Digital Residential Gateway, DRG

OPERATIONAL DIRECTIONS

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

1 GENERAL

The Digital Residential Gateway 22i (DRG22i) analog extension gateway enables cost-efficient integration of remote analog telephones or G3 fax machines the MX-ONE over an IP connection.

This document covers the operation of the DRG22i.

1.1 CAPACITY AND LIMITATIONS

Each DRG22i can handle the following:

- One or two analog telephones
- One or two fax machines
- One analog telephone and one fax machine

1.2 GLOSSARY

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

2 PROCEDURES

The DRG22i is either installed from the built-in Web interface or the DRG manager. This section describes the former.

2.1 ACCESSING THE WEB CONFIGURATION SERVER

Follow the steps below to access the Web Configuration Server:

- Connect the DRG22i to the network using the Wide Area Network (WAN) port.
- If a Dynamic Host Configuration Protocol (DHCP) server is being used, the DRG22i will request an IP address during startup.
- If a fixed IP address is to be used, press the Reset button on the back of the DRG22i and hold for about 10 seconds. The DRG22i reboots and the LEDs flash when the Reset button is then released. Thereafter, the DRG22i obtains **factory default** status with an IP address of 192.168.254.254 and a subnet mask of 255.255.255.0.
- Open a Web browser (Internet Explorer 5.5 or higher), and disable the caching of Web pages.
- Enter the IP address of the DRG22i in the address box.
- If the Web Configuration Server is password protected, you will be prompted to enter your password. The default password is DRGPASS (case sensitive). Enter **operator**, if a username is requested.

The Web Configuration Server main view appears on the screen. The Web Configuration Server main view consists of a number of menu links to the left. Clicking each will display its content (configuration or status information) in the main window accordingly.

2.2 WEB CONFIGURATION SERVER

This section describes the configuration settings available in the Web Configuration Server. Click the links in the menu to choose a configuration area.

Warning: There is no check that the entered values are valid or have the correct format. If invalid values are entered, the data may be lost, in which case a factory default procedure must be performed. For information on resetting the DRG22i to default parameters, see page 31.

2.3 WAN

The network configuration includes settings for the DRG22i to work in a network. Either choose a DHCP server to automatically supply the DRG22i with IP address configuration, or use a fixed IP address. If a fixed IP address is used, all network configurations need to be performed manually in the DRG22i.

The DRG22i is equipped with two Ethernet ports; the access WAN port and the local LAN port. The WAN port is connected to an external network, such as the Internet, while the LAN port makes it possible to set up a private network.

Note: Be careful when setting these values to avoid conflicts in the network.

The current status of the WAN side of the DRG22i is shown in the WAN Status page. Click Update to update the settings.

2.4 WAN CONFIGURATION

The connection characteristics to the network are set in the WAN Settings page.

For an explanation of the different functions, see below.

Table 1 WAN Configuration

Function	Description
Device Operating Mode	Select if the DRG22i is working in **Bridge** or **Router** mode.
Obtain WAN configuration dynamically	If Obtain WAN configuration dynamically is selected, the IP address, Netmask, Gateway, and DNS are provided through DHCP
Specify fixed WAN configuration	If Specify fixed WAN configuration is selected, the IP address, Netmask, Gateway, and DNS are manually configured.
Host Name	Hostname for client
Domain Name	Domain name for client resolution
Multicast Limits Broadcast Limit	The value specifies the maximum limit on the percentage of broadcast packets that will be bridged to the destination interface (as a percentage of the source side bandwidth).
Multicast Limits Multicast Limit	The value specifies the maximum limit on the percentage of multicast packets that will be bridged to the destination interface (as a percentage of the source side bandwidth) LAN.

For the settings to take effect, click **Save WAN Settings** , and restart the DRG22i.

2.5 PPPOE CONFIGURATION

Point-to-point protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames in Ethernet frames, see below. It is used mainly with cable modem and DSL services. It offers standard PPP features, such as authentication, encryption, and compression.

Figure 1: WAN PPPoE Configuration

For an explanation of the different functions, see below.

Table 2 PPPoE Configuration

Function	Description
Enable PPPoE	Select **No** to not use PPPoE, or select **Yes** to use PPPoE.
Authentication Username	Insert the username, provided by the service provider
Authentication Password	Insert the password, provided by the service provider
Settings Idle Timeout	Idle timeout before PPP connection is closed due to inactivity
Settings Echo Timeout	The duration between PPP echo requests being sent to the server.
Settings Echo count	The number of unanswered PPP echo requests before the PPP connection is closed.
Settings Service Name	Given name of the PPPoE service
Settings AC Name	Given PPPoE AC name

For the settings to take effect, click **Save PPPoE Settings** , and restart the DRG22i.

2.6 IPSEC

Appending communication security, IPsec is a communication protocol based on IP, see below. TCP/IP and UDP/IP gain security from IPsec without being aware of it. IPsec provides encryption, integrity insurance, and authentication of data. Encryption protects data from peeping even if the communication path is monitored. Encrypted data does not make sense to anyone but the intended party. Integrity insurance means that modifications to data can be detected. Authentication verifies the identity of the origin of data.

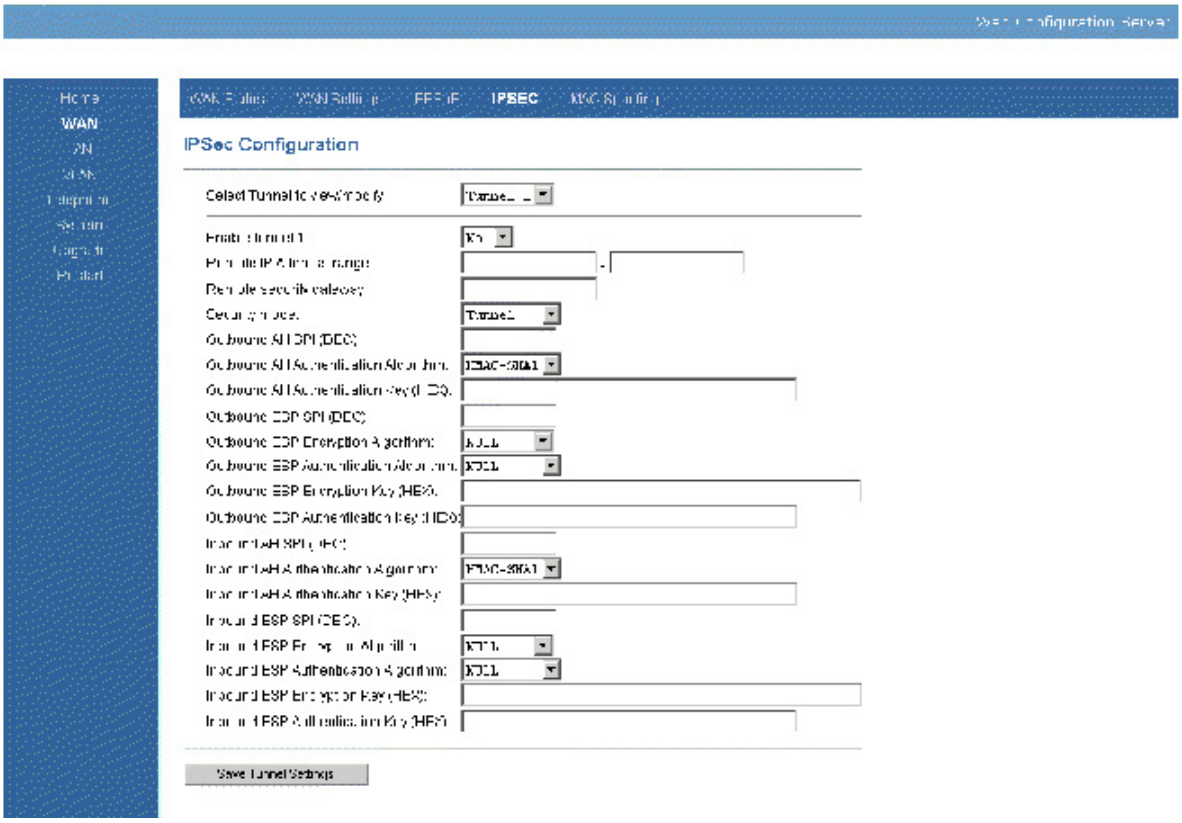

Figure 2: IPsec Configuration

For explanation of the different functions, page 7.

