DRG

Digital Residential Gateway

DRG 11/22 SW R2N
Configuration Guide

Contents

1 Introduction

This configuration guide is for the products Digital Residential Gateway (DRG) 11 and DRG 22 and based on the R2N SW release.

This document describes the configuration of the DRG using:

- DHCP
- SNMP
- HDD
- PFDP
- Web GUI

The purpose of this document is to explain the basic functions in an understandable way. The information is intended for experienced personnel with knowledge of Ethernet networks and Voice-over-IP (VoIP) (SIP, H.323, and MGCP).

2 Configuration Parameters

This chapter provides a summary of configuration parameters in DRG 11/22, see the following table. The parameters are configured in the INI file, and the INI file must be encoded by a proprietary tool before it can be loaded by a DRG. For further information on this tool, contact the DRG TAC (Technical Assistant Center).

For more information of parameters in DRG 11/22, refer to *Appendix A- Configuration Parameters for DRG 11/22 SW R2N.*

No.	Parameter Name	No.	Parameter Name
1.	AJB_MAXDELAY	225.	L2CWTONE
2.	ALARM_SUPPRESS_LEVEL	226.	L2DOMAINNAME
3.	ALTERNATEGK	227.	L2FAXT38
4.	AUTO_JB_SWITCH	228.	L2FLASH_OOB
5.	BUSY	229.	L2GKPIP
6.	CALLAGENTADDRESS	230.	L2GKSIP
7.	CALLAGENTADDRESS2	231.	L2HAMODE
8.	CALLAGENTPORT	232.	L2MEDIADIRECTION
9.	CALLAGENTPORT2	233.	L2OUTBOUNDPROXY
10.	CALLERID1ONOFF	234.	L2OUTBOUNDPROXYPORT
11.	CALLERID2ONOFF	235.	L2PROXY_REQUIRE_PRIVACY
12.	CALLERIDNAME1	236.	L2REVPOLFORPAY
13.	CALLERIDNAME2	237.	L2SIPPIP
14.	CALLFORWARD	238.	L2SIPPPORT
15.	CALLSIG_TOS	239.	L2SIPSIP
16.	CALLSIGPORT1	240.	L2SIPSPORT
17.	CALLSIGPORT2	241.	L2SUSPENDTIMER
18.	CALLTRANS	242.	L2TRANSPORT_TYPE
19.	CALLTRANSATT	243.	LINE1AUTHPSWD
20.	CALLWAITING	244.	LINE1AUTHUSER
21.	CCBSOFF	245.	LINE1MSGACCOUNT
22.	CCBSON	246.	LINE1NUMBER
23.	CFNOANSWEROFF	247.	LINE1ONOFF
24.	CFNOANSWERON	248.	LINE1PORT
25.	CFONBUSYOFF	249.	LINE2AUTHPSWD
26.	CFONBUSYON	250.	LINE2AUTHUSER
27.	CFUNCONDITIONALOFF	251.	LINE2MSGACCOUNT
28.	CFUNCONDITIONALON	252.	LINE2NUMBER
29.	CICUSTOM	253.	LINE2ONOFF
30.	CLCUSTOM	254.	LINE2PORT
31.	CLIR	255.	MAXRSIPDELAY
32.	CLIR_OFF	256.	MGCPHAMODE
33.	CLIR_OFF_PREFIX	257.	MSG_WAIT_INDICATOR
34.	CLIR_ON	258.	NATIP
35.	CLIR_PREFIX	259.	NATMODE
36.	CONF	260.	NETWORK_BUSY
37.	CONFDROP	261.	NTPSERVERIP
38.	CONFIRM	262.	OFF_HOOK_WARN
39.	COUNTRY	263.	OUTOFBANDDTMF
40.	CUSTOM_1	264.	PIGGYBACK
41.	CUSTOM_10	265.	PORTFWDIP1
42.	CUSTOM_11	266.	PORTFWDIP2
43.	CUSTOM_12	267.	PORTFWDIP3
44.	CUSTOM_13	268.	PORTFWDIP4
45.	CUSTOM_14	269.	PORTFWDIP5

No.	Parameter Name	No.	Parameter Name
46.	CUSTOM_15	270.	PORTFWDIP6
47.	CUSTOM_16	271.	PORTFWDIP7
48.	CUSTOM_17	272.	PORTFWDIP8
49.	CUSTOM_18	273.	PORTFWDMAX1
50.	CUSTOM_19	274.	PORTFWDMAX2
51.	CUSTOM_2	275.	PORTFWDMAX3
52.	CUSTOM_20	276.	PORTFWDMAX4
53.	CUSTOM_3	277.	PORTFWDMAX5
54.	CUSTOM_4	278.	PORTFWDMAX6
55.	CUSTOM_5	279.	PORTFWDMAX7
56.	CUSTOM_6	280.	PORTFWDMAX8
57.	CUSTOM_7	281.	PORTFWDMIN1
58.	CUSTOM_8	282.	PORTFWDMIN2
59.	CUSTOM_9	283.	PORTFWDMIN3
60.	CW_OFF_PREFIX	284.	PORTFWDMIN4
61.	CWOFF	285.	PORTFWDMIN5
62.	CWON	286.	PORTFWDMIN6
63.	CWSTAT	287.	PORTFWDMIN7
64.	DHCPDOMAIN	288.	PORTFWDMIN8
65.	DHCPPOOLMAX	289.	PORTFWDPROT1
66.	DHCPPOOLMIN	290.	PORTFWDPROT2
67.	DHCPSERV	291.	PORTFWDPROT3
68.	DHCPSTATICID1	292.	PORTFWDPROT4
69.	DHCPSTATICID2	293.	PORTFWDPROT5
70.	DHCPSTATICID3	294.	PORTFWDPROT6
71.	DHCPSTATICID4	295.	PORTFWDPROT7
72.	DHCPSTATICID5	296.	PORTFWDPROT8
73.	DHCPSTATICID6	297.	POUNDSPEEDDIAL
74.	DHCPSTATICID7	298.	PRIORITYTAG_CALL
75.	DHCPSTATICID8	299.	PRIORITYTAG_RTP
76.	DHCPSTATICIDTYPE1	300.	PULSE_METER
77.	DHCPSTATICIDTYPE2	301.	RATELIMIT
78.	DHCPSTATICIDTYPE3	302.	REORDER
79.	DHCPSTATICIDTYPE4	303.	RESTARTTRAP
80.	DHCPSTATICIDTYPE5	304.	RETURNCALL
81.	DHCPSTATICIDTYPE6	305.	RING_AMPLITUDE
82.	DHCPSTATICIDTYPE7	306.	RING_CADENCE_0
83.	DHCPSTATICIDTYPE8	307.	RING_CADENCE_1
84.	DHCPSTATICIP1	308.	RING_CADENCE_2
85.	DHCPSTATICIP2	309.	RING_CADENCE_3
86.	DHCPSTATICIP3	310.	RING_CADENCE_4
87.	DHCPSTATICIP4	311.	RING_CADENCE_5
88.	DHCPSTATICIP5	312.	RING_CADENCE_6
89.	DHCPSTATICIP6	313.	RING_CADENCE_7
90.	DHCPSTATICIP7	314.	RING_CADENCE_8
91.	DHCPSTATICIP8	315.	RING_CADENCE_9
92.	DIALPLAN	316.	RING_FREQ
93.	DIALPULSE	317.	RINGBACK
94.	DIALTIMEOUT	318.	RINGSIGNAL1
95.	DIALTONE	319.	RINGSIGNAL2
96.	DND_OFF	320.	RINGTONE_1
97.	DND_ON	321.	RINGTONE_2
98.	DROP	322.	RINGTONE_3
99.	DS_DEFAULT	323.	RINGTONE_4
100.	DS_H323	324.	RINGTONE_5
101.	DS_MGCP	325.	RINGTONE_6
102.	DS_RTP	326.	RINGTONE_7

No.	Parameter Name	No.	Parameter Name
103.	DS_SIP	327.	RINGTONE_8
104.	DS_SNMP	328.	ROUTEDESTIP1
105.	DST	329.	ROUTEDESTIP2
106.	EARLYH245	330.	ROUTEDESTIP3
107.	ENAUTHFAILTRP	331.	ROUTEDESTIP4
108.	ENDPOINTDOMAINNAME	332.	ROUTEDESTIP5
109.	FASTCON	333.	ROUTEDESTIP6
110.	FAXTONEDETECT	334.	ROUTEDESTIP7
111.	FJB_DELAY	335.	ROUTEDESTIP8
112.	FLASH	336.	ROUTEGATEWAYIP1
113.	FLASHHOOKMAXTIMER	337.	ROUTEGATEWAYIP2
114.	FLASHHOOKMINTIMER	338.	ROUTEGATEWAYIP3
115.	FULLRRQ	339.	ROUTEGATEWAYIP4
116.	GKDISCOVERY	340.	ROUTEGATEWAYIP5
117.	H235K	341.	ROUTEGATEWAYIP6
118.	H235MODE	342.	ROUTEGATEWAYIP7
119.	H323_URLID	343.	ROUTEGATEWAYIP8
120.	H323ALIAS1	344.	ROUTEINT1
121.	H323ALIAS2	345.	ROUTEINT2
122.	HOLD	346.	ROUTEINT3
123.	HTTPLAN	347.	ROUTEINT4
124.	HTTPWAN	348.	ROUTEINT5
125.	IF0CICUSTOM	349.	ROUTEINT6
126.	IF0DHCP	350.	ROUTEINT7
127.	IF0DNSDOMAINNAME	351.	ROUTEINT8
128.	IF0DNSHOSTNAME	352.	ROUTEMETRIC1
129.	IF0ENABLED	353.	ROUTEMETRIC2
130.	IF0IPADDRESS	354.	ROUTEMETRIC3
131.	IF0IPDNS	355.	ROUTEMETRIC4
132.	IF0IPGATEWAY	356.	ROUTEMETRIC5
133.	IF0IPNETMASK	357.	ROUTEMETRIC6
134.	IF0L3PROT	358.	ROUTEMETRIC7
135.	IF0NETCONF	359.	ROUTEMETRIC8
136.	IF0PPP_ECHOCOUNT	360.	ROUTESUBNETMASK1
137.	IF0PPP_ECHOTO	361.	ROUTESUBNETMASK2
138.	IF0PPP_IDLETO	362.	ROUTESUBNETMASK3
139.	IF0PPP_PASSWORD	363.	ROUTESUBNETMASK4
140.	IF0PPP_USERNAME	364.	ROUTESUBNETMASK5
141.	IF0PRIORITYTAG	365.	ROUTESUBNETMASK6
142.	IF0STANDARDCLIENTID	366.	ROUTESUBNETMASK7
143.	IF0VLANTAG	367.	ROUTESUBNETMASK8
144.	IF1CICUSTOM	368.	RTPPORTEND
145.	IF1DHCP	369.	RTPPORTSTART
146.	IF1DNSDOMAINNAME	370.	RXGAIN
147.	IF1DNSHOSTNAME	371.	SDP_OFFER_MULTIMEDIA
148.	IF1ENABLED	372.	SIP_INVITE_NO_SDP
149.	IF1IPADDRESS	373.	SIP_INVITE_TIMER
150.	IF1IPDNS	374.	SIP_NOTIFY_KEEPALIVE
151.	IF1IPGATEWAY	375.	SIP_NOTIFY_NAT_MAPPING_TIMEOUT
152.	IF1IPNETMASK	376.	SIP_SEND_PRACK
153.	IF1NETCONF	377.	SIP_SESSION_TIMER
154.	IF1PRIORITYTAG	378.	SIP_TEL_URI
155.	IF1STANDARDCLIENTID	379.	SIP_URI_USER_PARAM
156.	IF1VLANTAG	380.	SNMPENABLE
157.	ILIM	381.	SNMPLAN
158.	IMPEDANCE	382.	SNMPREADCOMMUNITY
159.	INBANDDTMF	383.	SNMPWAN

No.	Parameter Name	No.	Parameter Name
160.	INCSTANDPORT	384.	SNMPWRITECOMMUNITY
161.	JB_TYPE	385.	SQUELCHDTMF
162.	KEEPALIVETIME1	386.	STEALTHPING
163.	KEEPALIVETIME2	387.	STP
164.	KEYPADTYPE	388.	STUNCLIENTMODE
165.	L1_3PC	389.	STUNDEFSERVERI
166.	L1_LOCAL_RINGING	390.	STUNDEFSERVERII
167.	L1ALTGKCHK	391.	STUNDEFSERVERIII
168.	L1ALTGKCHKINTERVAL	392.	STUNSERVERADDR
169.	L1ANONYMOUS_DISPLAY_NAME	393.	STUNSERVERPORT
170.	L1ANONYMOUS_FROM_HEADER	394.	STUTTER_DIAL
171.	L1ANONYMOUS_TO_HEADER	395.	SYSLOG_SVR
172.	L1ATTXFER	396.	T1
173.	L1C5S	397.	T2
174.	L1CALLFWDIND	398.	T3
175.	L1CALLFWDRMD	399.	T38_ECC_COUNT
176.	L1CCBSDURATION	400.	T38_ECC_COUNT_IMAGE
177.	L1CCBSINTERVAL	401.	T38ECT
178.	L1CF	402.	T38FAX1
179.	L1CFUNCOND	403.	T38FAX2
180.	L1CFUNCONDNUM	404.	T38PROT
181.	L1CLIR	405.	T38RMAN
182.	L1CODEC1	406.	T4
183.	L1CODEC2	407.	T5
184.	L1CODEC3	408.	T6
185.	L1CONFXFER	409.	TELEVENTPAYLOAD
186.	L1CWTONE	410.	TERM1NAME
187.	L1DOMAINNAME	411.	TERM2NAME
188.	L1FAXT38	412.	TERMIDFQDN
189.	L1FLASH_OOB	413.	THRUPUTBITMAX
190.	L1GKPIP	414.	THRUPUTPKTMAX
191.	L1GKSIP	415.	THRUPUTWINSIZE
192.	L1HAMODE	416.	TIMEZONE
193.	L1MEDIADIRECTION	417.	TOSLIMITER
194.	L1OUTBOUNDPROXY	418.	TRAPHOSTCOMMUNITY
195.	L1OUTBOUNDPROXYPORT	419.	TRAPHOSTIPADDRESS
196.	L1PROXY_REQUIRE_PRIVACY	420.	TUNNELH245
197.	L1REVPOLFORPAY	421.	TXGAIN
198.	L1SIPPIP	422.	USERAGENT
199.	L1SIPPPORT	423.	V1
200.	L1SIPSIP	424.	V10
201.	L1SIPSPORT	425.	V11
202.	L1SUSPENDTIMER	426.	V12
203.	L1TRANSPORT_TYPE	427.	V13
204.	L2_3PC	428.	V14
205.	L2_LOCAL_RINGING	429.	V15
206.	L2ALTGKCHK	430.	V16
207.	L2ALTGKCHKINTERVAL	431.	V2
208.	L2ANONYMOUS_DISPLAY_NAME	432.	V3
209.	L2ANONYMOUS_FROM_HEADER	433.	V4
210.	L2ANONYMOUS_TO_HEADER	434.	V5
211.	L2ATTXFER	435.	V6
212.	L2C5S	436.	V7
213.	L2CALLFWDIND	437.	V8
214.	L2CALLFWDRMD	438.	V9
215.	L2CCBSDURATION	439.	VER_MGCP10
216.	L2CCBSINTERVAL	440.	VER_NCS10

No.	Parameter Name	No.	Parameter Name
217.	L2CF	441.	VLANLIMITER
218.	L2CFUNCOND	442.	VLANTAG_CALL
219.	L2CFUNCONDNUM	443.	VLANTAG_RTP
220.	L2CLIR	444.	WANMACSPOOF
221.	L2CODEC1	445.	WEB_ROOT
222.	L2CODEC2	446.	WEB_USER
223.	L2CODEC3	447.	WWWONOFF
224.	L2CONFXFER	448.	WWWPORT

3 Configuration using DHCP

This chapter describes how to configure DRGs by using DHCP. The DHCP options are in effect when the DRG is in one of the following cases:

- When requesting or renewing the IP address of the DRG from the DHCP server
- When rebooting after power down
- When rebooting after configuration in main software or after loading default configuration file (a.k.a operators default file)
- When renewing its IP-address after timer T1 or T2 expiration

NOTE! The DRG only handles DHCP options when main application is loaded. When in downloader mode, it does not honor DHCP option 43.

The table below lists the DHCP options supported in DRG 11/22:

Option	Description	Example	Explanation
1	Subnet mask		
2	Time offset		
3	Default router		
6	Domain name server		
12	Hostname		
15	Domain name		
43	Vendor specific information		
51	Lease time		
53	DHCP message type		
54	Server identifier		
55	Parameter request list		
60	Vendor class identifier	drg-drg1122-DMA0021-R2N01	
61	Client identifier		
66	TFTP server name	tftp.example.com	
67	Boot filename	drg/drg1122/filename.r0	
82	Relay agent information		
120	SIP server		
224	HTTP server configuration	on,8080,600	"on": the HTTP server; "8080": the TCP port using by the HTTP server; "600": the duration for a successful login
225	VoIP configuration	192.168.32.250, sip.example.com, 5060, 1200	

226	VoIP line number	111, 222, 444	
227	VoIP username	Kalle Anka	
228	VoIP password	Secret, secret2, secret3	
229	VoIP callerID	Kalle.Anka, 444	
230	VoIP domain	sip.example.com	
231	VoIP CLIP	on, off, ”sweden”	
232	VoIP dialplan		
233	VoIP interdigit delay		
234	Management & Voice VLAN configuration	VVVV, P	“VVVV”: the VLAN ID; “P”: the priority
235	Layer 3 QoS configuration	30, 25, 63	
236–239	Reserved		
240	SNMP management server		
241	HDD management server	cdsp://192.168.1.1:8080 /cdsp2	
242	STUN server	stun.example.org, 10.0.0.2	
243–254	Reserved		
255	End option		

For more information on the DHCP options, refer to RFC 2132 and RFC 3942.

3.1 Description

3.1.1 Option 43 – Vendor Specific

To separate the end user specific configuration parameters from the service related configuration parameters, any parameters that are end user specific can be returned in an option 43 response message. It is possible to use encapsulated[1] vendor options in both directions; from the DHCP server to the DRG and from the DRG to the DHCP server. The parameters that can be configured in Option 43 are illustrated in the following table:

[1] Refer to RFC 2132 section 8.4

Option	Parameter	Type	Direction	Example
1	Configuration filename	Text	Both	example.ini
2	Firmware version	Text	Both	DMA0021-R2N01.r0
3	Upgrade method	Text	Server–DRG	auto, tftp, http
4	Upgrade server	IP address	Server–DRG	tftp.example.org
5	VoIP line control	Array of Boolean	Server–DRG	On or off
6	VoIP line status	Array of Boolean	DRG–Server	On or off

NOTE! The DRG supports DHCP Option43 in plain text format. The DRG automatically detects the format and choose the correct handler. When Option 43 in both plain text format and encapsulated options are used simultaneously, the latter one in the message takes the higher priority.

3.1.2 Option 60–Class ID

Option 60 is used to identify the vendor class using a string that includes information for the platform, module and firmware version, e.g. "drg-drg1122 -DMA0021-R2N01". The string can be overwritten by an operator and any arbitrary string can be used.

3.1.3 Option 61–Client ID

Option 61 is used to identify the DHCP client. This field (7 bytes) is expected to contain the DRG MAC address, but it can be changed to other value.

3.1.4 Option224– HTTP Server Configuration

Option 224 is used to configure the HTTP server embedded in the DRG. The syntax of the option is a record of {boolean, unsigned integer 16, unsigned integer 32}, which defines {server on or off, TCP port used by HTTP server, duration for a successful login}.

3.1.5 Option225– VoIP Configuration

Option 225 is used to configure the VoIP server. The syntax of the option is an array of {IP-address, IP-address, unsigned integer 16, unsigned integer 16, unsigned integer 32}, which defines {serve224r 1, server 2, port 1, port 2, keep alive}.

3.1.6 Option226– VoIP Line Number

Option 226 is used to configure the VoIP line number. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	Line number 1, e.g. 111
2	Line number 2, e.g. 222
3	Line Number 3, e.g. 333
4	Line Number 4, e.g. 444

3.1.7 Option227– VoIP Username

Option 227 is used to configure the VoIP user name. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	User name 1, e.g. Hewey
2	User name 2, e.g. Dewey
3	User name 3, e.g. Newey
4	User name 4, e.g. Lewey

3.1.8 Option 228–VoIP Password

Option 228 is defined to configure the VoIP password. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	password 1, e.g. secret1
2	password 2, e.g. secret2
3	password 3, e.g. secret3
4	password 4, e.g. secret4

3.1.9 Option229–VoIP Caller ID

Option 229 is defined to configure the VoIP caller ID. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	Caller ID 1, e.g. H. Duck
2	Caller ID 2, e.g. D. Duck
3	Caller ID 3, e.g. N. Duck
4	Caller ID 4, e.g. L. Duck

3.1.10 Option230– VoIP Domain

Option 230 is defined to configure the VoIP domain. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	Domain 1, e.g. sip.example.com
2	Domain 2, e.g. sip2.example.com

3.1.11 Option 231–VoIP CLIP

Option 231 is defined to configure the VoIP CLIP. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	Line 1 CLIP enable, e.g. on
2	Line 2 CLIP enable, e.g. on
3	Line 3 CLIP enable, e.g. on
4	Line 4 CLIP enable, e.g. on
5	CLIP type, e.g. “Sweden”

3.1.12 Option232–VoIP Dial Plan

Option 232 is defined to configure the dial plan. The syntax of the option is a text string with maximum length of 255 characters.

3.1.13 Option233– VoIP Inter-digit Delay

Option 233 is defined to configure the VoIP inter-digit delay. The syntax of the option is an unsigned integer 8.

Option	
1	User name 1, e.g. Hewey
2	User name 2, e.g. Dewey
3	User name 3, e.g. Newey
4	User name 4, e.g. Lewey

3.1.14 Option234–VLAN Configuration

Option 234 is defined to configure the management and voice VLAN. The syntax of the option uses encapsulated vendor-specific options. Refer to the example in Section 3.2.2 for more information.

Option	
1	User name 1, e.g. Hewey
2	User name 2, e.g. Dewey
3	User name 3, e.g. Newey
4	User name 4, e.g. Lewey

3.1.15 Option235– Layer 3 QoS Configuration

Option 235 is defined to configure the layer 3 QoS parameters. The syntax of the option is a record of integer.

3.1.16 Option240– SNMP management server

Option 240 is defined to configure the SNMP management server. The syntax of the option is an array of IP address.

3.1.17 Option 241–HDD Management Server

Option 241 is defined for the Home Device Director (HDD) management server. The IP address of the HDD server is specified in this field.

3.1.18 Option242– STUN Server

Option 242 is defined to configure the STUN server. The syntax of this option is an array of IP address.

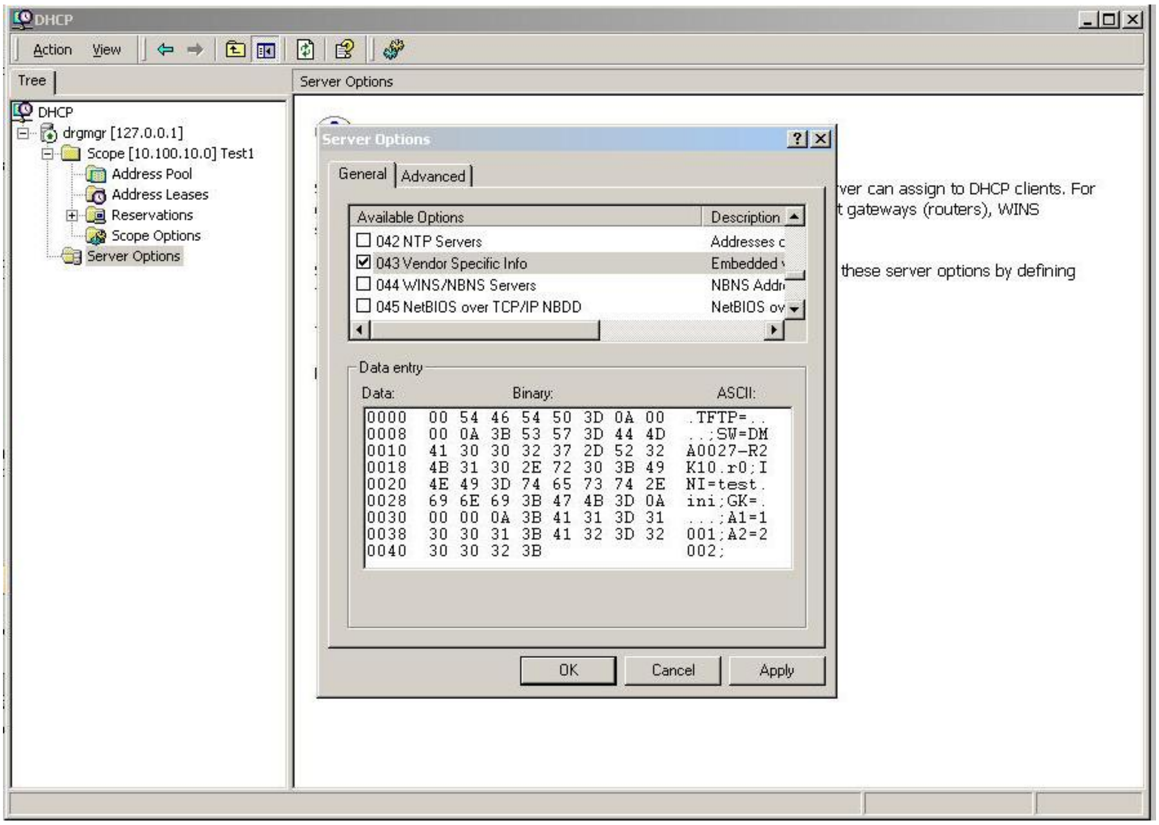
3.2 Configuration on Different Platforms

3.2.1 Windows

On Windows system, follow the below steps to configure the parameters described in this chapter:

1. Go to Windows **Administrative Tools**.
2. Open **DHCP**.
3. Right click **Server Options**.
4. On the Action menu, select **Configure Options**.
5. In the Configuration Options dialog box, click **General** tab.
6. In the list of **Available Options**, select the **043 Vendor Specific Info** check box.
7. Configure the parameters in the **ASCII** field.

