Multicast Traffic Configuration User Guide

BROADCOM CONFIDENTIAL

Revision History

Revision	Date	Change Description
CPE-AN2200-R	06/16/15	Initial release

Table of Contents

List of Figures

About This Document

Purpose and Audience

This document details the multicast traffic configuration options for BCM963XX DSL Linux reference boards using the Broadcom WebUI. This document is aimed for users of the BCM963XX DSL Linux reference boards.

Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use.

For a comprehensive list of acronyms and other terms used in Broadcom documents, go to:
http://www.broadcom.com/press/glossary.php.

Document Conventions

The following conventions may be used in this document:

Convention	Description
Bold	User input and actions: for example, type **exit**, click **OK**, press **Alt+C**
Monospace	Code: `#include <iostream>` HTML: `<td rowspan = 3>` Command line commands and parameters: `wl [-l] <command>`
< >	Placeholders for *required* elements: enter your <username> or `wl <command>`
[ ]	Indicates *optional* command-line parameters: `wl [-l]` Indicates bit and byte ranges (inclusive): [0:3] or [7:0]

References

The references in this section may be used in conjunction with this document.

> **Note:** Broadcom provides customer access to technical documentation and software through its Customer Support Portal (CSP) and Downloads and Support site (see Technical Support).

For Broadcom documents, replace the "xx" in the document number with the largest number available in the repository to ensure that you have the most current version of the document.

Document (or Item) Name	Number	Source
[1] Internet Group Management Protocol, Version 2	RFC2236	tools.ietf.org
[2] Internet Group Management Protocol, Version 3	RFC3376	tools.ietf.org
[3] Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding (IGMP/MLD Proxying)	RFC4605	tools.ietf.org

Technical Support

Broadcom provides customer access to a wide range of information, including technical documentation, schematic diagrams, product bill of materials, PCB layout information, and software updates through its customer support portal (https://support.broadcom.com). For a CSP account, contact your Sales or Engineering support representative.

In addition, Broadcom provides other product support through its Downloads and Support site (http://www.broadcom.com/support/).

Introduction

Multicast forwarding of MLD and IGMP controlled traffic is divided into three main areas:

- Multicast Source – allowing a WAN service to be a source of multicast traffic.
- Proxy – correctly replying to Queries from the WAN port.
- Snooping – delivering multicast traffic to the LAN ports that request it.

In some configurations, it is reasonable for a WAN service to be configured as a Multicast Source without configuring the kernel to act as a proxy. This would be in a situation where the device serving Multicast Traffic is either always presenting all traffic on the WAN port or has some outside method of determining what Traffic should be sent to the Gateway.

Routed WAN Mode

In this mode, IGMP and MLD reports are handled internally. An IGMP Proxy service responds to Queries from the WAN Device on the WAN port and the IGMP Snooping facility directs the multicast traffic to the correct port.