Table 3 IPsec Configuration

Function	Description
Select Tunnel to View/Modify	This option selects which one of the eight tunnels of the DRG22i to view or modify.
Enable Tunnel	This option enables or disables the tunnel previously selected.
Remote IP Address range	The IP address range of the remote host
Remote Security Gateway	The computer acts as gateway of the other side of DRG22i. If the DRG22i is establishing the trust connection with the computer through internet, this gateway is the gateway of that particular computer to connect to the internet.
Security Mode	To specify whether the tunnel using transport of tunnel mode. Selecting tunnel mode will require the ESP parameters to be specified as well.
Outbound AH SPI (DEC)	The outbound SPI value if AH is implemented. This will be applied for the outgoing communication. The value should be filled with decimal value.
Outbound AH Authentication Algorithm	The outbound AH algorithm. This will be applied for the outgoing communication. The value is either HMAC-SHA1 or HMAC-MD5.
Outbound AH Authentication Key (HEX)	The outbound AH authentication key. This will be applied for the outgoing communication. The value must be filled with hexadecimal without **0x** .

Function	Description
Outbound ESP SPI (DEC)	The outbound SPI value if ESP is implemented. This will be applied for the outgoing communication. The value should be filled with decimal value.
Outbound ESP Encryption Algorithm	The outbound ESP encryption algorithm. This will be applied for the outgoing communication. The value is either DES-CBC or 3DES-CBC.
Outbound ESP Authentication Algorithm	The outbound ESP authentication algorithm. This will be applied for the outgoing communication. The value is either HMAC-SHA1 or HMAC-MD5.
Outbound ESP Encryption Key (HEX)	The outbound ESP Encryption key. This will be applied for the outgoing communication. The value must be filled with hexadecimal without **0x** .
Outbound ESP Authentication Key (HEX)	The outbound ESP authentication key. This will be applied for the outgoing communication. The value must be filled with hexadecimal without **0x** .
Inbound AH SPI (DEC)	The inbound SPI value if AH is implemented. This will be applied for the outgoing communication. The value should be filled with decimal value.
Inbound ESP Encryption Algorithm	Inbound ESP encryption algorithm. This will be applied for the outgoing communication. The value is either DES-CBC or 3DES-CBC.
Inbound ESP Authentication Algorithm	The inbound ESP authentication algorithm. This will be applied for the outgoing communication. The value is either HMAC-SHA1 or HMAC-MD5.
Inbound ESP Encryption Key (HEX)	The inbound ESP Encryption key. This will be applied for the outgoing communication. The value must be filled with hexadecimal without **0x** .
Inbound ESP Authentication Key (HEX)	The inbound ESP authentication key. This will be applied for the outgoing communication. The value must be filled with hexadecimal without **0x** .

For the settings to take effect, click **Save Tunnel Settings**, and restart the DRG22i.

2.7 LAN CONFIGURATION

The DRG22i is equipped with two Ethernet ports; the access port (WAN) and the local port (LAN). The WAN port is connected to an external network (Internet), while the LAN port, see page 10, is used to set up a private network.

Figure 3: LAN Settings

For an explanation of the different functions, see below.

Table 4 LAN Settings

Function	Description
Network Settings IP address	DRG22i LAN port IP. Default Gateway for client connected on DRG22i LAN side.
Network Settings Subnet Mask	Specifies the subnet mask of the LAN. Usage of a C-class network is recommended. For example, 255.255.255.0.

For the settings to take effect, click **Save LAN Settings** , and restart the DRG22i.

2.8 DHCP SERVER CONFIGURATION

DHCP server configuration, see page 11, in which a client host **leases** an IP address, can be useful in a large-scale network, because it assigns an IP address, and many other options, such as DNS and WINS Servers.

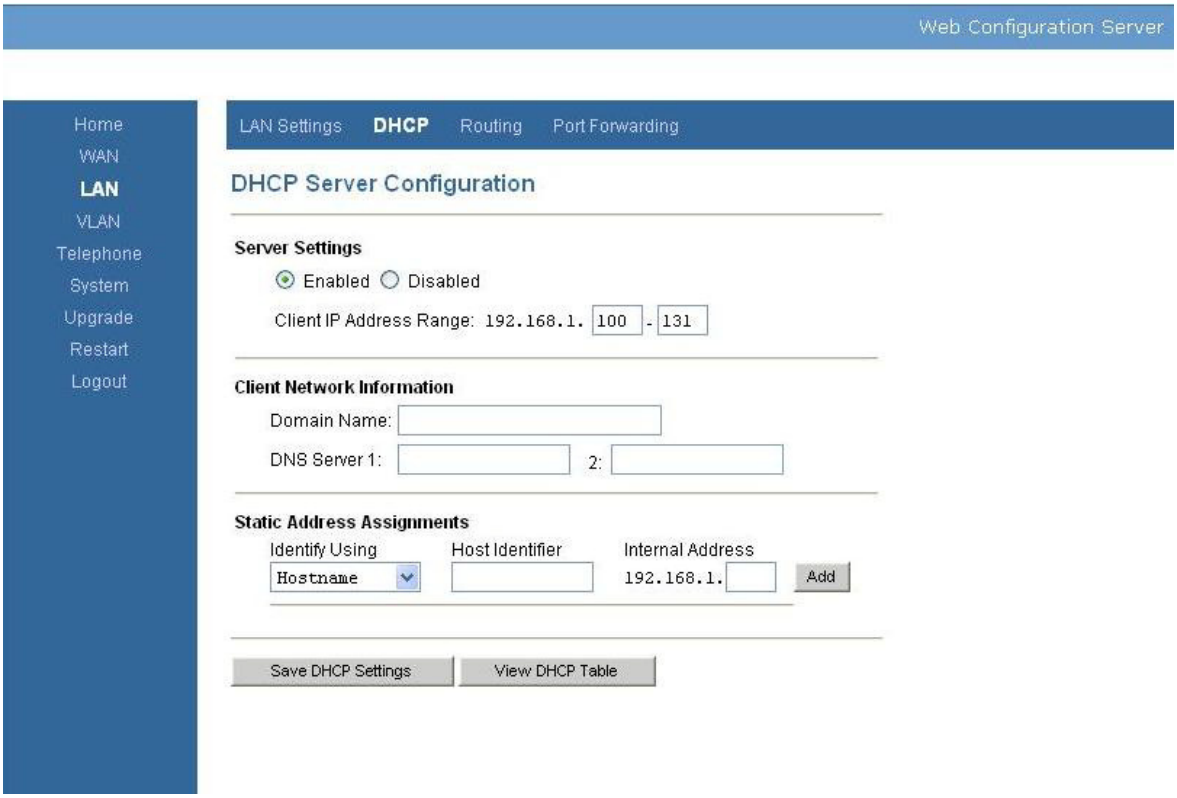

Figure 4: DHCP Server Configuration

For explanation of the different functions, see below.

Table 5 DHCP Server Settings

Function		Description
Server Settings		
		Enable or disable the internal DHCP Server.
	Client IP Address Range	Minimum and Maximum limit on the DHCP IP address. Subnet specified under LAN settings will be used.
Client Network Information		
	Domain Name	The LAN domain name provided to DHCP clients during the DHCP process.
	DNS Server	This statically assigned DNS server IP address will be provided to clients during the DHCP process.
Static Address Assignment		
	Identify Using	Up to eight static DHCP address assignments can be configured. To add a static IP assignment, enter the LAN device host name (must be unique in the private network) or MAC address.
	Host Identifier	Specify the Internal address to be assigned and click **Add** .

By clicking **View DHCP Table** , it is possible to see the allocated addresses and equipment connected to the LAN.

For the settings to take effect, click **Save DHCP Settings**, and restart the DRG22i.

2.9 ROUTER CONFIGURATION

It is possible to assign static routes or enabling the RIP protocol, see below.