Figure 3-1 DHCP configuration on Windows



Available Options	Description
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

```
0000   00 54 46 54 50 3D 0A 00   .TFTP=..
0008   00 0A 3B 53 57 3D 44 4D   ..;SW=DM
0010   41 30 30 32 37 2D 52 32   A0027-R2
0018   4B 31 30 2E 72 30 3B 49   K10.r0;I
0020   4E 49 3D 74 65 73 74 2E   NI=test.
0028   69 6E 69 3B 47 4B 3D 0A   ini;GK=.
0030   00 00 0A 3B 41 31 3D 31   ...;A1=1
0038   30 30 31 3B 41 32 3D 32   001;A2=2
0040   30 30 32 3B               002;
```

ver can assign to DHCP clients. For
t gateways (routers), WINS

these server options by defining

3.2.2 Linux/Unix

On Linux/Unix systems, you must configure the parameters as described in this chapter, in the file `/etc/dhcpd.conf`. Refer to the sample DHCP configuration file below:

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
#

############################      Start      of      Local      Definitions
########################
# vendor-specific option space
# It can be used as control from server, or status from client to server
option space drg;
option drg.config-filename     code 1    = text;
option drg.firmware-filename   code 2    = text;
option drg.upgrade-method      code 3    = text;  # auto, http, or tftp
option drg.upgrade-server      code 4    = ip-address;
option drg.voip-port-control   code 5    = array of boolean;
option drg.voip-port-status    code 6    = array of boolean;
# Production use only
option drg.mac-address                   code 7     = text;
option drg.default-filename    code 8    = text;

# CLIP option space
option space clip;
option clip.enable             code 1 = array of boolean;
option clip.type               code 2 = text;

# domain option space
option space domain;
option domain.domain1                    code 1 = text;
option domain.domain2                    code 2 = text;
option domain.domain3                    code 3 = text;
option domain.domain4                    code 4 = text;

# callerid option space
option space callerid;
option callerid.name1                    code 1 = text;
option callerid.name2                    code 2 = text;
option callerid.name3                    code 3 = text;
option callerid.name4                    code 4 = text;

# username option space
option space username;
option username.username1      code 1 = text;
option username.username2      code 2 = text;
option username.username3      code 3 = text;
option username.username4      code 4 = text;

# password option space
option space password;
option password.password1      code 1 = text;
option password.password2      code 2 = text;
option password.password3      code 3 = text;
option password.password4      code 4 = text;

# line option space
option space line; # Number associated with a line
option line.number1            code 1 = text;
option line.number2            code 2 = text;
option line.number3           code 3 = text;
option line.number4           code 4 = text;

# config option space
option space config;
option config.server1                    code 1 = ip-address;
option config.server2                    code 2 = ip-address;
option config.port            code 3 = unsigned integer 16;
option config.keepalive                  code 4 = unsigned integer 32;

# vlan option space
option space vlan;
option vlan.vlan-mgmt                            code 1      =   {unsigned
integer 16, unsigned integer 8}; # vid, pri
option vlan.vlan-voip-signalling         code 2    = {unsigned integer 16,
unsigned integer 8};
option vlan.vlan-voip-media              code 3    = {unsigned integer 16,
unsigned integer 8};

# l3qos option space
option space l3qos;
option l3qos.diffserv-mgmt               code 1     = unsigned integer 8;
option l3qos.diffserv-voip-signalling   code 2      = unsigned integer 8;
option l3qos.diffserv-voip-media         code 3     = unsigned integer 8;

# Standard options
option log-servers            code 7     = array of ip-address;
option vendor-class-identifier  code 60   = text;
option client-identifier      code 61    = text;
option tftp-server-name                  code 66    = text;
option bootfile-name          code 67    = text;
option user-dhcp-class                   code 77    = text;
option sip-server             code 120= array of ip-address;

# Packetfront private options
# Server configuration
option snmp-server            code 240   = array of ip-address;
option hdd-server             code 241   = array of ip-address;
option stun-server            code 242   = array of ip-address;

# VLAN configuration
option vlan-mgmt                code 234 = encapsulate vlan;
# QoS
option l3qos-mgmt             code 235   = encapsulate l3qos;

# HTTP server configuration
option http-server            code 224   = {boolean, unsigned integer 16,
unsigned integer 32}; # enable, port, timeout

# VoIP confguration
option voip-config            code 225   =  array  of  {ip-address,  ip-
address, unsigned integer 16, unsigned integer 32}; # server1, server2,
port, keepalive
#option voip-line-number                 code 226   = encapsulate line;
option line-encapsulation     code 226   = encapsulate line;
option voip-username          code 227   = encapsulate username;
option voip-password          code 228   = encapsulate password;
option voip-callerid          code 229   = encapsulate callerid;
option voip-domain            code 230   = encapsulate domain;
option voip-clip              code 231   = encapsulate clip;
option voip-dialplan          code 232   = text; # Maximum of 255 chars
option voip-interdigit-delay  code 233   = unsigned integer 8;
#################### End of Local Definitions ####################
```

```
####################################################################
############################ Configurations #######################
ddns-update-style interim;
ping-check true;
ignore client-updates;

subnet 172.19.33.0 netmask 255.255.255.0 {
  range 172.19.33.71 172.19.33.74;
  max-lease-time 20;
  default-lease-time 20;

  group {
      # Configuration for a specific CPE device
      host 000f5de00037 {
      hardware ethernet 00:0f:5d:e0:00:37;
      option domain-name-servers 172.19.33.147,172.19.33.56;
      option dhcp-parameter-request-list = concat(option dhcp-parameter-request-list,3A,3B);
      option ntp-server 172.19.33.147;
      option host-name "fthostname";
      option domain-name domain-test;
      option dhcp-renewal-time 3000;
      option dhcp-rebinding-time 300;
      vendor-option-space drg;
      option drg.default-filename "vgw.def";
      option drg.voip-port-control off,off,off,off;
      option drg.config-filename "auto://172.19.33.70/dummy3.ini";
      option drg.upgrade-method "tftp";  #auto, http or tftp
      option drg.upgrade-server 172.19.33.147;
      option drg.firmware-filename "DMA0121-ALPHA131.r0";
      option http-server on 8080 30;  #224
      option voip-config 1.1.1.1 2.2.2.2 16 32, 3.3.3.3 4.4.4.4 16 32; #225
      option line.number1      "111"; #226
      option line.number4      "444"; #226
      option username.username1 "u1";  #227
      option username.username2 "u2";  #227
      option password.password1 "p1";  #228
      option password.password2 "p2";  #228
      option callerid.name1 "c1"; #229
      option callerid.name2 "c2"; #229
      option domain.domain1 "d1"; #230
      option domain.domain2 "d2"; #230
      option clip.enable on, off; #231
      option clip.type "Sweden";   #231
      option voip-dialplan "xx.#"; #232
      option voip-interdigit-delay 10;   #233
      option vlan.vlan-mgmt 1 1;                  #234
      option vlan.vlan-voip-signalling 2 2;       #234
      option vlan.vlan-voip-media     3 3;        #234
      option l3qos.diffserv-mgmt 1;            #235
      option l3qos.diffserv-voip-signalling 2; #235
      option l3qos.diffserv-voip-media 3;      #235
      option snmp-server 1.1.1.1, 2.2.2.2;  #240
      option hdd-server 1.1.1.1, 2.2.2.2;   #241
      option stun-server 1.1.1.1, 2.2.2.2;  #242
      option tftp-server-name "172.19.33.147";  #66
      option bootfile-name "DMA0121-ALPHA131.r0"; #67
  }

  # Special group only used for production sites
  host 00-00-00-00-00-00 {
    hardware ethernet 00:00:00:00:00:00;
    next-server 10.0.0.2;
    vendor-option-space drg;
    option drg.mac-address "000f5de00037";
  }
}

}
```

4 Configuration using SNMP

This chapter introduces the manageable information in the DRG system. The DRG has an SNMP-agent implemented. An SNMP management station sends SNMP requests to an SNMP-agent and receives and processes SNMP notifications and traps. An SNMP-agent is responding to SNMP requests and generating SNMP traps.

If you have any trouble configuring the DRGs using SNMP, contact the DRG TAC.

4.1 The General MIB Tree

The following tree shows the public MIB information structure for SIP releases:

```
+--iso(1)
   |
   +--org(3)
      |
      +--dod(6)
         |
         +--internet(1)
            |
            |
            +--mgmt(2)
            |  |
            |  +--mib-2(1)
            |
            |
            +--private(4)
            |  |
            |  +--enterprises(1)
            |     |
            |     +--packetfront(9303)
            |        |
            |        +--pfMgmt(4)
            |           |
            |           +--pfDrgMib(3)
            |           |
            |           +--pfVoipMib(4)
            |           |
            |           +--serviceHttpServer(5)
            |           |
            |           +--pfDrg100Mib(9)
            |           |
            |           +--pfStunClient(12)
            |
            |
            +--snmpV2(6)
               |
               +--snmpDomain(1)
               |  |
               |  +--snmpUDPDomain(1)
               |
               +--snmpModules(3)
                  |
                  +--snmpTargetMIB(12)
                  |
                  +--snmpNotificationMIB(13)
```

The following tree shows the public MIB information structure for other releases (H.323 and MGCP):

```
+--iso(1)
   |
   +--org(3)
      |
      +--dod(6)
         |
         +--internet(1)
            |
            |
            +--mgmt(2)
            |  |
            |  +--mib-2(1)
            |
            |
            +--private(4)
            |  |
            |  +--enterprises(1)
            |     |
            |     +--packetfront(9303)
            |        |
            |        +--pfMgmt(4)
            |           |
            |           +--pfDrgMib(3)
            |           |
            |           +--pfVoipMib(4)
            |           |
            |           +--serviceHttpServer(5)
            |           |
            |           +--pfDrg100Mib(9)
            |
            |
            +--snmpV2(6)
               |
               +--snmpDomain(1)
               |  |
               |  +--snmpUDPDomain(1)
               |
               +--snmpModules(3)
                  |
                  +--snmpTargetMIB(12)
                  |
                  +--snmpNotificationMIB(13)
```

4.2 SNMP MIB-2

MIB-2 defines the management information base for network management of TCP/IP based networks. The sub-layer definitions are extended to IF MIB, IP MIB, SNMPv2 MIB, TCP MIB and UDP MIB respectively.

4.2.1 IF MIB

The IF MIB module describes generic objects for network interface sub-layers. The MIB is an updated version of MIB-2's ifTable, and incorporates the extensions defined in RFC 1229.

IF MIB is published in RFC 2863.

4.2.1.1 Capability Report

- Mib-2 interfaces group
  - **`ifTable`** is not supported.

4.2.2 IP MIB

The IP MIB describes objects for managing IP and ICMP implementations, but excluding their management of IP routes.

4.2.2.1 Capability Report

- IP group
  - table **`ipAdEnt`** is not supported
  - variation ipForwarding is not supported

Variation	Access	Description
ipAdEntAddr	read-only	unsupported
ipAdEntIfIndex	read-only	unsupported
ipAdEntNetMask	read-only	unsupported
ipAdEntBcastAddr	read-only	unsupported
ipAdEntReasmMaxSize	read-only	unsupported

- ICMP group
  - All OIDs are supported

4.2.3 SNMPv2 MIB

The SNMPv2 MIB describes objects for managing SNMPv2 implementations.

4.2.3.1 Capability Report

Variation	Access	Description
sysContact	read-only	only read supported, write of this object is not supported

sysName	read-only	only read supported, write of this object is not supported
sysLocation	read-only	only read supported, write of this object is not supported
sysServices	read-only	unsupported, return a faulty value
sysORLastChange	read-only	unsupported, always return 0
sysORUpTime	read-only	unsupported, always return 0

4.2.4 TCP MIB

The TCP MIB describes objects for managing TCP implementations.

4.2.4.1 Capability Report

All OIDs are supported.

4.2.5 UDP MIB

The UDP MIB describes objects for managing UDP implementations.

4.2.5.1 Capability Report

All OIDs are supported.

4.2.6 Configuration Examples

4.2.6.1 Print out the value of IF-MIB::ifNumber

```
% snmpget -v 2c -c public <IpAddress> IF-MIB::ifNumber.0
IF-MIB::ifNumber.0 = INTEGER: 2
```

4.2.6.2 Print out the udp table of the DRG

```
% snmpwalk -v 2c -c public <IpAddress> UDP-MIB::udpTable
UDP-MIB::udpLocalAddress.0.0.0.0.0 = IpAddress: 0.0.0.0
UDP-MIB::udpLocalAddress.0.0.0.0.68 = IpAddress: 0.0.0.0
UDP-MIB::udpLocalAddress.0.0.0.0.161 = IpAddress: 0.0.0.0
UDP-MIB::udpLocalAddress.0.0.0.0.162 = IpAddress: 0.0.0.0
UDP-MIB::udpLocalAddress.0.0.0.0.1024 = IpAddress: 0.0.0.0
UDP-MIB::udpLocalAddress.172.19.33.194.520 = IpAddress: 172.19.33.194
UDP-MIB::udpLocalAddress.192.168.1.1.53 = IpAddress: 192.168.1.1
UDP-MIB::udpLocalAddress.192.168.1.1.67 = IpAddress: 192.168.1.1
UDP-MIB::udpLocalAddress.192.168.1.1.520 = IpAddress: 192.168.1.1
UDP-MIB::udpLocalPort.0.0.0.0.0 = INTEGER: 0
UDP-MIB::udpLocalPort.0.0.0.0.68 = INTEGER: 68
UDP-MIB::udpLocalPort.0.0.0.0.161 = INTEGER: 161
UDP-MIB::udpLocalPort.0.0.0.0.162 = INTEGER: 162
UDP-MIB::udpLocalPort.0.0.0.0.1024 = INTEGER: 1024
UDP-MIB::udpLocalPort.172.19.33.194.520 = INTEGER: 520
UDP-MIB::udpLocalPort.192.168.1.1.53 = INTEGER: 53
UDP-MIB::udpLocalPort.192.168.1.1.67 = INTEGER: 67
UDP-MIB::udpLocalPort.192.168.1.1.520 = INTEGER: 520
```

4.3 DRG Enterprises MIB

The enterprise MIBs defined to manage DRG 11/22 is introduced as follows. Configuration examples are also given for each enterprise MIB. You can find their detailed definitions in the appendices listed below:

MIB	Appendix
PACKETFRONT-DRG-MIB	B
PACKETFRONT-DRG100-MIB	C
PACKETFRONT-HTTP-MIB	D
PACKETFRONT-VOIP-MIB	E
PACKETFRONT-STUN-MIB	F

Note: The PACKETFRONT-STUN-MIB is only supported in the SIP release.

4.3.1 PACKETFRONT-DRG-MIB

4.3.1.1 Capability Report

Only non-supported objects are listed in this section. If an object is fully supported as described in the MIB definition, it is not listed here.

- **`vlanTp`**

Group **`vlanTp`** is not supported in this release.

- **`vlanStatic`**

Group **`vlanStatic`** is not supported in this release.

4.3.1.2 Configuration Examples

4.3.1.2.1 Example 1: get product information

In this example, some product information is obtained, including the product platform, software or firmware image revision and product MAC address.

1. Get the product platform.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::productPlatform.0
PACKETFRONT-DRG-MIB::productPlatform.0 = STRING: "DRG100"
```

2. Get the software image (main application) revision.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::productSwImageRev.0
PACKETFRONT-DRG-MIB::productSwImageRev.0 = STRING: "DMA0021-R2N01"
```

3. Get the firmware image (downloader) revision.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::productFwImageRev.0
PACKETFRONT-DRG-MIB::productFwImageRev.0 = STRING: "cxc_132_4898-R3B25"
```

4. Get the DRG MAC address.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::productMacAddress.0
PACKETFRONT-DRG-MIB::productMacAddress.0 = STRING: 0:f:5d:fe:7b:55
```

4.3.1.2.2 Example 2: upgrade the software image for the DRG

In this example, the software image file “DMA0022-R2N01.r0” is upgraded from a TFTP server with the IP address “192.168.1.100”.

1. Set the TFTP server IP.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadServer.0 = 192.168.1.100
PACKETFRONT-DRG-MIB::downloadServer.0 = STRING: "192.168.1.100"
```

2. Set the software name.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadFile.0 = DMA0022-R2N01.r0
PACKETFRONT-DRG-MIB::downloadFile.0 = STRING: "DMA0022-R2N01.r0"
```

3. Set the upgrading method as TFTP.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadMethod.0 = 1
PACKETFRONT-DRG-MIB::downloadMethod.0 = INTEGER: tftp(1)
```

4. Trigger the start of upgrade.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadAction.0 = 2
PACKETFRONT-DRG-MIB::downloadAction.0 = INTEGER: startDownload(2)
```

4.3.1.2.3 Example 3: upgrade the .INI file for the DRG

In this example, the .INI file "test.ini” is upgraded from a TFTP server with the IP address “192.168.1.100”.

1. Set the TFTP server IP.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadServer.0 = 192.168.1.100
PACKETFRONT-DRG-MIB::downloadServer.0 = STRING: "192.168.1.100"
```

2. Set the software name.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadFile.0 = test.ini
PACKETFRONT-DRG-MIB::downloadFile.0 = STRING: "test.ini"
```

3. Set the upgrading method as TFTP.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadMethod.0 = 1
PACKETFRONT-DRG-MIB::downloadMethod.0 = INTEGER: tftp(1)
```

4. Trigger the start of upgrade.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::downloadAction.0 = 2
PACKETFRONT-DRG-MIB::downloadAction.0 = INTEGER: startDownload(2)
```

4.3.1.2.4 Example 4: add an entry in the VLAN table

In this example, an entry is added in the VLAN table which has the definition as follows:

VLAN	100
Priority	3
WAN	Y
LAN	N
VLAN NAME	v1

First, the values in the three port list needs to be calculated. Each bit in the port-lists is calculated based on the table below:

	Y	N
EgressPorts	1	0
UntaggedPorts	0	0
UnmodifiedPorts	0	0

After being calculated, the port-list is as follows:

	WAN	**LAN**		
	Y	N		
vlanStaticEgressPorts	1	0	00 0000 0000 0000	0x8000
vlanStaticUntaggedPorts	0	0	00 0000 0000 0000	0x0000
vlanStaticUnmodifiedPorts	0	0	00 0000 0000 0000	0x0000

The configuration procedure is as follows:

1. Check the current VLAN table. In this example, it is empty.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticTable = No Such Instance currently
exists at this OID
```

2. Create a new entry in the VLAN static table.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticRowStatus.1 i 4
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: createAndGo(4)
```

3. Configure the VLAN name.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticName.1 s v1
PACKETFRONT-DRG-MIB::vlanStaticName.1 = STRING: "v1"
```

4. Configure the VLAN ID.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticVlanId.1 i 100
PACKETFRONT-DRG-MIB::vlanStaticVlanId.1 = INTEGER: 100
```

5. Configure the VLAN priority.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticPriority.1 i 3
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 3
```

6. Configure the VLAN egress port list.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticEgressPorts.1 x "80"
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: 80
```

7. Save the configuration.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)
```

8. Verify the configuration.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticIndex.1 = INTEGER: 1
PACKETFRONT-DRG-MIB::vlanStaticName.1 = STRING: "v1"
PACKETFRONT-DRG-MIB::vlanStaticVlanId.1 = INTEGER: 100
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 3
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: 80
PACKETFRONT-DRG-MIB::vlanStaticUntaggedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticUnmodifiedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: active(1)
```

4.3.1.2.5 Example 5: modify an entry in the VLAN table

In this example, the VLAN entry added in Example 4 is modified. You are going to

- Change the priority to 5
- Change the membership of LAN to YES

After the modification, the VLAN table should have the following definition:

VLAN	100
Priority	5
WAN	Y
LAN	Y
VLAN NAME	v1

Similarly, you need to calculate the values of port-lists:

	WAN	**LAN**			**Need Updates**
	Y	Y			
vlanStaticEgressPorts	1	1	00 0000 0000 0000	0xC000	YES
vlanStaticUntaggedPorts	0	0	00 0000 0000 0000	0x0000	NO
vlanStaticUnmodifiedPorts	0	0	00 0000 0000 0000	0x0000	NO

The configuration procedure is as follows:

1. Dump contents of existing vlanStaticTable.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB:vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticIndex.1 = INTEGER: 1
PACKETFRONT-DRG-MIB::vlanStaticName.1 = STRING: "v1"
PACKETFRONT-DRG-MIB::vlanStaticVlanId.1 = INTEGER: 100
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 3
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: 80
PACKETFRONT-DRG-MIB::vlanStaticUntaggedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticUnmodifiedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: active(1)
```

2. Modify the VLAN priority.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticPriority.1 i 5
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 5
```

3. Modify egress port-list.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticEgressPorts.1 x “C0”
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: C0
```

4. Save the modification

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)
```

5. Verify the modification.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB:vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticIndex.1 = INTEGER: 1
PACKETFRONT-DRG-MIB::vlanStaticName.1 = STRING: "v1"
PACKETFRONT-DRG-MIB::vlanStaticVlanId.1 = INTEGER: 100
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 5
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: C0
PACKETFRONT-DRG-MIB::vlanStaticUntaggedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticUnmodifiedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: active(1)
```

4.3.1.2.6 Example 6: delete an entry from the VLAN table

In this example, the entry that you added and modified in previous examples is deleted. The configuration procedure is as follows:

1. Dump contents of existing vlanStaticTable to get the entry of vlan table entry.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB:vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticIndex.1 = INTEGER: 1
PACKETFRONT-DRG-MIB::vlanStaticName.1 = STRING: "v1"
PACKETFRONT-DRG-MIB::vlanStaticVlanId.1 = INTEGER: 100
PACKETFRONT-DRG-MIB::vlanStaticPriority.1 = INTEGER: 5
PACKETFRONT-DRG-MIB::vlanStaticEgressPorts.1 = Hex-STRING: C0
PACKETFRONT-DRG-MIB::vlanStaticUntaggedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticUnmodifiedPorts.1 = ""
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: active(1)
```

2. Delete the entry from the VLAN table.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::vlanStaticRowStatus.1 i 6
PACKETFRONT-DRG-MIB::vlanStaticRowStatus.1 = INTEGER: destroy(6)
```

3. Verify the operation.

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG-
MIB:vlanStaticTable
PACKETFRONT-DRG-MIB::vlanStaticTable = No Such Instance currently
exists at this OID
```

4.3.2 PACKETFRONT-DRG100-MIB

4.3.2.1 Capability Report

- **`selfTest`**

Object **`selfTest`** is not supported in this release.

4.3.2.2 Configuration Examples

4.3.2.2.1 Example 1: get port table information

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-DRG100-
MIB::drg100PortTable
PACKETFRONT-DRG100-MIB::drg100PortIndex.1 = INTEGER: 1
PACKETFRONT-DRG100-MIB::drg100PortIndex.2 = INTEGER: 2
PACKETFRONT-DRG100-MIB::drg100PortName.1 = STRING: "WAN"
PACKETFRONT-DRG100-MIB::drg100PortName.2 = STRING: "LAN1"
```

```
PACKETFRONT-DRG100-MIB::drg100PortDuplexAdmin.1 = INTEGER: halfDuplex(1)
PACKETFRONT-DRG100-MIB::drg100PortDuplexAdmin.2 = INTEGER: halfDuplex(1)
PACKETFRONT-DRG100-MIB::drg100PortDuplexStatus.1 = INTEGER: fullDuplex(2)
PACKETFRONT-DRG100-MIB::drg100PortDuplexStatus.2 = INTEGER: fullDuplex(2)
PACKETFRONT-DRG100-MIB::drg100PortFlowControlAdmin.1 = INTEGER: disabled(2)
PACKETFRONT-DRG100-MIB::drg100PortFlowControlAdmin.2 = INTEGER: disabled(2)
PACKETFRONT-DRG100-MIB::drg100PortFlowControlStatus.1 = INTEGER:
disabled(2)
PACKETFRONT-DRG100-MIB::drg100PortFlowControlStatus.2 = INTEGER:
disabled(2)
PACKETFRONT-DRG100-MIB::drg100PortSpeedAdmin.1 = INTEGER:
s100e06(100000000)
PACKETFRONT-DRG100-MIB::drg100PortSpeedAdmin.2 = INTEGER:
s100e06(100000000)
PACKETFRONT-DRG100-MIB::drg100PortVlanId.1 = INTEGER: 0
PACKETFRONT-DRG100-MIB::drg100PortVlanId.2 = INTEGER: 0
PACKETFRONT-DRG100-MIB::drg100PortVlanPriority.1 = INTEGER: 0
PACKETFRONT-DRG100-MIB::drg100PortVlanPriority.2 = INTEGER: 0
```

PACKETFRONT-DRG100-MIB::drg100PortVlanPriority.2 = No more variables left in this MIB View (It is past the end of the MIB tree)

4.3.3 PACKETFRONT-HTTP-MIB

4.3.3.1 Capability Report

- **`httpPasswordFormat`**

Object **`httpPasswordFormat`** is read-only in this release, writing is not supported.

