Application Note

BCM963XX

Trace Capture and Port Mirroring

CPE-AN2100-R

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

June 23, 2015

Revision History

Revision	*Date*	*Change Description*
CPE-AN2100-R	06/23/15	Initial release

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617

Table of Contents

List of Figures

About This Document

Purpose and Audience

This application note describes how to configure and use the Trace Capture and Port Mirroring tools to monitor and analyze BCM963XX traffic.

When developing and testing network products, it is often extremely valuable to be able to capture and analyze traces taken from a variety points in the system. This document provides directions to facilitate capturing a variety of traces.

This document also serves as an application note on the details of the port mirroring application that is supported in Linux 4.x releases of BCM963XX platforms. It is intended to be an aid in debugging issues on the xDSL bridge/router platforms. It can also be used to identify any malicious traffic in and out of the system in an easy manner.

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]

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/).

Linux Packet Trace Capture

Using the techniques detailed in this section, it is possible to capture a trace of packets seen by the Linux IP interface driver (br0, wl0, pp0, etc.) and stream these packets to another machine that has the capacity to write the trace to disk.

Getting Tcpdump

If the target system is built with the BUILD_TCPDUMP option enabled, then tcpdump is available on the filesystem.

If using a pre-built image, then first create a new build with the BUILD_TCPDUMP option.

1. Place the tcpdump executable on a server.
2. cd to /var/tmp on the target system.
3. Use “wget” to fetch the executable.
4. chmod the file to make it executable.

Capturing Traffic

1. On a machine (for example with address 192.168.1.5) connected to the target’s LAN interface, launch an instance of “netcat” to listen to arriving traffic on a TCP port and write it to a file.

```
nc -l -p 5999 > capturefile.cap
```

2. From the shell on the target:
   a. Instruct tcpdump to capture full packets of all traffic on the interface of interest, without placing the interface in promiscuous mode, and send it stdout.
   b. Pipe the output of tcpdump to netcat which is instructed to send its stdin across a tcp connection to a listening port on another machine

```
tcpdump  -i ppp0 -p -s1600 -w- | nc 192.168.1.5 5999
```

This approach works well for situations where there is only a moderate amount of traffic (a few megabits/s) and aside from br0 (where the port 5999 traffic from netcat is also present).

If monitoring interfaces including br0, it is necessary to use a filter to exclude the netcat connection.

```
tcpdump  -i br0 -p -s1600 -w- not port 5999 | nc 192.168.1.5 5999
```

It is also possible to use any valid tcpdump filter expression to narrow the scope of packets captured.

```
tcpdump  -i any -p -s1600 -w- port 53 | nc 192.168.1.5 5999
```

Refer to the pcap-filter(7) man page on a Linux system for more details on the filter syntax.

Caution! When TCP dump is enabled, Flow acceleration is automatically disabled.
i.e., Flow-cache will not learn the flows and traffic will continue to take the Linux networking path.

Port Mirroring

Port Mirroring monitors traffic on one interface, and mirrors (copies) the same traffic onto another interface.

The monitor interfaces are ATM and PTM WAN services. Only Ethernet over ATM (EoA) interfaces are supported.

The mirror interfaces are Ethernet, wireless, and USB LAN connections. Traffic can be mirrored for inbound only, outbound only, or in both directions.

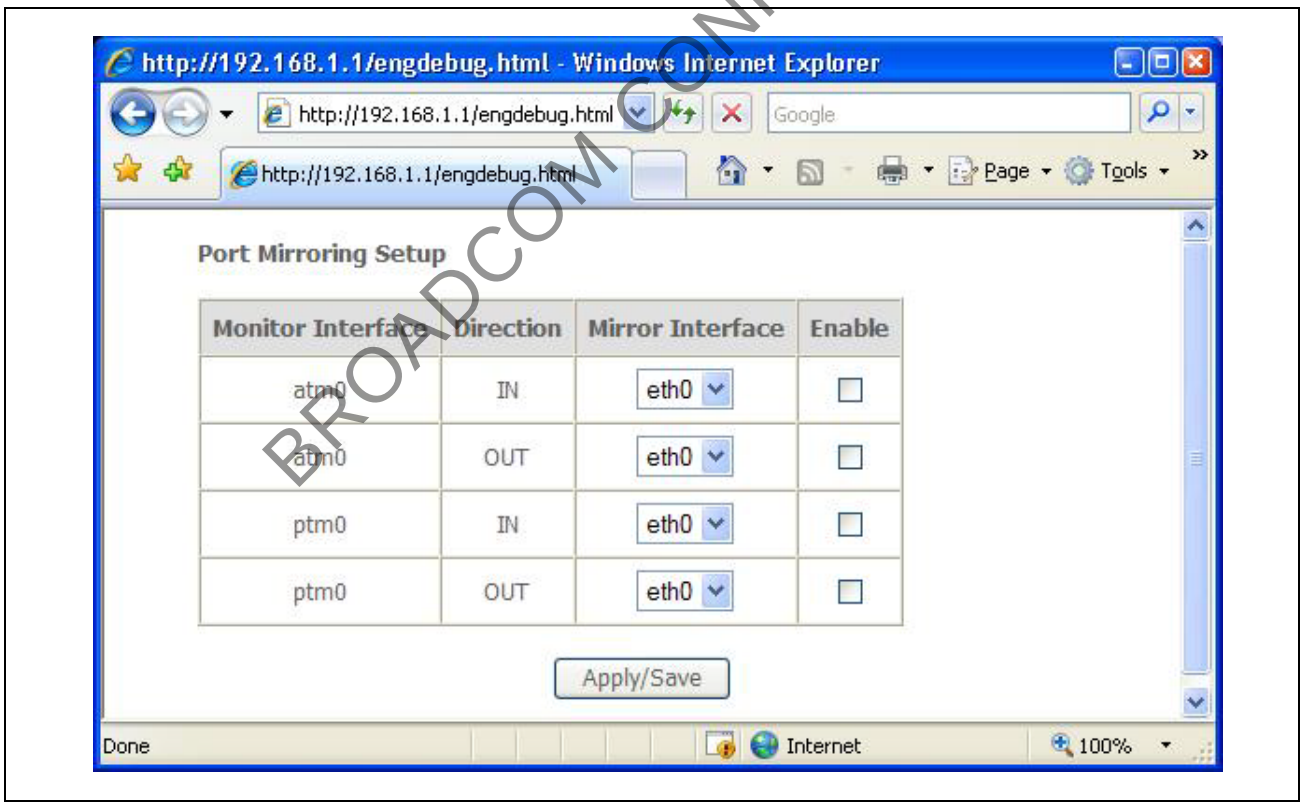
Note: For Port Mirroring to work on DSL/XTM interfaces, hardware (FAP/Runner) acceleration must be manually disabled prior to starting the mirroring.

Setup and Usage

The Port Mirroring configuration is accessed by entering http://192.168.1.1/engdebug.html or the CPE's local IP address to access WebGUI from a Web browser.

IP address 192.168.1.1 is the BCM963XX router's local IP address. Figure 1 shows the Web page.

Figure 1: Port Mirroring Setup Screen



For each direction of each configured WAN or Monitor interface, a LAN or Mirror interface is selected where the traffic will be sent to. The Enable check box must be checked in order to activate Port Mirroring for that interface. The settings on this Web page are saved persistently.

For BCM6358, BCM6348, and BCM6338 platforms, the virtual ports feature must be enabled to create the eth1.x ports.

Port Mirroring does not work on an unmanaged Ethernet switch interface.

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