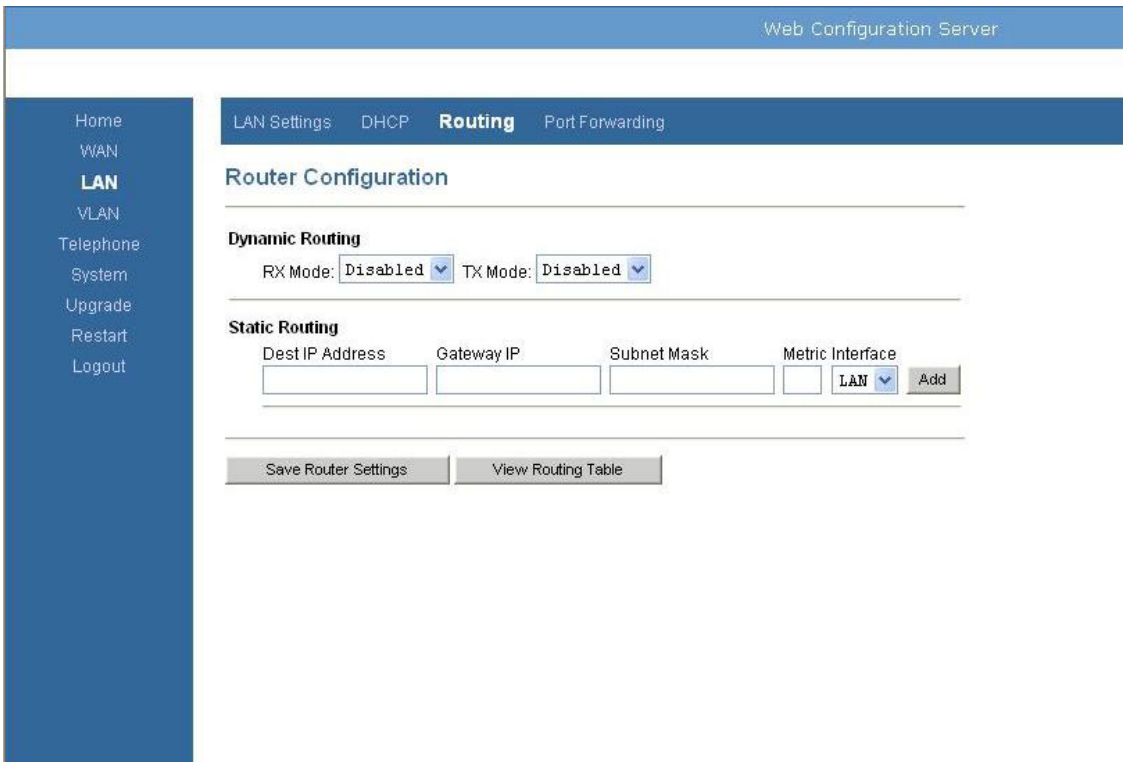

Figure 5: Routing Configuration

For an explanation of the different functions, see page 13.

Table 6 Router Configuration Settings

Function	Description
Dynamic Routing	RIP Routing protocol on/off. TX means send RIP packets and RX means listen to RIP packets. It is recommended to disable this function (not implemented in all software versions).
Static Routing	Configure static routes within the LAN.

By clicking **View Routing Table** , it is possible to view the current routing table.

For the settings to take effect, click **Save Router Settings** , and restart the DRG22i.

2.10 PORT FORWARDING

Port forwarding, see page 14, is a feature built into routers that perform NAT. It allows the router to forward any unrequested traffic generated from the Internet side of the router to a specified internal host. For example, a user may run an Apache Web Server on port 80 at machine 10.0.0.5, and may want this server accessible from the Internet. A rule can be added to the router so that any requests to port 80, that are not replies to those from the local network, are forwarded to IP address 10.0.0.5.

Many routers allows to assign a global rule such that all ports are forwarded to one internal server, or can specify different IP addresses for different ports. If a user has an FTP server running on 10.0.0.6, a separate port mapping can be created. From the outside world both port 80 and 21 are open even though the services are provided by independent internal computer systems

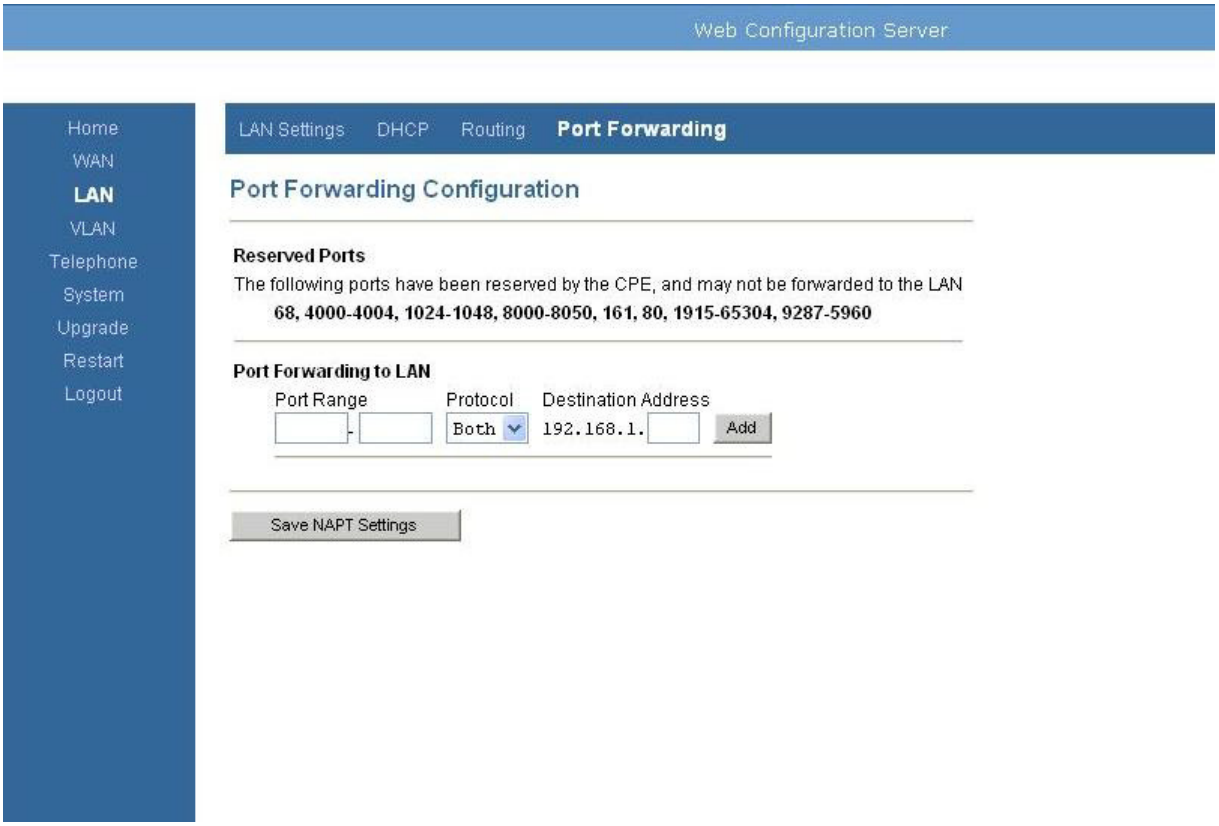

Figure 6: Port Forwarding Configuration

For explanation of the different functions, see below.

Table 7 Port Forwarding Configuration

Function	Description
Reserved Ports:	Under Reserved Ports all DRG22i reserved ports are listed.
Port Forwarding to LAN	Enter the specifications, which you will be forwarding to the LAN, including port range, protocol (Both, TCP, or UDP), and destination IP address.

For the settings to take effect, click **Save NAPT Settings** , and restart the DRG22i.

2.11 VLAN

The DRG22i can use IEEE 802.1Q Virtual LAN (VLAN). An Ethernet frame on a VLAN has an additional header or tag inserted that tells equipment in VLAN-aware networks which VLAN the frame belongs to (VLAN ID) and the priority of the frame.

The DRG22i can handle up to 16 VLANs.

A VLAN must be either tagged or untagged on LAN or WAN port.

The VLAN page shows the working configuration with untagged Internet VLAN and tagged VoIP/Management VLAN, see below.

1. In the **VLAN Tagging** page, click **Add VLAN** to bring up the **VLAN Editor** dialog box.

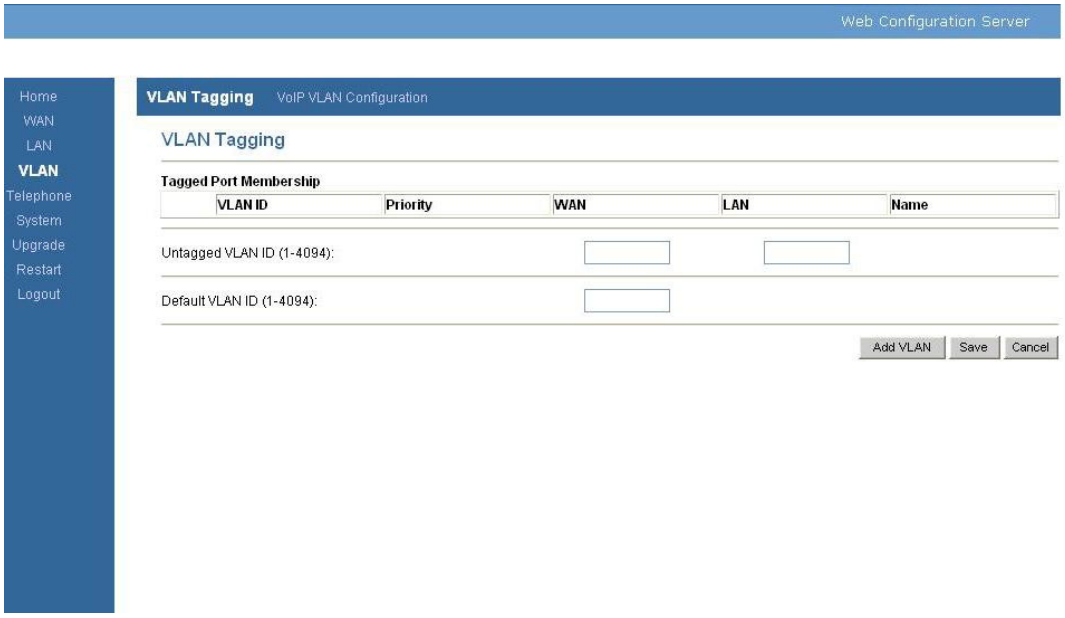

Figure 7: VLAN Tagging

2. Enter the parameters for the Management and Voice VLAN, and click **OK to return to the VLAN Tagging** page. The VLAN will be tagged at WAN and tagged at LAN.

