# Internet Group Management Protocol User Guide



## For BCM963xx DSL Linux

## Version 1.0

5300 California Avenue • Irvine, CA 92617-7013 USA • Phone: (949) 926-5000 • Fax: (949) 926-5203

# Table of Contents

# CPE IGMP User Guide

## REVISION HISTORY

| *Revision Number* | *Date* | *Change Description* |
|---|---|---|
| V1.0 | 01/29/2010 | Initial Release. |

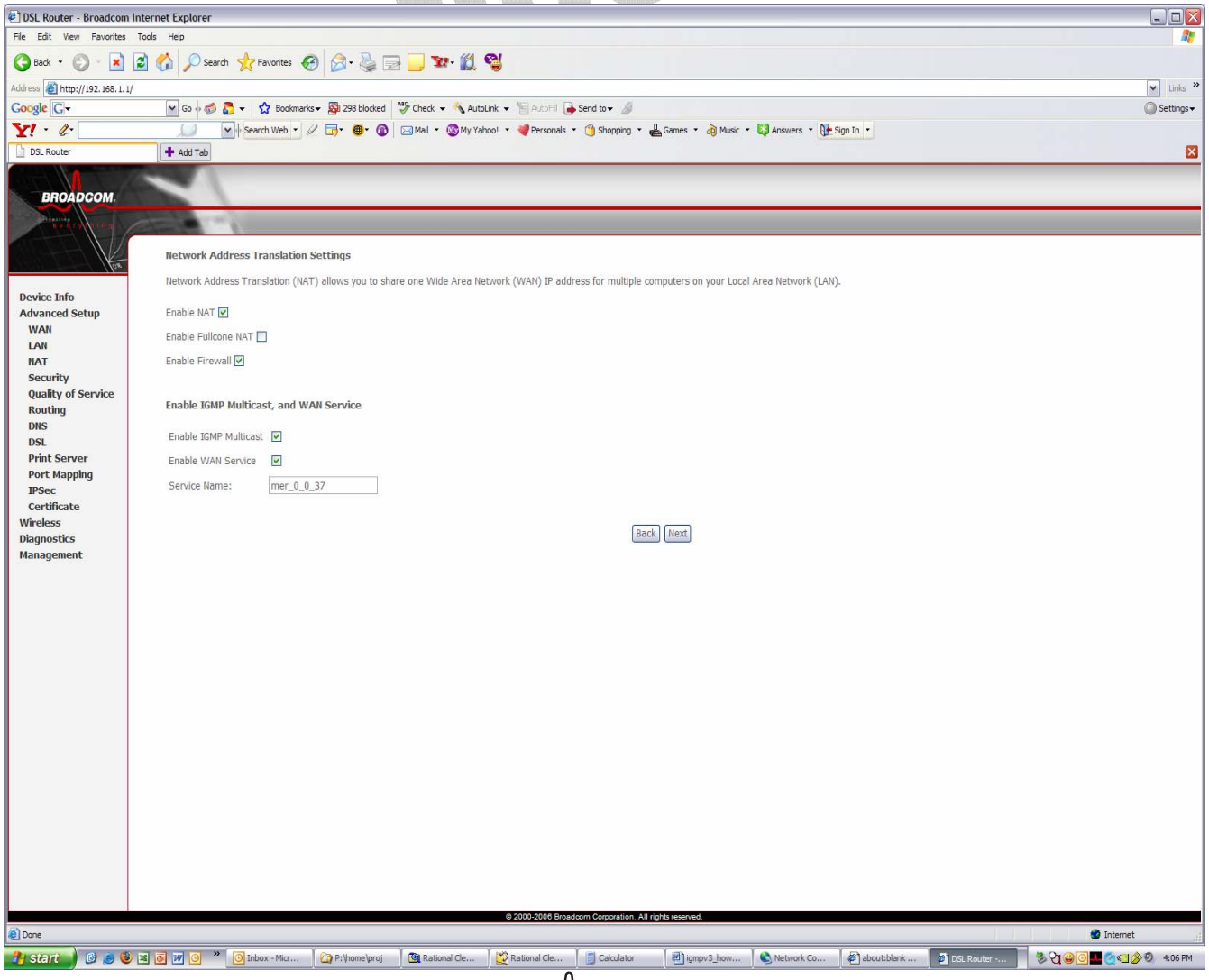
# 1.0 INTRODUCTION

Multicast forwarding in edge CPE equipment like xDSL systems is based on simple tree topology. It is not necessary to run a multicast routing protocol. It is sufficient to learn and proxy group membership information and simply forward multicast packets based upon that information. Broadcom xDSL CPE equipment supports IGMPv1, IGMPv2 and IGMPv3 based proxy/snooping feature for multicast forwarding information. IGMPv2 had some limitations that were enhanced by IGMPv3 (RFC3376) standard track RFC to support applications like IPTV through Source Specific Multicast (SSM). IGMPv3 also reduces host side complexity and enhances the state change (group change) operation performance.