4.3.3.2 Configuration Examples

4.3.3.2.1 Example 1: Disable/Enable HTTP server

In this example, the HTTP server is disabled at first and then enabled. The configuration procedure is as follows:

1. Read the current status of the HTTP server.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-HTTP-
MIB::httpStatus.0
PACKETFRONT-HTTP-MIB::httpStatus.0 = INTEGER: running(2)
```

2. Disable the HTTP server.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-HTTP-
MIB::httpAdminStatus.0 i 2
PACKETFRONT-HTTP-MIB::httpAdminStatus.0 = INTEGER: disabled(2)
```

3. Read the current status of the HTTP server.

```
% snmpget -v 2c -c public <IpAddress> PACKETFRONT-HTTP-
MIB::httpStatus.0
PACKETFRONT-HTTP-MIB::httpStatus.0 = INTEGER: stopped(4)
```

4. Enable the HTTP server.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-HTTP-
MIB::httpAdminStatus.0 i 1
PACKETFRONT-HTTP-MIB::httpAdminStatus.0 = INTEGER: enabled(1)
```

4.3.4 PACKETFRONT-VOIP-MIB

4.3.4.1 Capability Report

4.3.4.1.1 Capability Report for SIP Releases

The following common objects are not supported by SIP images:

- **voipIfServicesCallForwardBusyEnabled**
- **voipIfServicesCallForwardBusyNumber**
- **voipIfServicesCallForwardNoAnswerEnabled**
- **voipIfServicesCallForwardNoAnswerNumber**

The following objects under voipH323Options are not supported by SIP images:

- **voipH323SupportFastConnec**
- **voipH323SupportH245Tunnelling**
- **voipH323SupportEarlyH245**
- **voipH323GatekeeperDiscovery**
- **voipH323SupportAlternateGatekeeper**
- **voipH323GatekeeperFullRRQEnable**
- **voipH323GatekeeperIncludeURLID**
- **voipH323SecurityH235Mode**
- **voipH323SecurityH235Key**
- **voipH323SupportMessageWaitingIndicationBlink**
- **voipH323SupportMessageWaitingIndicationTone**
- **voipH323CallParkingTable**
- **voipH323CallParkingEntry**
- **voipH323CallParkingIndex**
- **voipH323CallParkingAlertEnable**
- **voipH323CallParkingNumber**

The following objects under voipMGCPOptions are not supported by SIP images:

- **`voipMGCPServerMode`**
- **`voipMGCPMaxRSIPDelay`**
- **`voipMGCPSupportPiggyback`**
- **`voipMGCPSquelchDTMF`**

The following objects under voipH248Options are not supported by SIP images:

- **`voipH248Profile`**
- **`voipH248ProfileVersion`**

4.3.4.1.2 Capability Report for H.323 Releases

The following common objects are not supported by H.323 images:

- **`voipIfAuthPasswd`**
- **`voipIfPrimaryServerPort`**
- **`voipIfSecondaryServerPort`**
- **`voipIfLocalSignalPort`**
- **`voipIfSignalTransportProtocol`**
- **`voipIfMsgWaitingAccount`**
- **`voipCallProgressStutterDial`**
- **`voipIfServicesCallForwardBusyEnabled`**
- **`voipIfServicesCallForwardBusyNumber`**
- **`voipIfServicesCallForwardNoAnswerEnabled`**
- **`voipIfServicesCallForwardNoAnswerNumber`**

The following objects under voipSIPOptions are not supported by H323 images:

- **`voipSIPSupportPrackMethod`**
- **`voipSIPIncludeUserParameter`**
- **`voipSIPNotifyKeepAliveEnabled`**
- **`voipSIPInviteTimerValue`**

- **voipSIPSessionTimerValue**
- **voipSIPNotifyTimerValue**
- **voipSIPInviteIncludeSdp**
- **voipSIPTelephoneURIEnabled**
- **voipSIPAnonymousTable**
- **voipSIPAnonymousEntry**
- **voipSIPAnonymousLineNumber**
- **voipSIPAnonymousFromHeaderEnabled**
- **voipSIPAnonymousToHeaderEnabled**
- **voipSIPAnonymousProxyRequiresPrivacyEnabled**
- **voipSIPAnonymousDisplayNameEnabled**
- **voipSIPFeaturesTable**
- **voipSIPFeaturesEntry**
- **voipSIPFeaturesLineNumber**
- **voipSIPLocalRingingEnabled**
- **voipSIPMediaDirection**
- **voipSIPSuspendTimer**
- **voipSIPPayphoneReversePolarityEnabled**
- **voipSIPOutOfBandFlashMethod**
- **voipSIPOutboundProxyAddress**
- **voipSIPOutboundProxyPort**

The following objects under voipMGCPOptions are not supported by H.323 images:

- **voipMGCPServerMode**
- **voipMGCPMaxRSIPDelay**
- **voipMGCPSupportPiggyback**
- **voipMGCPSquelchDTMF**

The following objects under voipH248Options are not supported by H.323 images:

- **`voipH248Profile`**
- **`voipH248ProfileVersion`**

4.3.4.1.3 Capability Report for MGCP Releases

The following common objects are not supported by MGCP images:

- **`voipDialTimeout`**
- **`voipDialPlan`**
- **`voipQuickDialEnabled`**
- **`voipCodecKeypadPayloadType`**
- **`voipIfAuthPasswd`**
- **`voipIfCallerIdEnabled`**
- **`voipIfCallerIdName`**
- **`voipIfLocalSignalPort`**
- **`voipIfSignalTransportProtocol`**
- **`voipIfKeepaliveTimeout`**
- **`voipIfMsgWaitingAccount`**
- **`voipCallProgressStutterDial`**

The following objects under voipServices are not supported by MGCP images:

- **`voipServicesHoldPrefix`**
- **`voipServicesDropPrefix`**
- **`voipServicesFlashPrefix`**
- **`voipServicesConfPrefix`**
- **`voipServicesConfdropPrefix`**
- **`voipServicesCallWaitingOnPrefix`**
- **`voipServicesCallWaitingOffPrefix`**
- **`voipServicesCallWaitingStatusPrefix`**

- **voipServicesCallTransPrefix**
- **voipServicesCallTransAttPrefix**
- **voipServicesCcbsOnPrefix**
- **voipServicesCcbsOffPrefix**
- **voipServicesCallForwardUnconditionalOnPrefix**
- **voipServicesCallForwardUnconditionalOffPrefix**
- **voipServicesCallForwardBusyOnPrefix**
- **voipServicesCallForwardBusyOffPrefix**
- **voipServicesCallForwardNoAnswerOnPrefix**
- **voipServicesCallForwardNoAnswerOffPrefix**
- **voipServicesAnonymousCallOnPrefix**
- **voipServicesAnonymousCallOffPrefix**
- **voipServicesReturnCallPrefix**
- **voipServicesCallWaitingDisablePerCallBasisPrefix**
- **voipServicesPermClirEnablePrefix**
- **voipServicesPermClirDisablePrefix**
- **voipServicesdDonotDisturbOnPrefix**
- **voipServicesdDonotDisturbOffPrefix**
- **voipIfServicesControlLineNumber**
- **voipIfServicesControlMode**
- **voipIfServicesCallWaitingEnabled**
- **voipIfServices3PartyCallEnabled**
- **voipIfServicesCallForwardEnabled**
- **voipIfServicesCallTransferEnabled**
- **voipIfServicesCcbsDuration**
- **voipIfServicesCcbsInterval**

- **`voipIfServicesConfCallTransferEnabled`**
- **`voipIfServicesClirEnabled`**
- **`voipIfServicesCallForwardUnconditionalEnabled`**
- **`voipIfServicesCallForwardUnconditionalNumber`**
- **`voipIfServicesCallForwardBusyEnabled`**
- **`voipIfServicesCallForwardBusyNumber`**
- **`voipIfServicesCallForwardNoAnswerEnabled`**
- **`voipIfServicesCallForwardNoAnswerNumber`**

The following objects under voipSIPOptions are not supported by MGCP images:

- **`voipSIPSupportPrackMethod`**
- **`voipSIPIncludeUserParameter`**
- **`voipSIPNotifyKeepAliveEnabled`**
- **`voipSIPInviteTimerValue`**
- **`voipSIPSessionTimerValue`**
- **`voipSIPNotifyTimerValue`**
- **`voipSIPInviteIncludeSdp`**
- **`voipSIPTelephoneURIEnabled`**
- **`voipSIPAnonymousTable`**
- **`voipSIPAnonymousEntry`**
- **`voipSIPAnonymousLineNumber`**
- **`voipSIPAnonymousFromHeaderEnabled`**
- **`voipSIPAnonymousToHeaderEnabled`**
- **`voipSIPAnonymousProxyRequiresPrivacyEnabled`**
- **`voipSIPAnonymousDisplayNameEnabled`**
- **`voipSIPFeaturesTable`**
- **`voipSIPFeaturesEntry`**

- **`voipSIPFeaturesLineNumber`**
- **`voipSIPLocalRingingEnabled`**
- **`voipSIPMediaDirection`**
- **`voipSIPSuspendTimer`**
- **`voipSIPPayphoneReversePolarityEnabled`**
- **`voipSIPOutOfBandFlashMethod`**
- **`voipSIPOutboundProxyAddress`**
- **`voipSIPOutboundProxyPort`**

The following objects under voipH323Options are not supported by MGCP images:

- **`voipH323SupportFastConnec`**
- **`voipH323SupportH245Tunnelling`**
- **`voipH323SupportEarlyH245`**
- **`voipH323GatekeeperDiscovery`**
- **`voipH323SupportAlternateGatekeeper`**
- **`voipH323GatekeeperFullRRQEnable`**
- **`voipH323GatekeeperIncludeURLID`**
- **`voipH323SecurityH235Mode`**
- **`voipH323SecurityH235Key`**
- **`voipH323SupportMessageWaitingIndicationBlink`**
- **`voipH323SupportMessageWaitingIndicationTone`**
- **`voipH323CallParkingTable`**
- **`voipH323CallParkingEntry`**
- **`voipH323CallParkingIndex`**
- **`voipH323CallParkingAlertEnable`**
- **`voipH323CallParkingNumber`**

The following objects under voipH248Options are not supported by MGCP images:

- **`voipH248Profile`**
- **`voipH248ProfileVersion`**

4.3.4.2 Configuration Examples

4.3.4.2.1 Configuration Examples for SIP releases

4.3.4.2.1.1 Example 1: Configure telephony information

In this example, the telephone information is configured, including:

- Turn on telephone lines
- Set the primary server address and port
- Set the authentication username
- Set the authentication password
- Set the telephone number
- Set the telephone domain
- Set the caller ID name
- Turn on the CLIP function

1. Turn on telephone lines:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.1 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.1 = INTEGER: enabled(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.2 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.2 = INTEGER: enabled(1)
```

2. Set the primary server address:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerAddress.1 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerAddress.1 = STRING:
"10.150.1.5"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerAddress.2 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerAddress.2 = STRING:
"10.150.1.5"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerPort.1 i 5060
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerPort.1 = INTEGER: 5060
```

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerPort.2 i 5060
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerPort.2 = INTEGER: 5060
```

3. Set the authentication username:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfAuthUser.1 = STRING: "5001"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfAuthUser.2 = STRING: "5002"
```

4. Set the authentication password:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthPasswd.1 s 1234
PACKETFRONT-VOIP-MIB::voipIfAuthPasswd.1 = STRING: "1234"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthPasswd.2 s 1234
PACKETFRONT-VOIP-MIB::voipIfAuthPasswd.2 = STRING: "1234"
```

5. Set the telephone number:

```
snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfLineNumber.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfLineNumber.1 = STRING: "5001"

snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfLineNumber.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfLineNumber.2 = STRING: "5002"
```

6. Set the telephone domain:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfDomain.1 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfDomain.1 = STRING: "10.150.1.5"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfDomain.2 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfDomain.2 = STRING: "10.150.1.5"
```

7. Set the caller ID name:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdName.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfCallerIdName.1 = STRING: "5001"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdName.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfCallerIdName.2 = STRING: "5002"
```

8. Turn on the CLIP function:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdEnabled.1 i 1
PACKETFRONT-VOIP-MIB::voipIfCallerIdEnabled.1 = INTEGER: enabled(1)
```

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdEnabled.2 i 1
PACKETFRONT-VOIP-MIB::voipIfCallerIdEnabled.2 = INTEGER: enabled(1)
```

9. Save and restart:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

4.3.4.2.1.2 Example 2: Get the prefixes of VoIP services

In this example, the prefixes of VoIP services are obtained.

1. Get the prefixes of VoIP services:

```
%snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-VOIP-
MIB::voipServicesPrefix
PACKETFRONT-VOIP-MIB::voipServicesHoldPrefix.0 = STRING: "f0"
PACKETFRONT-VOIP-MIB::voipServicesDropPrefix.0 = STRING: "f1"
PACKETFRONT-VOIP-MIB::voipServicesFlashPrefix.0 = STRING: "f2"
PACKETFRONT-VOIP-MIB::voipServicesConfPrefix.0 = STRING: "f3"
PACKETFRONT-VOIP-MIB::voipServicesConfdropPrefix.0 = STRING: "f5"
PACKETFRONT-VOIP-MIB::voipServicesCallWaitingOnPrefix.0 = STRING: "*43#"
PACKETFRONT-VOIP-MIB::voipServicesCallWaitingOffPrefix.0 = STRING: "#43#"
PACKETFRONT-VOIP-MIB::voipServicesCallWaitingStatusPrefix.0 = STRING: "*#43#"
PACKETFRONT-VOIP-MIB::voipServicesCallTransPrefix.0 = STRING: "f4"
PACKETFRONT-VOIP-MIB::voipServicesCallTransAttPrefix.0 = STRING: "*97"
PACKETFRONT-VOIP-MIB::voipServicesCcbsOnPrefix.0 = STRING: "5"
PACKETFRONT-VOIP-MIB::voipServicesCcbsOffPrefix.0 = STRING: "#37#"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardUnconditionalOnPrefix.0 =
STRING: "*21*"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardUnconditionalOffPrefix.0 =
STRING: "#21#"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardBusyOnPrefix.0 = STRING: "*22*"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardBusyOffPrefix.0 = STRING: "#22#"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardNoAnswerOnPrefix.0 = STRING: "*23*"
PACKETFRONT-VOIP-MIB::voipServicesCallForwardNoAnswerOffPrefix.0 = STRING: "#23#"
PACKETFRONT-VOIP-MIB::voipServicesAnonymousCallOnPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesAnonymousCallOffPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesReturnCallPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesCallWaitingDisablePerCallBasisPrefix.0
= STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesPermClirOnPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesPermClirOffPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesDonotDisturbOnPrefix.0 = STRING: "OFF"
PACKETFRONT-VOIP-MIB::voipServicesDonotDisturbOffPrefix.0 = STRING: "OFF"
```

4.3.4.2.1.3 Example 3: Change the prefixes for CLIR service and enable anonymous for SIP From header

In this example, the prefixes for CLIR service are configured, including:

- The prefix for turning on permanent CLIR
- The prefix for turning off permanent CLIR

- The prefix for turning on CLIR on per call basis
- The prefix for turning off CLIR on per call basis

Next, anonymous for SIP From header is enabled. To do this:

1. Set the prefix for turning on permanent CLIR:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipServicesPermClirOnPrefix.0 s *67
PACKETFRONT-VOIP-MIB::voipServicesPermClirOnPrefix.0 = STRING: "*67"
```

2. Set the prefix for turning off permanent CLIR:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipServicesPermClirOffPrefix.0 s *68
PACKETFRONT-VOIP-MIB::voipServicesPermClirOffPrefix.0 = STRING: "*68"
```

3. Set the prefix for turning on CLIR on per call basis:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipServicesAnonymousCallOnPrefix.0 s *31#
PACKETFRONT-VOIP-MIB::voipServicesAnonymousCallOnPrefix.0 = STRING:
"*31#"
```

4. Set the prefix for turning off CLIR on per call basis:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipServicesAnonymousCallOffPrefix.0 s *82
PACKETFRONT-VOIP-MIB::voipServicesAnonymousCallOffPrefix.0 = STRING:
"*82"
```

5. Enable anonymous for the SIP From header:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipSIPAnonymousFromHeaderEnabled.1 i 1
PACKETFRONT-VOIP-MIB::voipSIPAnonymousFromHeaderEnabled.1 = INTEGER:
true(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipSIPAnonymousFromHeaderEnabled.2 i 1
PACKETFRONT-VOIP-MIB::voipSIPAnonymousFromHeaderEnabled.2 = INTEGER:
true(1)
```

6. Save and restart:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

4.3.4.2.2 Configuration Example for H.323 releases

4.3.4.2.2.1 Example 1: Configure telephony information

In this example, the telephone information is configured, including:

- Turn on telephone lines
- Set the primary server address
- Set the H.323 alias
- Set the telephone number
- Set the caller ID name
- Turn on the CLIP function

1. Turn on the telephone line:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.1 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.1 = INTEGER: enabled(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.2 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.2 = INTEGER: enabled(1)
```

2. Set the primary server address and port:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerAddress.1 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerAddress.1 = STRING:
"10.150.1.5"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerAddress.2 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerAddress.2 = STRING:
"10.150.1.5
```

3. Set the H.323 alias:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfAuthUser.1 = STRING: "5001"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfAuthUser.2 = STRING: "5002"
```

4. Set the telephone number:

```
snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfLineNumber.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfLineNumber.1 = STRING: "5001"
```

```
snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfLineNumber.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfLineNumber.2 = STRING: "5002"
```

5. Set the caller ID name:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdName.1 s 5001
PACKETFRONT-VOIP-MIB::voipIfCallerIdName.1 = STRING: "5001"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdName.2 s 5002
PACKETFRONT-VOIP-MIB::voipIfCallerIdName.2 = STRING: "5002"
```

6. Turn on the CLIP function:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdEnabled.1 i 1
PACKETFRONT-VOIP-MIB::voipIfCallerIdEnabled.1 = INTEGER: enabled(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfCallerIdEnabled.2 i 1
PACKETFRONT-VOIP-MIB::voipIfCallerIdEnabled.2 = INTEGER: enabled(1)
```

7. Save and restart:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

4.3.4.2.3 Configuration Examples for MGCP releases

4.3.4.2.3.1 Example 1: Configure telephony information

In this example, the telephone information is configured, including:

- Turn on telephone lines
- Set the server address and port
- Set the domain name
- Set the maximum delay before RSIP
- Set the line name

1. Turn on telephone lines:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.1 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.1 = INTEGER: enabled(1)
```

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAdmin.2 i 1
PACKETFRONT-VOIP-MIB::voipIfAdmin.2 = INTEGER: enabled(1)
```

2. Set the server address and port:

Note that the objects voipIfPrimaryServerAddress and voipIfPrimaryServerPort are common for all telephone lines of DRG. Setting the objects for any one of the line is sufficient.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerAddress.1 s 10.150.1.5
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerAddress.1 = STRING:
"10.150.1.5"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfPrimaryServerPort.1 i 2427
PACKETFRONT-VOIP-MIB::voipIfPrimaryServerPort.1 = INTEGER: 2427
```

3. Set the domain name:

Note that the object voipIfDomain is common for all telephone lines of DRG. Setting the object for any one of the line is sufficient.

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfDomain.1 s drg1001
PACKETFRONT-VOIP-MIB::voipIfDomain.1 = STRING: "drg1001"
```

4. Set the maximum delay before RSIP:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipMGCPMaxRSIPDelay.0 i 6
PACKETFRONT-VOIP-MIB::voipMGCPMaxRSIPDelay.0 = INTEGER: 6 seconds
```

5. Set the line name:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.1 s aaln/1
PACKETFRONT-VOIP-MIB::voipIfAuthUser.1 = STRING: "aaln/1"

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipIfAuthUser.2 s aaln/2
PACKETFRONT-VOIP-MIB::voipIfAuthUser.2 = STRING: "aaln/2"
```

6. Save and restart:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

4.3.4.2.3.2 Example 2: Configure MGCP capability

In this example, the MGCP server mode is configured.

1. Configure the MGCP server mode:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-VOIP-
MIB::voipMGCPServerMode.0 b '1,2'
PACKETFRONT-VOIP-MIB::voipMGCPServerMode.0 = BITS: 60 ietf10(1) ncs10(2)
```

2. Save and restart:

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

4.3.5 PACKETFRONT-STUN-MIB

4.3.5.1 Capability Report

The following OIDs are not supported:

- **`stunServerPort.2`**
- **`stunServerPort.3`**
- **`stunServerPort.4`**

Note: The PACKETFRONT-STUN-MIB is only supported by SIP applications.

4.3.5.2 Configuration Examples

4.3.5.2.1 Example 1: Get the STUN client status information

In this example, the STUN client status information is obtained, including:

- The STUN client running status.
- The STUN client NAT type.
- The STUN client external IP address.

1. Get the STUN client status by snmpwalk

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-STUN-
MIB::stunClientStatus
PACKETFRONT-STUN-MIB::stunClientState.0 = INTEGER: stopped(2)
PACKETFRONT-STUN-MIB::stunClientNatType.0 = INTEGER: none(3)
PACKETFRONT-STUN-MIB::stunClientExternalIpAddress.0 = IpAddress:
0.0.0.0
PACKETFRONT-STUN-MIB::stunClientExternalIpAddress.0 = No more variables
left in this MIB View (It is past the end of the MIB tree)
```

4.3.5.2.2 Example 2: Get the STUN server configuration

In this example, the STUN server configuration is obtained. Four STUN servers can be configured. The second STUN server is configured as "stun.42networks.net" by default. All the four STUN servers share the port configured for the first STUN server (stunServerPort.1).

1. Get the STUN server configuration

```
% snmpwalk -v 2c -c public <IpAddress> PACKETFRONT-STUN-
MIB::stunServerTable
PACKETFRONT-STUN-MIB::stunServerAddress.1 = ""
PACKETFRONT-STUN-MIB::stunServerAddress.2 = STRING:
"stun.42networks.net"
PACKETFRONT-STUN-MIB::stunServerAddress.3 = ""
PACKETFRONT-STUN-MIB::stunServerAddress.4 = ""
PACKETFRONT-STUN-MIB::stunServerPort.1 = INTEGER: 3478

PACKETFRONT-STUN-MIB::stunServerPort.2 = INTEGER: 0
PACKETFRONT-STUN-MIB::stunServerPort.3 = INTEGER: 0
PACKETFRONT-STUN-MIB::stunServerPort.4 = INTEGER: 0
```

4.3.5.2.3 Example 3: Turn on STUN and configure the first STUN server

In this example, STUN function is turned on and the first STUN server is configured.

1. Turn on STUN

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-STUN-
MIB::stunAdminStatus.0 i 1
PACKETFRONT-STUN-MIB::stunAdminStatus.0 = INTEGER: enabled(1)
```

2. Configure the first STUN server

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-STUN-
MIB::stunServerAddress.1 s 172.19.33.15
PACKETFRONT-STUN-MIB::stunServerAddress.1 = STRING: "172.19.33.15"
```

3. Save and restart

```
% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigSave.0 i 1
PACKETFRONT-DRG-MIB::systemConfigSave.0 = INTEGER: save(1)

% snmpset -v 2c -c private <IpAddress> PACKETFRONT-DRG-
MIB::systemConfigRestartControl.0 i 2
PACKETFRONT-DRG-MIB::systemConfigRestartControl.0 = INTEGER:
restartNow(2)
```

5 Configuration using HDD

DRGs can be managed with Home Device Director (HDD) using the Configuration and Distribution Server Protocol (CDSP). The CDSP version 2 is supported in R2N.

Before the HDD can operate in the DRG service domain, the operator must make sure that all DRGs in the domain can find the HDD server. This can be done by presetting the HDD IP address parameter in each DRG device, or by utilizing the server discovery facility based on the DHCP options.

The DRG then will contact HDD and give control to HDD. For detailed information on how to use HDD to configure DRGs, refer to the ***HDD User Guide***.

6 Configuration using PFDP

The DRG 11/22 supports PacketFront Device Protocol (PFDP) version 1.1.9. Every 60 seconds, the DRG provides the following statistic information to BECS via the ASR:

- System info
- Port info
- Port statistics
- Port info multicast

You can configure the DRG 11/22 with following parameters via PFDP. For information on how to configure those parameters, refer to the ***iBOS Command Reference***.

1) Supported status/statistics via PFDP

   a) SysInfo QTLV

      ❖ Product Name

      ❖ Software version

      ❖ Product serial number

   b) PortInfo QTLV

      ❖ Port state (up/down, speed and duplex, subject to hardware limitations)

      ❖ List of MAC addresses of attached end stations

2) Supported query and configurations via PFDP

   a) PortMacRequest QTLV

      ❖ Find out what port a given MAC address resides on

   b) PortConfig/PortConfigStatus QTLVs

      ❖ Speed and duplex

      ❖ Default port QoS priority

   c) Reboot QTLV

7 Configuration using the Web GUI

The following sections describe the configuration settings available in the Web Configuration Server when logging in as operator.

WARNING! If invalid values are entered, the connection to the DRG 11/22 may be lost. In that case, a factory default procedure must be performed. Please refer to section 7.1 for information about how to reset the DRG 11/22.

The configuration pages include settings to change how the DRG 11/22 operates in a network. You can either choose to use a DHCP server that automatically supplies the DRG 11/22 with an IP address, or you can use a fixed IP address. If a fixed IP address is used, the DRG 11/22 network configuration must be done manually.

The DRG 11/22 is equipped with two Ethernet ports: the Wide Area Network (WAN) access port and the Local Area Network (LAN) port. The WAN port is connected to an external network (Internet) and the LAN port is connected to a single computer or to a local network.

7.1 Accessing the Web Configuration Server

Follow the steps below to access the Web Configuration Server:

1. Connect the DRG 11/22 to the network using the WAN port.
2. If a DHCP server is used, the DRG 11/22 will by default request an IP address during power up.
3. If a fixed IP address will be used, proceed as the steps below.
4. Click the Reset button on the back of the DRG 11/22 and keep the Reset button pressed for more than 10 seconds.
5. Make sure that the DRG 11/22 reboots when releasing the Reset button (LEDs on the DRG 11/22 will flash).
6. After this sequence the DRG 11/22 will be in "factory default" status and has the IP-address 192.168.254.254 and subnet mask 255.255.255.0.
7. Open a web browser (Internet Explorer 6.0 or advanced).

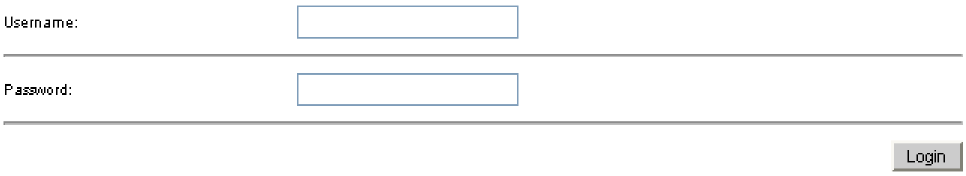
   NOTE! Make sure to disable caching of web pages and enable cookies in your web browser.
8. Enter the IP address of the DRG 11/22 in the address field.

The login GUI appears on the screen. There are two different login usernames: operator and admin (lower case). The user operator is able to browse all configuration pages of the DRG 11/22. The user admin can only browse pages with general information about the DRG 11/22. In default mode, the operator can only login from WAN; the admin can only login from LAN. The access mode can be configured on the “Security” page.

The *operator* default password is DRGPASS (upper case).

The *admin* default password should be blank.

Figure 7-1 DRG login



Username:

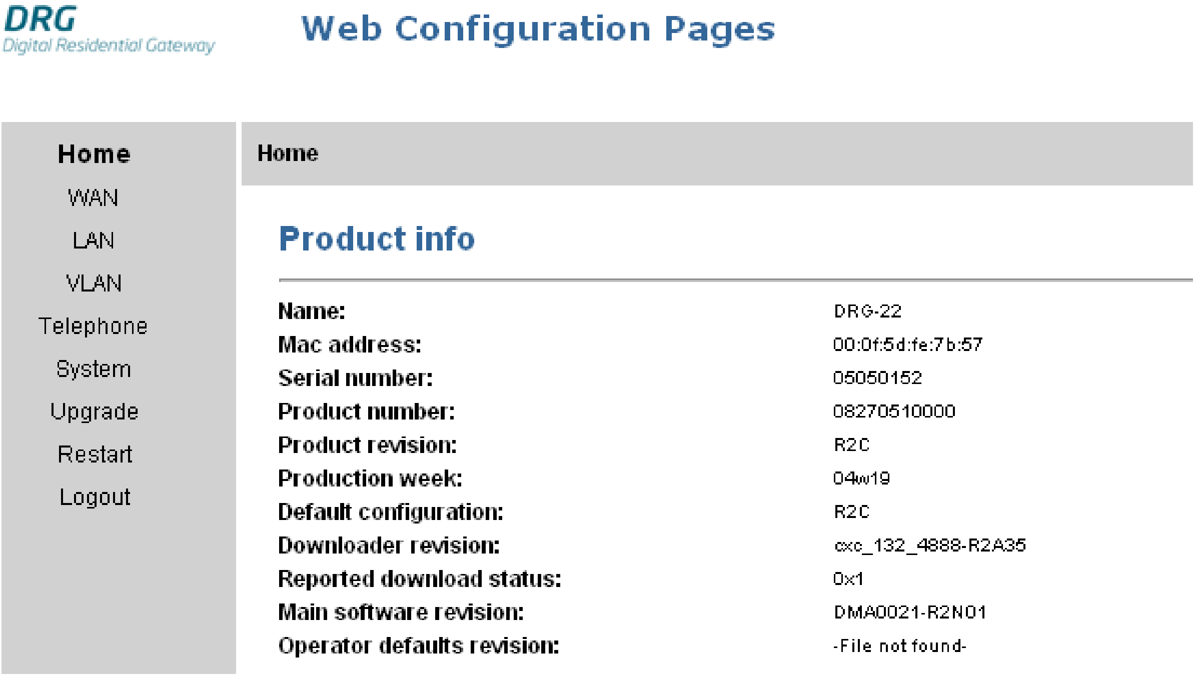
Password:

The Web Configuration Server main view appears on the screen. The left panel consists of a number of links to pages with configuration or status information. The following sections will present the details of the DRG 11/22 configuration.