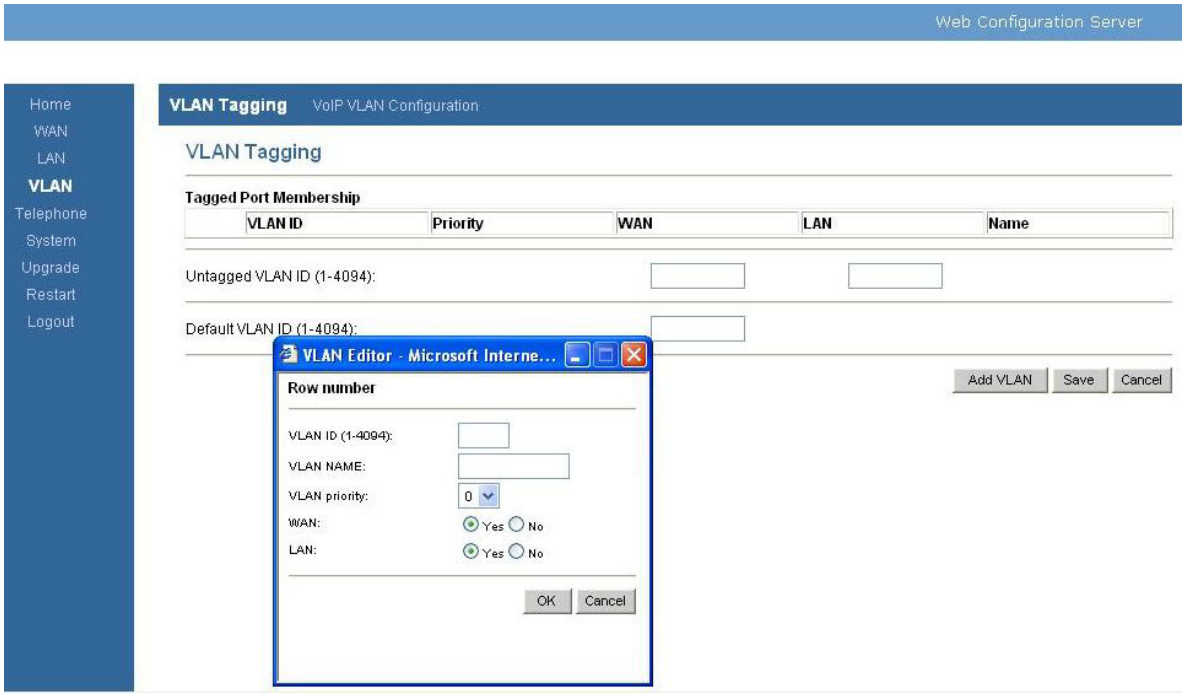

Figure 8: VLAN Editor

3. In the **VLAN Tagging** page, see below, enter the VLAN ID for the Management and Voice VLAN in the **Default VLAN ID on WAN port (1-4094)** box, and click **Save** .

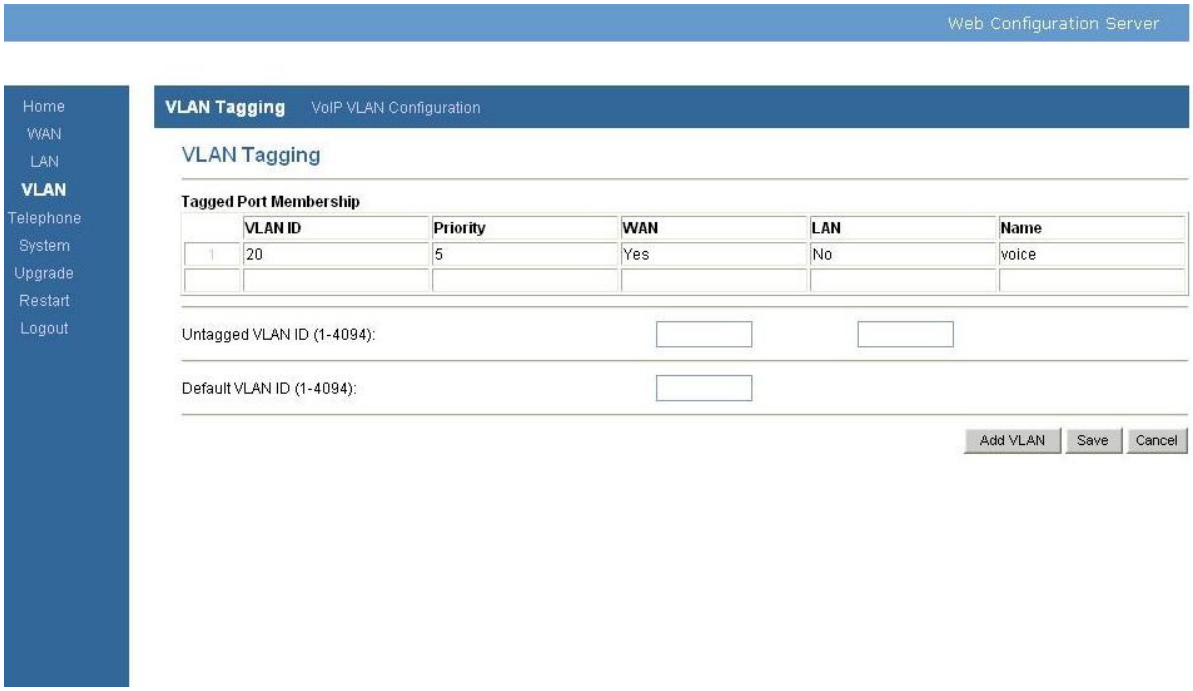

Figure 9: VLAN Tagging

4. In the **Telephony** page, see page 17, enter the VLAN ID and priority for the **Call Signaling** and **RTP** VLANs (same as for the Management VLAN in this configuration). Click **Save VoIP VLAN Settings** to return to the **VLAN Tagging** page.

Figure 10: Telephony Page

5. To create the **Data** VLAN, click **Add VLAN** to bring up the VLAN editor, see below, enter the parameters, and click OK to return to the **VLAN Tagging** page. This VLAN will be untagged at both WAN and LAN.

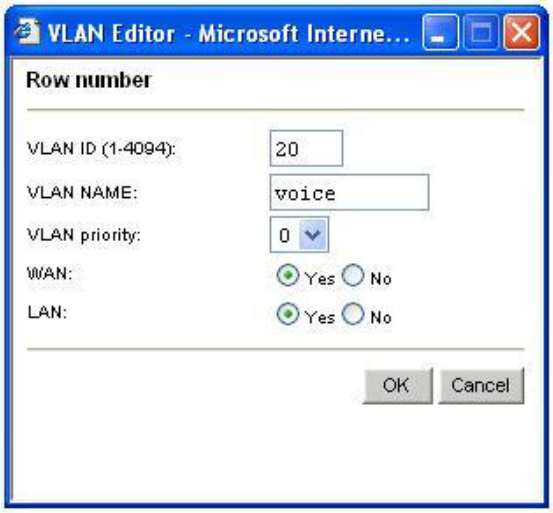

Figure 11: VLAN Editor

6. In the **VLAN Tagging** page, see page 18, enter the **Data** VLAN ID in the **Untagged VLAN ID on WAN port** and **Untagged VLAN ID on LAN port** boxes. Untagged VLAN ID settings have precedence over the WAN and LAN Yes/No setting, because only one untagged VLAN is acceptable per port.

