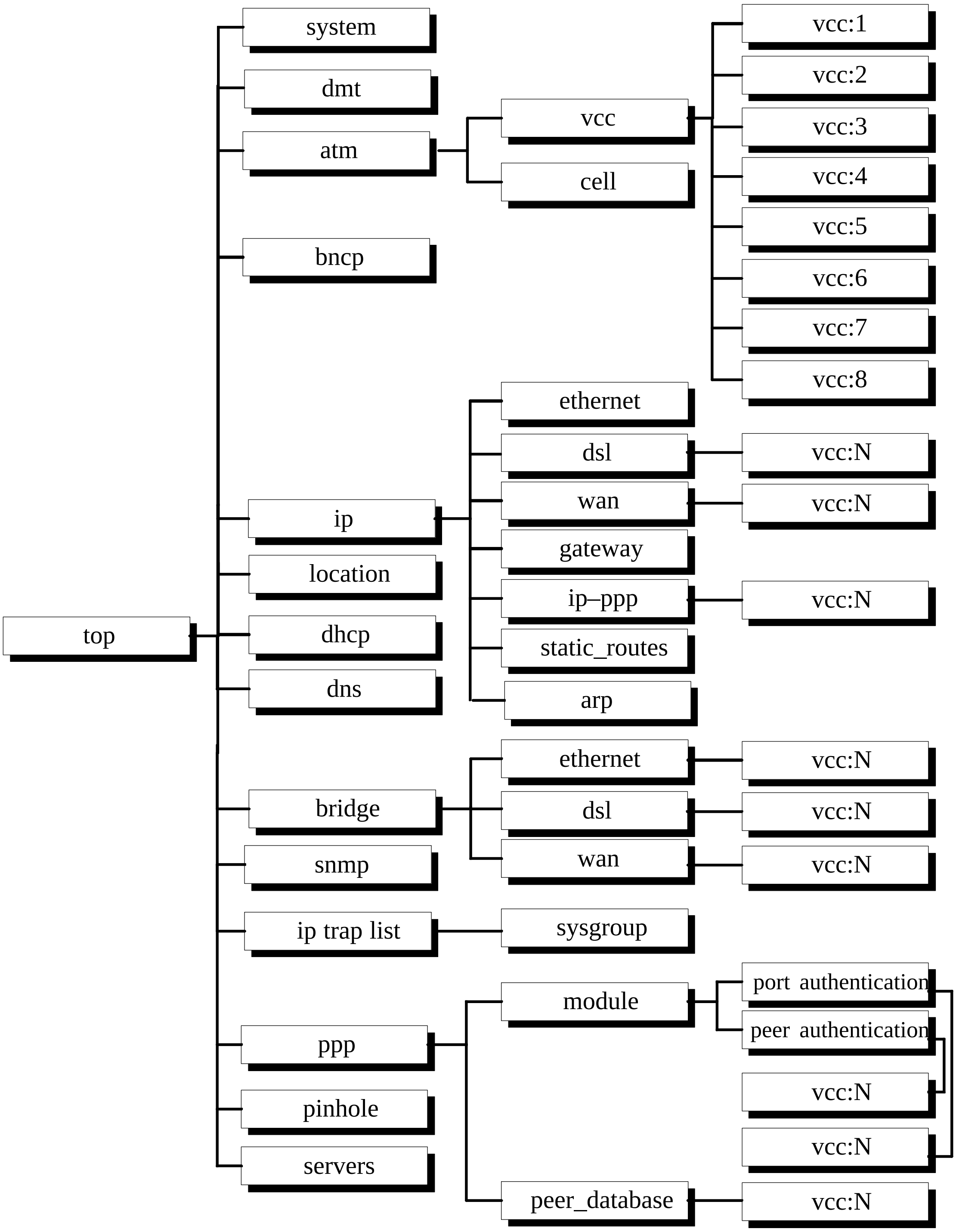
Example	`M11> download 1.12.123.123 config1.cfg`
	`***WARNING*** YOU ARE ABOUT TO DOWNLOAD A`
	`CONFIGURATION FILE.`
	`About to download configuration file:`
	`     server: 1.12.123.123`
	`     file: config1.cfg`
	`Do you wish to proceed? (type ’yes’ to`
	`confirm):yes`
	`Downloading`
	`Downloading file into RAM`
	
	`File Download was successful`
	
	`Replace existing configuration with down-`
	`loaded configuration? (type ’yes’ to con-`
	`firm):yes`
	`     172.16.0.0 has been added to the`
	`list`
	
	`Configuration data saved.`
	`M11>`

Command	**Upload configuration file**
Description	Uploads a configration file to a TFTP server.
Syntax	upload [server-ipaddress] [filename] {confirm}
Arguments	`server-ipaddress` is the IP address of the TFTP server. `filename` is the name of the configuration file. If invoked as `upload` with no arguments, you will be prompted for information. If the optional `confirm` keyword is added, the transfer will proceed without further questions.

Example	`M11> upload 1.12.123.123 config2.cfg con-`
	`firm`

5.2.3 Config command hierarchy

The Config mode lets you configure the parameters of your M11. The command hierarchy consists of nodes and subnodes. Each node contains the configurable parameters of that particular function.



Config prompt

You reach the configuration mode of the M11 CLI by typing `config` at the Root prompt. When you are in Config mode, the CLI prompt consists of the name of your M11 followed by your current node in the hierarchy and two angle brackets (>>). For example, when you enter Config mode (by typing `config` at the Root prompt), the `M11 (top)>>` prompt reminds you that you are at the top of the Config hierarchy. If you move to the `ip` node in the Config hierarchy (by typing `ip` at the Config prompt), the prompt changes to `M11 (ip)>>` to identify your current location.

Navigating the Config hierarchy

You start at the `top` when you enter Config mode. The command line interface reminds you of your location by showing your current node after the M11 name:

```
M11 (top)>>
```

- **Moving from Config to Root**
  You can navigate from anywhere in the Config hierarchy back to the Root level by issuing the `quit` command at the Config command prompt and pressing ENTER.

  ```
  M11 (top)>> quit
  M11>
  ```

- **Moving from top to a subnode**
  You can navigate from the top node to a subnode by entering the node name (or the significant letters of the node name) at the Config prompt and pressing Enter. For example, you move to the ip subnode by entering `ip` and pressing Enter.

  ```
  M11 (top)>> ip
  M11 (ip)>>
  ```

  As a shortcut, you can use the significant letters of the node in place of the full node name at the Config prompt. The significant characters of a node name are the letters that uniquely identify the node. For example, only the `atm` Config node starts with a, you could enter one letter (a) to move to the atm node.

  ```
  M11 (top)>> a
  M11 (atm)>>
  ```

You would have to enter two or more letters (ppp) to move to the PPP node, since its node name shares the first letter with the preferences node.

- **Jumping down several nodes at once**
  You can jump down several levels in the Config hierarchy by entering the complete path to a node.

```
M11 (top)>> ip ip-ppp
M11 (ip ip-ppp)>>
```

- **Moving up one node**
  You can move through the Config hierarchy one node at a time by entering the `up` command.

```
M11 (ip ip-ppp)>> up
M11 (ip)>>
```

- **Jumping to the top node**
  You can jump to the top level from anywhere in the Config hierarchy by entering the `top` command.

```
M11 (ip ip-ppp)>> top
M11 (top)>>
```

- **Moving from one subnode to another**
  You can move from one subnode to another by entering a partial path that identifies how far back to climb.

```
M11 (ip ip-ppp)>> ppp module
M11 (ppp module)>>
```

- **Moving from any subnode to any other subnode**
  You can move from any subnode to any other subnode by entering a partial path that starts with a top-level Config command.

```
M11 (ip ip-ppp)>> ip gateway
M11 (ip gateway)>>
```

- **Issuing commands without changing nodes**
  You can issue a complete Config command from anywhere in the hierarchy without changing your current node.

  ```
  M11 (ip ip-ppp)>> set system diag high
  M11 (ip ip-ppp)>>
  ```

  Here, the diagnostic level is set high in the system without jumping to the node first.

Displaying current settings

You can use the `show` command to display the current Root settings of your M11. When you are in Config mode, you use the `show` command to display the current Config settings. If you enter the `show` command at the top level of the Config hierarchy, the command line interface displays the settings for all enabled functions in the M11. If you issue the `show` command at an intermediate node, you see all settings for that node and its subnodes.

Stepping through M11 configuration

The Nokia M11 command line interface includes a step mode to automate the process of entering configuration settings. When you use the Config step mode, the CLI prompts you for all required and optional information. You can enter the configuration values appropriate for your site without having to enter complete CLI commands.

When you are in step mode, the CLI prompts you to enter required and optional settings. If a setting has a default value or a current setting, the command line interface displays the default value for the command in parentheses. If a command has a limited number of acceptable values, those values are presented in brackets, with each value separated by a vertical line. For example, the following CLI step command indicates that the default value is off and that valid entries are limited to on and off.

```
option (off) [on|off]: on
```

You can accept the default value for a field by pressing the Enter key. To use a different value, type it in and press Enter.

You can enter the Config step mode by typing `set` from the top node of the Config hierarchy. You can enter step mode for a particular node by typing `set` *`node_name`*. For example:

```
M11 (top)>> set system
Stepping set mode (press Control-X <Enter> to exit)
```

```
system
name (”M11”): Kutoja
Diagnostic Level (High): medium
Stepping mode ended
```

See Chapter 4 for step mode installation examples.

Validating your configuration

You can use the `validate` command to make sure that your configuration settings have been entered correctly. If you use the `validate` command, M11 verifies that all required settings are present and that the settings are consistent.

```
M11 (top)>> validate
Error: Subnet mask is incorrect
Global Validation did not pass inspection!
```

You can use the `validate` command to verify your configuration settings at any time. Your M11 automatically validates your configuration any time you save a modified configuration.

Config command reference

The top level configuration command nodes are listed below:

●	system	M11 system options
●	preference	CLI preferences
●	dmt	DMT (ADSL) option
●	atm	ATM options
●	bncp	BNCP options
●	ip	TCP/IP options
●	location	Location Manager options
●	dhcp	DHCP options
●	dns	DNS options
●	bridge	Bridge options
●	snmp	SNMP options
●	ppp	PPP options
●	pinhole	NAT/NAPT server configuration
●	servers	Local integrated server configuration

The sections below explain the commands under each top level configuration node.

System settings

You can configure system settings to assign a name to your Nokia M11 and to specify what types of messages you want the diagnostic log to record.