Figure 1: Routed WAN Mode
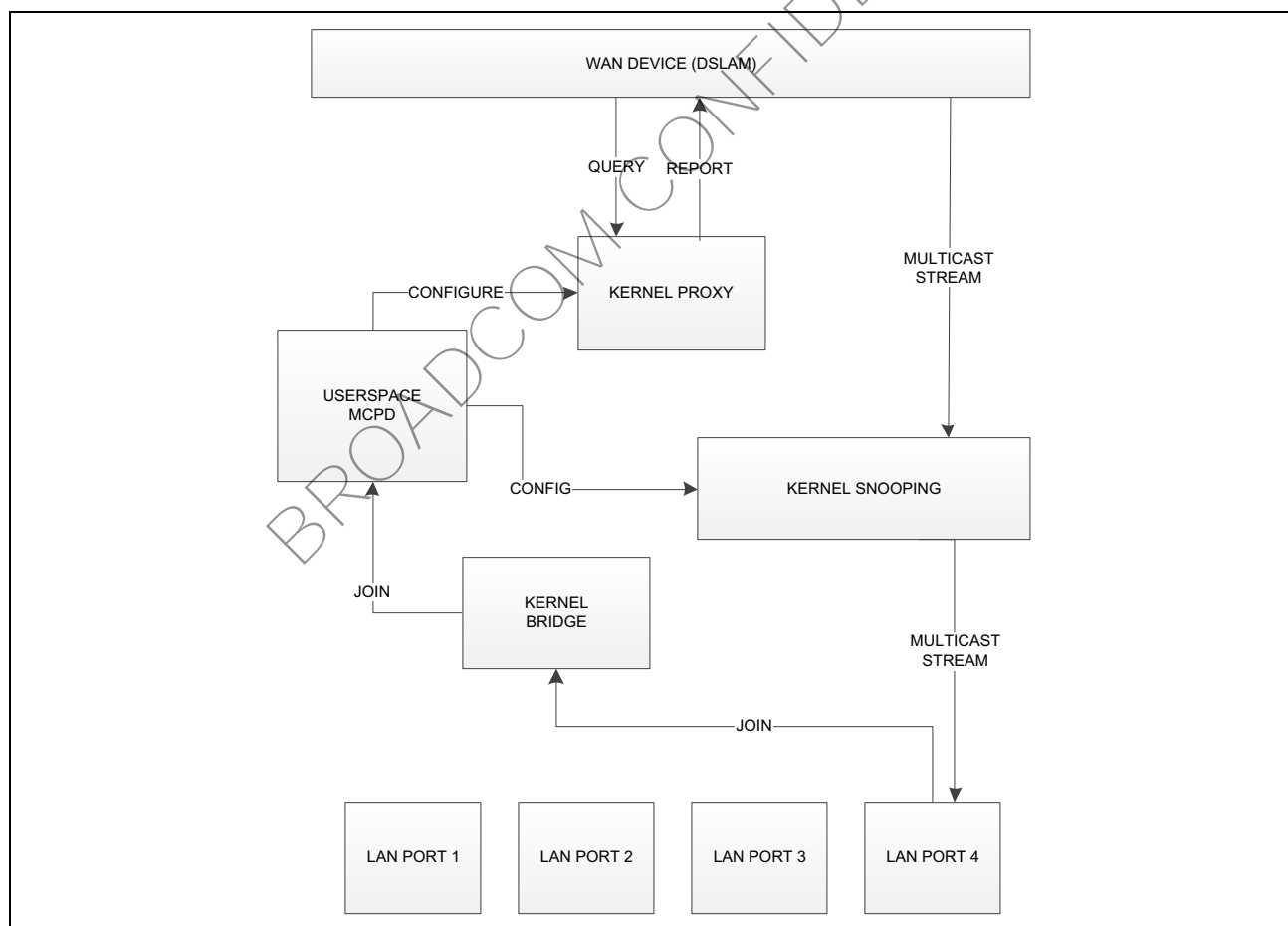
Notice that the IGMP and MLD reports ("JOIN") received by the bridge are *not* forwarded out the WAN port. They are instead redirected to the MCPD process that handles the configuration of the Proxy and Snooping processes.

Bridged WAN Mode

In Bridged WAN Mode, the system no longer acts as a Proxy between the LAN and WAN ports. Queries from the WAN side go directly through the bridge to the LAN Ports, and IGMP/MLD reports from the LAN ports go directly through the bridge to the WAN.

The only job for MCPD in this configuration is to inspect the IGMP/MLD reports and use them to configure the Kernel Snooping process. This ensures that the Multicast Traffic only goes to the LAN ports that have requested it, conserving bandwidth on other ports.