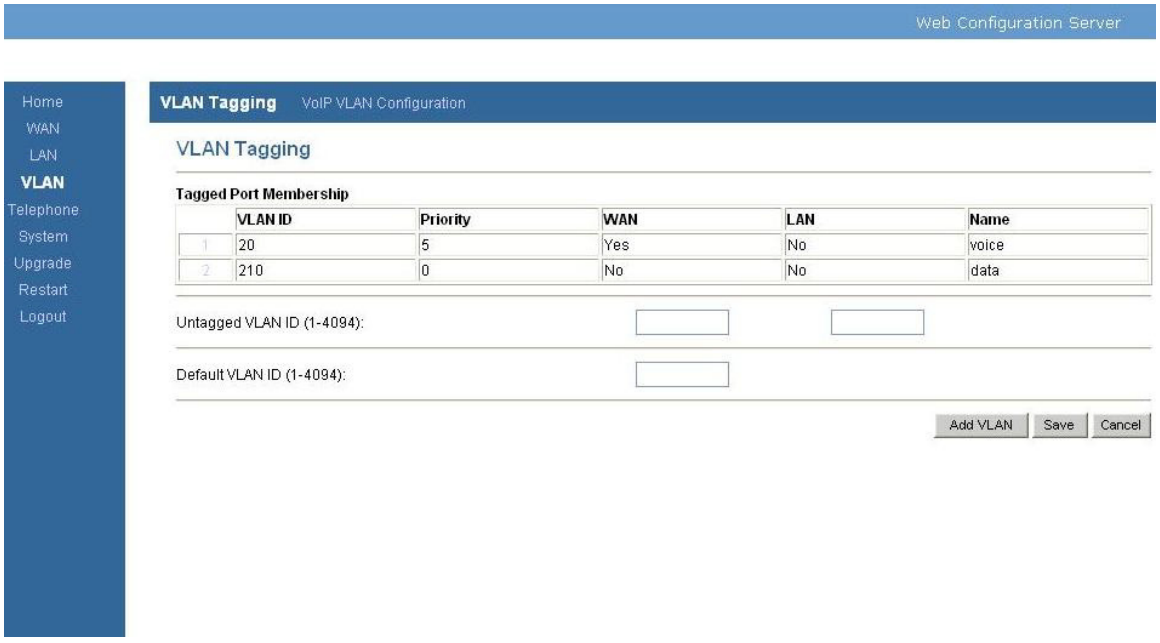

Figure 12: VLAN Tagging

7. Click **Save**, and restart the DRG22i.

2.12 TELEPHONE

The DRG22i includes IP telephony with two separate telephone lines, see below. The IP telephony can easily be switched on or off. The individual telephone lines can also be switched on or off and be set up separately.

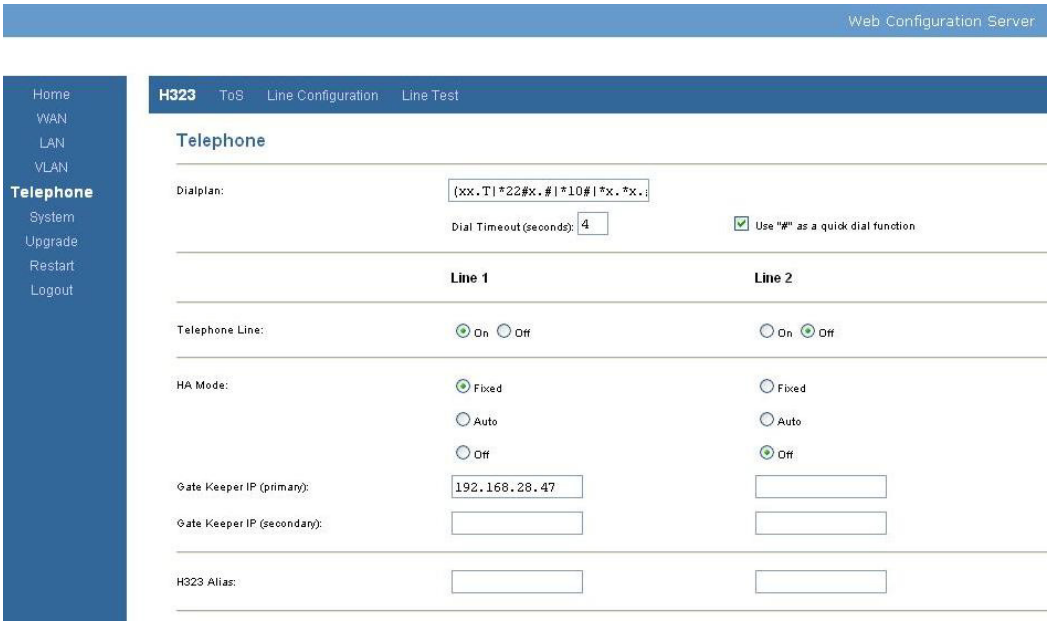

Figure 13: Telephony Settings

For an explanation of the different functions, see below.

Table 8 Telephony Settings

Function	Description
Dial plan	The dial plan gives the DRG22i a map to determine when a complete number has been dialed. (T = by timeout, # = by pressing #). The default value is (x.T | x.#) For information on how to define hotlines and add prefixes using this field, see section 2.12.1 Configuring the hotline Function and section 2.12.2 Adding Prefixes..
Dial timeout (seconds)	The number of seconds that the DRG22i waits before it sends a complete telephone number. This is necessary, since the whole telephone number is sent at once and not digit by digit. The default value is four seconds.
For each telephone line (Line 1 and Line 2), the following settings are available:	
Telephone line	Switch the telephone line on or off. (The telephone must be set to ON for this setting to take effect)
HA mode	High Availability (support for the secondary gatekeeper) Fixed, Auto, Off (If a secondary GK is not available, this value **must** be Off).
Gatekeeper IP (primary)	The primary IP address for the gatekeeper which is responsible for managing the DRG22i in the specific net. If HA-mode is set to Auto, the primary gatekeeper tells the DRG22i during its registration an IP-address to the Alt-GK.
Gatekeeper IP (secondary)	The secondary gatekeeper IP address (when HA mode is set to Fixed).

Function	Description
H323 alias	The DRG22i name to use when registering the DRG22i at the gate keeper. **NOTE** The H.323 alias and the telephone number must be set to unique values for each telephone line in order for the system to accept the values.
Outgoing Display Name	The name to be presented on the receivers caller display. (The network must support this function!)
Telephone number	The telephone number of the specific telephone line.
Incoming CLIP	If turned ON, the telephone number, on incoming calls, is presented in the caller display attached to the DRG22i.
Keep alive timeout (seconds)	The interval that the DRG22i suggest to send the keep-alive messages to the Gatekeeper. If the keep-alive time is sent from the gatekeeper, it will override the DRG22i local setting. The default is 1200 seconds.
Ring signal [0 - 9]	Choose between 10 ring signals (0-9).
Preferred codecs	Shows the current Codecs/Fax settings.

Note: Click Save after choosing the options.

Click Set **Codecs/Fax** to open the **Codecs and Fax Configuration** dialog box and change the settings.

It is possible to set up which codecs to be used (G.711u/A-law being mandatory, G.729 optional) and their preferred priority, see below.

Note: Since this release of MX-ONE does not support T.38 fax, this check box must not be selected.

Table 9 Codec and Fax Settings

Function	Description
Codec	Codec selection. G.711u/A being mandatory, G.729 optional.
SS	Silence Suppression ON/OFF.
Packet	Packetization time in ms. Possible range 10 - 150 ms. The default value is 30 ms.
Keypad	Enable Out-of-band signaling with DTMF tones.
Priority	Codec priority. Voice codec negotiation and priority is always performed between two end-points and depending on which side that initiates the negotiation, the chosen codec may be different from the local priority order.

It is possible to choose whether to use Silence Suppression (SS) or not, on outgoing speech.

The possibility to set up EC Echo Cancellation (EC) is **not** implemented. EC is always used during speech, but **not** during fax (T.38) transmissions.

The Keypad box tells which transmission method to be used for user input DTMF signaling (that is, phone banking). *None* means inband, which should be used with G.711 only. H.225 or H.245 should be used primarily with G.729, but could also be used with G.711.

Note: Click Save after choosing the options.

Caller ID method should be set up by loading an appropriate .ini file. The default is the Swedish DTMF requirement.

2.12.1 CONFIGURING THE HOTLINE FUNCTION

The DRG extensions can be configured as hotlines provided that the revision of the DRG firmware is R2H2xx or later. The configuration is done using the **Dial plan** and **Dial timeout** fields, where the dial plan data defines the hotline number and the dial timeout data defines the delay time from the handset is lifted until the hotline number is dialed.

The following syntax is used when configuring the hotline number using the **Dial plan** field:

(xx.#|xx.T|<:hotline number>T)

The table below shows some examples on hotline configurations:

Table 10

Type of hotline	Dial plan field	Dial timeout field	Result
Immediate hotline	(xx.#|xx.T|<:1021>T)	0	Send SIP INVITE to 1021 (hotline number) as soon as the phone goes off hook.
Slow hotline	(xx.#|xx.T|<:1021>T)	10	Send SIP INVITE to 1021 (hotline number) ten seconds after the phone goes off hook.
Hotline deactivation	Any	Any	A hotline is deactivated by defining another dial plan.