Command	**Set system name**
Description	Specifies the name of your Nokia M11. Each Nokia M11 is assigned a name as a part of its factory initialisation. The default name for Nokia M11 is "M11". Once you have assigned a name to your Nokia M11, you can type that name in the Open Location text field of your browser to open a connection to your Nokia M11.
Syntax	set system name [name]
Arguments	`name` is an alphanumeric string of 64 characters maximum.
Example	`M11> set system name M11`

Command	**Set diagnostic level**
Description	Specifies the types of log messages you want M11 to record. All messages with a level number equal to or greater than the level you specify are recorded.
Syntax	set system diagnostic-level {level}
Arguments	If you enter the command without the optional `level` argument, the Nokia CLI displays the current diagnostic level setting. The values for the `level` argument are: 1 or low Trivial status messages. 2 or medium Messages that can help monitor the network traffic. 3 or high Status messages that may be significant but do not constitute errors. 4 or warning Recoverable error conditions and useful operator information. 5 or failure Messages describing error conditions that may not be recoverable.
Example	`M11> set system diagnostic-level 3`

Command	**Set password**
Description	Specifies the administrator, user-administrator, or user password for a Nokia M11. When you issue the `set system password` command, you are prompted to repeat the new password to verify that you entered it correctly the first time. To prevent anyone from observing the password you enter, characters in the old and new passwords are not displayed as you type them. A password can be as many as eight alphanumeric characters. Passwords are case-sensitive and cannot include special characters or leading, trailing, or embedded spaces. For example, if you assign a password of “NokiA” to an M11, you could not enter “NOKIA”, “nokia”, “Nokia”, or “Nokia “ (with a trailing space) as an acceptable password.
Syntax	set system password [admin | user-admin | user]
Arguments	Arguments `admin`, `user-admin` and `user` specify whether administrator, user-administrator or user password will be set. User password gives only viewing rights. User-admin password gives rights to change PAP and CHAP usernames and passwords and configure pinhole settings. You must set an admin password before you can set user or user-admin passwords.
Example	`M11> set system password admin *****`

Note

The password goes into effect immediately. You have to save the configuration but you do not have to restart the M11 for the password to take effect. Assigning a password to M11 does not affect communications through the device.

CLI preferences

You can set the CLI preferences to customise your environment.

Command	**Set CLI help mode**
Description	Specifies whether you want command help and prompting information displayed. By default, the CLI verbose preference is turned off. If you turn it on, the CLI displays help for a node when you navigate to that node.
Syntax	set preference verbose [on | off]
Arguments	The argument enables/disables verbose mode.
Example	`M11> set preference verbose off`

Command	**Set display length**
Description	Specifies how many lines of information you want the CLI to display at one time.
Syntax	set preference more [lines]
Arguments	The `lines` argument specifies the number of lines you want to see at one time. By default, the command line interface shows you 16 lines of text before displaying the prompt `More ... [y|n]?`. If you enter 0 as the `lines` argument, the CLI displays information as an uninterrupted stream (which is useful for capturing information to a text file).
Example	`M11> set preference more 20`

ATM settings

You can enable ATM over ADSL operation and configure up to eight ATM channels into use. You can select between five different ways to encapsulate your payload in an ATM channel.

Command	**Enable/disable specific ATM channel**
Description	Enables/disables the specific logical ATM virtual channels. M11 supports up to eight ATM virtual channels.
Syntax	set atm vcc [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8] option [on | off]
Arguments	The first argument `1|2|3|4|5|6|7|8` specifies the channel and the second argument enables/disables it.
Example	`M11> set atm vcc 1 option off`

Command	**Set virtual path identifier for ATM channel**
Description	Sets the virtual path identifier for the specific logical ATM channel. M11 is delivered to you with a default virtual circuit identifier so usually you do not have to change this setting.
Syntax	set atm vcc [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8] vpi [0–255]
Arguments	The first argument `1|2|3|4|5|6|7|8` specifies the channel and the second argument sets the virtual path identifier.
Example	`M11> set atm vcc 2 vpi 30`

Command	**Set virtual channel identifier for ATM channel**
Description	Sets the virtual channel identifier for the specified logical ATM channel. M11 is delivered to you with a default circuit identifier and usually you do not have to change this setting.
Syntax	set atm vcc [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8] vci [0–65535]
Arguments	The first argument `1|2|3|4|5|6|7|8` specifies the channel and the second argument sets the virtual channel identifier.
Example	`M11> set atm vcc 2 vci 1221`

Command	**Set payload encapsulation for specific ATM channel**
Description	Defines how the payload is encapsulated to the specified logical ATM channel.
Syntax	set atm vcc [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8] encap [ip-llc | ip-vcmux | ether-llc | ether-vcmux | ppp-vcmux | ppp-llc]
Arguments	The first argument `1|2|3|4|5|6|7|8` specifies the channel and the second argument sets the encapsulation. The `ip-llc` and `ether-llc` encapsulations are according to RFC 1483 with LLC/SNAP encapsulation for IP and Ethernet frames, respectively. The `ip-vcmux` and `ether-vcmux` encapsulation are vc-multiplexed according to RFC 1483 for IP and Ethernet frames, respectively. In `ppp-vcmux` encapsulation both bridged and routed protocols are first encapsulated to point-to-point protocol (PPP) which is, in turn, encapsulated to ATM according to RFC 1483 vc-multiplexing. `ppp-llc` is PPP over ATM, LLC/NLPID encapsulation.
Example	`M11> set atm vcc 2 encap ip-llc`

Command	**Set transmit priority**
Description	Sets transmit priorities to VCCs. The channel with high priority gets more upstream bandwidth than low priority channel.
Syntax	set atm [vcc x] tx-priority [high|low] tx-max-kbps [0 – 1000]
Arguments	The `tx-priority` argument sets the priority of the VCC to high or low. The `tx-max-kbps` argument defines the maximum transmit rate of the VCC.
Example	`m11> set atm vcc 1 tx-priority high tx-max-kbps 400`

DMT (ADSL) setting

Command	**Set ADSL mode**
Description	Sets ADSL operational mode as defined in the respective standards.
Syntax	set dmt type (multi) [lite|dmt|ansi|multi]
Arguments	`lite` argument sets the ADSL lite mode according to G.992.2 `dmt` argument sets the ADSL mode according to G.992.1 `ansi` argument sets the ADSL mode according to T1.413 issue II `multi` argument sets the ADSL mode according to the equipment in the other end of the line.

Example	`m11> set dmt type dmt`
	`m11>`

TCP/IP settings

You can use the Nokia command line interface to specify whether TCP/IP is enabled, identify a default gateway, and to enter TCP/IP settings for the Nokia M11 Ethernet port and all active ATM/ADSL channels.

Depending on the ATM channel encapsulation, the IP settings are configured in different nodes (dsl, wan or ip-ppp) of the Config hierarchy as shown in Figure 5-15.

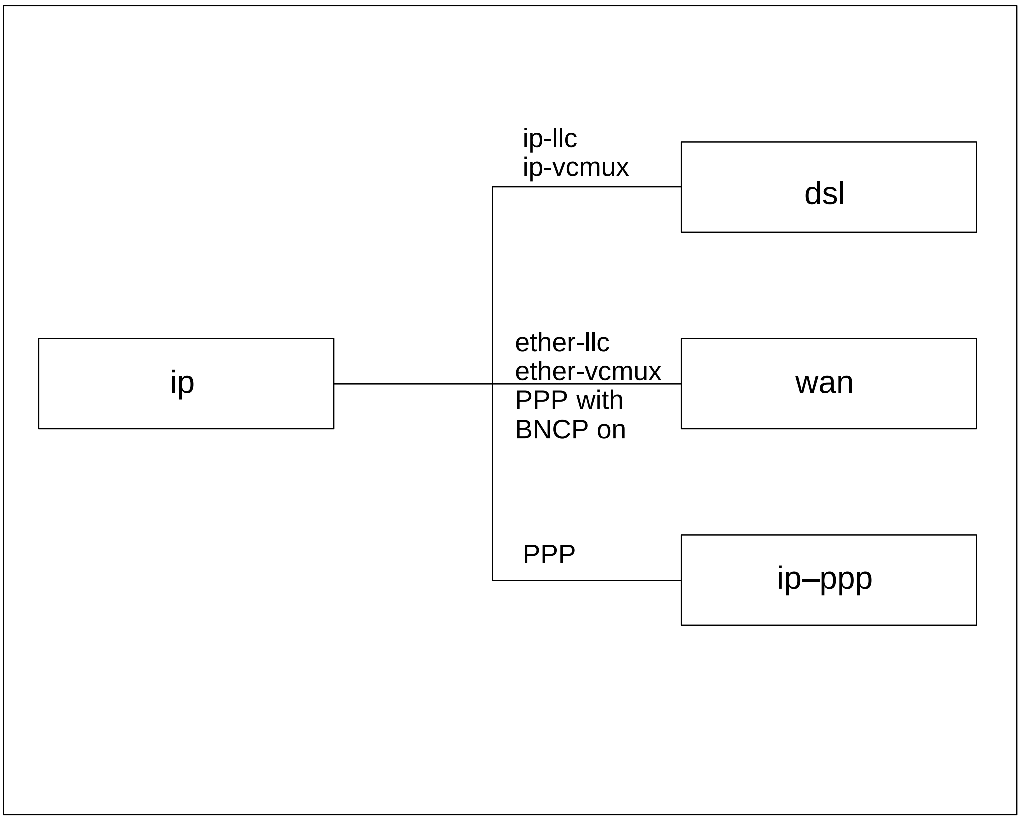


Figure 5-16 IP setting nodes

Command	Enable/disable TCP/IP services
Description	Enables/disables TCP/IP services in M11. You must enable TCP/IP services before you can enter other TCP/IP settings for the M11. If you turn off TCP/IP services and save the new configuration, M11 clears its TCP/IP settings.
Syntax	set ip option [on|off]
Arguments	The argument enables/disables TCP/IP
Example	`M11> set ip option on`

Command	Enable/disable Ethernet port
Description	Enables/disables communications through the Ethernet port in M11. You must enable TCP/IP functions for an Ethernet port before you can configure its network settings.
Syntax	set ip ethernet option [on|off]
Arguments	The argument enables/disables Ethernet port.
Example	`M11> set ip ethernet option on`

Command	Set Ethernet port IP address
Description	Assigns an IP address to the Ethernet port. The IP address you assign to an Ethernet port must be unique on your network.
Syntax	set ip ethernet address [ip_address]
Arguments	The `ip_address` argument is the IP address, in dotted decimal notation
Example	`M11> set ip ethernet address 191.212.11.11`

Command	Set broadcast address
Description	Specifies the broadcast address for the TCP/IP network connected to the Ethernet port. IP hosts use the broadcast address to send messages to every host on your network simultaneously.
Syntax	set ip ethernet broadcast [broadcast_address]
Arguments	The broadcast address for most networks is the network number followed by 255. For example, the broadcast address for the 192.31.222.0 network would be 192.31.222.255.
Example	`M11> set ip ethernet broadcast 191.212.11.255`