Figure 2: Bridged WAN Mode
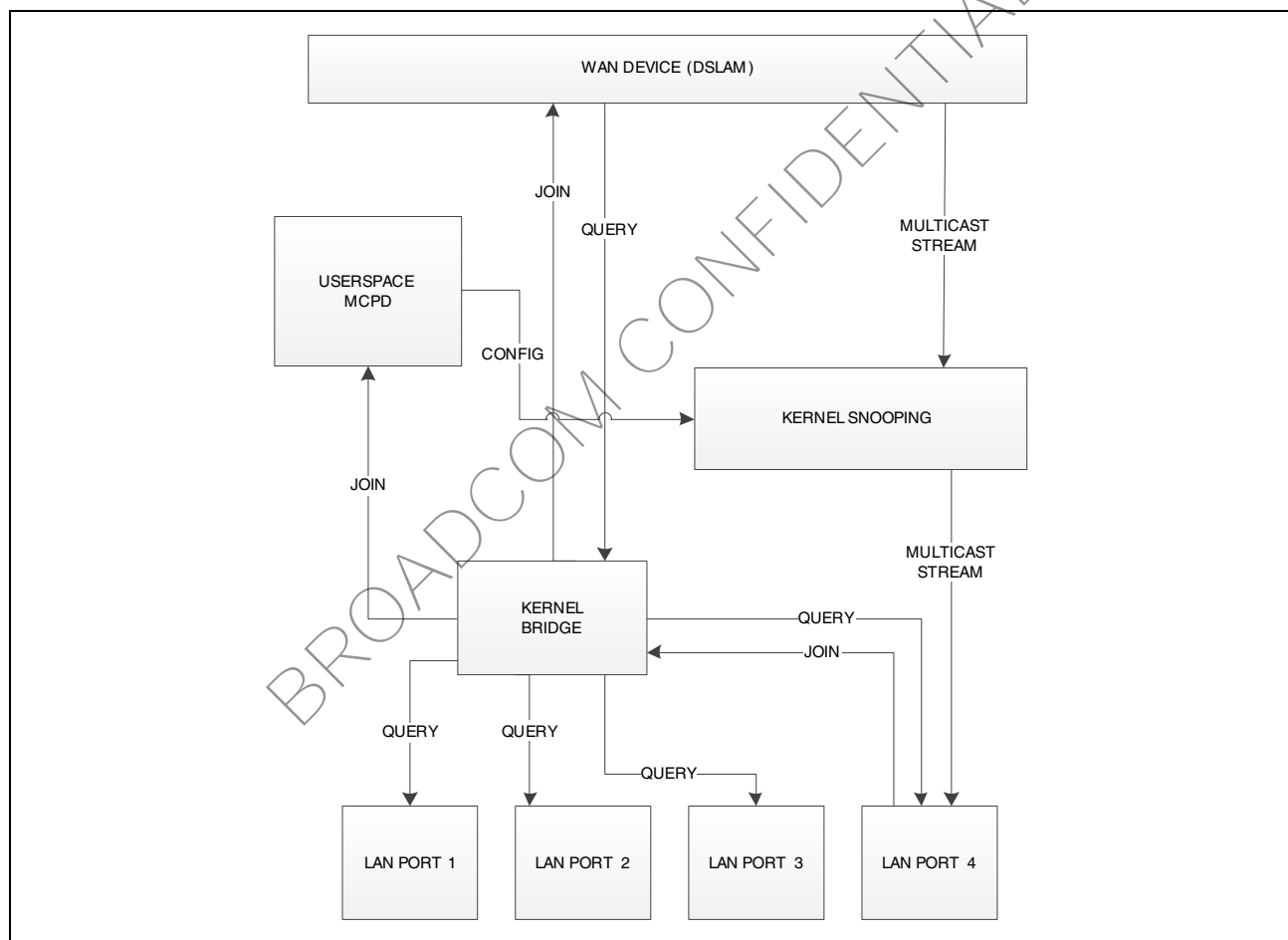
Configuring Multicast Source and Proxy

Multicast Source, which is the ability of a WAN service to be a source for Multicast Traffic, and IGMP/MLD Proxy, which is the notion of configuring the kernel to respond to IGMP/MLD queries on the WAN service, are both configured from the WAN Service menu.

Routed Service Configuration

When selecting a Routed Service on a WAN interface, you will be prompted to select which Multicast processes you want to be active on the Service.

Note that selecting "Enable IGMP Multicast Proxy" will automatically check "Enabled IGMP Multicast Source", as it would not make sense to have Proxy active on a WAN service which can't be a Multicast Source.