7.2 Product Info

The Product info page provides an overview of the DRG 11/22. If you have to contact the help desk, provide the "Downloader revision" and the "Main software revision".

Figure 7-2 Product info



Product info

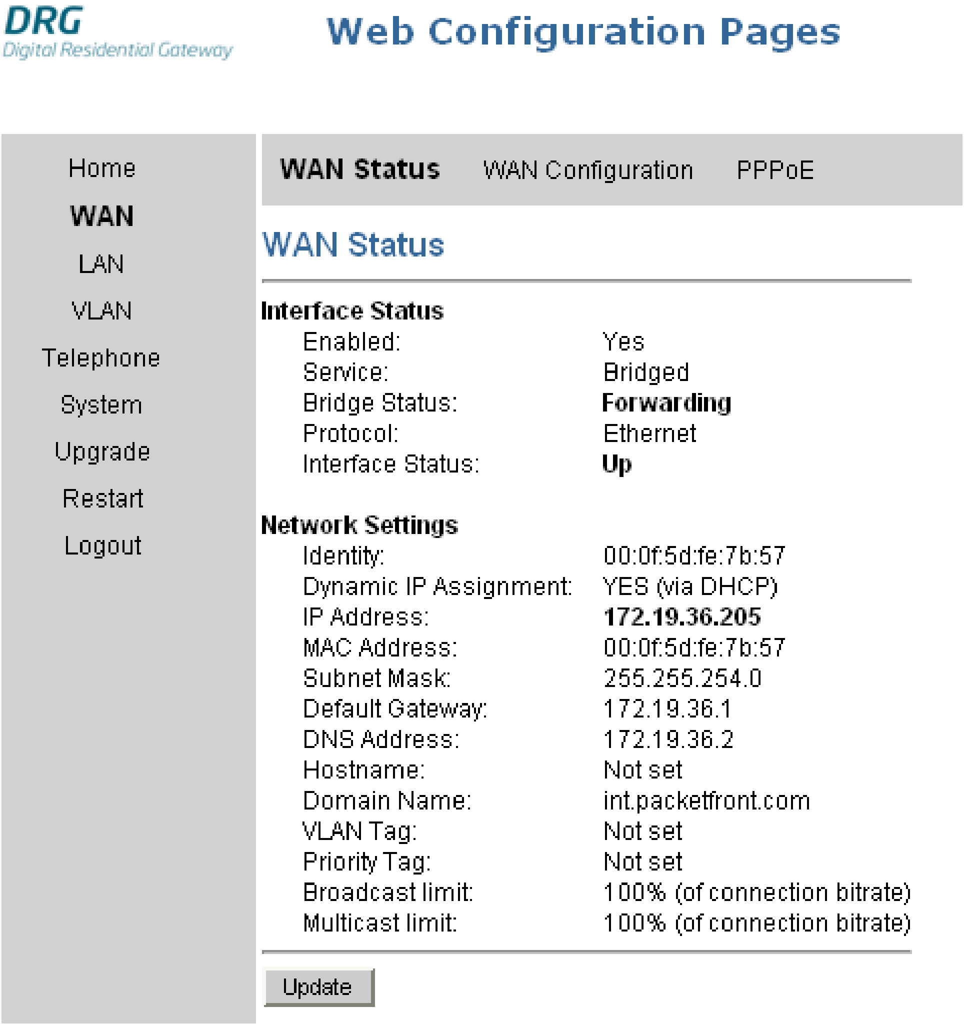
Name:	DRG-22
Mac address:	00:0f:5d:fe:7b:57
Serial number:	05050152
Product number:	08270510000
Product revision:	R2C
Production week:	04w19
Default configuration:	R2C
Downloader revision:	cxc_132_4888-R2A35
Reported download status:	0x1
Main software revision:	DMA0021-R2N01
Operator defaults revision:	-File not found-

7.3 WAN Settings

7.3.1 WAN Status

The WAN Status page shows the current status of the WAN-side of the DRG 11/22 including the interface status and networks settings.

Figure 7-3 WAN status



WAN Status

Interface Status

Enabled:	Yes
Service:	Bridged
Bridge Status:	**Forwarding**
Protocol:	Ethernet
Interface Status:	**Up**

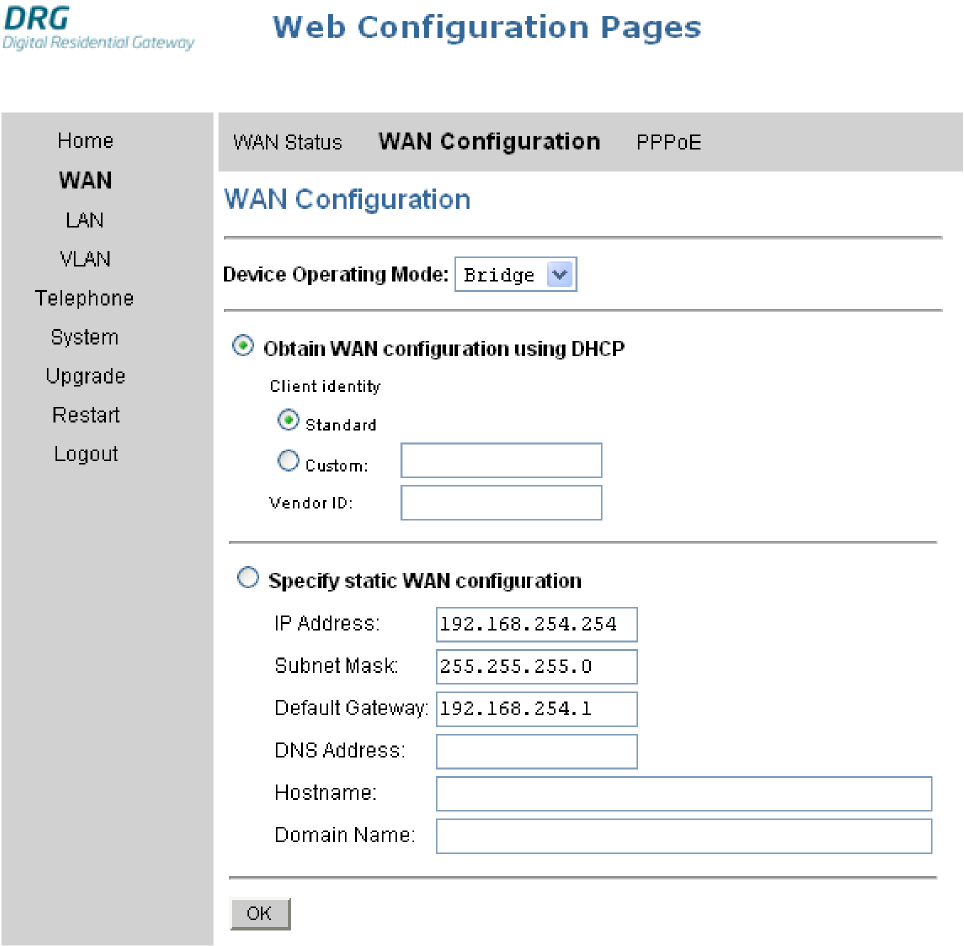
Network Settings

Identity:	00:0f:5d:fe:7b:57
Dynamic IP Assignment:	YES (via DHCP)
IP Address:	**172.19.36.205**
MAC Address:	00:0f:5d:fe:7b:57
Subnet Mask:	255.255.254.0
Default Gateway:	172.19.36.1
DNS Address:	172.19.36.2
Hostname:	Not set
Domain Name:	int.packetfront.com
VLAN Tag:	Not set
Priority Tag:	Not set
Broadcast limit:	100% (of connection bitrate)
Multicast limit:	100% (of connection bitrate)

7.3.2 WAN Configuration

The WAN Configuration page includes settings for the WAN port.

Figure 7-4 WAN configuration



DRG Digital Residential Gateway — Web Configuration Pages

WAN Configuration

Device Operating Mode: Bridge

● Obtain WAN configuration using DHCP

Client identity

● Standard

○ Custom:

Vendor ID:

○ Specify static WAN configuration

IP Address: 192.168.254.254

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.254.1

DNS Address:

Hostname:

Domain Name:

OK

The following table gives a detailed description of each value that can be configured on the WAN Configuration page:

Function	Description
Device Operating Mode	Select whether the DRG 11/22 will be working in “Bridge” or “Router” mode.
Obtain WAN configuration using DHCP	If selected, the IP Address, Subnet Mask, Default Gateway and DNS Address will be provided via DHCP.
Client Identity	Specify the unique identifier of the DHCP clients. The "Standard" (default) value is based on the MAC address. The "Custom" parameter is a string of hexadecimal values, e.g. 000123.
Vendor ID	The identifier of vendor information to the DHCP server. The parameter is an ASCII-string, e.g. "DRG 11/22".
Specify static WAN configuration	If selected, the IP Address, Subnet Mask, Default Gateway, DNS Address, Host Name and Domain Name should be manually configured.
IP Address	Enter the IP-address of the DRG.
Subnet Mask	Enter the subnet mask of the DRG.
Default Gateway	Enter the IP-address of the default gateway.

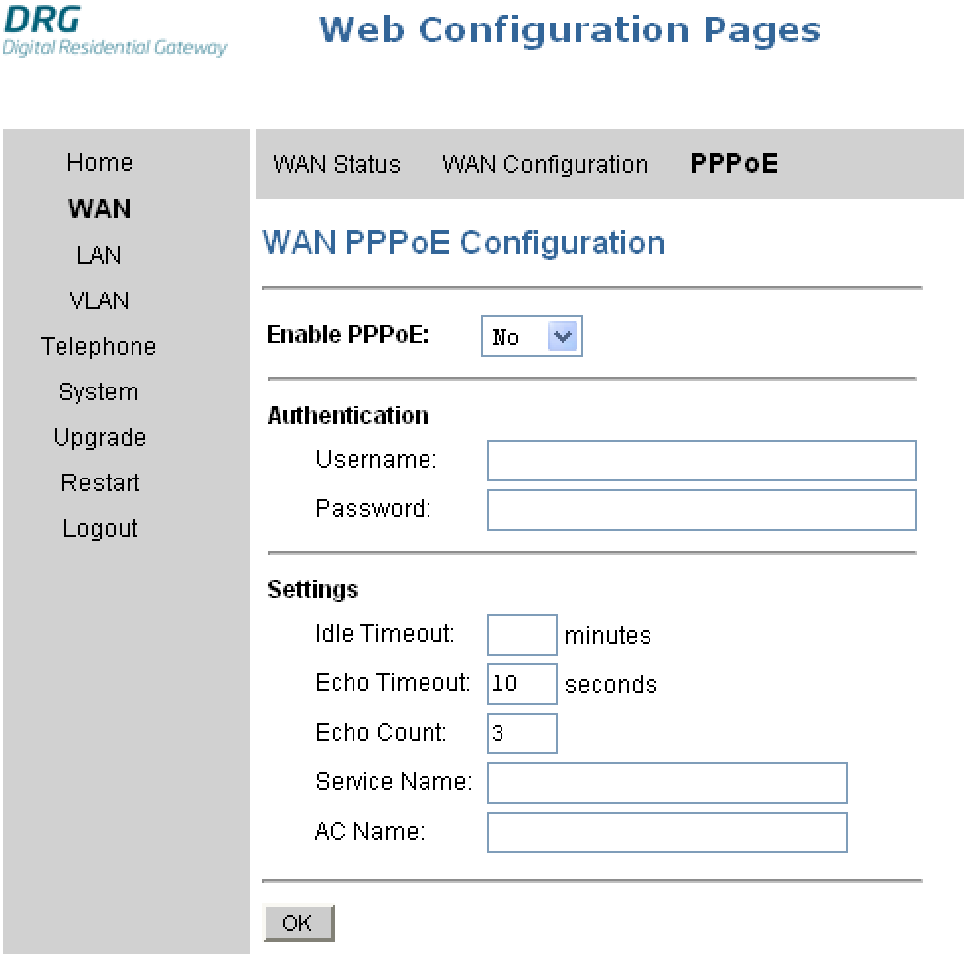
Function	Description
DNS Address	Enter the IP-address of the DNS server. **NOTE**! If a DNS address is specified without the DNS server reachable in the network, the DRG will try to reach a DNS for 90 seconds. During this time, the DRG would appear "dead" from the point of view of a DRG HDD, but it will start up normally later.
Hostname	Hostname for client
Domain Name	Domain name for client resolution

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.3.3 PPPoE Configuration

The WAN PPPoE Configuration page includes settings to use PPPoE (Point-to-Point Protocol over Ethernet).

Figure 7-5 WAN PPPoE configuration



WAN PPPoE Configuration

Enable PPPoE: No

Authentication

Username:

Password:

Settings

Idle Timeout: minutes

Echo Timeout: 10 seconds

Echo Count: 3

Service Name:

AC Name:

The following table gives a detailed description of each value that can be configured on the PPPoE Configuration page:

Function	Description
Enable PPPoE	Select Yes to use PPPoE or No to stop.
Authentication Username	Insert the username provided by the service provider.
Authentication Password	Insert the password provided by the service provider.
Idle Timeout (minutes)	Idle timeout before PPP connection is closed due to inactivity
Echo Timeout (seconds)	Duration between PPP echo requests sent to the server
Echo count	The number of unanswered PPP echo requests allowed before the PPP connection is closed.
Service Name	Given name of the PPPoE service.
AC Name	Given PPPoE AC (Access Concentrator) name.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

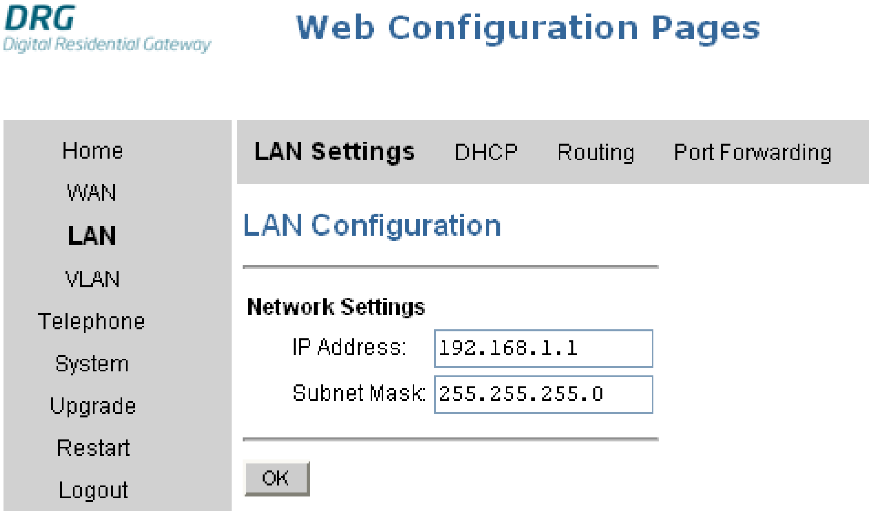
NOTE! DRG cannot act as a PPPoE server. The PPPoE configuration is only valid for the DRG Management IP address and not for LAN port connected devices.

7.4 LAN Settings

7.4.1 LAN Configuration

The LAN Configuration page includes settings for the LAN usage.

Figure 7-6 LAN configuration



LAN Configuration

Network Settings

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

The following table gives a detailed description of each value that can be configured on the LAN Configuration page:

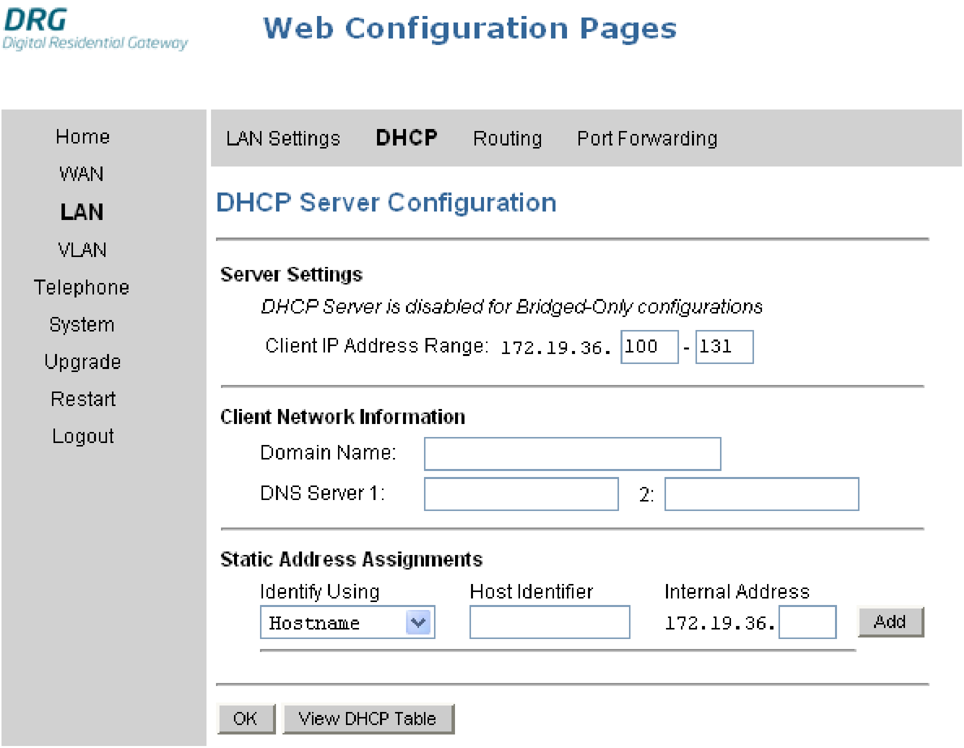
Function	Description
IP Address	Specify the DRG 11/22 LAN port IP Address. Default Gateway for client connected to DRG 11/22 LAN side
Subnet Mask	Specify the subnet mask of the LAN. Usage of a C-class network is recommended, e.g. 255.255.255.0.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.4.2 DHCP Server Configuration

The DHCP Server Configuration page is for configuration of the DRG 11/22 internal DHCP server.

Figure 7-7 DHCP server configuration



DHCP Server Configuration

Server Settings

DHCP Server is disabled for Bridged-Only configurations

Client IP Address Range: 172.19.36. 100 - 131

Client Network Information

Domain Name:

DNS Server 1: 2:

Static Address Assignments

Identify Using: Hostname

Host Identifier

Internal Address: 172.19.36.

The following table gives a detailed description of each value that can be configured on the DHCP Server Configuration page:

Function	Description
Server Settings	Enable or disable the internal DHCP Server.
Client IP Address Range	Upper and lower limits on the DHCP IP address allowed Subnet specified under LAN settings will be used.
Client Network Information:	
Domain Name	LAN domain name provided to DHCP clients during the DHCP process.
Client Network Information DNS Server	This statically assigned DNS server IP address(s) that 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, select the Hostname or the MAC address of the LAN device (should be unique in the private network) as the Host Identifier.
Host Identifier	Specify the Host Name or the MAC address entered as the Host Identifier upon the option in Identify Using item.
Internal Address	Specify the Internal address to be assigned and click Add.

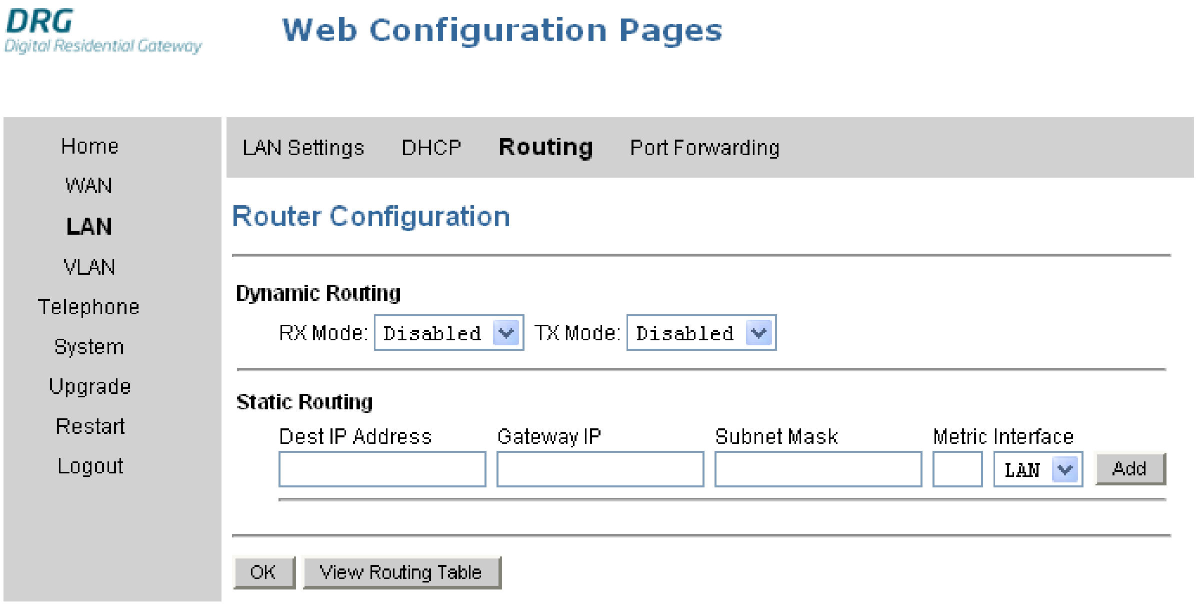
By clicking **View DHCP Table**, it is possible to see the allocated addresses and equipment connected to the LAN.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.4.3 Router Configuration

The Router Configuration page includes specifications for setting dynamic or static routing.

Figure 7-8 Router configuration



RX Mode: Disabled TX Mode: Disabled

Interface: LAN

The following table gives a detailed description of each value that can be configured on the Router Configuration page:

Function	**Description**
Dynamic Routing	If dynamic routing is used, TX/RX interfaces are enabled or disabled.
Static Routing	Configure static routes within the LAN.

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

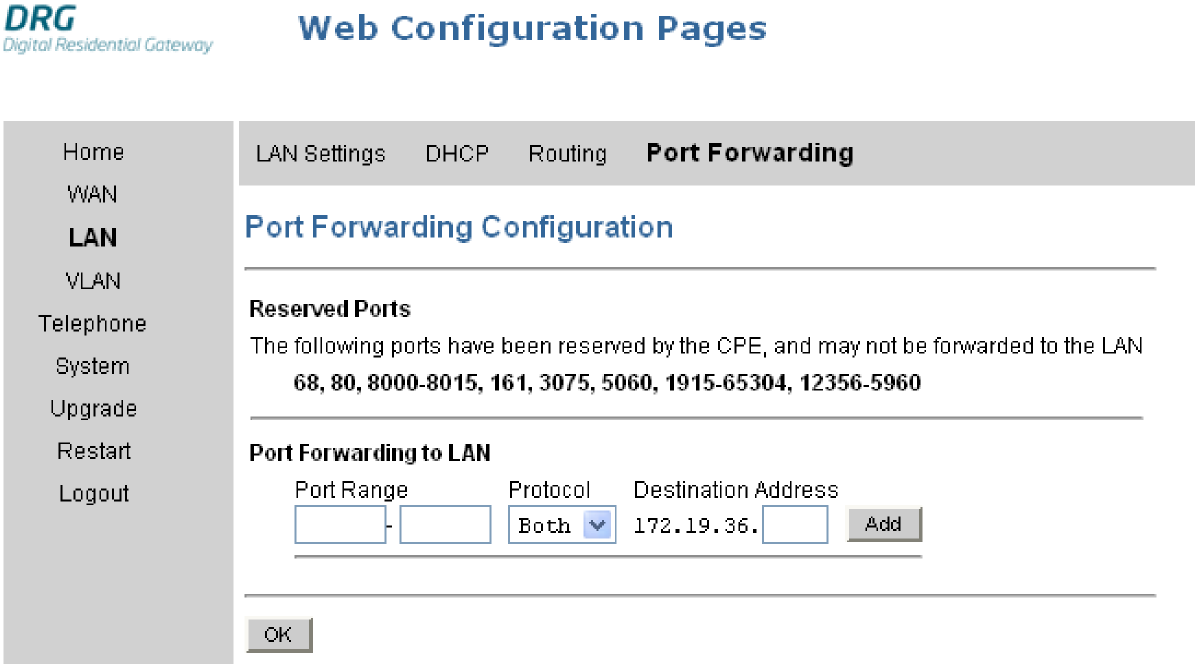
To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.4.4 Port Forwarding Configuration

The Port Forwarding Configuration allows you to make local computers or servers available to the Internet for different services (for example, FTP or HTTP).

Port Forwarding is designed for FTP, Web Server or other server-based services. Once port forwarding is set up, requests from the Internet will be forwarded to the corresponding local server.

Figure 7-9 Port forwarding configuration



Reserved Ports

The following ports have been reserved by the CPE, and may not be forwarded to the LAN

68, 80, 8000-8015, 161, 3075, 5060, 1915-65304, 12356-5960

Port Forwarding to LAN

Port Range: -

Protocol: Both

Destination Address: 172.19.36.