Command	Set netmask
Description	Specifies the subnet mask for the TCP/IP network connected to the Ethernet port. The subnet mask specifies which bits of the 32-bit binary IP address represent network information.
Syntax	set ip ethernet netmask [netmask]
Arguments	The default subnet mask for most networks is 255.255.255.0 (Class C subnet mask).
Example	`M11> set ip ethernet netmask 255.255.255.0`

Command	Enable/disable RIP send function
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to advertise its routing tables to other routers on your network. RIP cannot be activated if address mapping is ON.
Syntax	set ip ethernet rip_send [off | v1 | v2 | v1-compat]
Arguments	Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the sending of RIPv2 packets using IP broadcast.
Example	`M11> set ip ethernet rip_send off`

Command	Enable/disable RIP receive function
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to update its routing tables with information received from other routers on your network. RIP cannot be activated if address mapping is ON.
Syntax	set ip ethernet rip_receive [off | v1 | v2 | v1-compat]
Arguments	Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the receiving of both RIPv1 and RIPv2 packets.
Example	`M11> set ip ethernet rip_receive off`

Command	Enable/disable the management through Ethernet port
Description	Enables/disables the management of M11 through the Ethernet port. Note that if you disable management through the Ethernet port and restart your M11, you can no longer manage M11 from your local network with telnet or Web browser.
Syntax	set ip ethernet restrictions [none|admin-disabled]
Arguments	The `restrictions` argument is used to enable/disable management through the Ethernet port. `None` means that M11 can be managed through the Ethernet port and `admin-disabled` disables the possibility to manage M11 through the Ethernet port.
Example	`m11> set ip ethernet restrictions admin-disabled`

Command	Enable/disable default gateway
Description	Specifies whether M11 should send packets to a default gateway if it does not know how to reach the destination host.
Syntax	set ip gateway option [on|off]
Arguments	The argument enables/disables the default gateway option.
Example	`M11> set ip gateway option on`

Command	**Select gateway interface**
Description	Specifies how M11 should route information to the default gateway.
Syntax	set ip gateway interface [ip_address | ppp_vccx]
Arguments	If you select `ip_address`, you must enter the IP address of a host acting as a default gateway on a local or remote network. If you specify a PPP on ATM channel, M11 uses the default gateway being used by the remote PPP peer behind that ATM channel. Acceptable values for "x" are the ATM channels using ppp–vcmux encapsulation.
Example	`M11> set ip gateway interface ip-address`

Command	**Set default gateway IP address**
Description	Specifies the IP address of the default IP gateway. Only applies when the default gateway interface is `ip-address`.
Syntax	set ip gateway default [ip_address]
Arguments	`ip_address` argument is the IP address of the default gateway.
Example	`M11> set ip gateway default 191.233.22.1`

Command	**Enable IP packet forwarding and route distribution between ATM VCC interfaces**
Description	Enable/disable IP packet forwarding and route distribution between ATM VCC interfaces. If only one VCC is used, this option can be ignored.
Syntax	set ip interwan-routing [on|off]
Arguments	The argument enables/disables interwan routing.
Example	`M11> set ip interwan-routing on`

Use the following commands to configure settings for routing IP over PPP link.

Command	Enable/disable routing IP over PPP link
Description	Enables/disables IP routing through the specified logical ATM channel using ppp-vcmux encapsulation.
Syntax	set ip ip-ppp {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux, encapsulation you can leave the argument `vccx` out. The on/off argument enables/disables routing.
Example	`M11> set ip ip-ppp vcc1 option off`

Note

You must enable IP routing before you can enter other IP routing settings for the serial port. If you turn off IP routing and save the new configuration, the Nokia M11 clears IP routing settings.

Command	Set IP address to ATM channel using PPP-vcmux encapsulation
Description	Assigns an IP address to the specified logical ATM channel using ppp-vcmux encapsulation.
Syntax	set ip ip-ppp {vccx} address [ip_address]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. If you specify an IP address other than 0.0.0.0, your Nokia M11 will not negotiate its IP address with the remote peer. If the remote peer does not accept the IP address specified in the `ip_address` argument as valid, the link will not come up. The default value for the `ip_address` argument is 0.0.0.0, which indicates that the WAN port will use the IP address assigned to it by the remote peer. Note that the remote peer must be configured to supply an IP address to your Nokia M11 if you enter 0.0.0.0 for the `ip_address` argument.
Example	`M11> set ip ip-ppp vcc2 address 0.0.0.0`

Command	Set peer IP address
Description	Specifies the IP address of the peer on the other end of the logical ATM link using ppp-vcmux encapsulation.
Syntax	set ip ip-ppp {vccx} peer-address [ip_address]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. If you specify an IP address other than 0.0.0.0, your Nokia M11 will not negotiate the remote peer’s IP address. If the remote peer does not accept the address in the `ip_address` argument as its IP address (typically because it has been configured with another IP address), the link will not come up. The default value for the `ip_address` argument is 0.0.0.0, which indicates that the WAN port will accept the IP address returned by the remote peer. If you enter 0.0.0.0, the peer system must be configured to supply this address.
Example	`M11> set ip ip-ppp vcc2 peer-address 0.0.0.0`

Command	Enable/disable address mapping on ATM link using PPP-vcmux encapsulation
Description	Specifies whether you want M11 to use NAPT on the specified ATM link using ppp-vcmux encapsulation when communicating with remote routers. Address mapping lets you conceal details of your network from remote routers, which is useful when connecting to an Internet Service Provider. By default, the address mapping is turned on.
Syntax	set ip ip-ppp {vccx} addr-mapping [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables address mapping on that channel.
Example	`M11> set ip ip-ppp vcc2 addr-mapping on`

Command	Enable/disable RIP send function on PPP link
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to advertise its routing tables to router on the other side of the specified ATM link using ppp-vcmux encapsulation. RIP cannot be activated if address mapping is ON.
Syntax	set ip ip-ppp {vccx} rip-send [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the sending of RIPv2 packets using IP broadcast.
Example	`M11> set ip ip-ppp vcc2 rip-send off`

Command	Enable/disable RIP receive function on PPP link
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to update its routing tables with information received from other routers on the other side of the specified ATM link using ppp-vcmux encapsulation. RIP cannot be activated if address mapping is ON.
Syntax	set ip ip-ppp {vccx} rip-receive [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the receiving of both RIPv1 and RIPv2 packets.
Example	`M11> set ip ip-ppp vccx rip-receive off`

Command	Enable/disable the management through PPP link
Description	Enables/disables the management of M11 through the specified ATM link using ppp-vcmux encapsulation.
Syntax	set ip ip-ppp {vccx} restrictions [none|admin-disabled|admin-only]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is used to configure restrictions. `None` means that there are no management restrictions, `admin-disabled` disables the possibility to manage M11 through this link, `admin-only` makes this link the dedicated management channel which can only be used for management purposes.
Example	`m11> set ip ip-ppp vcc1 restrictions admin-disabled`

Command	Enable/disable IP routing on channels using IP over ATM or bridged encapsulations
Description	Enables/disables IP routing on the specified ATM channel using the IP over ATM encapsulations (ip-llc, ip-vcmux) or bridged encapsulations (ether-llc, ether-vcmux).
Syntax	set ip dsl {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel and the second argument enables/disables IP routing. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out.
Example	`M11> set ip dsl vcc2 option off`

Command	Set IP address to channels using IP over ATM or bridged encapsulations
Description	Assigns an IP address to the specified logical ATM channel using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} address [ip_address]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument is the IP address of that channel. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. If you enter 0.0.0.0 as the IP address, M11 will retrieve the IP address through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip dsl vcc2 address 0.0.0.0`

Command	Set broadcast address to channels using IP over ATM or bridged encapsulations
Description	Assigns a broadcast IP address to the specified logical ATM channel using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} broadcast [broadcast_address]
Arguments	The first argument identifies the ATM channel. The second argument is the broadcast address to be assigned to that channel. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. If you enter 0.0.0.0 as the IP broadcast address, M11 will retrieve the IP address through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip dsl vcc2 broadcast 0.0.0.0`

Command	**Set network mask to channels using IP over ATM or bridged encapsulations**
Description	Assigns an IP network mask to the specified logical ATM channel using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} netmask [netmask]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument is the network mask for that channel. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. If you enter 0.0.0.0 as the network mask, M11 will retrieve the IP address through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip dsl vcc2 netmask 0.0.0.0`

Command	**Enable/disable address mapping on channels using IP over ATM or bridged encapsulations**
Description	Specifies whether you want M11 to use NAPT on the specified ATM link (vccx, x = 1 ... 8) using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation when communicating with remote routers. Address mapping lets you conceal details of your network from remote routers. This is useful when connecting to an Internet Service Provider.
Syntax	set ip dsl {vccx} addr-mapping [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables address mapping on that channel. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out.
Example	`M11> set ip dsl vcc2 addr-mapping off`

Command	**Enable address resolution proxy server function on channels using IP over ATM or bridged encapsulations**
Description	Specifies whether you want M11 to act as a address resolution proxy server on your LAN for the IP addresses behind the specified ATM link using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} proxy-arp [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8) . The second argument enables/disables the proxy ARP function. If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out.
Example	`M11> set ip dsl vcc2 proxy-arp off`

Command	**Enable/disable RIP send function on channels using IP over ATM or bridged encapsulations**
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to advertise its routing tables to router on the other side of the specified ATM link using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} rip-send [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the sending of RIPv2 packets using IP broadcast. RIP cannot be activated if address mapping is ON.
Example	`M11> set ip dsl {vccx} rip-send off`

Command	**Enable/disable RIP receive function on channels using IP over ATM or bridged encapsulations**
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to update its routing tables with information received from other routers on the other side of the specified ATM link using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation.
Syntax	set ip dsl {vccx} rip-receive [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the receiving of both RIPv1 and RIPv2 packets. RIP cannot be activated if address mapping is ON.
Example	`M11> set ip dsl vcc2 rip-receive off`

Command	**Flush routes**
Description	Enabled `flush routes` function deletes the learned routes from the routing table when the PPP connection is disconnected. Address mapping must be off.
Syntax	flush-routes [on|off]
Arguments	The argument enables/disables the flush routes function.
Example	`M11> flush-routes on`