The reverse is not true. It is perfectly acceptable to mark a WAN Service as a Multicast Source, but to not want Proxy running. In this case, no IGMP or MLD reports are sent toward the WAN service.
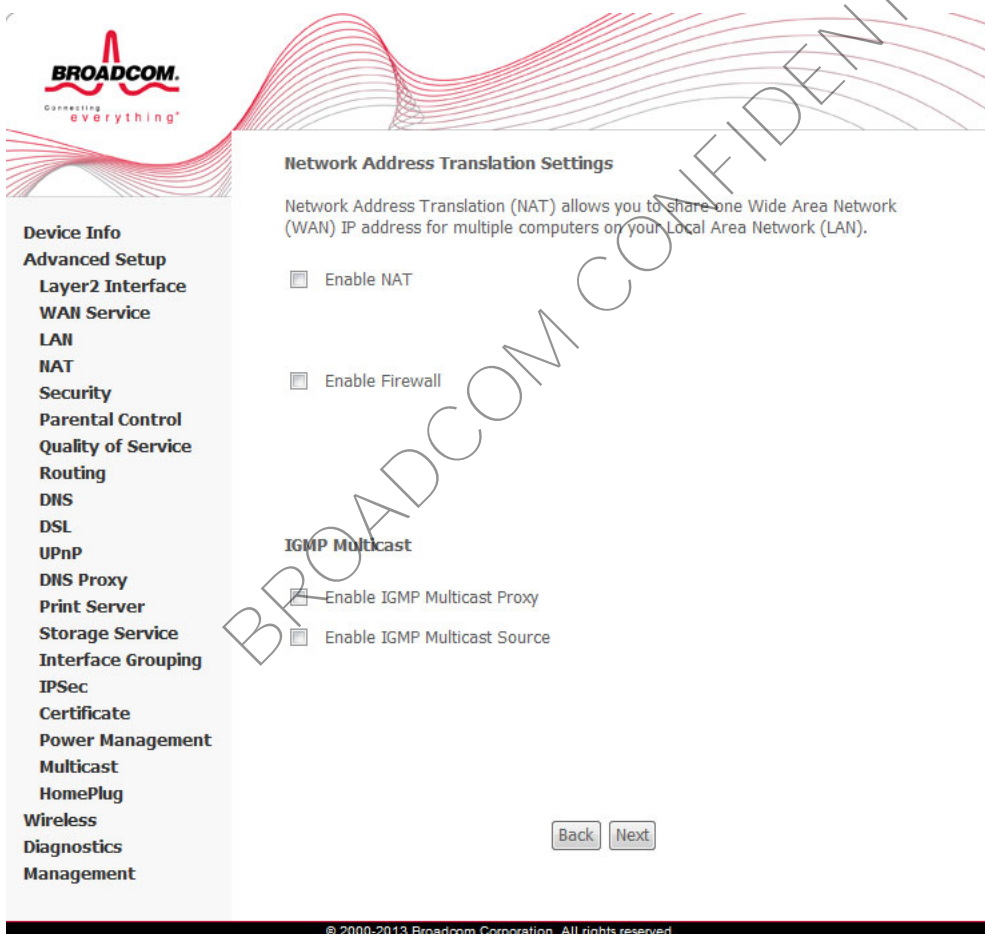
Bridged Service Configuration

In a Bridge WAN Service, there is only one configurable item related to IGMP/MLD; whether or not the WAN service can act as a Multicast Source.

When the user selects a Bridging WAN service type, a checkbox appears below the Bridging option.

If this WAN service will be a source for Multicast Traffic, the box should be checked.

Configuring Snooping

IGMP and MLD Snooping are configured from the LAN page. There are three possible configurations for Snooping:

- Off
- Standard Mode
- Blocking Mode.

The option to choose Standard Mode or Blocking Mode only appears when the "Enable IGMP Snooping" or "Enable MLD Snooping" option is checked.

Snooping Disabled

If "Enable IGMP Snooping" is not checked, the options for Standard and Blocking Mode do not appear on the screen.

Any multicast traffic received will be broadcast to all LAN ports on the bridge without any consideration as to if any of those LAN ports have requested that traffic or not.

Standard Mode Snooping

For any multicast group, the multicast traffic will be flooded to all ports in the bridge until at least one IGMP/MLD report is received for that multicast group. Once a report is received, the multicast traffic will only be forwarded to the port that requested it.

Blocking Mode Snooping

For any multicast group, the multicast traffic will only be forwarded to the LAN ports that have sent IGMP/MLD reports requesting that group.

The difference between Blocking and Standard Modes is that Standard Mode will flood the traffic if there are no requesters, while Blocking Mode will not.

LAN to LAN Multicast

LAN to LAN Multicast is automatically enabled until the first WAN service is configured.

Once there is a WAN service, the ability to operate (and snoop for) LAN to LAN multicasts is controlled by setting the pull down menu option to Enable or Disable on the LAN page.

Features

Source Specific Multicast

In IGMP V2 and MLD V3, the concept of "Source Specific Multicast" was added. This allows the user to specify not only the IP address of the multicast group, but also the source of that group.

According to RFC 3376, SSM multicast groups are those in the 232.0.0.0/8 range for IPV4 and the FF3x::/96 range for IPV6.