The following table gives a detailed description of each value that can be configured on the Port Forwarding Configuration page:

Function	Description
Reserved Ports	All the DRG 11/22 reserved ports are listed.
Port Forwarding to LAN	Enter the specifications to forward to the LAN, including port range, protocol (Both, TCP or UDP) and the destination IP address.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.5 VLAN Settings

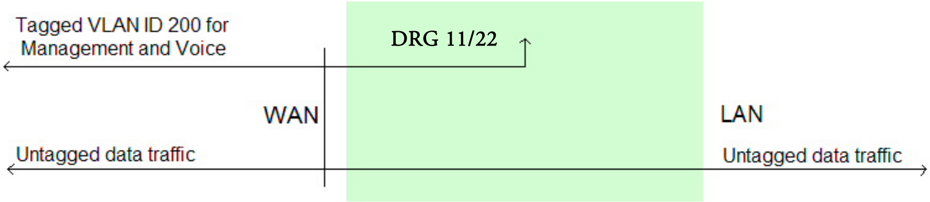
7.5.1 VLAN Tagging

The DRG 11/22 supports IEEE 802.1Q VLAN (Virtual LAN). An Ethernet frame on a VLAN has an additional header/tag inserted that tells the equipment in VLAN-aware networks which VLAN the frame belongs to (VLAN ID) and the priority of the frame. The DRG 11/22 can handle up to 16 VLANs.

7.5.2 Example Configuration

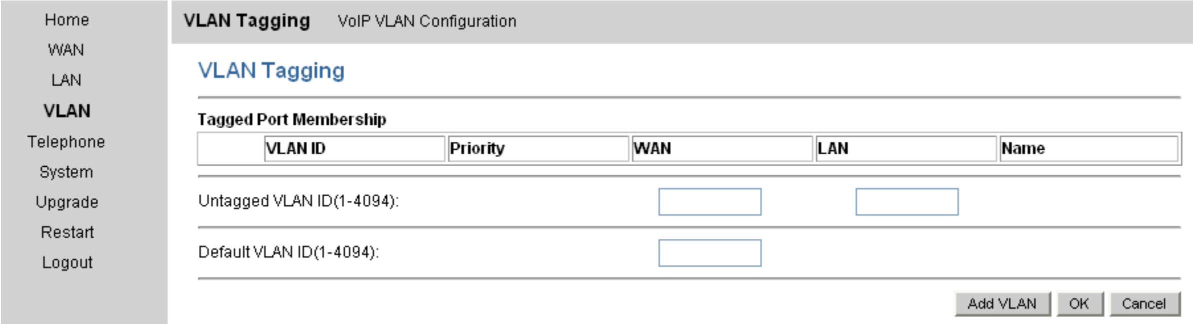
Figure 7-10 illustrates the untagged Internet VLAN and tagged VoIP/Management VLAN, which can be configured for the DRG 11/22 on the **VLAN Tagging** page.

Figure 7-10: Traffic flow tagged and untagged



To create a VoIP/Management VLAN, perform the following steps:

1. On the **VLAN Tagging** tab, click **Add VLAN**. The VLAN editor is displayed.



VLAN Tagging

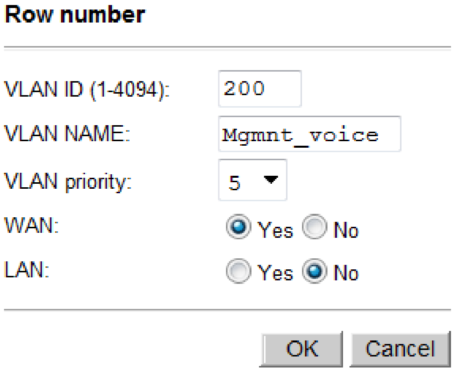
Tagged Port Membership

	VLAN ID	Priority	WAN	LAN	Name

Untagged VLAN ID(1-4094):

Default VLAN ID(1-4094):

2. Enter parameters for the VoIP/Management VLAN. To include WAN as a tagged VLAN member, select “Yes” at WAN. To not include LAN as a tagged VLAN member, select “No” at LAN. Click **OK**.



Row number

VLAN ID (1-4094): 200

VLAN NAME: Mgmnt_voice

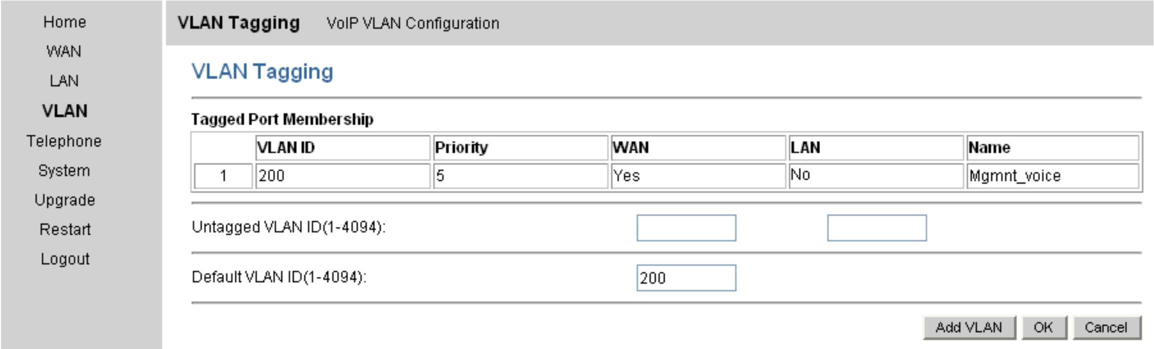
VLAN priority: 5

WAN: ● Yes ○ No

LAN: ○ Yes ● No

3. In the **Default VLAN ID (1-4094)** field, enter the VLAN ID for the VoIP/Management VLAN (in this example, 200) and click **OK**. A confirmation dialog is displayed. Click **OK** in the dialog.

   When traffic is sent to the WAN interface, the traffic goes through the default VLAN.



VLAN Tagging

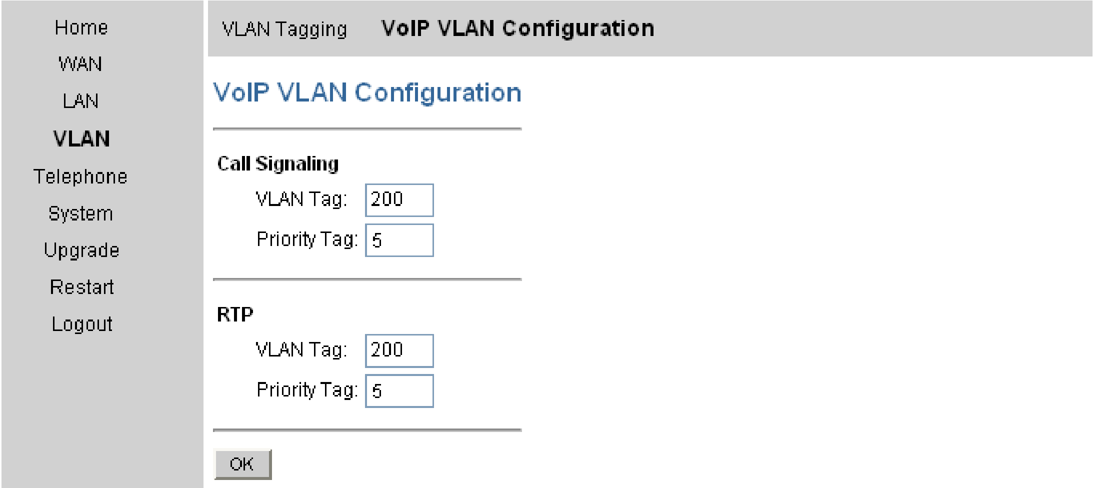
Tagged Port Membership

	VLAN ID	Priority	WAN	LAN	Name
1	200	5	Yes	No	Mgmnt_voice

Untagged VLAN ID(1-4094):

Default VLAN ID(1-4094): 200

4. Select the **VoIP VLAN Configuration** tab. Enter VLAN ID and priority for the Call Signaling and RTP VLANs (the same as for the VoIP/Management VLAN in this configuration). Click **OK**.



VoIP VLAN Configuration

Call Signaling

VLAN Tag: 200

Priority Tag: 5

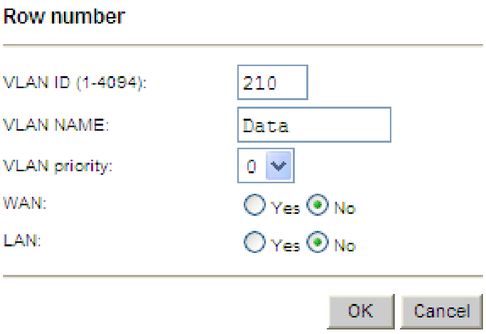
RTP

VLAN Tag: 200

Priority Tag: 5

To create the “Data” VLAN, perform the following steps:

1. Select the **VLAN Tagging** tab.
2. Click **Add VLAN** and enter parameters. As the “Data” VLAN will be untagged at both WAN and LAN, do not include WAN and LAN in the VLAN here. Click **OK**.



Row number

VLAN ID (1-4094): 210

VLAN NAME: Data

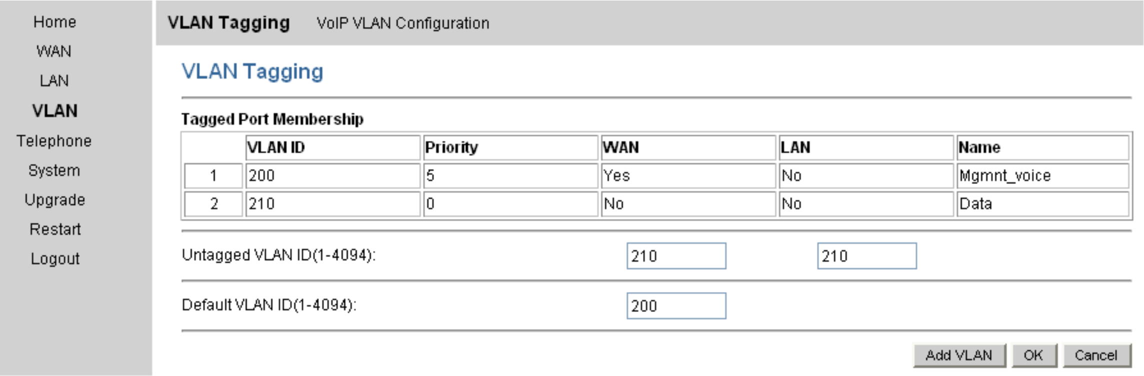
VLAN priority: 0

WAN: ○ Yes ● No

LAN: ○ Yes ● No

3. Enter the “Data” VLAN ID (in this example, 210) in fields **Untagged VLAN ID(1-4094)** aligned on WAN column and LAN column. This configuration sets the VLAN as untagged and makes both WAN and LAN members in the untagged VLAN.

Note: Untagged VLAN ID settings have precedence over the WAN and LAN.



VLAN Tagging

Tagged Port Membership

	VLAN ID	Priority	WAN	LAN	Name
1	200	5	Yes	No	Mgmnt_voice
2	210	0	No	No	Data

Untagged VLAN ID(1-4094):	210	210
Default VLAN ID(1-4094):	200	

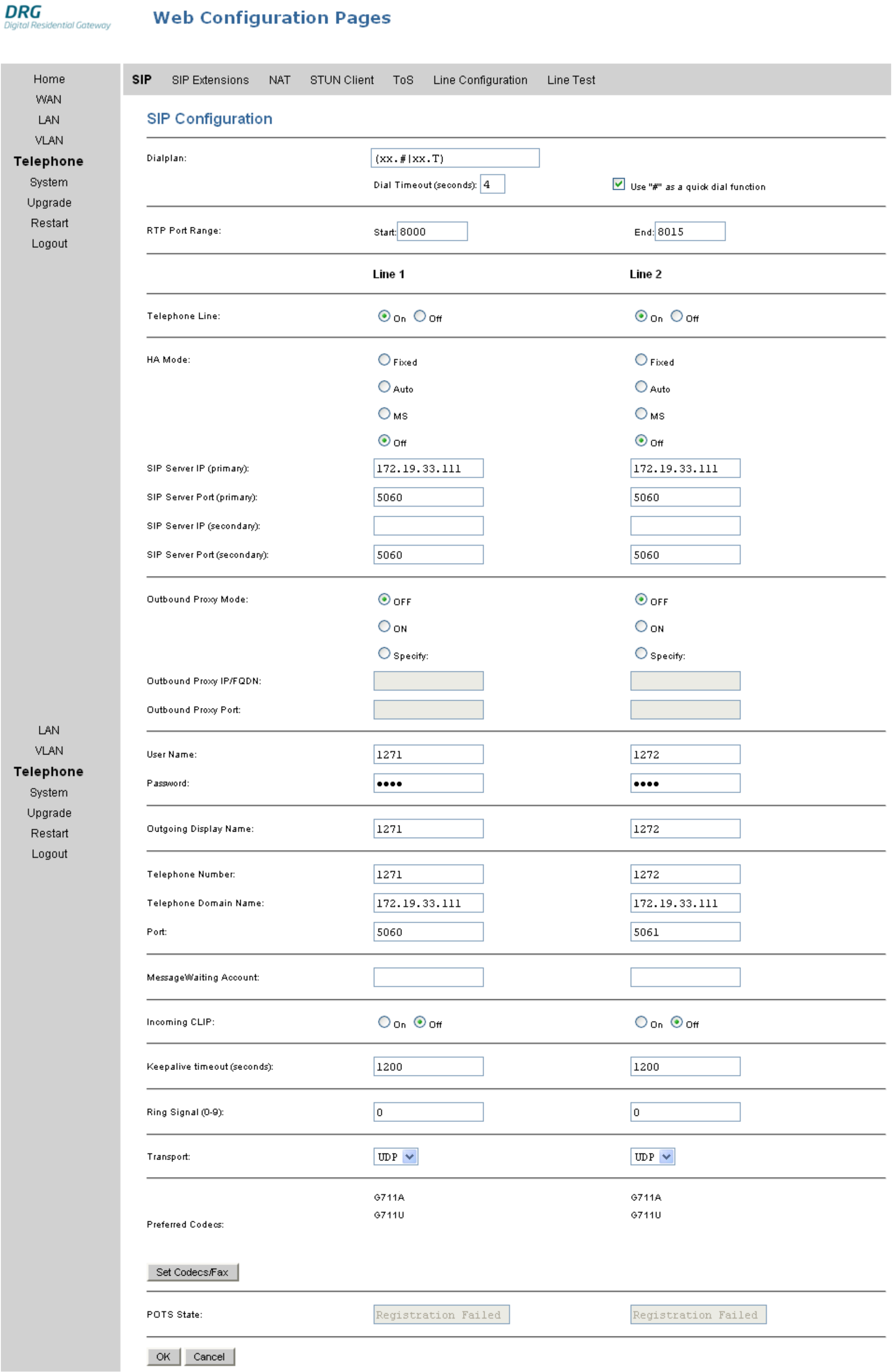
4. Click **OK** and restart the DRG 11/22.

7.6 Telephone SIP Settings

(Apply only to DRG 11/22 running SIP)

The DRG 11/22 includes IP-telephony with one or two separate telephone lines. Each individual telephone line can be switched ON or OFF and configured separately.

Figure 7-11 Telephone SIP configuration



SIP Configuration

Dialplan: (xx.#|xx.T)

Dial Timeout (seconds): 4 ☑ Use "#" as a quick dial function

RTP Port Range: Start: 8000 End: 8015

	Line 1	Line 2
Telephone Line:	● On ○ Off	● On ○ Off
HA Mode:	○ Fixed ○ Auto ○ MS ● Off	○ Fixed ○ Auto ○ MS ● Off
SIP Server IP (primary):	172.19.33.111	172.19.33.111
SIP Server Port (primary):	5060	5060
SIP Server IP (secondary):		
SIP Server Port (secondary):	5060	5060
Outbound Proxy Mode:	● OFF ○ ON ○ Specify:	● OFF ○ ON ○ Specify:
Outbound Proxy IP/FQDN:		
Outbound Proxy Port:		
User Name:	1271	1272
Password:	••••	••••
Outgoing Display Name:	1271	1272
Telephone Number:	1271	1272
Telephone Domain Name:	172.19.33.111	172.19.33.111
Port:	5060	5061
MessageWaiting Account:		
Incoming CLIP:	○ On ● Off	○ On ● Off
Keepalive timeout (seconds):	1200	1200
Ring Signal (0-9):	0	0
Transport:	UDP	UDP
Preferred Codecs:	G711A G711U	G711A G711U
POTS State:	Registration Failed	Registration Failed

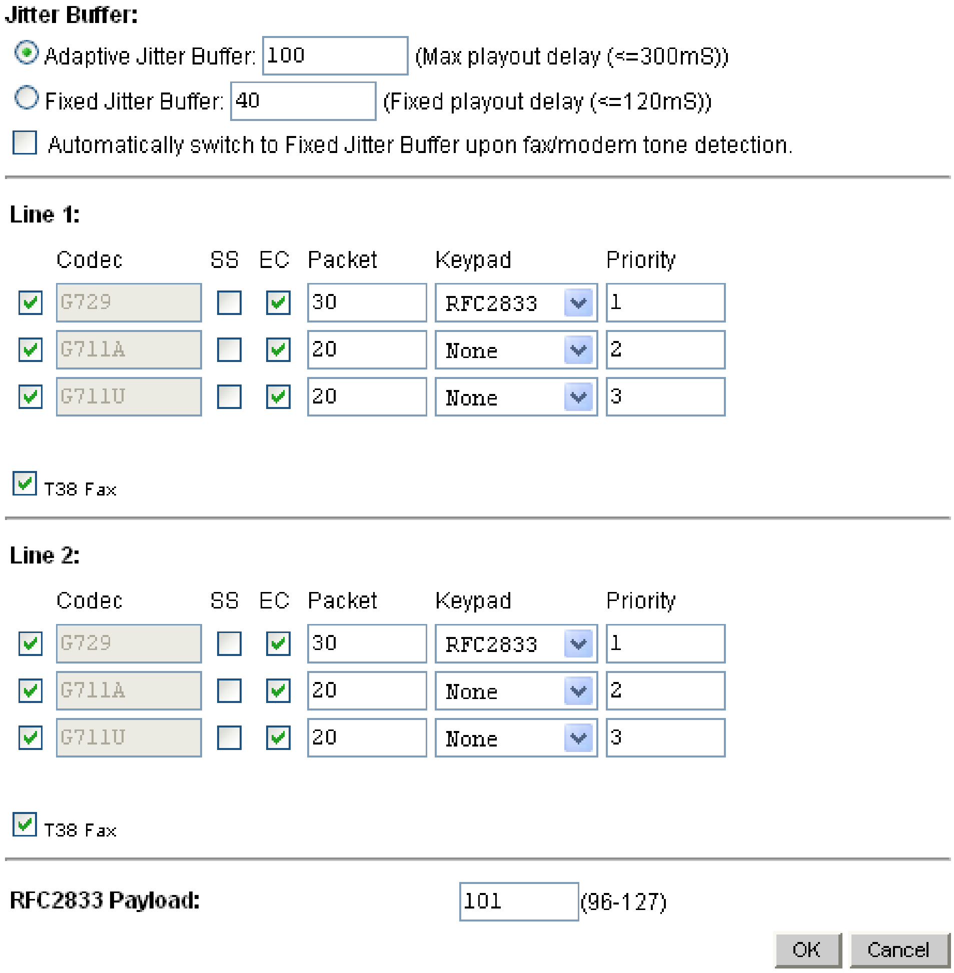
Function	**Description**
Dialplan	The Dialplan gives the DRG 11/22 a map to determine, when a complete number has been dialed. (T = by timeout, # = by pressing #). Default value for SIP version is (xx.#|xx.T) The current SIP revision can support the use of Dialplan to enable a hotline function. Below is an example of a Dialplan that enables a hotline function along with normal dialing: (xx.#|xx.T|<:1860>T) Substrings xx.# and xx.T are normal dial patterns, while <:1860>T enables hotline. If DIALTIMEOUT=4 (i.e., T=4), then the user will be able to dial any number that matches (xx.#|xx.T) within 4 seconds after off-hook. If no key is pressed within that duration, then the hotline will be activated and number 1860 will be dialed. DIALTIMEOUT can be set to zero so that the hotline will be triggered immediately.
Dial Timeout (seconds)	The number of seconds that the DRG 11/22 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. Default value is 4 seconds.
Use "#" as a quick dial function	When this field is enabled, # will be used as a quick-dial function, if it is in the end of a dial string. It will be removed before the dial string is sent to the server. When this field is disabled, # will not be removed.
RTP Port Range	Set the start and end port-range for RTP (Rapid Transport Protocol) protocol ports. Default values are 8000 and 8015.
Telephone line	Switch the telephone line On or Off. (Telephone must be set to ON, for this setting to take effect) Default value is Off.
HA mode	High Availability (support for secondary system): Off = Disable HA functionality. Fixed = Basic HA mode, when the primary server configured in the field "SIP Server IP (primary)" fails, the secondary server configured in the field "SIP Server IP (secondary)"will be registered, and when secondary server configured registers unsuccessfully, the primary server will be registered. Occasions when both servers configured fail may exist. Refer to below. Auto = This is the same as option Fixed. MS = When the primary server configured in the field "SIP Server IP (primary)" fails, the secondary server configured in the field "SIP Server IP (secondary)"will be registered. After the secondary server is registered successfully, the status of the primary server will be detected. Once the primary server configured register is available, the secondary server will be unregistered and the primary server registered. Occasions when both servers configured fail may exist.
SIP Server IP (primary)	The primary IP address for the SIP server/proxy that is responsible for managing the DRG 11/22 in the specific net. If HA-mode is set to Auto, the primary SIP server/proxy provides the DRG 11/22 with an IP-address to the secondary system during registration. FQDN (Fully Qualified Domain Name) is also possible to use.
SIP Server Port (primary)	Used port for primary system

Function	Description
SIP Server IP (secondary)	IP-address to secondary system.
SIP Server Port (secondary)	Used port for secondary system.
Outbound Proxy Mode	OFF = The outbound proxy is not used. All SIP REQUEST messages are sent to the SIP peer directly once the peer contact information is known. ON = The outbound proxy is used. It is assumed that the outbound proxy is the same server as the registrar, and all SIP REQUEST messages (except those for REGISTER) are sent to the outbound proxy. Specify = The outbound proxy is used. All SIP REQUEST messages are sent to a specific port of the outbound proxy with the specified IP or FQPN.
Outbound Proxy IP/FQPN	The IP address or FQPN of the outbound proxy
Outbound Proxy Port	The port of the specified outbound proxy
User Name	SIP user name.
Password	SIP user password.
Outgoing display Name	The name to be presented on the receiver's caller display (must be supported by network).
Telephone Number	The telephone number of the specific telephone line (can also be an e-mail address). Limited to 25 characters before the @-sign.
Telephone Domain Name	The domain-name, limited to 25 characters (after the @-sign). It can be the FQDN name or IP address.
Port	Outgoing signalling port on that particular telephone-line
Message Waiting Account	The account address for the voice message received storage
Incoming CLIP (Caller Line Identity Presentation)	Caller ID On/Off. If turned On, the telephone number of incoming calls will be presented on the caller display attached to the DRG 11/22.
Keep-alive timeout (seconds)	The interval that the DRG 11/22 suggests to network to send the keep-alive messages to the network. If keep-alive time is sent from the network, it will override the DRG 11/22 local setting.
Ring signal [0 - 9]	Choose between 10 different ring signals that the DRG 11/22 can provide (0-9).
Transport	Configure whether signaling will use UDP (User Diagram Protocol) or TCP (Transmission Control Protocol).
Preferred Codecs	Shows the current Voice Codecs/Fax settings. Click Set Codecs/Fax to change settings as described in Figure 7-18 Codec and fax configuration below.
POTS State	The states of the phone lines registered or unregistered.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

Click **Set Codecs/Fax** to change the settings. The Codecs and Fax Configuration window appears:

Figure 7-12 Codec and fax configuration



Jitter Buffer:

● Adaptive Jitter Buffer: 100 (Max playout delay (<=300mS))

○ Fixed Jitter Buffer: 40 (Fixed playout delay (<=120mS))

□ Automatically switch to Fixed Jitter Buffer upon fax/modem tone detection.

Line 1:

	Codec	SS	EC	Packet	Keypad	Priority
☑	G729	□	☑	30	RFC2833	1
☑	G711A	□	☑	20	None	2
☑	G711U	□	☑	20	None	3

☑ T38 Fax

Line 2:

	Codec	SS	EC	Packet	Keypad	Priority
☑	G729	□	☑	30	RFC2833	1
☑	G711A	□	☑	20	None	2
☑	G711U	□	☑	20	None	3

☑ T38 Fax

RFC2833 Payload: 101 (96-127)

The following table gives a detailed description of each value that can be configured on the Codecs and Fax Configuration window:

Function	Description
Jitter Buffer	
Adaptive Jitter Buffer	If Adaptive Jitter Buffer is preferred, which is pre-selected, specify the maximum value (up to 300 ms).
Fixed Jitter Buffer	If Fixed Jitter Buffer is preferred, select Fixed Jitter Buffer, and specify the buffer size (up to 120 ms).
Automatically switch to Fixed Jitter Buffer upon fax/modem tone detection	DRG will switch to Fixed Jitter Buffer mode automatically when there is Fax detected. Select to enable the function.
Line 1 Codec selection	It is possible to configure what Codecs to be used (G.711U/A and G.729 optional), the packet size (10 ms – 150 ms) and their preferred priority. Voice Codec negotiation/priority is always performing between 2 end-points and depending on which side that initiates the negotiation, the chosen Codec may be different from the local priority order. It is also possible to configure support for the T.38 fax protocol. One can also choose whether to use SS (Silence Suppression) or not.

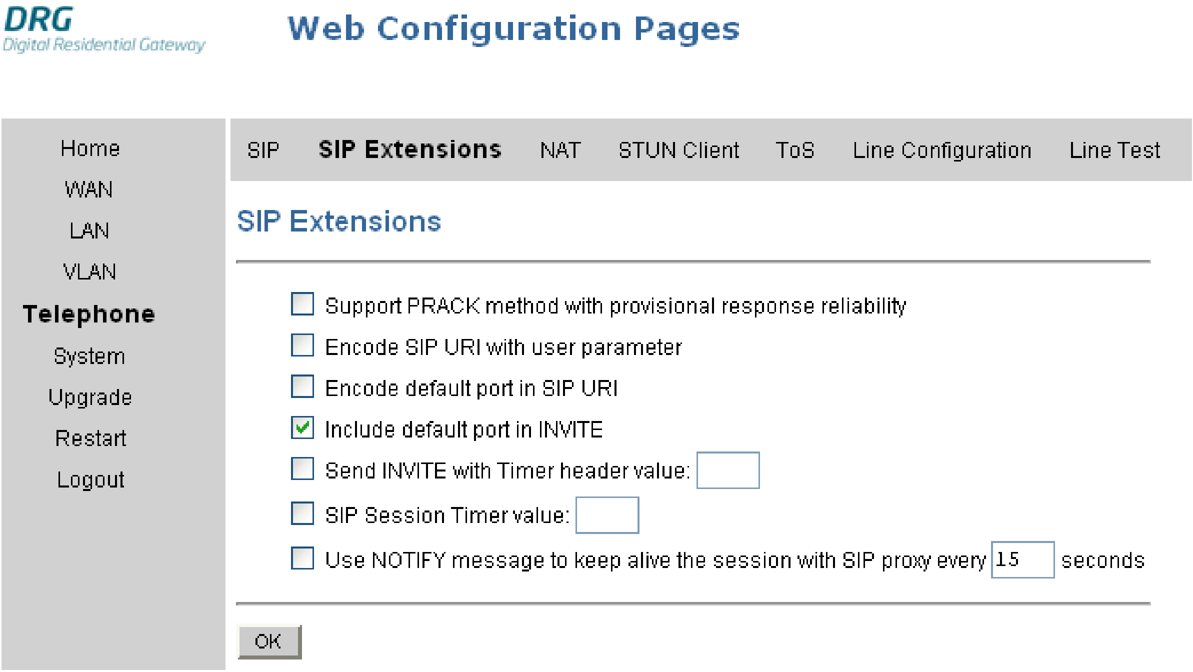
	The "Keypad" field tells which transmission method to be used for user inputting DTMF signaling (i.e. phone banking). "None" means inband, which should be used with G.711 only. When RFC2833 method is selected, users can input the RFC2833 Payload value between 96 and 127. (This function is valid only with SIP and H323 software versions.) SIP INFO and DTMF RELAY methods are valid only with SIP software versions.
Line 2 Codec selection	Refer to “Line 1 Codec selection” above.
T38 Fax	Select the function to enable T38 Fax function.