Command	Enable/disable the management through channels using IP over ATM or bridged encapsulations
Description	Enables/disables the management of Nokia M11 through the specified ATM link using ip-llc, ip-vcmux, ether-llc, or ether-vcmux encapsulation. This command can be also used to configure a dedicated management channel.
Syntax	set ip dsl {vccx} restrictions [none|admin-disabled|admin-only]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using one of these encapsulations, you can leave the argument `vccx` out. The second argument is used to configure restrictions. `None` means that there are no restrictions, `admin-disabled` disables the possibility to manage M11 through this port, `admin-only` makes this channel the dedicated management channel which can only be used for management purposes.
Example	`m11> set ip dsl vcc2 restrictions admin-only`

Command	Enable/disable IP routing on ATM channel
Description	Enables/disables IP routing on the specified ATM channel using PPP over ATM encapsulation in bridged mode (BNCP option on).
Syntax	set ip wan {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument enables/disables the function.
Example	`M11> set ip wan vcc2 option off`

Command	**Set IP address to channels using PPP over ATM encapsulation in bridged mode**
Description	Assigns an IP address to the specified logical ATM channel using PPP over ATM encapsulation in bridged mode (BNCP option on).
Syntax	set ip wan {vccx} address [ip_address]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is the IP address for that channel. If you enter 0.0.0.0 as the network mask M11 will retrieve the IP address through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip wan vcc2 address 0.0.0.0`

Command	**Set broadcast address to channels using PPP over ATM encapsulation in bridged mode**
Description	Assigns a broadcast IP address to the specified logical ATM channel using PPP over ATM encapsulation in bridged mode (BNCP option on).
Syntax	set ip wan {vccx} broadcast [broadcast_address]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is the broadcast address for that channel. If you enter 0.0.0.0 as the broadcast address, M11 will retrieve the IP address through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip wan vcc2 broadcast 0.0.0.0`

Command	Set netmask to channels using PPP over ATM encapsulation in bridged mode
Description	Assigns an IP network mask to the specified logical ATM channel using ppp over ATM encapsulation in bridged mode.
Syntax	set ip wan {vccx} netmask [netmask]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is the netmask address for that channel. If you enter 0.0.0.0 as the netmask, M11 will retrieve the netmask through the remote peer using Dynamic Host Configuration Protocol.
Example	`M11> set ip wan vcc2 netmask 0.0.0.0`

Command	Enable/disable address mapping on channels using PPP over ATM encapsulation in bridged mode
Description	Specifies whether you want M11 to use NAPT on the specified ATM link using PPP over ATM encapsulation in bridged mode (BNCP option on) when communicating with remote routers. Address mapping lets you hide details of your network from remote routers. This is useful when connecting to an Internet Service Provider.
Syntax	set ip wan {vccx} addr-mapping [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is enables/disables address mapping.
Example	`M11> set ip wan vcc2 addr-mapping off`

Command	Enable proxy ARP function on channels using PPP over ATM encapsulation in bridged mode
Description	Specifies whether you want M11 to act as a address resolution proxy server on your LAN for the IP addresses behind the specified ATM link using PPP over ATM encapsulation in bridged mode.
Syntax	set ip wan {vccx} proxy-arp [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out. The second argument is enables/disables proxy ARP function.
Example	`M11> set ip wan vcc2 proxy-arp on`

Command	Enable/disable RIP send function on channels using PPP over ATM encapsulation in bridged mode
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to advertise its routing tables to router on the other side of the specified ATM link using PPP over ATM encapsulation in bridged mode (BNCP option on).
Syntax	set ip wan {vccx} rip-send [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using PPP over ATM encapsulation in bridged mode, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the sending of RIPv2 packets using IP broadcast. RIP cannot be activated if address mapping is ON.
Example	`M11> set ip wan vcc2 rip-send off`

Command	**Enable/disable RIP receive function on channels using PPP over ATM encapsulation in bridged mode**
Description	Specifies whether M11 should use Routing information protocol (RIP) broadcasts to update its routing tables with information received from other routers on the other side of the specified ATM link using PPP over ATM encapsulation in bridged mode.
Syntax	set ip wan {vccx} rip-receive [off | v1 | v2 | v1-compat]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using PPP over ATM encapsulation in bridged mode, you can leave the argument `vccx` out. Both RIP version 1 and RIP version 2 functionalities can be simultaneously activated. `v1-compat` argument enables the receiving of both RIPv1 and RIPv2 packets. RIP cannot be activated if address mapping is ON.
Example	`M11> set ip wan vcc2 rip-receive off`

Command	**Enable/disable the management through channels using PPP over ATM encapsulation**
Description	Enables/disables the management of M11 through the specified ATM link using PPP over ATM encapsulation.
Syntax	set ip wan {vccx} admin-disable [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). If there is only one ATM channel using PPP over ATM encapsulation in bridged mode, you can leave the argument `vccx` out. The second argument disables/enables management through ATM channel using PPP-vcmux encapsulation.
Example	`M11> set ip wan vcc2 admin-disable on`

Static route settings

A static route identifies a manually configured pathway to a remote network. Unlike dynamic routes, which are acquired and confirmed periodically from other routers, static routes do not time out. Consequently, static routes are useful when working with PPP, since an intermittent PPP link may make maintenance of dynamic routes problematic.

You can configure as many as 16 static IP routes for a Nokia M11. Use the following commands to maintain static routes to the Nokia M11 routing table:

Command	**Add a static route**
Description	Adds a static route to the routing table.
Syntax	set ip static-routes destination-network [net_address] netmask [netmask] interface [ip-address|ppp-vccx] gateway-address [gate_address] metric [integer]
Arguments	Type a destination network address in the `net_address` argument in dotted decimal notation. The `net_address` argument cannot be 0.0.0.0. `netmask` is the subnet mask of the destination network. The subnet mask associated with the destination network must represent the same network class (A, B, or C) or a lower class (such as a class C subnet mask for a class B network number) to be valid. `ip-address|ppp-vccx` argument indicates whether the static route can be reached directly through the gateway IP address or through any active PPP channel (`ppp-vccx`, where x = 1 ... 8). `gate_address` identifies the default gateway IP address. The gateway address is not needed if `ppp-vccx` is selected as the gateway interface. The default metric is 1. Type a number from 1 to 16 for the `integer` argument to indicate the number of routers (actual or best guess) a packet must traverse to reach the remote network. You can type a metric of 1 to indicate either: The remote network is one router away and the static route is the best way to reach it; The remote network is more than one router away but the static route should not be replaced by a dynamic route, even if the dynamic route is more efficient. Metric 16 indicates that the route is disabled.
Example	`M11> set ip static-routes destination-network 192.111.122.0 netmask 255.255.255.0 ip-address gateway-address 192.111.1.1 metric 3`

Command	Set destination network address of a static route
Description	Specifies the network address for the static route.
Syntax	set ip static-routes destination-network [net_address]
Arguments	Type a network address in the `net_address` argument in dotted decimal notation. The `net_address` argument cannot be 0.0.0.0.
Example	`M11> set ip static-routes destination-network 192.111.122.0`

Command	Modify netmask of a static route
Description	Specifies the subnet mask for the IP network at the other end of the static route.
Syntax	set ip static-routes destination-network [net_address] netmask [netmask]
Arguments	`net_address` is the destination network address of the static route. Type the `net_address` and `netmask` arguments in dotted decimal notation. The subnet mask associated with the destination network must represent the same network class (A, B, or C) or a lower class (such as a class C subnet mask for a class B network number) to be valid.
Example	`M11> set ip static-routes destination-network 192.111.122.0 netmask 255.255.255.0`

Command	Modify the interface to static route
Description	Specifies if the static route entry is accessible via a certain PPP link or via a non-PPP link (IP-address).
Syntax	set ip static-routes destination-network [net_address] interface [ip-address|ppp-vccx]
Arguments	The first argument identifies the static route and the second argument whether the route is accessible via a PPP link or a non-PPP link. `ppp-vccx`, where x= 1 ... 8, identifies the ATM channel using PPP.
Example	`M11> set ip static-routes destination-network 192.111.122.0 interface ppp-vcc1`

Command	**Modify default gateway for static route**
Description	Specifies the IP address of the gateway for the static route.
Syntax	set ip static-routes destination-network [net_address] gateway-address [gate_address]
Arguments	The `net_address` argument identifies the static route and `gate_address` sets the IP address of the default gateway.
Example	`M11> set ip static-routes destination-network 192.111.122.0 gateway-address 192.111.1.1`

Command	**Modify metric for the static route**
Description	Specifies the metric for the static route.
Syntax	set ip static-routes destination-network [net_address] metric [integer]
Arguments	The `net_address` argument identifies the static route. The default metric is 1. Enter a number from 1 to 16 for the `integer` argument to indicate the number of routers (actual or best guess) a packet must traverse to reach the remote network. You can enter a metric of 1 to indicate either: The remote network is one router away and the static route is the best way to reach it; The remote network is more than one router away but the static route should not be replaced by a dynamic route, even if the dynamic route is more efficient. Metric 16 indicates that the route is disabled.
Example	`M11> set ip static-routes destination-network 192.111.122.0 metric 3`

Command	**Delete static route (Note: Deleting a static route removes all information associated with that route.)**
Description	Deletes a static route.
Syntax	delete ip static-routes destination-network [net_address]
Arguments	`net_address` is the destination network address of the static route.
Example	`M11> delete ip static-routes destination-network 192.111.122.0`

Command	**Set static ARP table entry**
Description	Sets a static IP address – MAC address mapping to the ARP table. This command can be used if you have devices on the Ethernet which do not understand ARP requests. You must have admin rights to configure static ARP table entries.
Syntax	set ip static-arp ip-address [ip-address] hardware-address [hardware-address]
Arguments	The `ip-address` argument defines the IP address assigned to the device. The `hardware-address` argument is the hardware MAC address of the device.
Example	`m11> set ip static-arp ip-address 192.168.1.2 hardware-address 00.40.43.02.20.1f`

BNCP setting

Command	**Enable/disable BNCP**
Description	Specifies whether the Bridge Network Control Protocol (BNCP) option can be used on ATM channels using ppp-vcmux encapsulation. See `set ip wan` commands above.
Syntax	set bncp option [on|off]
Arguments	The argument enables/disables BNCP option.
Example	`M11> set bncp option on`

DHCP settings

As a Dynamic Host Control Protocol (DHCP) server, your Nokia M11 can assign IP addresses and provide configuration information to other devices on your network dynamically. A device that acquires its IP address and other TCP/IP configuration settings from M11 can use the information for 30 minutes (this is known as the DHCP lease).

Note
If you use M11 as a DHCP server, make sure that the devices on your network are not configured to use IP addresses in Nokia M11's DHCP address range. Network conflicts can result when a device on your network uses an IP address that M11 has already assigned to another device.