Broadcom software has a compile time configurable feature that allows SSM and ASM (the original style which does not specify source) addresses to use a "First In" protocol. This means that the first Join Report that arrives for a given address will determine whether it is an ASM or an SSM multicast group – without regard to the RFC 3376 limits. When there are no more listeners to the multicast group, it reverts back to the "First In" state and allows the next Join Report to determine whether it is ASM or SSM.

This compile time configuration is set in the "mcpd.h" header file.

DNAT Multicast

For IGMPV2 (IPV4), this feature allows the kernel and packet accelerators to be configured so that the incoming multicast group address on the WAN is translated to different multicast group address on the LAN.

This feature is not supported by MCPD and must be configured by the customer.

An interface is provided in snoopctl_api.c, in the function snoop_update_igmp().

For this feature, the function now supports an "rxGrp", which is the WAN side address to be translated and a "txGrp" with is the LAN side output address.

Configuring IGMP and MLD Parameters

The IGMP and MLD parameters are configured under the Multicast tab. Though the IGMP and MLD parameters are separately configurable, the parameter definitions are identical.

Multicast Precedence

This allows the user to set the precedence of multicast traffic streaming through from the WAN services to the LAN ports.

The setting is either "Disabled" (the default) or a number indicating precedence. A precedence setting of 1 gives the highest priority to multicast traffic.

Multicast Strict Grouping Enforcement Version

This feature applies to configurations with multiple WAN services in different interface groups.

When enabled, multicast streams arriving on a particular WAN service can only be routed to LAN ports in the same interface grouping.

Default Version

This is the IGMP or MLD protocol version that is used toward the WAN side. On the LAN side, the IGMP Queries are understood by all IGMPv1, IGMPv2 and IGMPv3 hosts and M LD Queries are understood by all MLDv1 and MLDv2 hosts.

By default, the default version is IGMP version 3 and MLD Version 2.

Query Interval

This is the time between General Membership Queries.

Query Response Interval

This is the expected response time to a General Membership Query.

Last Member Query Interval

This is the time between the Last Member Queries (the queries which are sent in response to a Leave Report).

Robustness Value

The Robustness Value is an indication of the trustworthiness of the network. The higher the robustness, the more retries are executed before a timeout is declared.

Maximum Multicast Groups

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

Maximum Multicast Data Sources (IGMPv3/MLDv2)

This value sets the maximum number of group sources allowed per multicast group. It can be changed dynamically between the values 1 to 24. To change to more than 24, recompile the IGMP code to modify "MCPD_MAX_UPSTREAM_SSM_SRS" value in userpsace/private/apps/mcpd/mcpd.h.

Maximum Multicast Group Members

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

Fast Leave Enable

"Fast Leave" refers to the feature in MCPD which keeps track of all listeners to a given multicast stream. When MCPD determines that there are no more listeners (i.e. all listeners have sent Leave reports), MCPD will discontinue the stream immediately, freeing the bandwidth up more quickly than via the standard system of Group Specific Queries.

Admission Control for PON

Delayed admission is a feature relevant to PON architectures.

PON architecture always uses bridged WAN interfaces, but some users do not want IGMP Joins and Leaves to cross the bridge from LAN to WAN unless the multicast group is approved by the PON software module.

When this feature is activated, IGMP reports received from the LAN are held in a pending state. They are not permitted to pass through to the WAN service until MCPD has processed the report in userspace and checked with PON software.

Once the check is complete, the IGMP reports are either forwarded or dropped based on the response from the PON software.

This feature is configured when GPON is built but can be turned off by manually editing the /var/mcpd.conf file and reloading MCPD.

Building Images with Proxy and Snooping Enabled

> **Note:** By default, MCPD Proxy/Snooping is enabled in most build profiles. Check the build profile before making any modifications.

1. At the shell, type:
   > `make menuconfig`

2. Load the correct profile (e.g. 963268GW).

3. Under "Firewall, ALGs, and Networking Features".

4. Select "Multicast Proxy (mcpd)" as dynamic build.

5. Select "Multicast snooping" as enabled (the asterisk should be visible).

6. Save profile and build.

BROADCOM®

Connecting
e v e r y t h i n g®

Broadcom Corporation

5300 California Avenue

Irvine, CA 92617

Phone: 949-926-5000

Fax: 949-926-5203

E-mail: info@broadcom.com

Web: www.broadcom.com