Click **OK** and return to the Telephone SIP Configuration page.

7.6.1 SIP Extensions

(Apply only to DRG 11/22 running SIP)

Figure 7-13 SIP extensions



SIP Extensions

□ Support PRACK method with provisional response reliability

□ Encode SIP URI with user parameter

□ Encode default port in SIP URI

☑ Include default port in INVITE

□ Send INVITE with Timer header value:

□ SIP Session Timer value:

□ Use NOTIFY message to keep alive the session with SIP proxy every 15 seconds

The following table lists the detailed description of each value configured on the SIP Extensions Configuration page:

Function	Description
Support PRACK method with provisional response reliability	The PRACK request plays a similar role as that of the ACK, but for provisional responses it is a normal SIP message like BYE. As such, its own reliability is ensured hop-by-hop through each stateful proxy. There is an important difference, however, PRACK has its own response. If this was not the case, the PRACK message could not have traversed proxy servers compliant to RFC 2543. More info in RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP).
Encode SIP URI with user parameter	Encode SIP URI with user parameters. Encode default port in SIP URI – Include standard port in SIP URI even though it is not mandatory according to standard.
Encode default port in SIP URI	Include standard port in SIP URI even though it is not mandatory according to standard.
Include default port in INVITE	Include default port in the INVITE even though it is not mandatory according to standard.

Function	Description
Send INVITE with timer header value	If the called UA (User Agent) or the SPS requires a session timer for a requested session and the calling UA does not include the Session-Expires header in the INVITE message, then the called UA or the SPS may reject the request with a 487-request failure message. If the use of a session timer is desirable but optional for the session, and the calling UA does not include the Session-Expires header in the INVITE, then the called UA or SPS may add a Session-Expires header to the next session setup message. In this case, the SPS will add the Session-Expires header to the INVITE message and the called UA will add the Session-Expires header to the 200 OK response messages.
SIP Session timer value	The SIP Session Timer Support feature adds the capability to periodically refresh SIP sessions by sending repeated INVITE requests. The repeated INVITE requests or re-INVITEs are sent during an active call log to allow UAs or proxies to determine the status of a SIP session. Without this keep-alive mechanism, proxies that remember incoming and outgoing requests (stateful proxies) may continue to retain call state needlessly. If a UA fails to send a BYE message at the end of a session or if the BYE message is lost because of network problems, a stateful proxy will not know that the session has ended. The re-INVITES ensure that active sessions stay active and completed sessions are terminated.
Use NOTIFY message to keep alive the session with SIP proxy every 15 seconds	The function will make DRG 11/22 send SIP NOTIFY messages to the SIP proxy at a regular interval. Such NOTIFY message can keep the connection with SIP proxy alive, as well as the NAT port mapping if DRG 11/22 is sitting behind NAT.

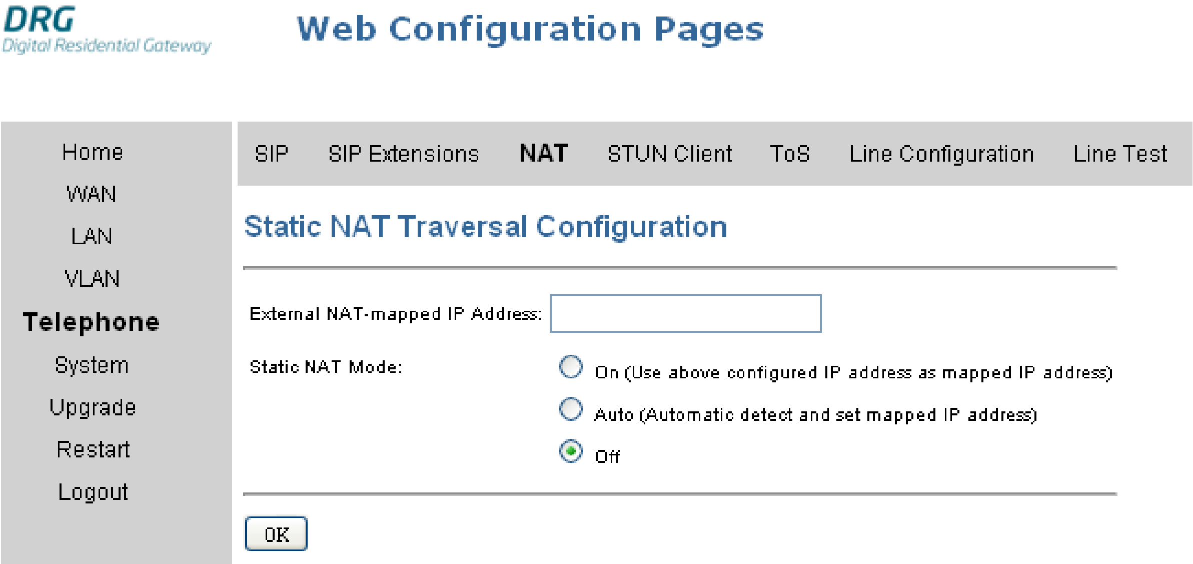
To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.6.2 NAT

(Apply only to DRG 11/22 running SIP)

The DRG 11/22 can be installed behind routers utilizing NAT (Network Address Translation). To allow the DRG 11/22 to pass a NAT, the DRG 11/22 can be configured in different ways.

Figure 7-14 NAT traversal configuration



Static NAT Traversal Configuration

External NAT-mapped IP Address:

Static NAT Mode:
○ On (Use above configured IP address as mapped IP address)
○ Auto (Automatic detect and set mapped IP address)
● Off

The NAT Traversal function can be used to allow the DRG 11/22 to register to a SIP proxy server even though the DRG 11/22 is connected behind a NAT device.

Port forwarding needs to be activated in NAT device for all telephone ports used by the DRG 11/22, e.g. the RTP port range and the SIP signaling ports.

The Keep-alive timeout, refer to the Telephony SIP table above, may need to be set to a lower value if the DRG 11/22 loses its registration to the SIP server before the default timeout of 1200 seconds.

NOTE! Message Keep-alive timeout can also be configured, refer to page 52.

The following table lists the detailed description of each value configured on the Static NAT Traversal Configuration page:

Function	Description
External NAT-mapped IP Address	IP address that the NAT device uses on WAN side. If the DRG 11/22 is set to Auto mode, the IP address of the outside IP will be automatically entered.
Static NAT Mode	On = Enable NAT Traversal function using manual setting. Auto = IF (“received” parameter in INVITE or REGISTER IP-address is not equal to internal IP-address) then enter NAT-mode. Off = NAT Traversal function disabled.

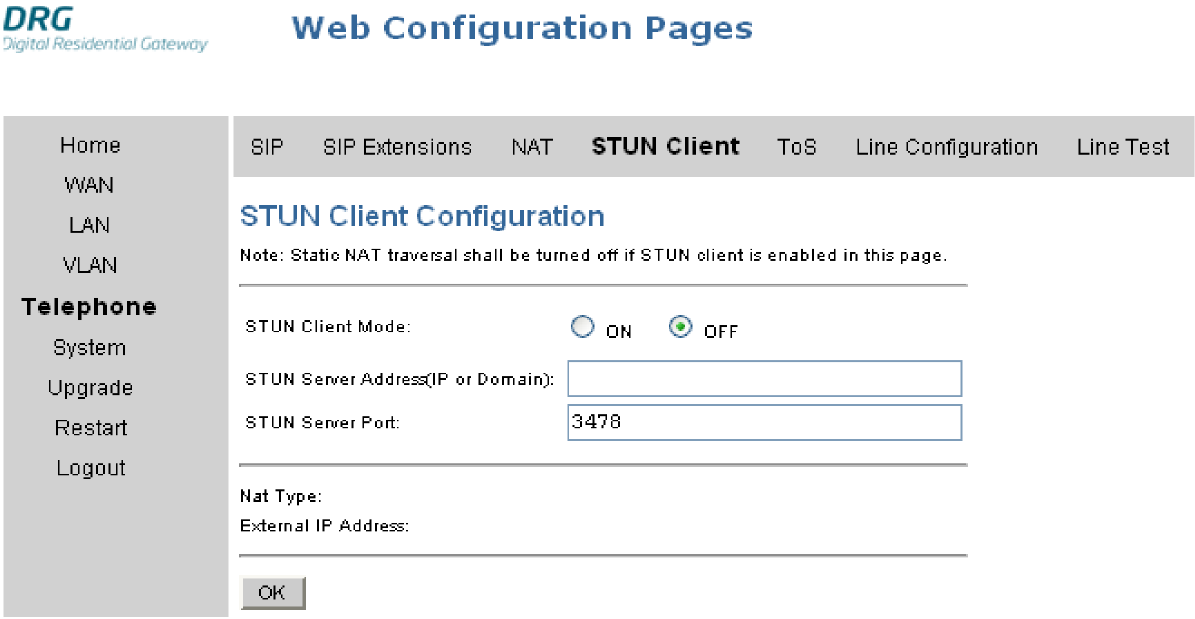
To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.6.3 STUN Client

(Apply only to DRG 11/22 running SIP)

The STUN Client Configuration implements the client function, as defined in RFC3489 STUN (Simple Traversal of UDP (User Datagram Protocol) through NATs (Network Address Translators)).

Figure 7-15 STUN client configuration



STUN Client Configuration

Note: Static NAT traversal shall be turned off if STUN client is enabled in this page.

STUN Client Mode: ○ ON ● OFF

STUN Server Address(IP or Domain):

STUN Server Port: 3478

Nat Type:

External IP Address:

NOTE! Static NAT traversal must be turned off if STUN Client is enabled. These two functions cannot work simultaneously.

The following table lists the detailed description of each value configured on the Stun Client Configuration page:

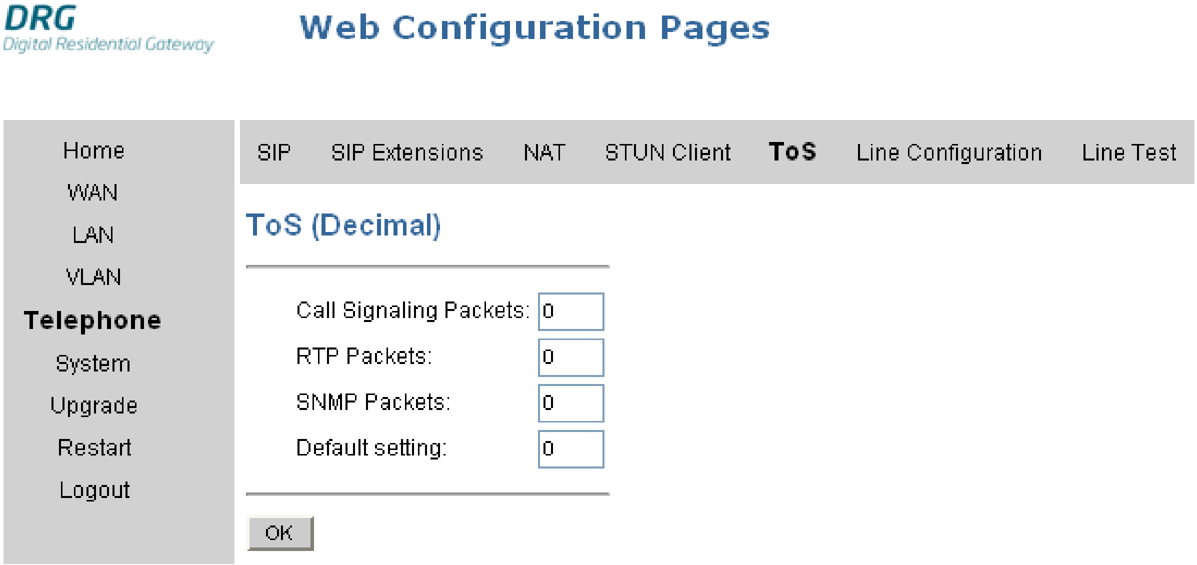
Function	**Description**
STUN Client Mode	Select ON to enable the function and OFF to disable it.
STUN Server Address (IP or Domain)	Specify the IP address or FQDN Domain name of the STUN Server.
STUN Server Port	Specify the port number of the STUN server. The default value is 3478.
Nat Type	This field displays the NAT type that the DRG 11/22 is connected behind and will be updated automatically if STUN client function is removed. There are several values: UDP_BLOCK: UDP packets are blocked by network. NO_NAT: DRG 11/22 is not behind any NAT. FULL_CONE_NAT: DRG 11/22 is behind full cone NAT. RESTRICT_NAT: DRG 11/22 is behind restricted NAT. PORT_RESTRICT_NAT: DRG 11/22 is behind port restricted NAT. SYMMETRIC_NAT: DRG 11/22 is behind symmetric NAT.
External IP Address	This field displays the mapped external IP Address when STUN is enabled.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.6.4 ToS

Outgoing telephone packets from the DRG 11/22 can be marked with ToS (Type of Service) values on both Call Signaling Packets and RTP packets.

Figure 7-16 ToS



ToS (Decimal)

Call Signaling Packets: 0

RTP Packets: 0

SNMP Packets: 0

Default setting: 0

The following table lists the detailed description of each value configured on the ToS Configuration page:

Function	Description
Call Signaling Packets	ToS value for Calling Signaling Packets with the default value of 192, DiffServ Code Point CS6
RTP Packet	ToS value for RTP Packets with the default value of 160, DiffServ Code Point CS5
SNMP Packets	ToS value for RTP Packets
Default setting	Default ToS value to be applied if no manual setting

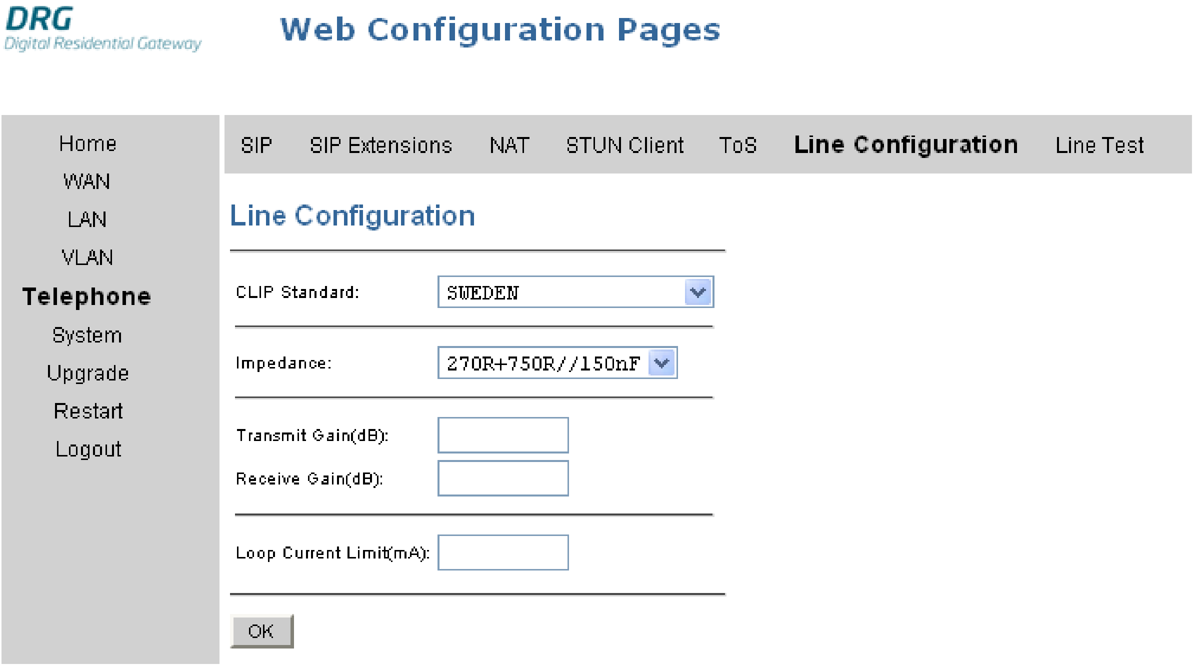
For more information about DiffServ Code Points, please read RFC 2474.

To make the settings or changes take effect, click **OK** and restart the DRG 100.

7.6.5 Line Configuration

Calling CLIR mode and some other electrical property settings of the call line are available on Line Configuration page.

Figure 7-17 Line configuration



CLIP Standard: SWEDEN

Impedance: 270R+750R//150nF

Transmit Gain(dB):

Receive Gain(dB):

Loop Current Limit(mA):

The following table lists a detailed description for each value configured on the Line Configuration page:

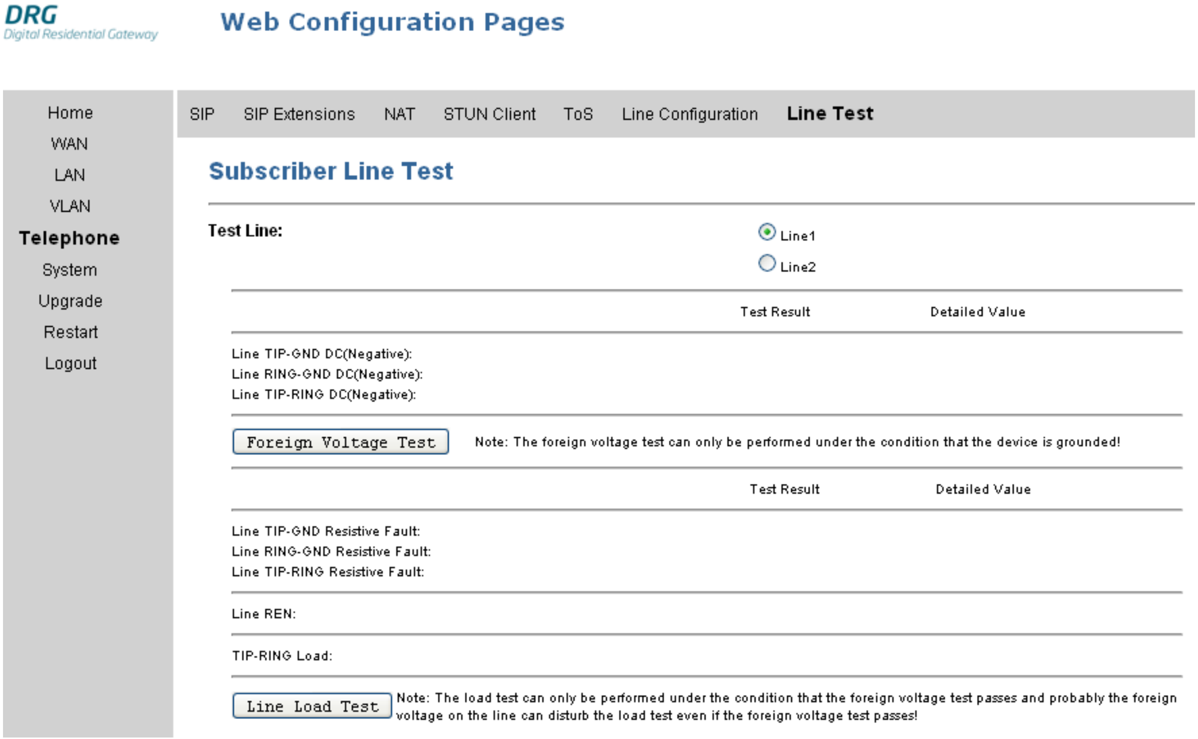
Function	**Description**
CLIP (Caller Line Identity Presentation) Standard	CLIP should be selected according to the geographic location of the user, and the default option is SWEDEN. **NOTE**! If none of the predefined standards are applicable, contact your DRG supplier for further assistance.
Impedance	Impedance value setting for the telephone lines are: 600R 900R 600R+2.16uF* 900R+2.16uF* 270R+750R//150nF (Default) 220R+820R//120nF 220R+820R//115nF 370R+620R//310nF
Transmit Gain	Analog to digital converter gain/attenuation value of the telephone lines; the value should be from -64dB to +6dB in 0.1dB steps. The default value is 0dB.
Receive Gain	Digital to analog converter gain/attenuation value for the telephone lines; the value should be from -64dB to +6dB in 0.1dB steps. The default value is -6dB.
Loop Current Limit	Constant loop current value for the telephone lines; the value may be set between20mA and 41mA in 3mA steps. The default current is 20mA.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.6.5.1 Line Test

The Subscriber Line Test page provides useful information for subscriber line troubleshooting.

Figure 7-18 Line test



Subscriber Line Test

Test Line: ● Line1 ○ Line2

	Test Result	Detailed Value
Line TIP-GND DC(Negative):		
Line RING-GND DC(Negative):		
Line TIP-RING DC(Negative):		

Note: The foreign voltage test can only be performed under the condition that the device is grounded!

	Test Result	Detailed Value
Line TIP-GND Resistive Fault:		
Line RING-GND Resistive Fault:		
Line TIP-RING Resistive Fault:		

Line REN:

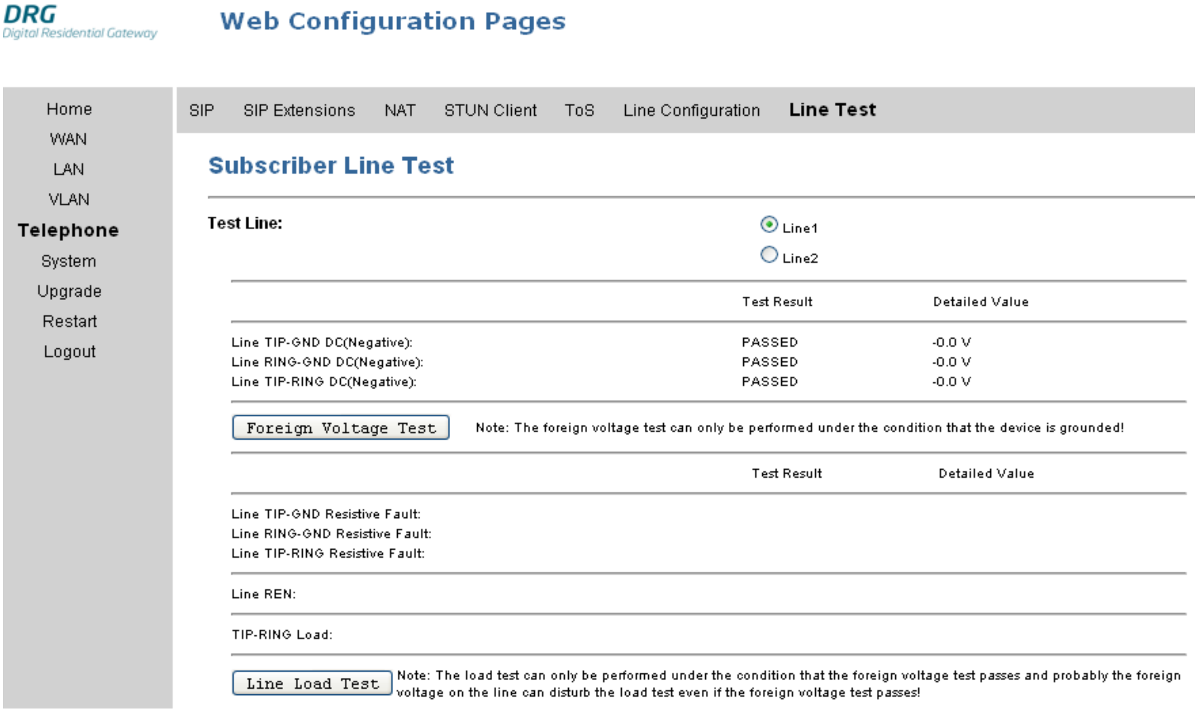
TIP-RING Load:

Note: The load test can only be performed under the condition that the foreign voltage test passes and probably the foreign voltage on the line can disturb the load test even if the foreign voltage test passes!

Select the Line on which the test is to be performed and click **Foreign Voltage Test**, the test takes about 2 seconds.

NOTE! The foreign voltage test can only be performed when the device is grounded.

Figure 7-19 Foreign voltage test result



Subscriber Line Test

Test Line: ● Line1 ○ Line2

	Test Result	Detailed Value
Line TIP-GND DC(Negative):	PASSED	-0.0 V
Line RING-GND DC(Negative):	PASSED	-0.0 V
Line TIP-RING DC(Negative):	PASSED	-0.0 V

Note: The foreign voltage test can only be performed under the condition that the device is grounded!