2.12.2 ADDING PREFIXES

The DRG extensions can be configured for automatic adding of prefixes provided that the revision of the DRG firmware is R2H2xx or later. The configuration is done using the **Dial plan** and **Dial timeout** fields, where the dial plan data defines the prefix and the dial timeout data defines the delay time from the handset is lifted until the number (including the prefix) is dialed.

The following syntax is used when configuring prefixes using the **Dial plan** field:

(<:prefix>xx.#|<:prefix>xx.T)

The table below shows some examples on prefix configurations:

Prefix	Dial plan field	Dial timeout field	Result
00	(<:00>xx.#|<:00>xx.T)	0	The prefix 00 is added for all calls. If dialing 112, the SIP INVITE will contain 00112. The call is initiated when the handset is lifted.

00 (with delay)	(<:00>xx.#|<:00>xx.T)	10	The prefix 00 is added for all calls. If dialing 112, the SIP INVITE will contain 00112. The call is initiated 10 seconds after the handset is lifted.
Prefix deactivation	Any	Any	A prefix is deactivated by defining another dial plan.

2.13 TOS/DIFFSERV

ToS/Differentiated services, see below, is a layer 3 protocol used at the edge of an enterprise which tags each frame, either at the originating device or at an intermediate point, to identify the requested level of service. It includes a Differentiated Services Code Point (DSCP) which specifies how each switch handles the frame.

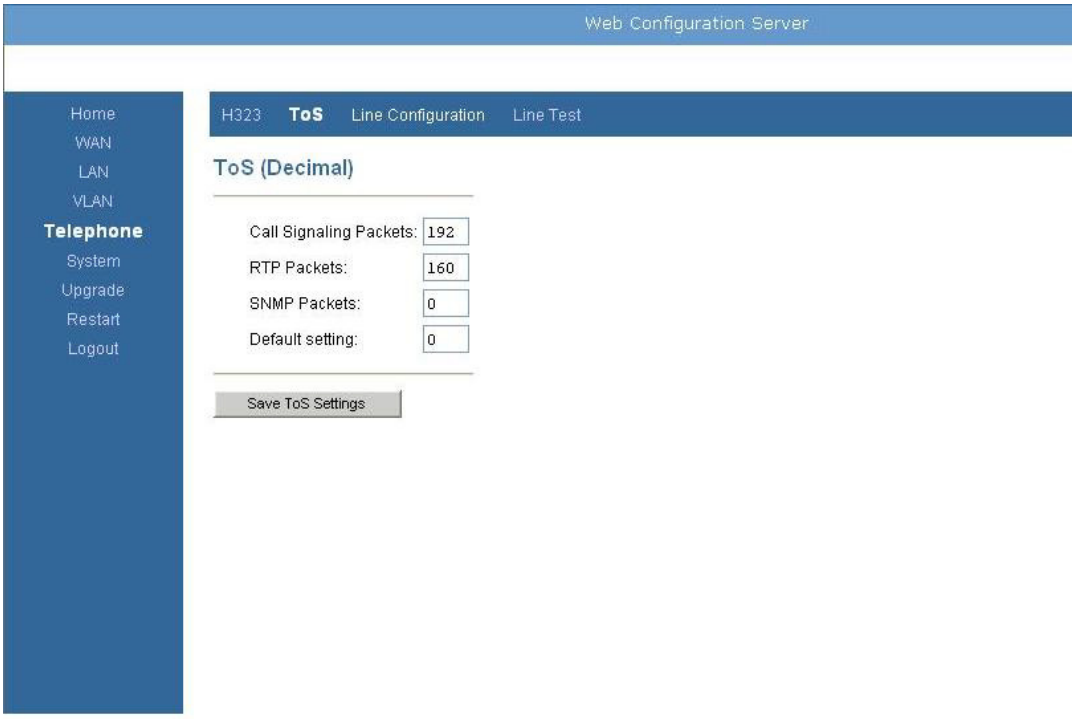

Figure 14: ToS/DiffServ Configuration

Outgoing telephone packets from the DRG22i can be marked with ToS/DiffServ values on both Call Signaling Packets and in RTP packets.

The value range to use in the fields is (hexadecimal) 0 to FF, where FF means that all eight bits are set in the TOS header. 0 means all bits are set to 0 in the TOS header.

Default Values: C0 = 11000000 , DiffServ Code Point CS6. A0 = 10100000 , DiffServ Code Point CS5.

For more information about DiffServ Code Points, see RFC 2474.

2.14 CHANGE PASSWORD

The DRG22i is equipped with password protection, which may be changed, see below. In order for the system to accept the new password you need to enter your old password.

Default password = DRGPASS

NOTE The password is case sensitive. You can only set the access mode of the current user.

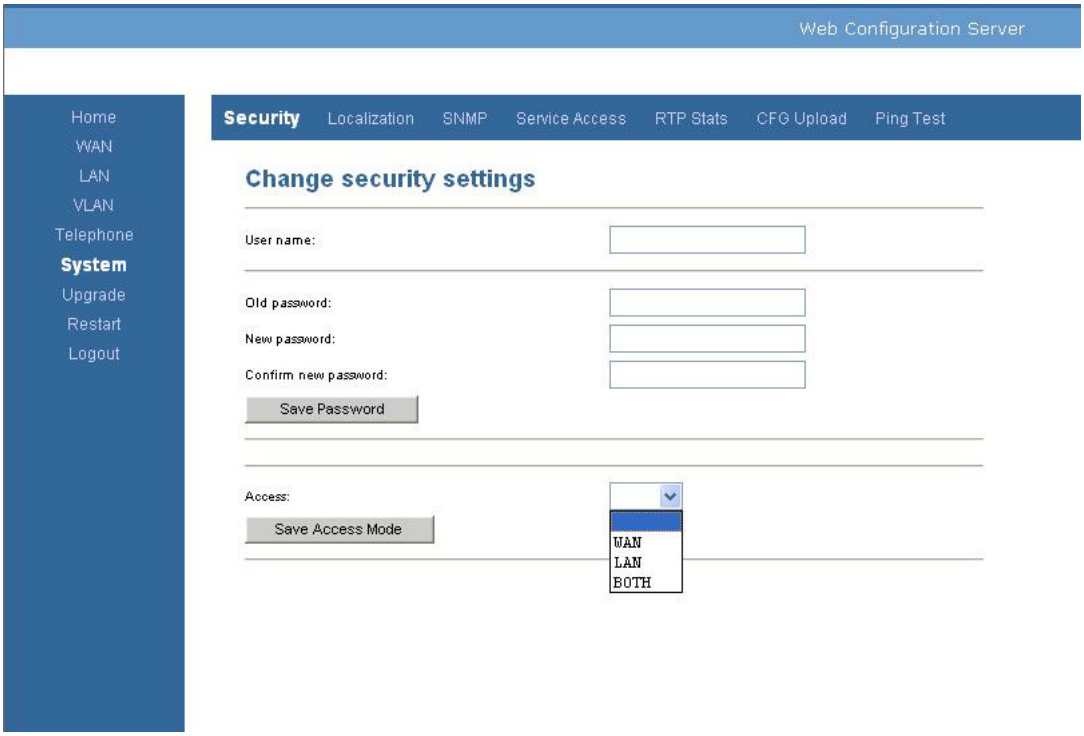

Figure 15: Change Security Settings

For an explanation of the different functions, see below.

Table 11 Set Security Password Settings

Function	Description
User name:	Enter your current login name.
Old password:	Enter your old password.
New password:	Enter your new password.
Confirm new password:	Reenter your new password.
Access:	Choose the access mode, that is, from where to access the Web Configuration pages of the DRG22i: WAN = can only access from WAN LAN = can only access from LAN BOTH = can access both from WAN and LAN

For the settings to take effect, click **Save Password** or **Save Access Mode** and restart the DRG22i.