# 2.0 HOW TO ENABLE IGMP PROXY

While creating any non-bridge, i.e., router wan service, user has to select “Enable IGMP” if he wants to create IGMP enabled WAN connection. This is shown below.



# 3.0 How To Enable IGMP Snooping

Snooping can be enabled on LAN Web GUI page. There are two modes of snooping, Standard Mode and blocking mode. If the user does not select any snooping mode, then Linux Bridge floods the multicast packets to all its ports.

## 3.1 Standard Mode Snooping

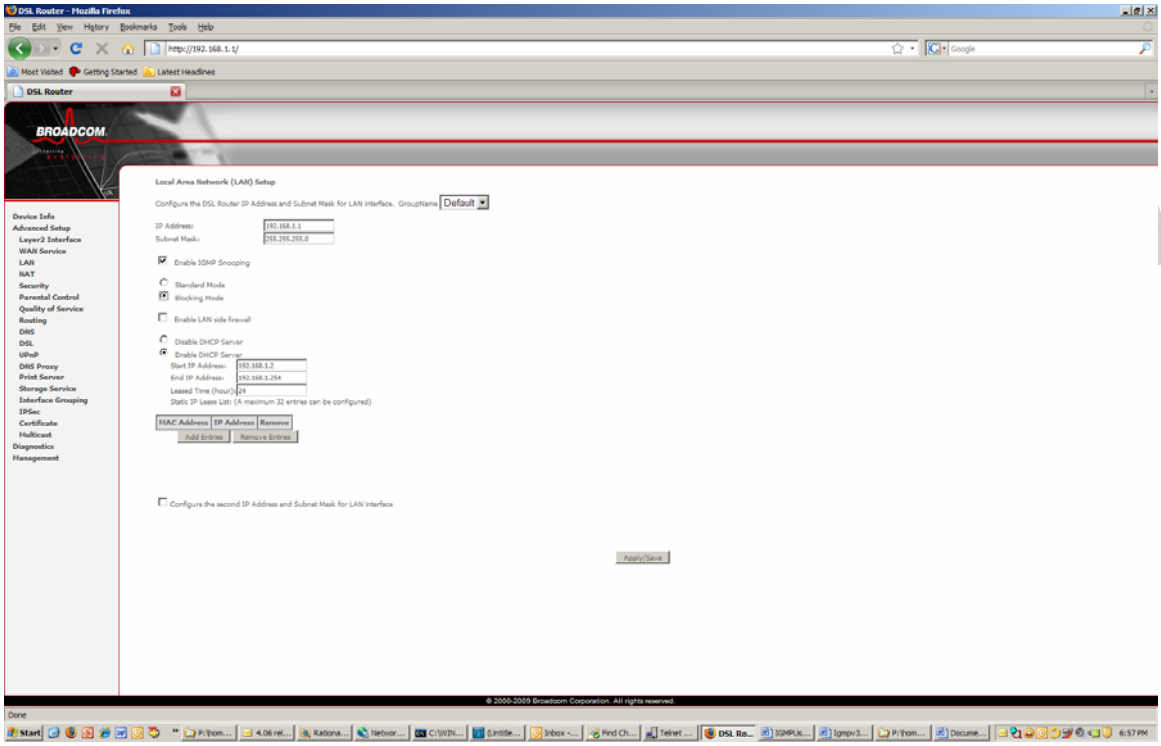
If there is no IGMP report for a multicast group, G then, there won't be any snooping for the group, G. All the multicast packets belong to this group gets flooded to all the bridge ports.

But, if there is a IGMP report for a multicast group, G then, the multicast data packets belong to this group gets snooped and only forwarded to the ports on which IGMP membership reports arrived prior to this. This behavior is group by group basis and not for a whole bridge.

## 3.2 Blocking Mode Snooping

In this mode, always no packets get forwarded if there are no memberships. Bridge will only forward a group G, to those ports which have sent IGMP report prior to this.

Snooping can be enabled on LAN page as show below



# 4.0 HOW TO CONFIGURE IGMP PARAMETERS

Multicast Web GUI option on the advanced tab provides a way to configure some of the IGMP parameters

## 4.1 IGMP Default Version

This configuration allows us to set the WAN side version of IGMP protocol version. LAN side it always sends IGMPv3 queries as these are understood by all IGMPv1, IGMPv2 and IGMPv3 hosts. IGMP proxy/snooping module can handle all the backward compatibility issues if it receives any version of IGMP messages.

By default it starts with IGMP version 3.