Command	**Set DHCP service**
Description	Sets DHCP services in M11. You must enable DHCP services before you can enter other DHCP settings for M11. If you turn off DHCP services and save the new configuration, M11 clears its DHCP settings. M11 can also relay DHCP requests to another server
Syntax	set dhcp option [off | server | relay-agent] start-address [ip_address] end-address [ip_address] lease-time [time]
Arguments	The first argument disables DHCP (`off`), enables M11 DHCP server (`server`) or makes M11 act as a relay agent (`relay-agent`). `start-address` and `end-address` arguments define the DHCP address range. `lease-time` argument defines how often the PC has to renew its DHCP lease.
Example	`M11> set dhcp option server start-address 192.168.1.1 end-address 192.168.1.254 lease-time 00:01:00:00`

Command	Enable/disable DHCP services
Description	Enables/disables DHCP services in M11. You must enable DHCP services before you can enter other DHCP settings for M11. If you turn off DHCP services and save the new configuration, M11 clears its DHCP settings. M11 can also relay DHCP requests to another server
Syntax	set dhcp option [off | server | relay-agent]
Arguments	The argument disables DHCP (`off`), enables M11 DHCP server (`server`) or makes M11 act as a relay agent (`relay-agent`)
Example	`M11> set dhcp option server`

Command	Specify start of DHCP address range
Description	Specifies the first address in the DHCP address range.
Syntax	set dhcp start-address [ip_address]
Arguments	`ip_address` argument is the first IP address in the DHCP address range.
Example	`M11> set dhcp start-address 192.168.1.1`

Command	Specify end of DHCP address range
Description	Specifies the last address in the DHCP address range.
Syntax	set dhcp end-address [ip_address]
Arguments	`ip_address` argument is the last IP address in the DHCP address range.
Example	`M11> set dhcp end-address 192.168.1.254`

Command	Set DHCP lease time
Description	Sets the time how often the PC has to renew the DHCP lease.
Syntax	set dhcp lease-time [time]
Arguments	`time` argument sets the lease time.
Example	`M11> set dhcp lease-time 00:01:00:00`

Command	**Set M11 as DHCP relay agent**
Description	Configures M11 as a DHCP relay agent which relays the DHCP requests to an external DHCP server
Syntax	set dhcp option relay-agent server-address [ip_address]
Arguments	`server-address` argument specifies the IP address of the external DHCP server.
Example	`M11> set dhcp option relay-agent server-address 192.3.2.1`

Domain Name System settings

Domain Name System (DNS) is an information service for TCP/IP networks that uses a hierarchical naming system to identify network domains and the hosts associated with them. You can identify one primary DNS server and one secondary server.

Command	**Set domain name**
Description	Specifies the default domain name for your network. When an application needs to resolve a host name, it appends the default domain name to the host name and asks the DNS server if it has an address for the “fully qualified host name”.
Syntax	set dns domain-name [domain_name]
Arguments	`domain_name` is the default domain name for your system.
Example	`M11> set dns domain-name nokia.com`

Command	**Set IP address of primary name server**
Description	Specifies the IP address of the primary DNS name server.
Syntax	set dns primary-address [ip_address]
Arguments	`ip_address` is the IP address of your primary name server.
Example	`M11> set dns primary-address 10.98.16.250`

Command	Set IP address of secondary name server
Description	Specifies the IP address of the secondary DNS name server.
Syntax	set dns secondary-address [ip_address]
Arguments	`ip_address` is the IP address of your secondary name server. Enter 0.0.0.0 if your network does not have a secondary DNS name server.
Example	`M11> set dns secondary-address 0.0.0.0`

Bridging settings

Bridging lets Nokia M11 learn host addresses to minimise traffic. When bridging is enabled M11 maintains a table of up to 256 MAC addresses. Entries that are not used within 10 minutes are dropped. If the bridging table fills up, the oldest table entries are dropped to make room for new entries.

Command	Enable/disable bridging
Description	Enables/disables bridging services in M11. You must enable bridging services within M11 before you can enable it for a specific interface.
Syntax	set bridge option [on|off]
Arguments	The argument enables/disables bridging.
Example	`M11> set bridge option on`

Command	Enable bridging for Ethernet interface
Description	Enables/disables bridging services for the M11 Ethernet interfaces.
Syntax	set bridge ethernet option [on|off]
Arguments	The argument enables/disables bridging for Ethernet interfaces.
Example	`M11> set bridge ethernet option on`

Command	**Enable bridging on channels using PPP over ATM encapsulation**
Description	Enables/disables bridging services for the Nokia M11 ATM channel using ppp-vcmux encapsulation.
Syntax	set bridge wan {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8) and the second argument enables/disables bridging on that channel. If there is only one ATM channel using ppp-vcmux encapsulation, you can leave the argument `vccx` out.
Example	`M11> set bridge wan vcc2 option off`

Command	**Enable bridging on channels using bridged encapsulations**
Description	Enables/disables bridging services for a Nokia M11 ATM channel using ether-llc or ether-vcmux encapsulation.
Syntax	set bridge dsl {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8) and the second argument enables/disables bridging on that channel. If there is only one ATM channel using either one of these encapsulations, you can leave the argument `vccx` out.
Example	`M11> set bridge dsl vcc2 option off`

Command	**Enable/disable bridging between ATM VCC channels**
Description	Enables/disables bridging between ATM VCC channels. If only one VCC is used, this option can be ignored.
Syntax	set bridge interwan-bridging [on|off]
Arguments	The argument enables/disables bridging between VCCs
Example	`M11> set bridge interwan-bridging off`

PPP settings

PPP settings allow you to fine tune the operation of the point-to-point protocol. PPP settings also provide the means to set the authentication parameters, passwords and usernames. These settings must be set separately for each ATM channel using ppp-vcmux encapsulation.

You can use the authentication commands to specify how your M11 will authenticate itself to a remote peer. The settings for port authentication in the local Nokia M11 must match the authentication that is expected by the remote peer. For example, if the remote peer requires CHAP authentication and has a name and CHAP secret for M11, you must enable CHAP and specify the same name and secret in the local M11 before a link can be established.

You can also specify that your Nokia M11 will use CHAP, PAP or both to authenticate a remote peer when a PPP link is being established.

Command	**Enable/disable PPP processing**
Description	Enables/disables PPP processing on the specified ATM channel using ppp-vcmux encapsulation.
Syntax	set ppp module {vccx} option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8) and the second argument enables/disables PPP processing.
Example	`M11> set ppp module vcc2 off`

Command	**Set maximum receive unit**
Description	Sets the Maximum Receive Unit for the specified ATM channel.
Syntax	set ppp module {vccx} mru [integer]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `integer` argument can be any number between 128 and 2048. Normally, MRU size 1500 is required for IP traffic. Bridged encapsulation (BNCP) requires the MRU size 1520 in order to allow the maximum size Ethernet packet transmission.
Example	`M11> set ppp module vcc2 mru 1500`

Command	Enable/disable LCP echoing
Description	Specifies whether you want your M11 to send LCP echo requests on the specified ATM channel.
Syntax	set ppp module {vccx} lcp-echo-requests [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables LCP echoing. You must turn off LCP echoing if you do not want M11 to drop a PPP link to a nonresponsive peer.
Example	`M11> set ppp module vcc2 lcp-echo-requests off`

Command	Set Configure-NAK failure maximum
Description	Specifies the maximum number of Configure-NAK messages the PPP module can send without having sent a Configure-ACK message request on the specified ATM channel.
Syntax	set ppp module {vccx} failures-max [integer]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `integer` argument can be any number between 1 and 20.
Example	`M11> set ppp module vcc2 failures-max 10`

Command	Set unacknowledged configuration request maximum
Description	Specifies the maximum number of unacknowledged configuration requests that your M11 will send to the specified ATM channel.
Syntax	set ppp module {vccx} configure-max [integer]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `integer` argument can be any number between 1 and 10.
Example	`M11> set ppp module vcc2 configure-max 10`

Command	Set unacknowledged termination request maximum
Description	Specifies the maximum number of unacknowledged termination requests that your M11 will send before terminating the PPP link on the specified ATM channel.
Syntax	set ppp module {vccx} terminate-max [integer]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `integer` argument can be any number between 1 and 10.
Example	`M11> set ppp module vcc2 terminate-max 2`

Command	Set PPP timeout
Description	Specifies the number of seconds M11 must wait for communication activity before terminating the PPP link on the specified ATM channel.
Syntax	set ppp module {vccx} timeout [integer]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `integer` argument is the timeout in seconds. If you enter value 0, the connection will never time out.
Example	`M11> set ppp module vcc2 timeout 0`

Command	Enable/disable CHAP port authentication
Description	Enables/disables CHAP authentication for a port on the specified ATM channel. CHAP authentication must be enabled before you can enter other CHAP information. If CHAP is on, it will be the first authentication method offered to a remote peer during link negotiation.
Syntax	set ppp module {vccx} port-authentication chap-option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables CHAP port authentication.
Example	`M11> set ppp module vcc2 port-authentication chap-option on`

Command	**Set CHAP user name**
Description	Defines the name M11 sends in the CHAP response packet on the specified ATM channel.
Syntax	set ppp module {vccx} port-authentication chap-name [chap_name]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `chap_name` argument is consists of 1 - 32 alphanumeric characters. The information you enter must match the CHAP user name configured in the remote PPP peer’s authentication database. Your service provider will give you the CHAP user name.
Example	`M11> set ppp module vcc2 port-authentication chap-name myname`

Command	**Set CHAP password**
Description	Defines the CHAP secret for CHAP authentication on the specified ATM channel.
Syntax	set ppp module {vccx} port-authentication chap-secret [chap_secret]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `chap_secret` argument consists of 1 – 32 alphanumeric characters. The information you enter must match the CHAP secret used by the PPP peer. Your service provider will give you the CHAP password.
Example	`M11> set ppp module vcc2 port-authentication chap-secret mypassword`

Command	Enable/disable PAP port authentication
Description	Enables/disables PAP authentication on the specified ATM channel. PAP authentication must be enabled before you can enter other PAP information. If you disable PAP authentication and save the modified settings, your M11 retains its PAP settings.
Syntax	set ppp module {vccx} port-authentication pap-option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables PAP port authentication.
Example	`M11> set ppp module vcc2 port-authentication pap-option on`

Command	Set PAP user name
Description	Defines the name M11 sends in a PAP response packet on the specified ATM channel.
Syntax	set ppp module {vccx} port-authentication pap-name [pap_name]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `pap_name` argument consists of 1 - 32 alphanumeric characters. The information you enter must match the PAP username configured in the remote PPP peer’s authentication database. Your service provider will give you the PAP user name.
Example	`M11> set ppp module vcc2 port-authentication pap-name myname`