	Test Result	Detailed Value
Line TIP-GND Resistive Fault:		
Line RING-GND Resistive Fault:		
Line TIP-RING Resistive Fault:		

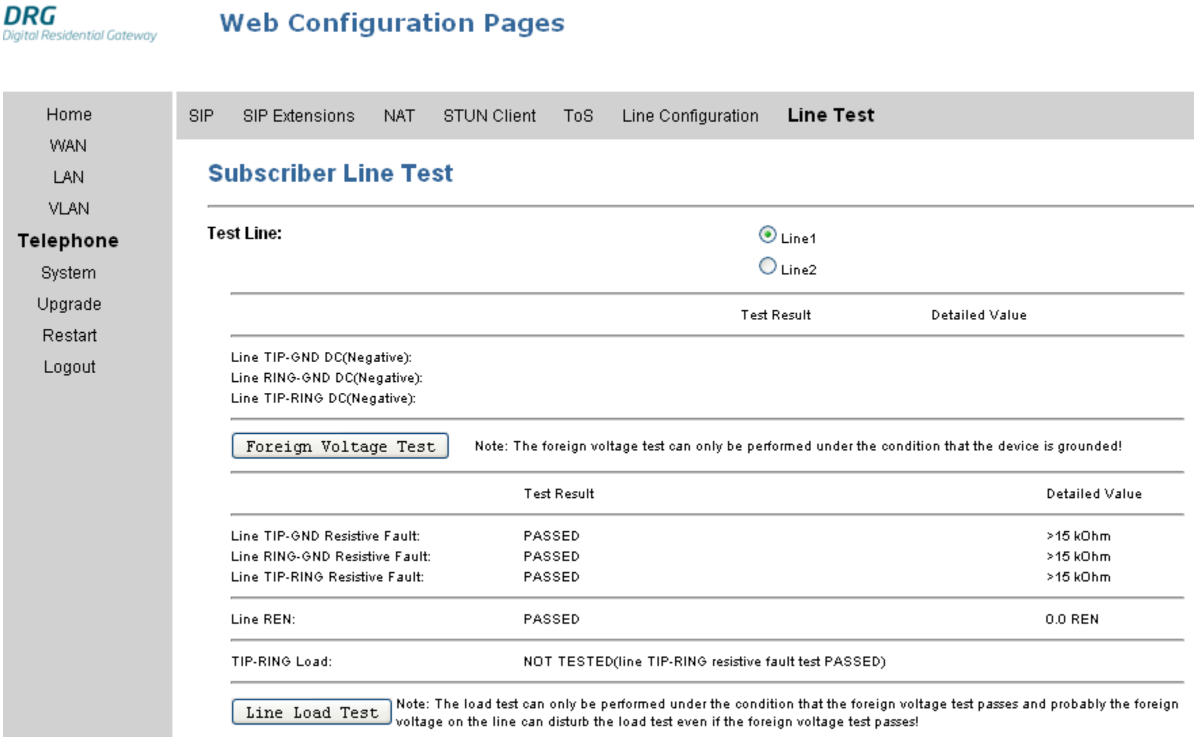
Line REN:

TIP-RING Load:

Note: The load test can only be performed under the condition that the foreign voltage test passes and probably the foreign voltage on the line can disturb the load test even if the foreign voltage test passes!

If the device can pass the foreign voltage test, then click **Line Load Test**. The test takes 12 seconds to 15seconds and the device needs to be restarted manually after the test.

Figure 7-20 Line load test result



Subscriber Line Test

Test Line: ● Line1 ○ Line2

	Test Result	Detailed Value
Line TIP-GND DC(Negative):		
Line RING-GND DC(Negative):		
Line TIP-RING DC(Negative):		

Foreign Voltage Test — Note: The foreign voltage test can only be performed under the condition that the device is grounded!

	Test Result	Detailed Value
Line TIP-GND Resistive Fault:	PASSED	>15 kOhm
Line RING-GND Resistive Fault:	PASSED	>15 kOhm
Line TIP-RING Resistive Fault:	PASSED	>15 kOhm
Line REN:	PASSED	0.0 REN
TIP-RING Load:	NOT TESTED(line TIP-RING resistive fault test PASSED)	

Line Load Test — Note: The load test can only be performed under the condition that the foreign voltage test passes and probably the foreign voltage on the line can disturb the load test even if the foreign voltage test passes!

Refer to the following table for the detailed line test description:

Test	**Description**
Foreign voltages The SLIC can only detect voltages between GND and Vbat. If there are foreign voltages outside this range, then the SLIC will be automatically deactivated (to save itself from damage). For the limitation of the SLIC, only negative voltage can be detected currently.	If the reported voltage is between GND and Vbat and meets the test pass criteria, then the test is marked as PASSED and the measured voltage provided. If the reported voltage is between GND and Vbat but does not meet the test pass criteria, then the test is marked as FAILED and the measured voltage provided. If the SLIC has been deactivated, then the test is marked as FAILED and the measured voltage is given as SHUTDOWN.
Resistive faults If the measured resistance is above 15kohm, the measured resistance is not accurate or particularly relevant.	If the reported resistance is >15kohm, then the test is marked as PASSED and the resistance is given as ">15kohm". If the reported resistance is <=15kohm, then the test is reported as FAILED and the reported resistance is provided.

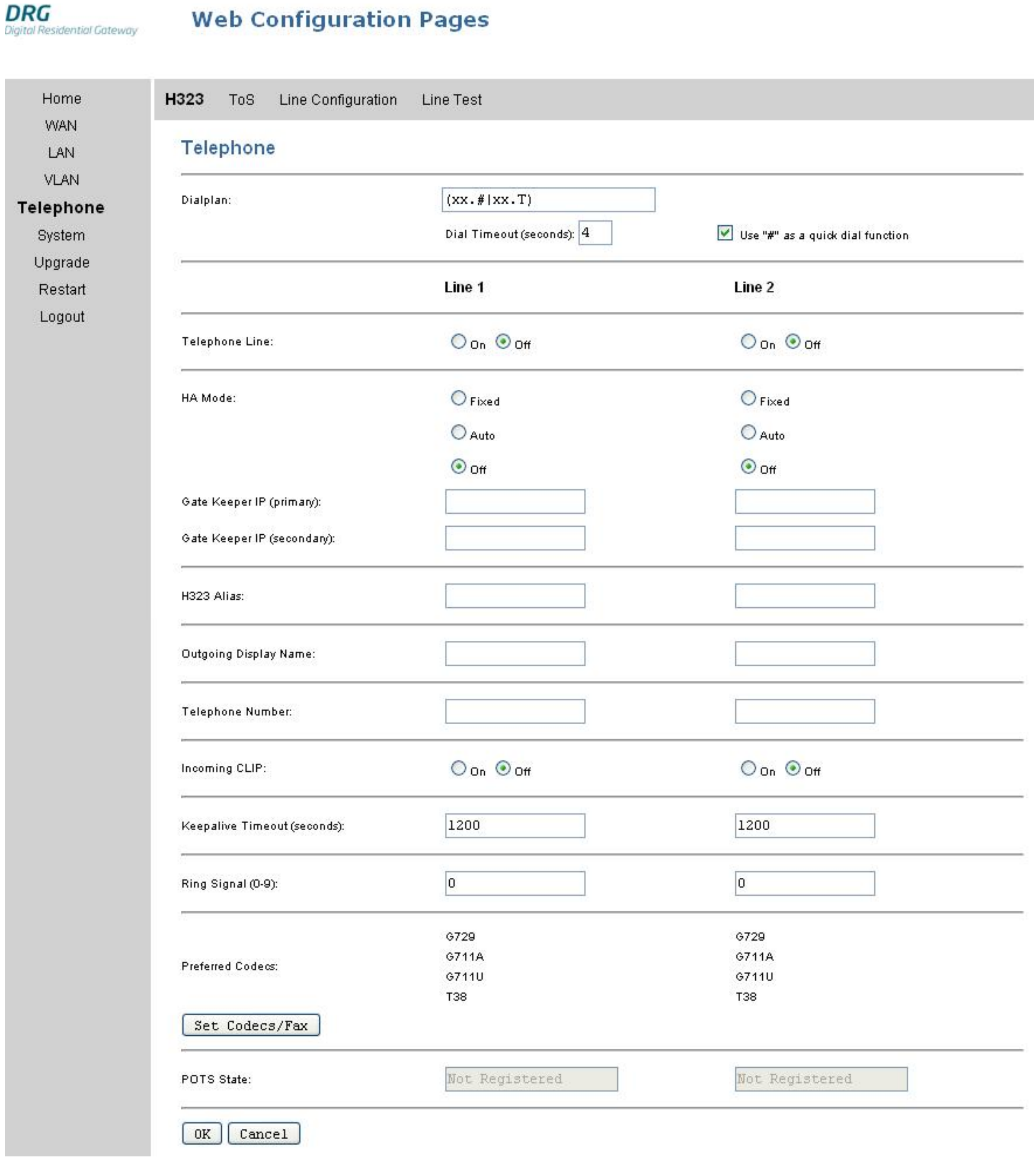
REN This test will only be performed, if the "Line TIP-RING resistive fault" test result is PASSED.	If the test is not performed, the result is given as "NOT TESTED (due to earlier failure)". No measured result is provided in this case. If the test is performed and the measured result is >3.0REN, then the result is given as FAILED and the measured result is provided. If the test is performed and the measured result is <=3.0REN, then the result is given as PASSED and the measured result is provided.
Line-Ring Load This test can only be performed, if the “Line TIP-RING resistive fault” test result is FAILED.	If the test is not performed, the result is given as "NOT TESTED (line TIP-RING resistive fault test PASSED)". No measured result is provided in this case. If the test is performed and the measured result means handset is offhook according to the criteria, then the result of “Offhook Handset” is provided. Besides, “Resistive” is provided.

7.7 Telephone H.323 Settings

(Apply only to DRG 11/22 running H.323)

The DRG 11/22 includes IP-telephony with one or two separate telephone lines. Each individual telephone line can be switched On or Off and configured separately.

Figure 7-21 Telephone H.323 configuration



Telephone

Dialplan: (xx.#|xx.T)

Dial Timeout (seconds): 4 ☑ Use "#" as a quick dial function

	Line 1	Line 2
Telephone Line:	○ On ● Off	○ On ● Off
HA Mode:	○ Fixed ○ Auto ● Off	○ Fixed ○ Auto ● Off
Gate Keeper IP (primary):		
Gate Keeper IP (secondary):		
H323 Alias:		
Outgoing Display Name:		
Telephone Number:		
Incoming CLIP:	○ On ● Off	○ On ● Off
Keepalive Timeout (seconds):	1200	1200
Ring Signal (0-9):	0	0
Preferred Codecs:	G729 G711A G711U T38	G729 G711A G711U T38
POTS State:	Not Registered	Not Registered

The following table gives a detailed description of each value that can be configured on the H.323 Configuration page:

Function	**Description**
Telephone:	
Dialplan	The Dialplan gives the DRG 11/22 a map to determine when a complete number has been dialed. (T = by timeout, # = by pressing #). Default value is "xx.T|xx.#".
Dial Timeout (seconds)	The number of seconds that the DRG 11/22 waits before it sends a complete telephone number. This is necessary since the whole telephone number is sent at once instead of digit by digit. Default value is 4 seconds.
Use "#" as a quick dial function	When this field is enabled, # will be used as a quick-dial function, if it is at the end of a dial string. It will be removed before the dial string is sent to the server. When this field is disabled, # will not be removed.
For each telephone line - Line 1 and Line 2, the following settings are available:	
Telephone Line	Switch the telephone line On or Off (Telephone must be set to ON, for this setting to take effect).
HA Mode	High Availability (support for the secondary gatekeeper) Fixed, Auto, Off.
Gatekeeper IP (primary)	The primary IP address for the Gatekeeper that is responsible for managing the DRG 11/22 in the specific net. If HA-mode is set to Auto, the primary Gatekeeper provides the DRG 11/22 with an IP-address to the AltGK during registration.
Gatekeeper IP (secondary)	IP-address to the secondary system
H.323 Alias	The DRG 11/22-name to use when registering the DRG 11/22 at the Gatekeeper. NOTE! The H.323 alias and the telephone number must be set to unique values for each telephone line.
Outgoing Display Name	The name to be presented on the receiver's caller display. (Network must support this function!)
Telephone Number	The telephone number of the specific telephone line.
Incoming CLIP	If turned On, the telephone number of incoming calls is presented on the caller display attached to the DRG 11/22.
Keep-alive Timeout (seconds)	The interval that the DRG 11/22 suggests sends the keep-alive messages to the Gatekeeper. If keep-alive time is sent from the Gatekeeper, it will override the DRG 11/22 local setting. Default is 1200 seconds.
Ring signal [0 - 9]	Choose from 10 different ring signals that the DRG 11/22 can use (0-9).
Preferred Codecs	Shows the current Codecs/Fax settings. Click the "Set Codecs/Fax" button to change settings, refer to section Telephony SIP above.
POTS State	The states of the phone lines, registered or unregistered

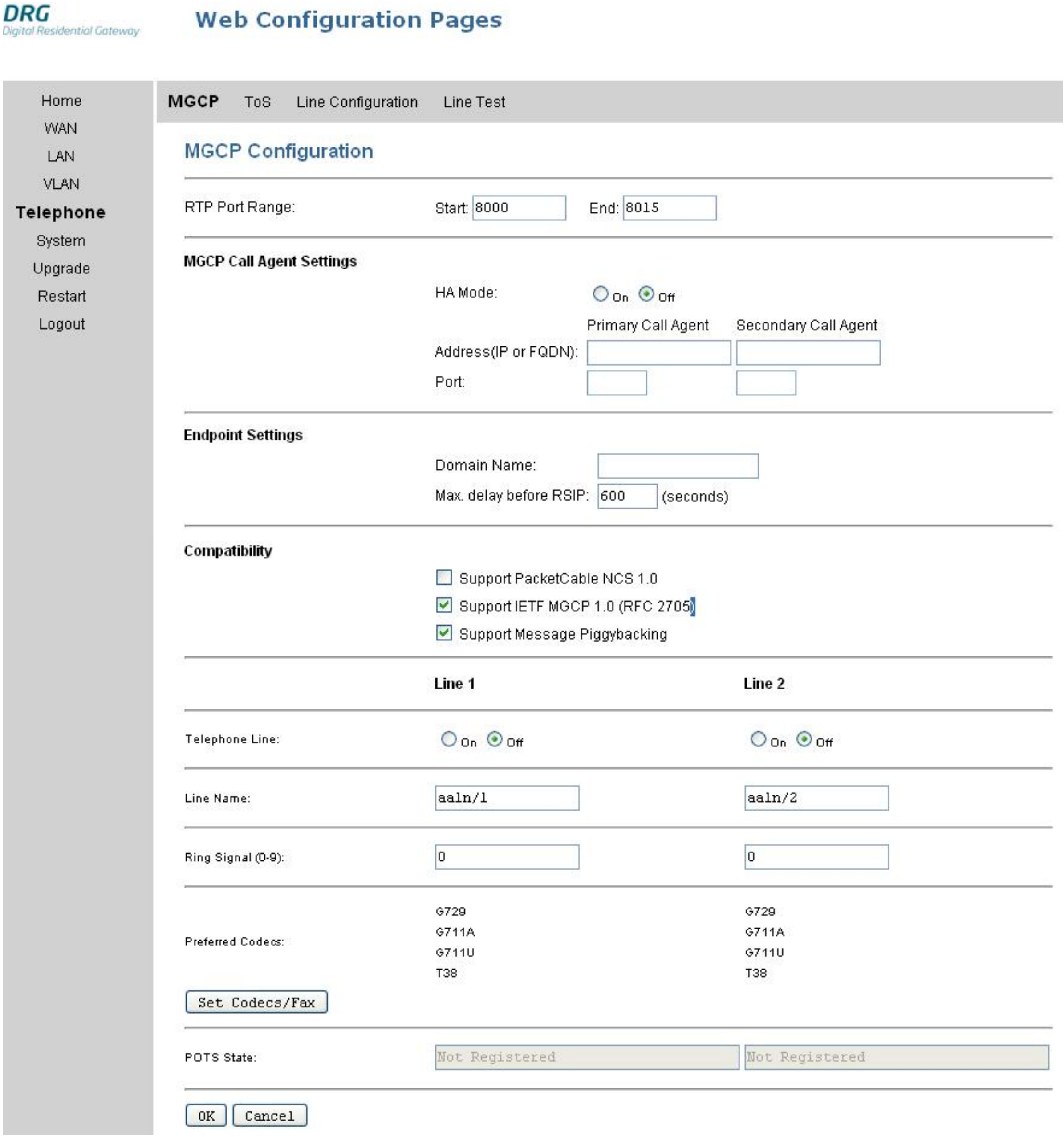
To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.8 Telephone MGCP Settings

(Apply only to DRG 11/22 running MGCP (Media Gateway Control Protocol))

The DRG 11/22 includes IP-SIP with one or two separate telephone lines. Each individual telephone line can be switched On or Off and configured separately.

Figure 7-22 Telephone MGCP configuration



MGCP Configuration

RTP Port Range: Start: 8000 End: 8015

MGCP Call Agent Settings

HA Mode: ○ On ● Off

	Primary Call Agent	Secondary Call Agent
Address(IP or FQDN):		
Port:		

Endpoint Settings

Domain Name:

Max. delay before RSIP: 600 (seconds)

Compatibility

□ Support PacketCable NCS 1.0

☑ Support IETF MGCP 1.0 (RFC 2705)

☑ Support Message Piggybacking

	Line 1	Line 2
Telephone Line:	○ On ● Off	○ On ● Off
Line Name:	aaln/1	aaln/2
Ring Signal (0-9):	0	0
Preferred Codecs:	G729 G711A G711U T38	G729 G711A G711U T38
POTS State:	Not Registered	Not Registered

The following table gives a detailed description of each value that can be configured on the MGCP Configuration page:

Function	Description
RTP Port Range	Set start and end port for RTP protocol ports. The default values are 8000 and 8015.
MGCP Call Agent Settings:	

Function	Description
HA Mode	High Availability (support for secondary server): When the registration to the primary server is failed, DRG will turn to make registration to the secondary server, while if there is failure upon the secondary server registration, DRG will register to the primary server. Set On to enable HA Mode or Of to disable it. The default setting is Off.
Address (IP or FQDN)	Addresses of the primary and secondary MGCP server Enter the IP address or the FQDN (Fully Qualified Domain Name).
Port	Signaling port numbers of the primary and secondary server, the default value is 2427.
Endpoint Settings:	
Domain Name	Specify the domain name.
Max. delay before RSIP ()	Specify the maximum delay before DRG 11/22 sends first RSIP after DRG 11/22 is up and running. Default value is 600 seconds.
Compatibility:	
Support PacketCable NCS 1.0	Enable or disable support for PacketCable NCS1.0.
Support IETF MGCP 1.0 (RFC 2705)	Enable or disable support for RFC2705.
Support Message Piggybacking	Enable or disable support for Message Piggybacking.
For each telephone line -Line 1 and Line 2, the following settings are available:	
Telephone line	Switch the telephone line On or Off. (Telephone must be set to ON, for this setting to take effect)
Line Name	Specify the line name, which should match configuration in the MGCP server.
Ring signal [0 - 9]	Choose one of the 10 different ring signals that the DRG 11/22 uses (0-9).
Preferred Codecs	Display the current Codecs/Fax settings. Click Set Codecs/Fax to change settings, refer to section "Telephony SIP" above.
POTS State	Display the states of the phone lines, registered or unregistered.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.9 System Settings

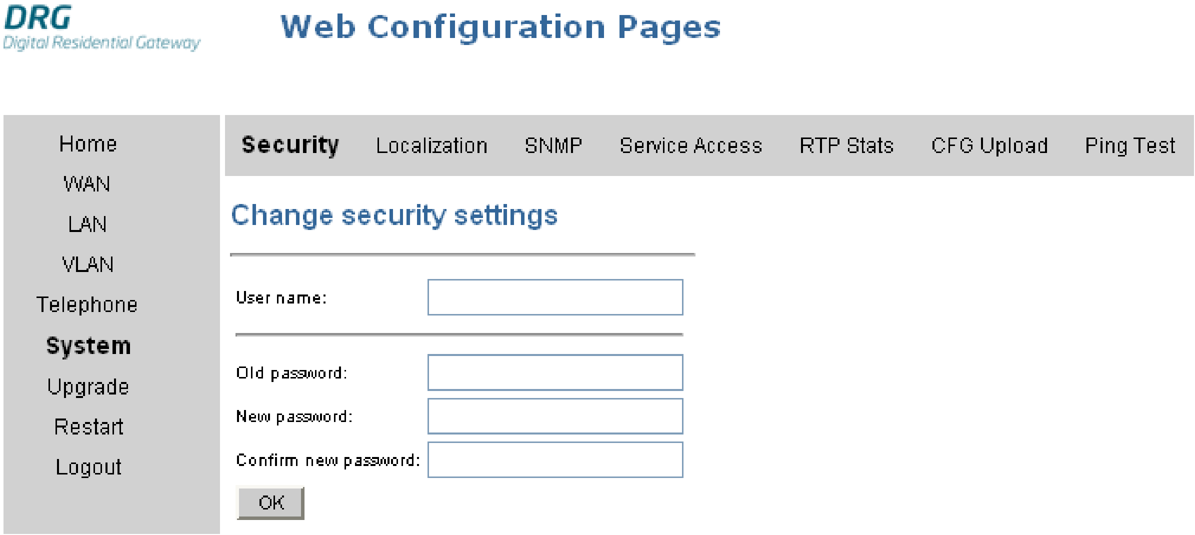
7.9.1 Security

The DRG is equipped with password protection and access control by changing the password. In order to make the system accept the new password, you need to enter your old password at first.

By default the *operator* can only access the DRG 11/22 from WAN and the *admin* can only access from LAN. To change the access mode, you need to enter your user name.

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

Figure 7-23 Change security settings



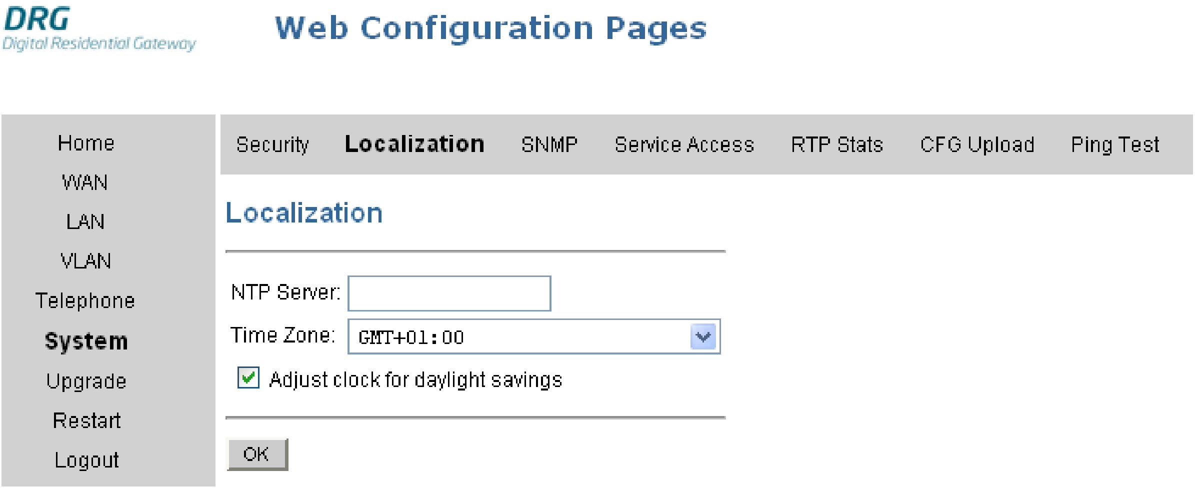
The following table gives a detailed description of each value that can be configured on the Security Settings page:

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 to confirm it.

To make the settings or changes take effect, click **OK** and restart the DRG 100.

7.9.2 Localization/Time setting

Figure 7-24 Localization



Localization

NTP Server:

Time Zone: GMT+01:00

☑ Adjust clock for daylight savings

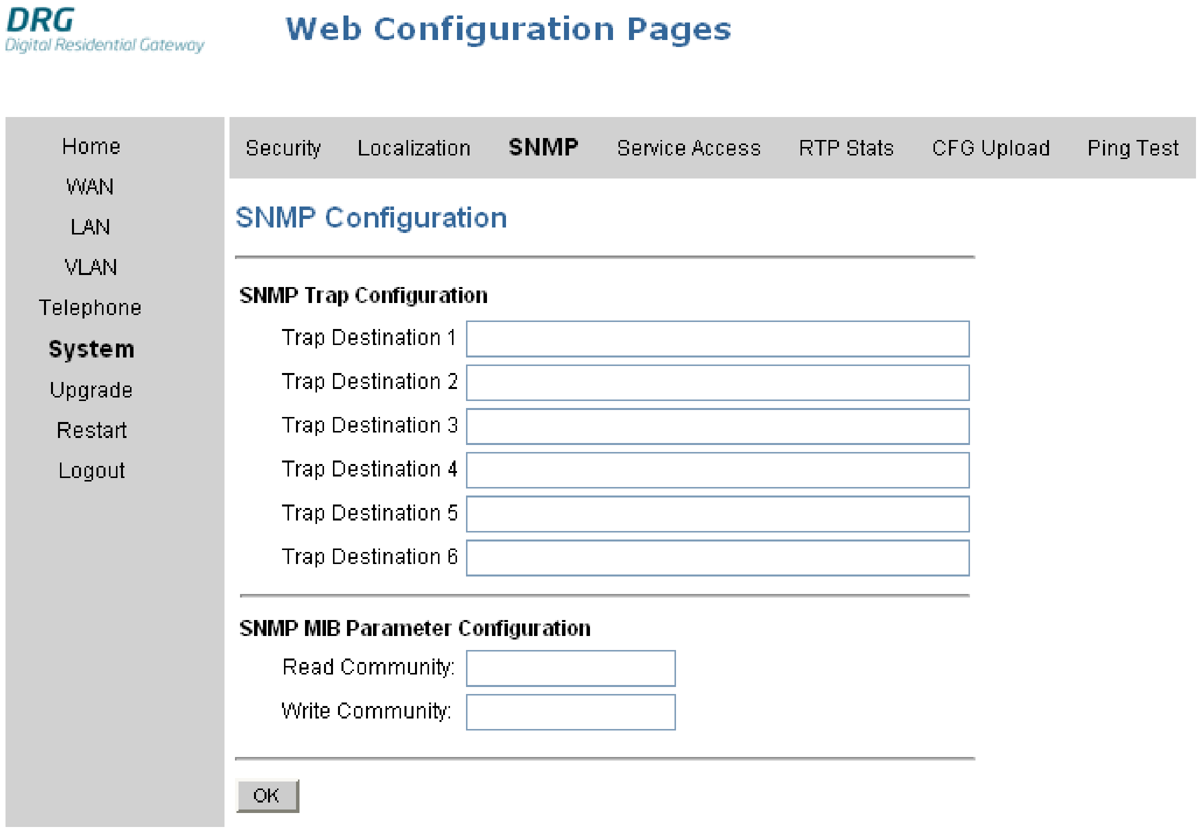
The following table gives a detailed description of each value that can be configured on the Localization page:

Function	**Description**
NTP Server	Specify the address of the NTP-server. An NTP (Network Time Protocol) server provides an accurate clock signal used for time synchronization.
Time Zone	Specify the time zone where the DRG 11/22 is located.
Adjust clock for daylight savings	Select and the DRG 11/22 will set the time one hour ahead.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.9.3 SNMP Configuration

Figure 7-25 SNMP configuration



The following table gives a detailed description of each value that can be configured on the SNMP Configuration page:

Function	**Description**
SNMP Trap Configuration	Configure multiple SNMP Trap Destinations to which the DRG 11/22 will send SNMP Traps.
Trap Destination 1~6	Specify the addresses (up to 6) where SNMP traps will be sent. Each address will be added to the SNMP White List, please refer to the SNMP White List on next page.
SNMP MIB Parameter Configuration	Configure the Read and Write SNMP Community.
Read Community	Specify the read community key. Default value is public.
Write Community	Specify the write community key. Default value is private.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.9.3.1 SNMP White List

SNMP White List provides a more secure interaction between DRG 11/22 and the Element Manager (EM). The white list is a list of IP addresses. The DRG 11/22 will check whether the source address requested by EM matches one of the hosts in the white list. If not, the request will be dropped. If the white list is empty, this check will not be done on the EM that wants to contact the DRG 11/22.