## 4.2 IGMP Query Interval

This configuration allows us to set the query interval. For more information see the reference section of this document.

## 4.3 IGMP Query Response Interval

This configuration allows us to set the query response interval. For more information see the reference section of this document.

## 4.4 IGMP Last Member Query Interval

This configuration allows us to set the last member query interval. For more information see the reference section of this document.

## 4.5 IGMP Robustness Value

This configuration allows us to set the robustness value. For more information see the reference section of this document.

## 4.6 Maximum Multicast Groups

This value sets the maximum number of groups allowed per interface. It can be changed dynamically

## 4.7 Maximum Multicast Data Sources (IGMPv3)

This value sets the maximum number of groups sources allowed per multicast group. It can be changed dynamically between values 1 to 24. If you want to change more than 24 we have to recompile the IGMP code to modify “MCPD_MAX_UPSTREAM_SSM_SRS” value in userpsace/private/apps/mcpd/mcpd.h

## 4.8 Maximum Multicast Group Members

This value sets the maximum number of groups allowed per group. It can be changed dynamically

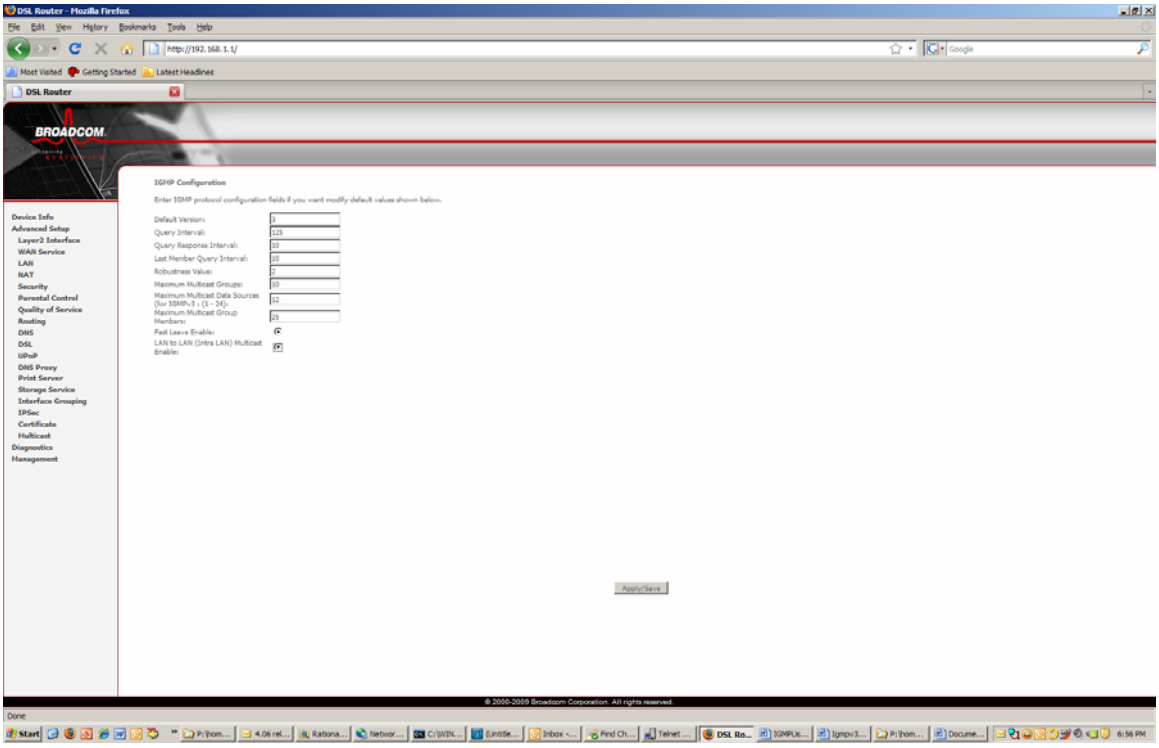
## 4.9 Fast Leave Enable

If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

## 4.10 LAN-2-LAN Multicast Enable

If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-2-LAN multicast feature should be enabled.

IGMP Multicast parameters can be set as shown below



## 5.0 BUILDING IGMP ENABLED IMAGE

To build IGMP Proxy/snooping enabled image follow the the steps below

Do make menu config

Load 96368GWV profile if you want to build voice image

Go to “Firewall, ALGs, and Networking Features” section

Select “IGMP v2/v3 Proxy” as dynamic build

Then, select “IGMPv2/v3 snooping” as a static build

Save the new profile and build.

By default, IGMP Proxy/Snooping is enabled in most of the build profiles. Check before you modify anything.



## 6.0 REFERENCES

RFC2236 Internet Group Management Protocol, Version 2
RFC3376 Internet Group Management Protocol, Version 3
RFC4605 Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")