Command	**Set PAP password**
Description	Defines the PAP password for PAP authentication on the specified ATM channel.
Syntax	set ppp module {vccx} port-authentication pap-password [pap_password]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The `pap_password` argument consists of 1 – 32 alphanumeric characters. The information you enter must match the PAP password used by the remote PPP peer. Your service provider will give you the PAP password.
Example	`M11> set ppp module vcc2 port-authentication pap-password mypassword`

Command	**Enable/disable CHAP peer authentication**
Description	Enables/disables CHAP authentication for a connection to a PPP peer on the specified ATM link.
Syntax	set ppp module {vccx} peer-authentication chap-option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables CHAP peer authentication.
Example	`M11> set ppp module vcc2 peer-authentication chap-option on`

Command	**Enable/disable PAP peer authentication**
Description	Enables/disables PAP authentication for a connection to a PPP peer on the specified ATM link.
Syntax	set ppp module {vccx} peer-authentication pap-option [on|off]
Arguments	The first argument identifies the ATM channel (vccx, x = 1 ... 8). The second argument enables/disables PAP peer authentication.
Example	`M11> set ppp module vcc2 peer-authentication pap-option on`

Command	Set host name for an authorised PPP peer
Description	Specifies the host name for an authorised PPP peer.
Syntax	set ppp peer-database peer-name [host_name]
Arguments	The `host_name` argument consists of 1 – 32 alphanumeric characters. The information you enter must match the username that will be received from the remote PPP peer when being authenticated.
Example	`M11> set ppp peer-database peer-name host`

Command	Set CHAP secret associated with PPP peer
Description	Specifies the secret associated with a PPP peer.
Syntax	set ppp peer-database peer-name [host_name] chap-secret [secret]
Arguments	The `secret` argument consists of 1 – 32 alphanumeric characters. The information you enter must match the secret that will be received from the remote PPP peer when being authenticated.
Example	`M11> set ppp peer-database peer-name host chap-secret mypassword`

Command	Set PAP password associated with PPP peer
Description	Specifies the password associated with a PPP peer.
Syntax	set ppp peer-database peer-name [host_name] pap-password [password]
Arguments	The `password` argument consists of 1 – 32 alphanumeric characters. The information you enter must match the password that will be received from the remote PPP peer when being authenticated.
Example	`M11> set ppp peer-database peer-name host pap-password mypassword`

SNMP settings

Simple Network Management Protocol (SNMP) lets a network administrator monitor problems on a network by retrieving settings on remote network devices. The network administrator typically runs an SNMP management station program on a local host to obtain information from SNMP agent such as M11.

Command	**Add community**
Description	Adds the specified name to the list of communities associated with M11. You can associate two communities with M11.
Syntax	set snmp community [name]
Arguments	By default, M11 is associated with the public community.
Example	`M11> set snmp community public`

Command	**Enable/disable SNMP trapping**
Description	Enables or disables SNMP trapping. If SNMP trapping is enabled, your Nokia M11 sends authentication traps to all SNMP trap destinations. You must enable trap authentication before you set up your trap destinations.
Syntax	set snmp traps authentication-traps [on|off]
Arguments	The argument enables/disables trapping.
Example	`M11> set snmp traps authentication-traps on`

Command	**Set SNMP trap destination**
Description	Identifies the destination of SNMP trap messages.
Syntax	set snmp traps ip-traps [ip_address] {community [community_name]}
Arguments	The `ip-address` argument is the IP address of the host acting as an SNMP console. The optional `community community_name` identifies the name of Nokia M11's community, which is included in the trap message the device sends to the management console. This name, which is not used for authentication, does not have to match a predefined community name.
Example	`M11> set snmp traps ip-traps 192.111.122.1 community public`

Command	**Set system contact**
Description	Identifies the system contact, such as the name, phone number, beeper number, or email address of the person responsible for M11.
Syntax	set snmp sysgroup contact [contact_info]
Arguments	You can enter up to 256 characters for the `contact-info` argument. You must put the `contact-info` argument in double-quotes if it contains embedded spaces.
Example	`M11> set snmp sysgroup contact 51166777`

Pinhole settings

Pinhole settings are used to configure static entries to NAPT table. The pinhole function allows access to servers, such as Web-HTTP servers, from outside your local LAN in cases where NAPT/address mapping is enabled. The settings affect the whole system.

Note
If you have a Web server on LAN, make sure that it has a different port number than M11’s integral Web server. You can change the M11’s Web server port through the integral server settings.

Command	**Configure pinhole**
Description	Configures pinhole.
Syntax	set pinhole name [name] protocol-select [tcp | udp | icmp | pptp] external-port-start [port_number] external-port-end [port_number] internal-ip [ip_address] internal-port [port_number]
Arguments	The `name` argument defines the unique pinhole entry name. The `protocol-select` argument specifies the protocol. The `external-port-start` specifies the start of the external port range. The `external-port-end` specifies the end of the external port range. Together the external port arguments define the available range of allowed external ports. The `internal-ip` argument specifies the IP address of the server located in LAN and the `internal-port` argument its port. Valid values for `port_number` are 0 – 65535.
Example	`m11> set pinhole name web-server protocol-select tcp external-port-start 80 external-port-end 80 internal-ip 192.168.1.180 internal-port 80`

Command	Set protocol
Description	Configures the protocol.
Syntax	set pinhole name [name] protocol-select [protocol]
Arguments	The `name` argument defines the unique pinhole entry name. The `protocol-select` argument defines the protocol. Protocols are TCP, UDP, ICMP, PPTP.
Example	`M11> set pinhole name web-server protocol-select tcp`

Command	Set external protocol port number range for WAN
Description	Sets the the external protocol port number range.
Syntax	set pinhole name [name] external-port-start [port_number] external-port-end [port_number]
Arguments	The `name` argument defines the unique pinhole entry name. The `port_number` argument defines the start and end of the external port range. Valid values are 0 – 65535.
Example	`M11> set pinhole name web-server external-port-start 80 external-port-end 80`

Command	Set server IP address in LAN
Description	Configures the server IP address where the protocol defined by the external port number is mapped in LAN port.
Syntax	set pinhole name [name] internal-ip [ip_address]
Arguments	The `name` argument defines the unique pinhole entry name. The `ip_address` argument is the IP address of the server on your LAN.
Example	`M11> set pinhole name web-server internal-ip 192.168.1.80`

Command	**Set server port on LAN**
Description	Configures the server port where the protocol defined by the external port number is mapped on LAN.
Syntax	set pinhole name [name] internal-port [port_number]
Arguments	The `name` argument defines the unique pinhole entry name. The `internal-port` argument specifies the internal port. Valid values for `port_number` are 0 – 65535.
Example	`M11> set pinhole name web-server internal-port 80`

Integrated server settings

These commands are used to configure the port number settings of the integrated HTTP and telnet servers in M11. This is needed when Pinhole functionality is used. The default port numbers of the integrated HTTP and telnet servers must be changed if there is, for example a Web server in the LAN and it must be accessed from the WAN. In this case, the port number of the integrated Web server in M11 must be changed into something other than the default port number 80.

Command	**Set integrated Web server port number**
Description	Changes the port number of the integrated Web server in M11.
Syntax	set servers web-http [0 – 32767]
Arguments	The argument defines the new port number for the integrated Web server.
Example	`M11> set servers web-http 81`

Command	**Set integrated telnet server port number**
Description	Changes the port number of the integrated telnet server in M11.
Syntax	set servers telnet-tcp [0 – 32767]
Arguments	The argument defines the new port number for the integrated telnet server.
Example	`M11> set servers telnet-tcp 90`

5.3 SNMP

The SNMP functionality in Nokia M11 is used only for setting and accessing the system contact information for the unit. Community strings for changing and accessing this information can be set. M11 can be activated to send SNMP traps in case somebody tries to access the unit with a wrong community string.

5.4 Software download

New software can be downloaded to M11 through the 10Base-T Ethernet interface or through one of the active ATM channels. Nokia M11 uses Trivial File Transfer Protocol (TFTP) to download the software from a TFTP server located on the Ethernet LAN. The downloading is activated from the console port using the following CLI command:

```
install [server_address] [filename] {confirm}
```

Command	**Download software update**
Description	Downloads a new version of the Nokia M11 operating software from a TFTP (Trivial File Transfer Protocol) server, validates the software image, and programs the image into the Nokia M11 memory. After you install new operating software, you must restart M11.
Syntax	install [server_address] [filename] {confirm}
Arguments	The TFTP server must be accessible on your Ethernet network or through one of the active ATM virtual channels and a route to the server must exist. The `server address` argument identifies the IP address of the TFTP server on which your Nokia M11 operating software is stored. The `filename` argument identifies the path and name of the operating software file on the TFTP server. If you include the optional `confirm` keyword, you will not be prompted to identify a TFTP server or file name. Your Nokia M11 begins the software installation using its default boot settings.

Example	`M11> install 192.168.1.1 M11c_500.d39`
	`*** WARNING *** YOU ARE ABOUT TO ERASE AND REPROGRAM THE NOKIA M11’S PERMANENT SOFTWARE STORAGE WITH A NEW SOFTWARE VERSION OBTAINED VIA THE TFTP PROTOCOL.`
	`About to install new Flash EPROM software image:`
	`     server: 192.168.1.1`
	`     file: “M11c_500.d39”`
	`Do you wish to proceed? (type ’yes’ to confirm): yes`
	`Installing`
	`M11>`

Chapter 6
How your Nokia M11 works

This chapter introduces the principles according to which Nokia M11 operates.

6.1 ADSL

ADSL stands for asymmetric digital subscriber line. It is a technology that enables the use of your normal telephone wires for very high speed data transmission. With ADSL technology, you can retrieve data from network through the telephone wires at rates up to 8 Mbit/s-plus and send data at rates up to 1 Mbit/s. The data rate depends on the length of the telephone cable from your premises to the central office, as well as noise and disturbances in the cable. The ADSL technology adapts to the line length and other line conditions and adjusts the speed in 32 kbit/s steps.

ADSL is standardized by both ANSI and ETSI. M11 uses the Discrete Multitone Technique (DMT). In DMT, the data is sent over the telephone wires in multiple 4 kHz channels. By tuning the use of these channels and the information content of these channels, Nokia M11 can adapt to different telephone lines.

6.2 ATM over ADSL

Nokia M11 can carry ATM cells on the ADSL line. It is possible to have up to eight (8) simultaneous connections to different networks from a single M11. The operator can also establish one dedicated management channel to M11.

6.3 Routing and bridging

Nokia M11 functions as a brouter, which means that it acts as a network router for TCP/IP traffic and as a network bridge for non-routable traffic.