2.15 LOCALIZATION/TIME SETTING

Network Time Protocol (NTP) built on top of TCP that assures accurate local time-keeping with reference to radio and atomic clocks located on the Internet, see below. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods

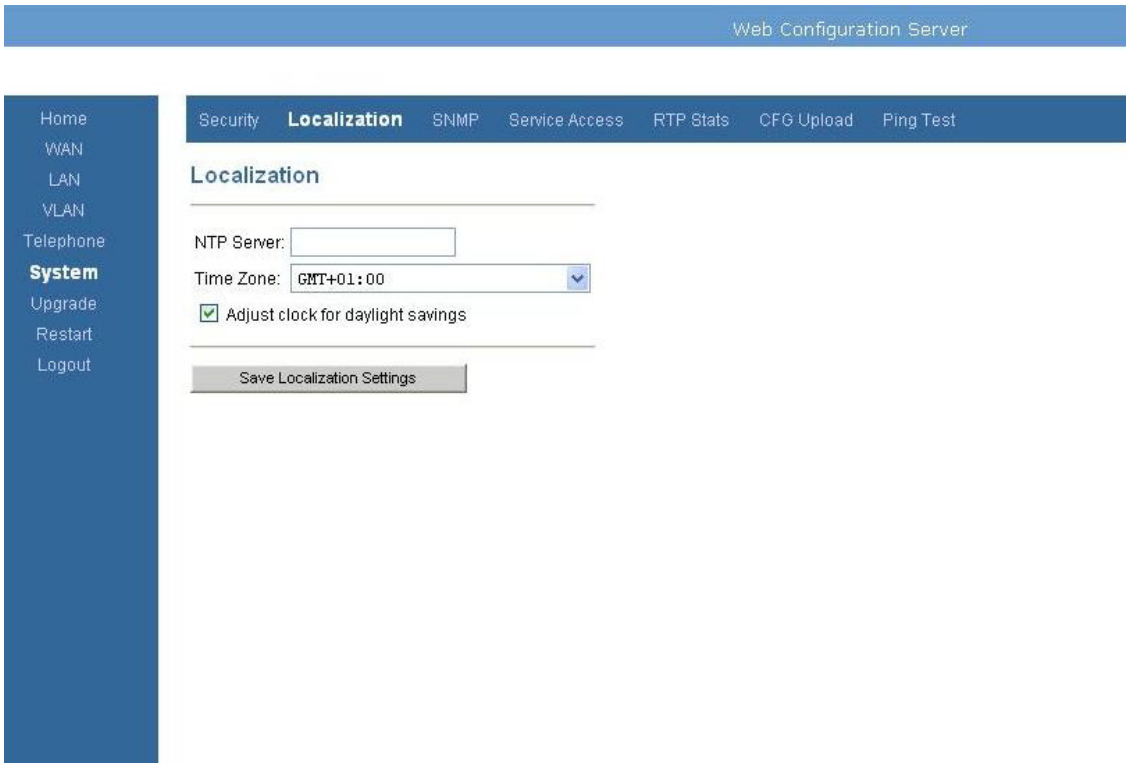

Figure 16: Localization Configuration

For explanation of the different functions, see page 26.

Table 12 Localization Configuration Settings

Function	Description
NTP Server	Specify the address of the NTP-server
Time Zone	Specify the time zone where the DRG22i is located
Daylight savings	By checking **Adjust to daylight savings** the DRG22i will set the time one hour ahead.

For the settings to take effect, click **Save Localizations Settings,** and restart the DRG22i.

2.16 SNMP CONFIGURATION

The Simple Network Management Protocol (SNMP) is used almost exclusively in TCP/IP networks, see below. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

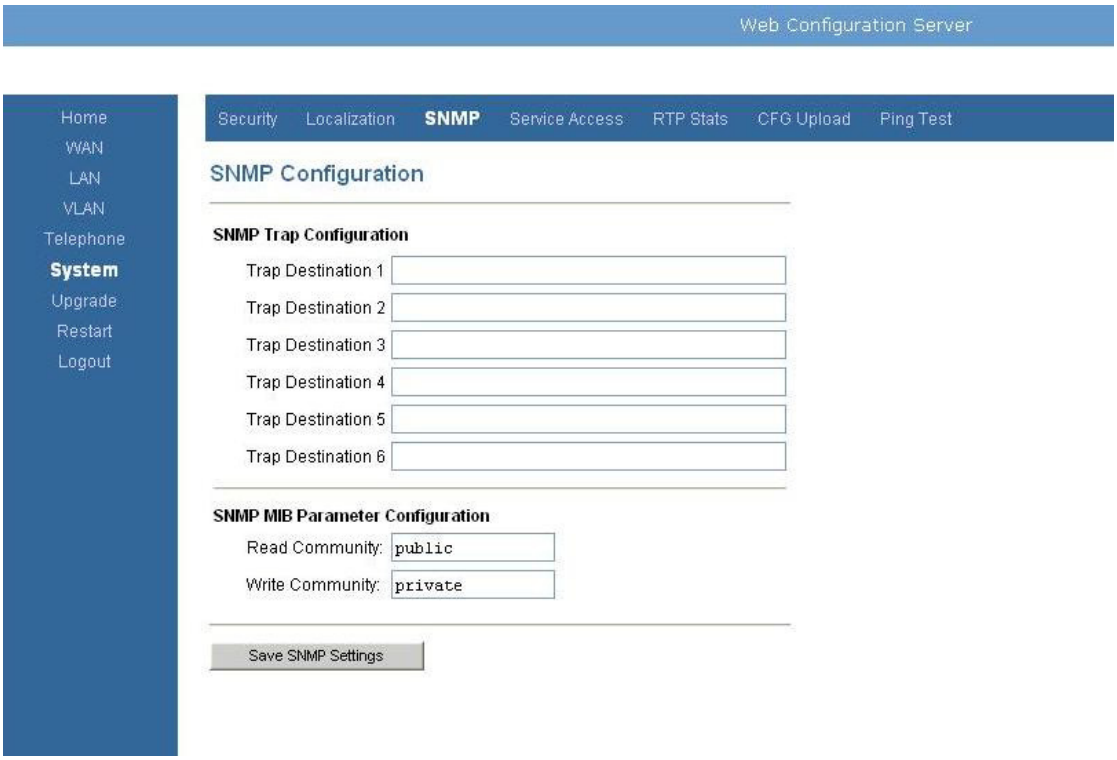

Figure 17: SNMP Configuration

For an explanation of the different functions, see page 27.

Table 13 SNMP Configuration Settings

Function	Description
SNMP Trap Configuration	Used for configuring multiple SNMP Trap Destinations to which the DRG22i will send SNMP Traps
Trap Destination 1	Specify the first address to which SNMP traps are sent
Trap Destination 2	Specify the second address to which SNMP traps are sent
Trap Destination 3	And so on
SNMP MIB Parameter Configuration	Configure Read and Write SNMP Community
Read Community	Specify the read community key. The default value is public.
Write Community	Specify the write community key. The default value is private.

For the settings to take effect, click **Save SNMP Settings** , and restart the DRG22i.

2.17 SERVICE ACCESS

Service Access allows the operator to limit access to different services from both the LAN and WAN ports, see page 28.

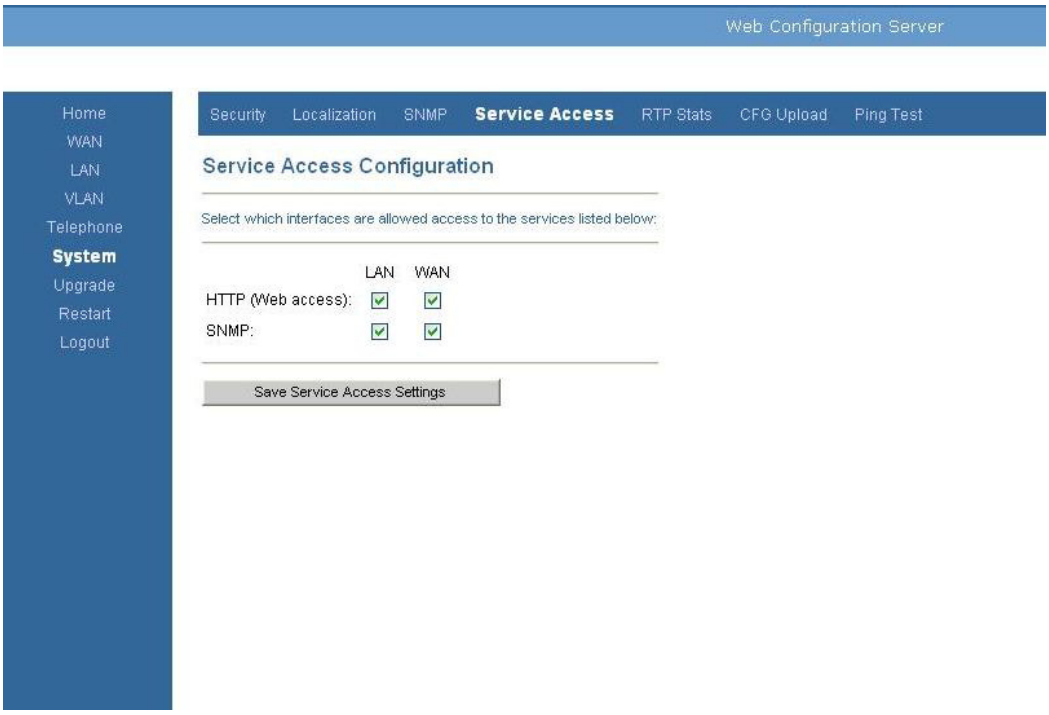

Figure 18: Service Access Configuration

For the settings to take effect, click **Save Service Access Settings,** and restart the DRG22i.