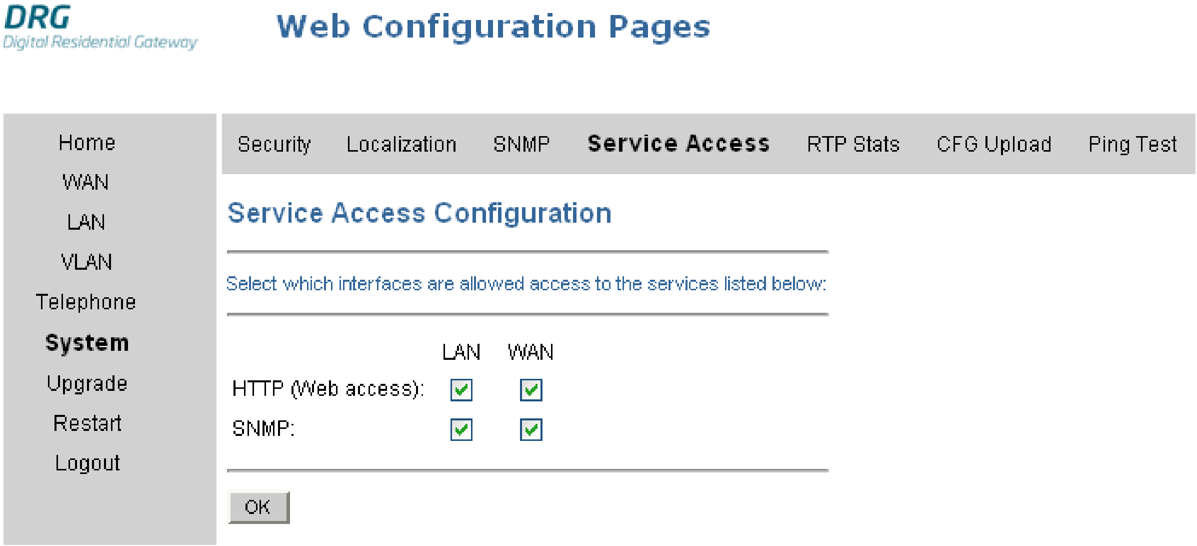
If the SNMP-trap list is empty, the SNMP White List function will be disabled and all management systems will be accepted by the DRG 11/22.

For example, if you specify Trap Destination 1: Drgmgr public 10.100.100.2 YYYYY, then IP address "10.100.100.2" will be added to the IP address White List, accepted as a manager authorized to manage the DRG 11/22.

7.9.4 Service Access

Service Access allows the operator to limit access to HTTP and SNMP services from both the LAN and WAN port.

Figure 7-26 Service access configuration



Service Access Configuration

Select which interfaces are allowed access to the services listed below:

	LAN	WAN
HTTP (Web access):	☑	☑
SNMP:	☑	☑

The following table gives a detailed description of each value that can be configured on the Service Access Configuration page:

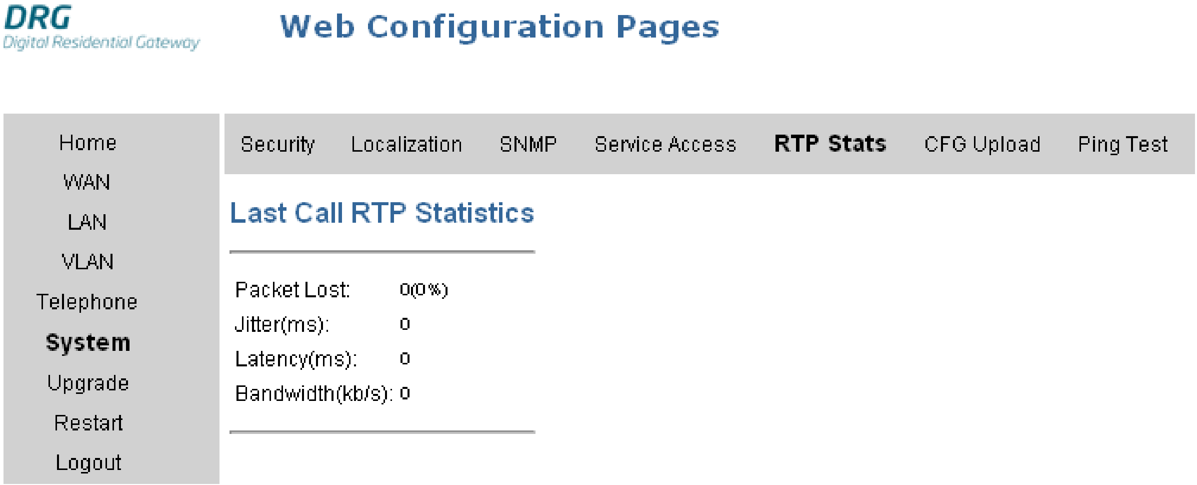
Function	Description
HTTP (Web Access)	Select the interfaces where user can access to the services, WAN or LAN.
SNMP	Select the interfaces where user can access to the services, WAN or LAN.

To make the settings or changes take effect, click **OK** and restart the DRG 11/22.

7.9.5 RTP Statistics

The Last Call RTP Statistics information makes it possible for an operator to remotely monitor the performance of a call in terms of bandwidth, jitter, packet loss, and latency. To get reliable data, call duration must be more than 60 seconds.

Figure 7-27 Last call RTP statistics



Last Call RTP Statistics

Packet Lost: 0(0%)
Jitter(ms): 0
Latency(ms): 0
Bandwidth(kb/s): 0

The RTP statistics are sent to the syslog server in the format of a standard syslog message. The parameter "SYSLOG_SVR" in the ini-file is used for specifying this function. No syslog messages are sent out unless this parameter is specified in the ini-file. The parameter has the following configuration format:

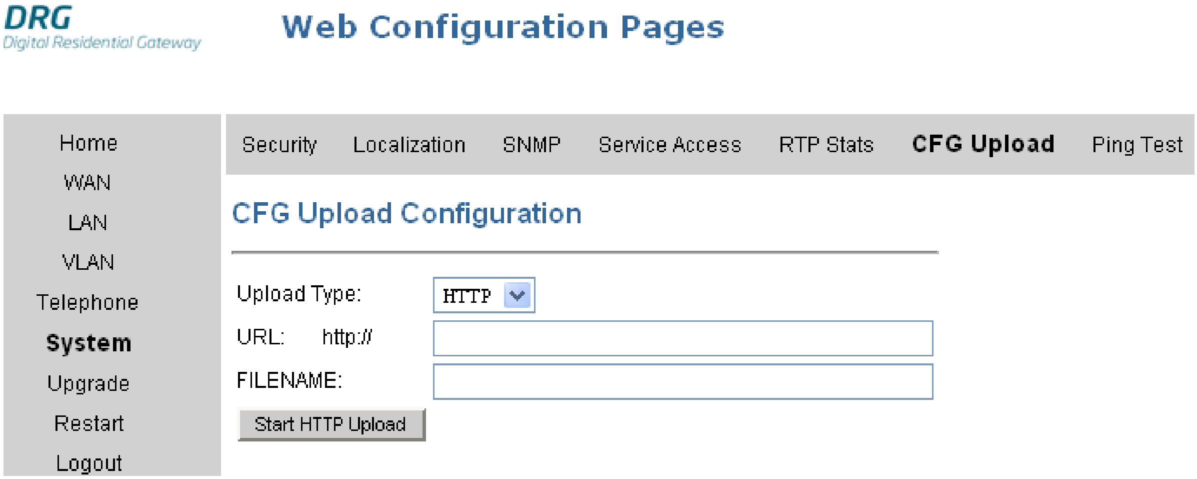
SYSLOG_SVR=servername[:port]

The default port value 514 will be applied if the port doesn't exist.

7.9.6 CFG Upload

The complete configuration of the DRG 11/22 can be uploaded to a remote server specified with a URL. The uploaded configuration may be useful for troubleshooting.

Figure 7-28 CFG upload configuraiton



CFG Upload Configuration

Upload Type: HTTP
URL: http://
FILENAME:

The following table gives a detailed description of each value that can be configured on the CFG Upload Configuration page:

Function	Description
Upload type	Only HTTP (POST) is currently supported.
URL	This is the remote address of the configuration data specified in the following format "FQDN:Port/Path", e.g. example.com:80/foo.cgi. The

	port is optional and 80 is used if not specified.
File Name	The name used for the uploaded configuration data file

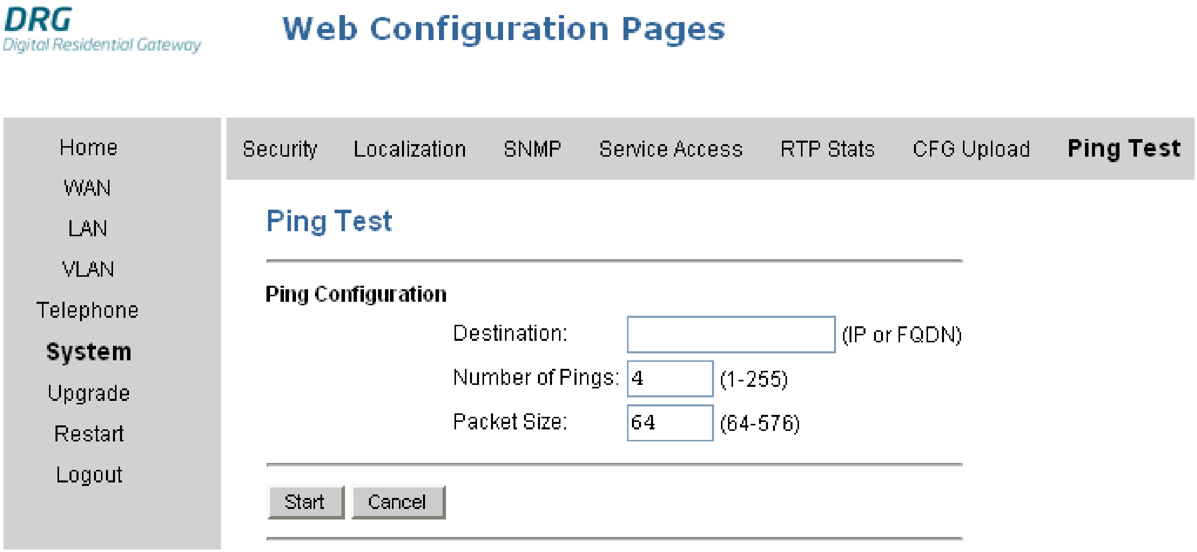
To make the settings or changes take effect, click **Start HTTP Upload** and restart the DRG 11/22.

7.9.7 PING Test

This feature makes it possible for users to perform a PING command from the Web GUI.

1. If the DRG is performing a PING operation for one user logged in the Web GUI, any other users already logged in will not be able to initiate a PING operation from the web GUI until the current operation is finished.
2. However, if a PING operation is requested by HDD, the DRG will exit any running PING operation (even if it was initiated by a web GUI user or a previous HDD instruction) and perform the new PING operation as requested.

Figure 7-29 Ping test



Ping Test

Ping Configuration

Destination: (IP or FQDN)

Number of Pings: 4 (1-255)

Packet Size: 64 (64-576)

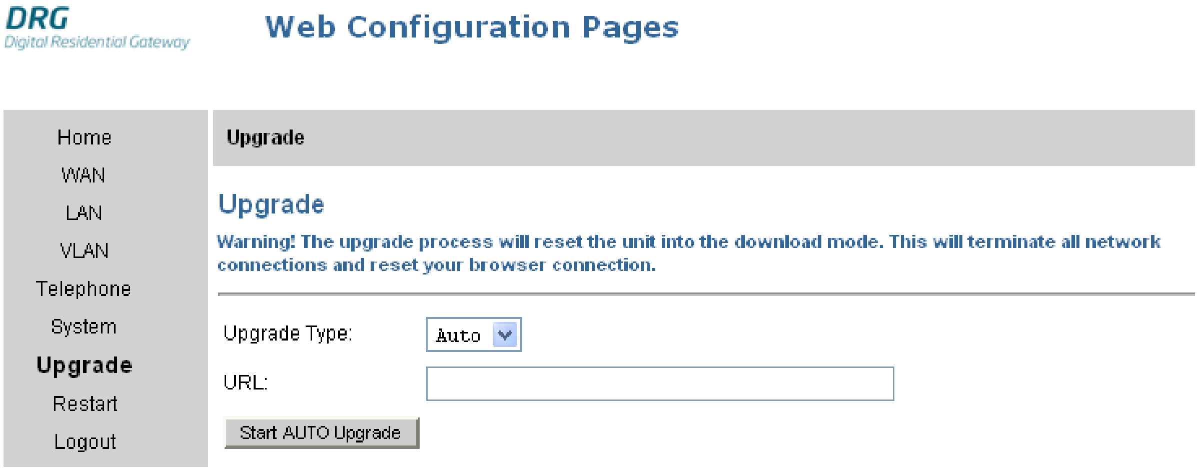
7.10 Upgrade Settings

There are three types of software upgrade methods:

- Auto
- HTTP
- TFTP

7.10.1 Auto Upgrade

Figure 7-30 Auto upgrade



Upgrade

Warning! The upgrade process will reset the unit into the download mode. This will terminate all network connections and reset your browser connection.

Upgrade Type: Auto

URL:

If "Auto" is selected, the DRG 11/22 will first try to use HTTP upgrade. If the upgrade fails, the DRG 11/22 will use TFTP.

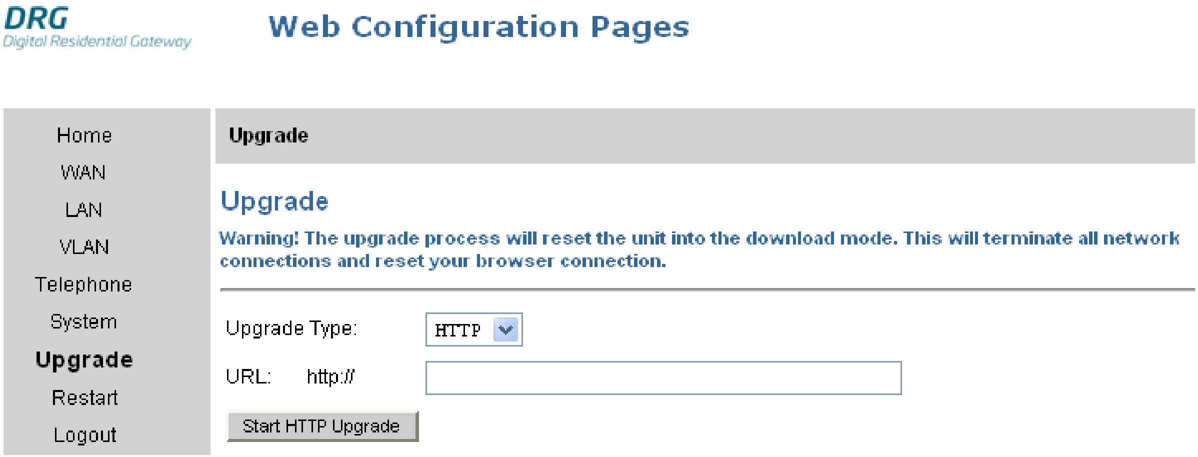
Function	Description
URL	Specify the URL of the HTTP/TFTP server. FQDN or IP address can be used.

Click **Start AUTO Upgrade** and restart the DRG 11/22 to apply the settings.

7.10.2 HTTP Upgrade

NOTE! When upgrading the software with HTTP, please make sure that the version of your downloader is higher than R2A01. This is required to support HTTP.

Figure 7-31 HTTP upgrade



Upgrade

Warning! The upgrade process will reset the unit into the download mode. This will terminate all network connections and reset your browser connection.

Upgrade Type: HTTP

URL: http://

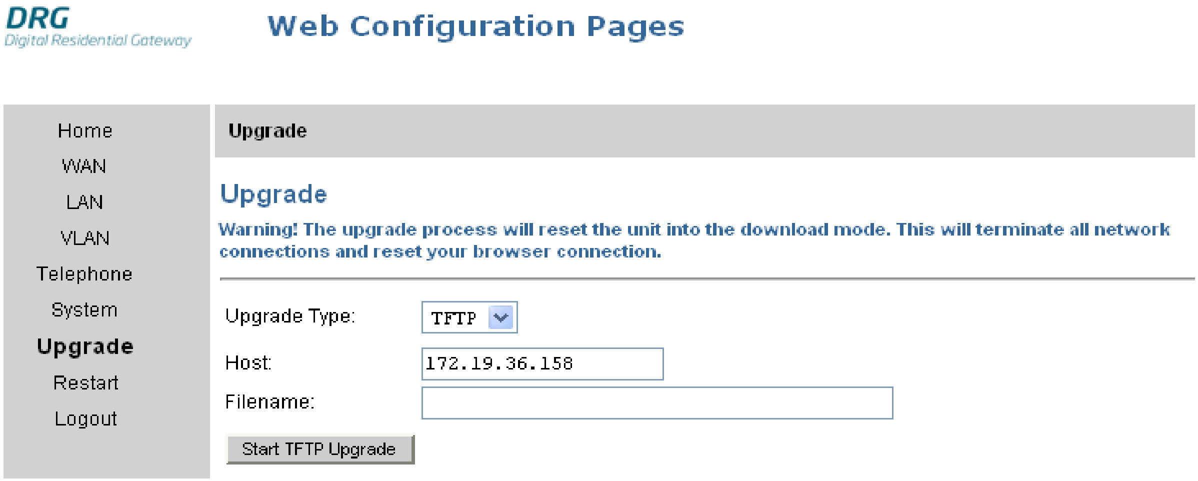
Upgrading of software and configuration through .ini-files is done by downloading a file from an HTTP-server.

Function	Description
URL	Specify the URL of the HTTP server. FQDN or IP address can be used.

Click **Start HTTP Upgrade** and restart the DRG 11/22 to apply the settings.

7.10.3 TFTP Upgrade

Figure 7-32 TFTP upgrade



Upgrade

Warning! The upgrade process will reset the unit into the download mode. This will terminate all network connections and reset your browser connection.

Upgrade Type: TFTP

Host: 172.19.36.158

Filename:

Upgrading of software and configuration using .ini-files is done by downloading a file from a TFTP-server.

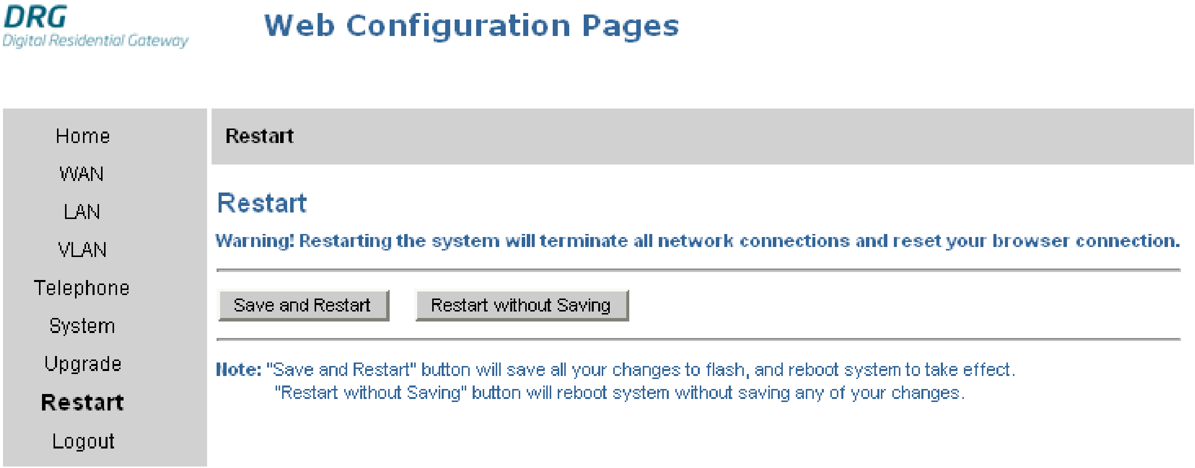
Function	Description
Host	Specify the IP address of the TFTP server.
Filename	Specify the upgrade file to download from the TFTP server. Only an IP address can be used to specify a TFTP server.

Click **Start TFTP Upgrade** and restart the DRG 11/22 to apply the settings.

7.11 Restart

After configuration changes have been made, the DRG 11/22 must be restarted to use the new settings. Click **Save and Restart** to save the settings and the DRG reboots to make the setting take effect. Click **Restart without Saving** to reboot the DRG without any changes to the original settings.

Figure 7-33 Restart



Restart

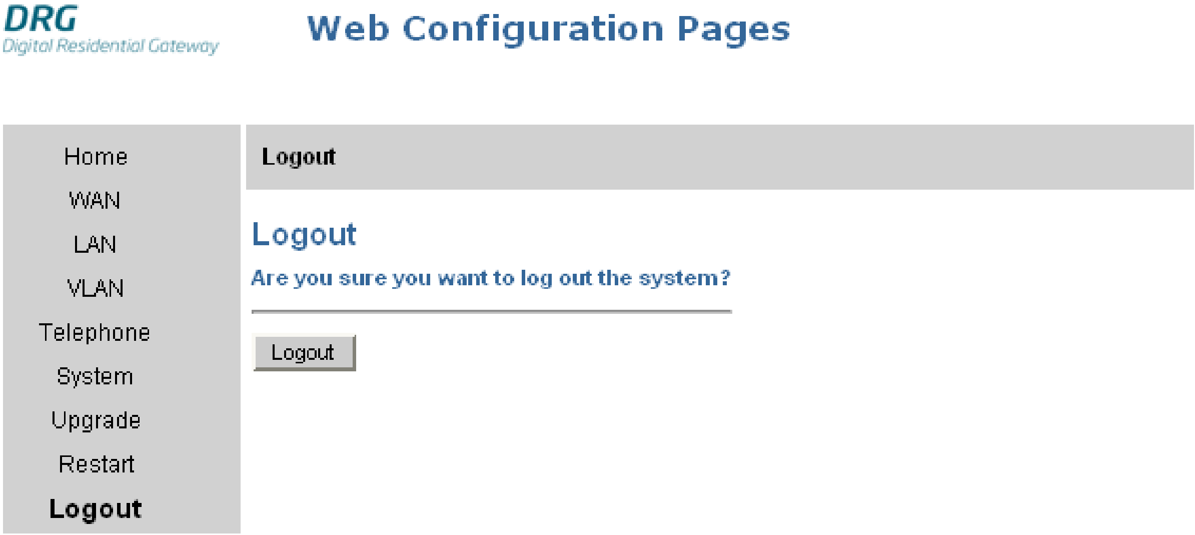
Warning! Restarting the system will terminate all network connections and reset your browser connection.

Note: "Save and Restart" button will save all your changes to flash, and reboot system to take effect.
"Restart without Saving" button will reboot system without saving any of your changes.

7.12 Logout

To close the session and logout from the DRG 11/22 unit, click **Logout**.

Figure 7-34 Logout



Logout

Are you sure you want to log out the system?

8 Standards and Protocols

DHCP - Dynamic Host Configuration Protocol

G3 – Fax model type

G711 - speech codec 10/20/30/40 ms

G729ab, G723.1 – speech codecs

G.165, G.167, G.168 – Echo Cancellation

H.248 – Control media gateways to support voice/fax calls. ITU is H.248, IETF is Megaco.

H.323 - Provide audio-visual communication sessions on any packet network

HTTP – Hyper Text Transfer Protocol

ICMP – Internet Control Message Protocol

IGMP – Internet Group Management Protocol

IEEE 802.1D - Transparent Bridging

IEEE 802.1Q - Virtual Bridged Local Network

IEEE 802.1p - QoS tagging in Ethernet frame

IEEE 802.2 – Logical Link Control

IEEE 802.3 - 10/100 MB Ethernet

IPv4 - Internet Protocol

MGCP – Media Gateway Control Protocol

NTP – Network Time Protocol

RTCP – Real Time Control Protocol

RTP – Real Time Protocol

SIP – Session Initiation Protocol

SNMP - Simple Network Management Protocol

T.38 – Fax protocol over TCP/IP

TCP - Transmission Control Protocol

TFTP – Trivial File Transfer Protocol

UDP - User Datagram Protocol

9 Abbreviations

BTE	Broadband Telephony Enabler
BWA	Broadband Wireless Access
CATV	Cable TV
CDS	Configuration Distribution Server
HDD	Home Device Director
CNI	Calling Number Identification
CoS	Class of Service
CPE	Customer Premises Equipment
DoS	Denial-of-Service
DRG	Digital Residential Gateway
DS	Differential Service
DTMF	Dual Tone Multi Frequency
FSK	Frequency Shift Keying
FTU	Fiber Termination Unit
GUI	Graphical User Interface
LAN	Local Area Network
LED	Light Emitting Diod
MCC	Media Converter for Cable TV
MDI	Medium Dependent Interface
MIB	Management Information Base

MTBF	Mean Time Between Failure
O&M	Operations and Maintenance
POTS	Plain Old Telephone Service
PNP	Private Numbering Plan
QoS	Quality of Service
SOHO	Small Office Home Office
TOS	Type of Service
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoD	Video-on-Demand
VoIP	Voice-over-Internet Protocol
WAN	Wide Area Network
xDSL	Digital Subscriber Line

Copyright and Legal Notices

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change without notice. PacketFront assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the software and this document.

Purchasers, licensees and users accept and acknowledge that the products contain components (including components carrying certain firmware) and combinations of components that constitute trade secrets protected by PacketFront or its partners. Purchasers, licensees and users warrant that the delivered products will not be opened or dismantled, copied, altered or in any other way modified. Furthermore, purchasers, licensees and users agree not to attempt to reverse engineer, disassemble, modify, translate, create derivate works, rent, lease, loan, or without written permission distribute or sublicense the software, in whole or in part.

The products and its hardware, firmware and software, including technical data, may be subject to EU and U.S export control laws, including the U.S Export Administration Act and its associated regulations and the International Traffic in Arms Regulations administered by the US Department of State, and may be subject to export or import regulations in other countries. Purchasers and licensees agree to comply strictly with all such regulations and acknowledge that it has the responsibility to obtain licenses to export, re-export, or import hardware, firmware and software.

Purchasers and licensees are not entitled to, and PacketFront is not in any event liable to pay, compensation for damages which delivered products or software has caused to other property or to persons or any other consequential damages, including but not limited to loss of profit, loss of production or any other indirect damages.