6.3.1 TCP/IP routing

As a router, Nokia M11 keeps track of the networks that are accessible through each network interface. If you have configured your M11 to use the Routing Information Protocol (RIPv1 or RIPv2), M11 exchanges information with other routers to learn about the best routes to remote networks and to advertise the networks for which M11 has the appropriate route.

When M11 receives a TCP/IP packet, it looks up the network portion of the packet's destination IP address in its routing table and then forwards the packet through the network interface that will let the packet reach its destination most efficiently.

6.3.2 Static and dynamic routes

Static routes identify pathways to destination networks that are stable over time or to networks that must always be available, even if a link is not currently open. These static routes let each router recognise how to reach the other, even if one router has not heard from the other recently.

Dynamic routes identify pathways to destination networks that may change over time. Dynamic routes are created and configured when routers broadcast RIP (Routing information protocol) packets, advertising the networks they can reach and the distance (number of routers) to each network.

6.3.3 Bridging

Nokia M11 can function as an Ethernet bridge. It can bridge all protocols or all non-routable (non-IP) protocols between all of its interfaces. The user just has to specify which interfaces take part in the bridging function. The bridging function automatically learns the MAC addresses located behind each of its active interfaces and uses this information to filter local traffic at an interface to prevent it from being unnecessarily relayed to other interfaces. For that purpose, M11 has a 256-slot MAC address table where it keeps these learned addresses. The table entries are also automatically deleted in case a specific address is not detected behind the interface during 10 minutes.

In bridge-only mode, a single IP address can be allocated to M11 if a remote management of M11 is required. The LAN IP address acts as a host IP address in this case.

6.4 Network Address Port Translation (NAPT)

Network Address Port Translation (NAPT) or Network Address Translation (NAT) is used to save IP addresses. When NAPT is enabled, the router has only one global IP address per each ATM channel. The LAN port uses private IP addresses which are not seen outside the router (typically 10.0.0.0 or 192.168.x.x). In normal operation, NAPT translates the IP addresses and TCP/UDP socket/port numbers between the LAN and WAN interface.

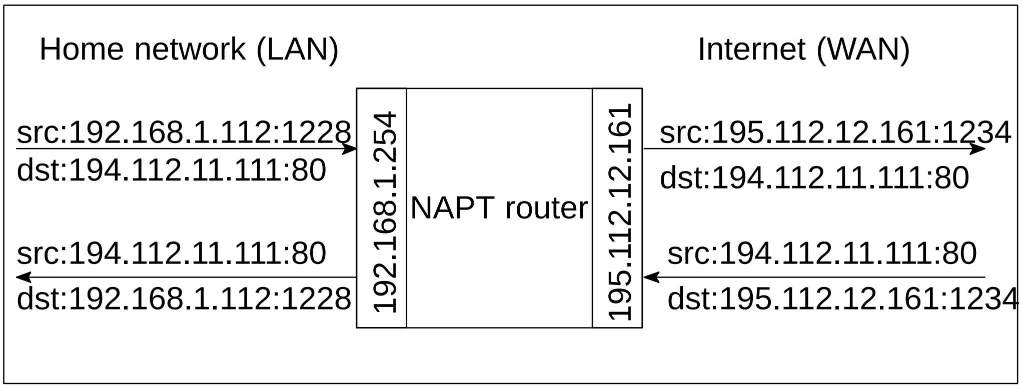


Figure 6-1 Principle of Network Address Port Translation

Normally, when the host in the home network sends a packet to the Internet, the NAPT adds timestamp, protocol (for example TCP, UDP), IP source address and source socket number as well as the IP destination address and the destination socket number into the database. The NAPT creates a new free socket number and replaces the original IP source address and source socket number. When a reply is received from WAN, the same table is used to map the IP destination address and destination socket number back to the original one. The entries from the NAPT cache/table are removed when the entry timeouts.

6.4.1 Pinhole

The basic NAPT functionality does not allow access from the Internet to a host on LAN because the private addresses cannot be seen outside the router. In order to support access from the global Internet to a server on a private subnet, the static NAPT mapping is used. In M11 this functionality is called pinhole.

In the static mapping, the WAN IP address and service related protocol/destination socket number are mapped to a private IP address and protocol/destination socket number. This functionality allows access from the Internet to only allowed server/services. If two services, such as HTTP servers in different machines, are located on the same LAN segment, they must have different socket numbers so that the NAPT can map the address correctly. Only one server on each socket number can be used.

6.5 IP address management

IP addresses can be used in M11 in two different ways:

- WAN interface belongs to one logical IP subnet and the Ethernet interface belongs to another logical IP subnet. This is how a normal router operates.
- WAN port has only one public IP address. The Ethernet interface uses private IP addressing. Network Address Port Translation (NAPT) is used to map the private IP addresses to and from a single public IP address. The operation is analogous to existing dial-up implementation, which consumes only a single IP address and is the most efficient way to use IP addresses.

The IP address of the WAN interface can be set statically or dynamically. Dynamic allocation of the IP address using IPCP (IP control protocol) is possible when PPP over ATM AAL5 is used on an ADSL WAN link. This operation is preferred when NAPT is used. For bridged WAN encapsulation, the DHCP client can be used to retrieve the IP configuration to the WAN port.

The IP address of the Ethernet interface and the subnet must be set statically. However, the built-in DHCP server functionality can be used to allocate an IP address, subnet mask, default gateway and DNS address to host.

When M11 operates in normal routing mode, the DHCP request can be relayed to the desired BOOTP/DHCP server. This functionality can be used if DHCP server is located outside M11.

6.6 IP multicast

IP multicast is is a technique which is used to conserve bandwidth when data is being sent to multiple receivers. Traditionally, in IP unicast, the source sends an individual copy of the information to each recipient. In IP multicast, only one copy of the multicast message will pass over any link in the network. Copies of the message will be made only where paths diverge at a router. This requires that all routers on the path support multicast. However, IP tunneling can be used to connect islands of multicast routers separated by routers which do not support multicast.

The receiver, who wants to receive a multicast transmission, must join a multicast host group. Multicast packets are only sent to LANs which have recipients of the particular multicast host group. Internet Group Management Protocol (IGMP) is used by multicast routers to learn the existence of host group members on their own subnets.

M11 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.

6.7 Payload encapsulation

Both routed and bridged protocols are encapsulated to the ATM uplink using either LLC/SNAP encapsulation (ether-llc or ip-llc) or VC multiplexing (ether-vcmux or ip-vcmux) according to RFC 1483. M11 also supports PPP over AAL5 encapsulation (ppp-vcmux and ppp-llc), where both bridged and routed protocols are first encapsulated to PPP (RFC 1661) which is, in turn, encapsulated to ATM according to IETF PPP over AAL5 using RFC 2364 VC multiplexing or LLL/NLPID encapsulation.

Typically, IP packets are encapsulated directly in the WAN interface using the selected encapsulation method (ip-llc, ip-vcmux, or ppp-vcmux). In some cases, bridged encapsulation can also be used for routed IP traffic. In these cases, the IP packets are encapsulated in

Ethernet MAC frames and the MAC frames are then encapsulated in the WAN interface using the selected encapsulation method (ether-llc, ether-vcmux, or ppp-vcmux).

The payload encapsulations are shown in Figure 6-2.

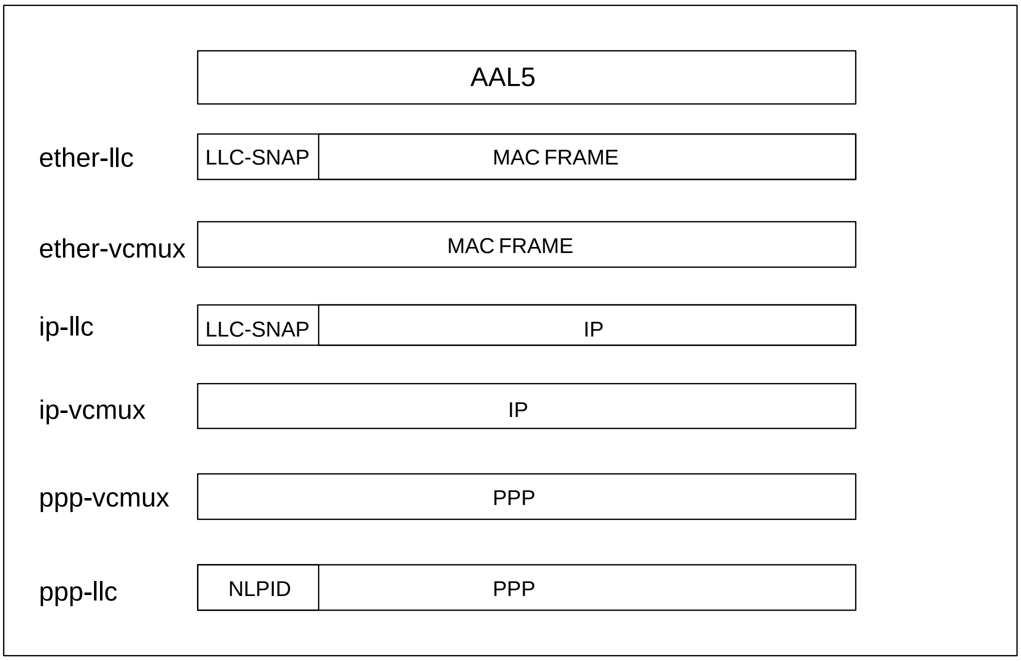


Figure 6-2 Payload encapsulations

6.8 Point-to-point protocol (PPP)

Point-to-point protocol is a set of network protocols which enable you to connect TCP/IP hosts and networks over serial connections.

The nodes at each end of a PPP link are referred to as peers. Unlike client-server networks, where one device is responsible of providing services to another, peer-to-peer network peers function as equals, providing services to one another as needed.

PPP provides a standard method of encapsulating network protocol information over point-to-point links. PPP defines a Link Control Protocol (LCP) which provides link configuration, peer authentication and link quality monitoring. Finally, PPP includes several Network Control Protocols (NCP) which specify how datagrams for a specific higher-level protocol using PPP as a datalink should be encapsulated.

Network control protocols establish and configure different network layer protocols, such as TCP/IP.

PPP encapsulation provides transmission of different network layer protocols simultaneously over the same link. Once a PPP link has been established, a PPP peer can negotiate the exchange of TCP/IP, IPX or Appletalk packets over the serial connection. Your M11 supports transmission of both IP (RFC 1332) and Ethernet (RFC 1638) packets over the PPP link.

The setup of a PPP link consists of the following phases:

- Link establishment
- Link configuration
- Authentication
- Network configuration
- Link up

During the link establishment, M11 synchronises its ADSL and ATM transmission to open a physical layer connection between Nokia M11 and the remote peer router through the ATM access network. When the physical connection has been established, the PPP protocol can actually begin its work.