2.18 UPGRADE

Upgrade of the software and configuration using .ini files is done by downloading a file from a TFTP server, see page 29.

Recommended Procedure for Downloading Software to DRG

1. Place the file on a TFTP server.
2. Open an HTTP session on the DRG from an Internet browser.

   Logon with the password **DRGPASS**.

   If requested for a username enter **operator**.
3. Click on the 'upgrade' screen on the DRG 'HTTP' menu.
4. Specify the IP address of the TFTP server and the SW file name and click 'OK'.

   If only the file name is specified it is assumed that the file is located in the default root directory of the TFTP server.
5. After the download the DRG should restart automatically. The 'HTTP' menu will be refreshed after the restart.
6. **Verify** that parameters have not been changed due to the .ini file (for example, the Dial plan in the Telephony menu). For proper DRG settings, refer to the relevant documentation for the *MX-ONE TELEPHONY SYSTEM .*

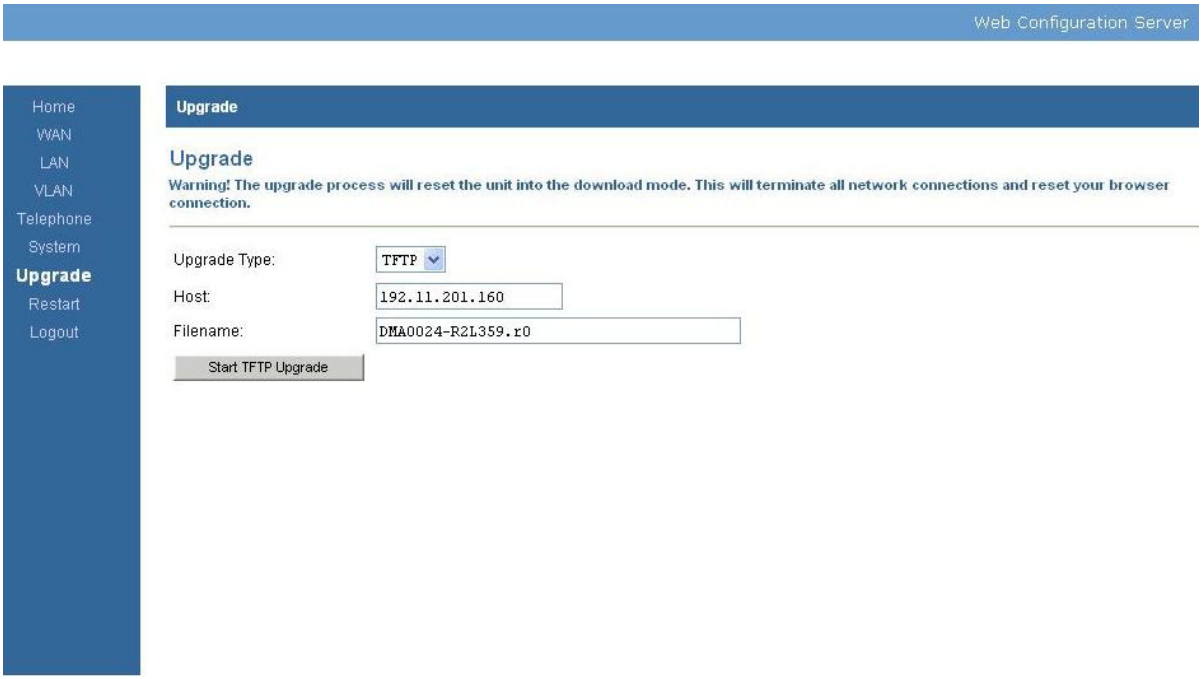

Figure 19: Upgrade Configuration

For explanation of the different functions, see below.

Table 14 Upgrade Configuration Settings

Function	Description
Upgrade Type	Select TFTP
Host	Specify the IP address of the TFTP server.
Filename	Specify the file that the DRG22i will download from TFTP server. This can either be the firmware image (DMA0024…) or the customized parameter settings file.

The download and installation are done automatically, including a restart of the DRG22i. When the installation is complete and the DRG22i has restarted, the startup page will be reloaded. If something goes wrong during download or installation, you will be notified as follows:

Downloader result codes (hexadecimal) :

0 (0x00) normal boot (no upgrade requested or needed)

bit-0 (0x01) upgrade requested or main app not valid

bit-1 (0x02) failed to download new image

bit-2 (0x04) TFTP server not defined

bit-3 (0x08) TFTP file not defined

bit-4 (0x10) TFTP session failed

bit-5 (0x20) CRC error in downloaded image

bit-6 (0x40) incompatible image

Examples: Try to download from a non-existing TFTP server result in code 0x7 (= 0x07)

- bit-2 0x04 TFTP server not defined plus…
- bit-1 0x02 failed to download new image plus…

- bit-0 0x01 upgrade requested or main app not valid

Try to download a non-existing file results in code 0xb (= 0x0b)

- bit-3 0x08 TFTP file not defined plus…
- bit-1 0x02 failed to download new image plus…
- bit-0 0x01 upgrade requested or main app not valid

2.19 RESTART

For the settings to take effect, the DRG22i must be restarted by clicking Restart, see page 31.

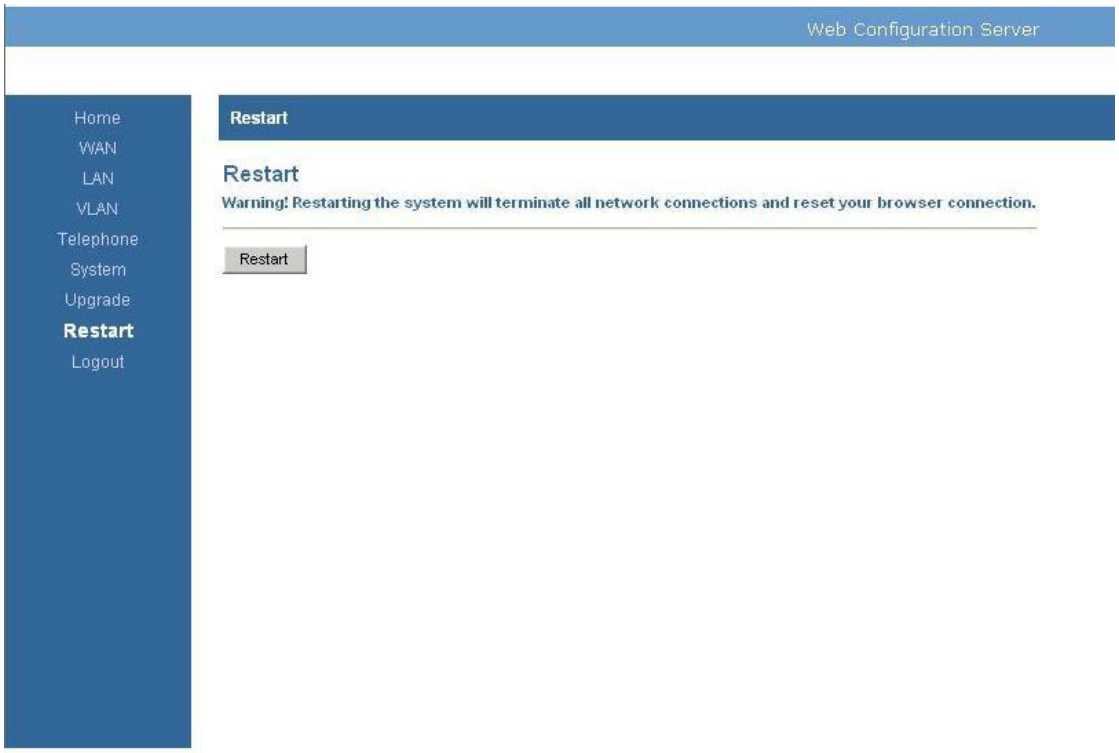

Figure 20: Restart

3 PERFORMING A FACTORY RESET

To reset, press and hold the Reset button on the back of the DRG22i for approximately 10 seconds. The flashing LEDs signal that the DRG22i is restarting. After this sequence, the DRG22i will be at **factory default** status and have the IP address 192.168.254.254 and subnet mask 255.255.255.0.