The next step is the PPP link configuration, which is done using a Link configuration Protocol (LCP). It allows optional modifications to the standard characteristics of the PPP link to be negotiated. Negotiable items are, for example, the maximum receive unit (MRU) and link authentication.

After link configuration, an authentication is performed using either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) if required or configured. If the authentication succeeds, the next step in PPP link establishment is the negotiation of network protocols which will be transferred over the PPP link. After this the link is up and running.

6.8.1 Authentication

The PPP protocol suite includes two optional authentication methods. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) ensure that unauthorised users do not have access to the network services. By default, authentication is not required as part of the PPP link process. However, if a peer requires authentication, it must negotiate the use of an authentication protocol during the link establishment phase.

The manner in which each peer will authenticate the other is negotiated during the link configuration phase, when each peer specifies whether it requires authentication and, if it does, the authentication method it uses. If a link peer requires authentication, the other peer must submit its name and authentication information before the link can proceed. If the peer fails to send valid authentication information, the authenticator terminates the PPP link.

The authentication method used by one peer can be different from the authentication method used by the other peer. For example, a peer at one end of a link may require authentication while the other end of the link may not. Similarly, one end of a link may use PAP to authenticate peers while the other end uses CHAP.

6.8.2 Network configuration

M11 supports IPCP and BNCP network control protocols. IPCP network control protocol is used to exchange the IP configuration parameters. Typically IP addresses are exchanged. M11 is also able to retrieve the IP addresses from the far end or allocate an IP address to the far end. M11 also supports IPCP extension for DNS allocation (RFC 1877) that is used to configure DNS servers dynamically.

BNCP is used to establish the bridged PPP connection.

6.9 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol allows one host on a TCP/IP network to provide configuration information to other hosts on that network. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. When DHCP is enabled, the DHCP client requests configuration information, such as an IP address and network information, from a DHCP server each time it is restarted. The DHCP server responds to the request by sending the client an IP address and information about the network, such as the network's subnet mask, broadcast address, name service information, authentication information, and routing information.

6.9.1 DHCP for LAN clients

M11 can provide addresses for as many as 253 devices on the network connected to its Ethernet port. When M11 receives a DHCP request from a client computer, it determines what address to assign by checking its DHCP lease table to identify an unused address in its DHCP range. When it finds an address that should be free, M11 sends a broadcast message on the network to verify that no other host is using the same IP address. If another host indicates that it is using the selected address, M11 selects another address and repeats the sequence until it finds an address that is not in use.

Dynamic allocation of IP addresses means that an IP address can be reused when it is no longer needed by the client to which it is assigned. Dynamic IP address allocation is particularly useful in situations where clients connect to a network temporarily or where a site needs to share a limited pool of IP addresses among a group of clients that do not need permanent IP addresses.

Nokia M11 can also act as a DHCP relay agent. It can relay DHCP requests to an external DHCP server.

6.9.2 DHCP for WAN port configuration

It is possible to configure Nokia M11 in such a way that it operates as a DHCP client. It can retrieve IP addresses for the ADSL/ATM channels from the network. However, the following requirements must be met:

- ADSL/ATM channels use VC multiplexed or LLC/SNAP RFC 1483 encapsulations for IP or Ethernet packets.
- IP address information of the WAN interface has been set to 0.0.0.0

Nokia M11 sends a DHCP broadcast message asking for configuration information from any available DHCP server. If there is an active DHCP server behind the WAN interface, M11 accepts and uses the network configuration settings the DHCP server provides to configure the WAN port parameters.

6.10 Domain Name Service (DNS) relay

Nokia M11 can act as a Domain Name Service relay for the LAN clients. M11 LAN IP address acts as a DNS server address for all hosts connected to the LAN. M11 recognises its own name and responds to name queries with its own name. All other name queries Nokia M11 forwards to a primary or secondary Domain Name Server whose address has been configured to Nokia M11 either dynamically or statically.

Appendix A Technical specifications

A.1 Features

Software features	
Bridging	Self-learning bridge with 256 MAC addresses
Routing	Static routes, RIP and RIPv2
Data encapsulation formats	RFC 1483 IP and Ethernet over ATM PVCs Point-to-point Protocol over ATM AAL5 PVCs
Protocol conformity	RFC 1483, PPP over AAL5, ADSL/ATM
IP address management	NAPT, DHCP server for LAN clients, DHCP client for WAN ports, DNS relay

Hardware features	
ATM features	
ATM connections	PVC, up to 8 channels
Service categories	UBR, limited CBR
ADSL interface	
Physical layer	ANSI T1.413 Issue 2 (ANSI ADSL), ITU-T G.992.1 (ITU-T ADSL), ITU-T G.992.2 (ITU-T ADSL Lite), and ITU-T G.996.1 (Handshake) compatible
ADSL line connector	RJ-11
Cabling	Standard telephone wiring

Hardware features	
Data interface	
Ethernet 10Base-T	IEEE 802.3, DIX V.2
Data connector	RJ-45
Local management interface	
LMI connector	RJ-45
Indicator lights	
LAN	LAN activity, status and collision
DSL	ADSL line status
STA	M11 status

A.2 Mechanical construction and power supply

M11 ADSL router is a stand-alone device which can also be wall-mounted using a wall-mount kit.

Mechanical construction	
Width	294 mm
Height	56 mm
Depth	237 mm
Weight	2.5 kg

M11 has an in-built power supply. The characteristics of the mains connection are presented in Table A-1.

Mains connection	
Voltage	100 ... 240 V_{AC}
Frequency	45 ... 65 Hz
Power consumption	9 W

Table A-1 Mains connection

A.3 Ambient conditions, EMC and safety

Ambient conditions

Operating temperature range	0 to 40°C
Humidity	10% to 90% non-condensing

EMC

M11 complies with the following specifications, provided that the device is connected to an earthed socket outlet:

EN55022 class B	Emission
EN50082-1: 1992	Immunity
ITU-T K21	Overvoltage protection

M11 does not require the use of shielded cables.

Safety

M11 complies with the following specification:

EN 60950

Glossary

Abbreviations

AAL	ATM Adaptation Layer
ACK	Acknowledgement
ACT	Active
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BNCP	Bridge Network Control Protocol
BOOTP	Bootstrap Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
COL	Collision
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DMT	Discrete Multitone
DNS	Domain Name Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ETSI	European Telecommunications Standards Institute

FTP	File Transfer Protocol
HEC	Header Error Correction
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
INA	Inactive
IP	Internet Protocol
IPX	Internetwork packet exchange
ISP	Internet Service Provider
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Logical Link Control
LMI	Local Management Interface
LNK	Link
MAC	Media Access Control
MRU	Maximum Receive Unit
NAPT	Network Address Port Translation
NAT	Network Address Translation
NCP	Network Control Protocol
NLPID	Network Layer Protocol Identification
NVRAM	Non-volatile RAM
OSI	Open System Interconnection
PAP	Password Authentication Protocol
PC	Personal Computer
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PVC	Permanent Virtual Circuit
RAM	Random Access Memory

RFC	Request For Comments
RIP(v2)	Routing Information Protocol (version 2)
SNAP	Subnetwork Access Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STA	Status
TCP	Transmission Control Protocol
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
WAN	Wide Area Network
WWW	World Wide Web

Terms

10Base-T

10 Mbit/s Ethernet specification using two pairs of twisted cabling. 10Base-T is a part of the IEEE 802.3 specification.

Appletalk

Series of communications protocols by Apple Computer.

ATM access network

An access network where traffic from the subscribers is multiplexed and forwarded using ATM technology.

bridge

A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic.

broadcast

A packet delivery system where a copy of a given packet is given to all hosts attached to the network.

brouter

A device which is both a bridge and a router.

command line interface

Character-based user interface where a command line ending with <CR> character is used to configure a device. The device interprets the command and returns a character-based response.

Config command hierarchy

A hierarchy of nodes which contain the configurable parameters of M11. It is used to configure M11 through the command line interface. See Root command hierarchy.

Digital Subscriber Line Access Multiplexer

A network element which multiplexes the traffic coming from the high-speed subscriber lines and forwards this traffic to the ATM network.

domain name service

Domain name service (DNS) is used for translating names of network nodes into addresses.

dynamic routing

Dynamic routing maintains information of routes that may change over time. Dynamic routes are created and configured when routers broadcast Routing information protocol packets advertising the networks they can reach and the distance (number of routers) to each network.

encapsulation

Wrapping of data in a protocol header.

Ethernet

LAN specification IEEE 802.3.

firewall

A system or a group of systems that enforce access control between two networks.

default gateway

A default gateway is the router to which M11 will send a packet if it does not know how to reach the packet’s destination host.

half-duplex

Communication between terminals one direction at a time.

host

Computer system on a network.

Internet Group Management Protocol

IGMP is used by multicast router to learn the existence of host group members on their subnet.

IP network

Data communications network based on the Internet Protocol.

low-pass filter

Passive filter used for separating the telephone signal from data signals in the digital subscriber line.

MAC address

Ethernet address.

multiplexer

A device where several logical connections are combined into one physical connection.

ping

Packet Internet Groper. A program used to test the reachability of destinations by sending them an ICMP echo request and waiting for a reply.

pinhole

Pinhole allows access to a home network from the public Internet when Network Address Port Translation is used.

POTS filter

A device used for separating the telephone signal from data signals in the digital subscriber line.

proxy

A mechanism whereby one system “fronts“ for another system in responding to protocol requests.

Root command hierarchy

A hierarchy of commands used to monitor the performance of your M11, display and reset M11 statistics, and issue administrative commands to restart M11 functions through the command line interface.

router

A system responsible for making decisions about which of several routes the network traffic will follow.

routing table

A table in a router according to which the routing decisions are made. It contains addresses of other routers and the distance (number of hops) to those routers.

serial console connection

Serial connection behind the hatch in the front panel of M11. It is used for configuring M11 locally.

socket

In TCP applications socket specifies the TCP service access point defined by the source and destination ports.

static routing

Static routing maintains information of the routes to destination networks that are stable over time or to networks that must always be available, even if a link is not currently open. Static routes must be configured manually into the routing table.

subnet mask

A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion.

telecommuter

A person who works at home with data communications to the central office.

telnet

A virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as a normal terminal users of that host.

virtual channel

A communications channel which provides for the sequential unidirectional transport of ATM cells.

virtual channel connection

A concatenation of virtual channel links that extends between the points where the ATM service users access the ATM layer.

virtual channel link

A means of unidirectional transport of ATM cells between the point where the Virtual channel identifier value is assigned and the point where that value is translated or removed.

Web browser

A software that is used to browse the World Wide Web.