APPLICATION NOTE

SSL/IPS Accelerator Troubleshooting Guide

05/02/02

16215 Alton Parkway • P.O. Box 57013 • Irvine, California 92619-7013 • Phone: 949-450-8700 • Fax: 949-450-8710

REVISION HISTORY

Revision #	*Date*	*Change Description*
SSL/IPS-AN100	05/02/02	Initial release.

Broadcom Corporation
16215 Alton Parkway
P.O. Box 57013
Irvine, California 92619-7013

TABLE OF CONTENTS

OVERVIEW

The purpose of this document is to assist in debugging any issues that may be encountered when installing or using any of the Broadcom 580X/582X series of SSL and IPSec accelerator boards. This document pulls information from the ReadMe files, as well as tips from the HTML documentation found on the CD.

INSTALLATION ISSUES

GENERAL INSTALLATION TROUBLESHOOTING

The following subsections describe general installation troubleshooting items.

Verify the Minimum Requirements

Verify that the host machine meets the minimum Windows® or Linux requirements.

Windows

- Pentium-based computer that meets Windows 2000 software requirements
- One open PCI version 2.2, 32/64-bit, PCI 33/66-MHz slot
- 128 MB RAM (minimum)
- Microsoft® Windows 2000 Server family with Service Pack 2 or later
- Microsoft.NET 32 or 64 bit version
- Web server support (Windows Internet Information Server)

Linux

- Pentium-based computer that meets Linux software requirements
- All Linux RPM packages (Apache 1.3.x, mod_ssl 2.8.x, OpenSSL 0.9.6.c or higher, MM 1.1.x, GZip 1.2.4, and Perl 5.6.0)
- One open PCI version 2.2, 32/ 64-bit, PCI 33/66-MHz slot
- 128 MB RAM (minimum)

Solaris

- Sparc station with Solaris 2.6, 7 or 8 Operation environment
- One open PCI version 2.2, 32/64 bit, PCI 33/66-MHz slot
- Apache based SSL-Server requires Apache-1.3.22, Openssl-0.9.6c and Modssl-2.8.5-1.3.22
- Iplanet based SSL-Server requires Iplanet6 or Iplanet4
- Snmp support requires Solstice Enterprise Agents installed with its patches (snmp.txt)

Using the Latest BIOS

Make sure the system is using the latest BIOS by checking with your motherboard manufacturer and see if there is update available.

Install Board into Another PCI Slot

Try installing the board into another PCI slot, because the particular slot that the CryptoNetX adapter is installed in can be malfunctioning. Power the host machine down and try installing the adapter in another PCI slot.

Adapters

Using Another Adapter

Although all CryptoNetX adapters are thoroughly tested before shipping, the card may have been damaged during shipping or by electrostatic discharge. If another adapter is available that is known to work properly, power the host machine down and go through the same installation procedure.

Removing Other Adapters

Other PCI cards may be malfunctioning and cause the CryptoNetX adapter to fail. Remove all other PCI cards from the host machine and see if the adapter installs normally.

Install Adapter into Another Machine

The host machine itself may have a problem. If another host machine is available, try installing the CryptoNetX adapter into another host.

DRIVER INSTALLATION

Windows

Windows Compatibility

The current version of the driver works with Windows 2000 SP2, as well as the Windows.NET 32 and 64 bit versions.

Before the CryptoNetX Driver Installation

Before installing the IIS Support application, make sure IIS is operational on the system.

When installing the driver on a Windows 2000 Server with Terminal Services installed, change to Install mode. By default, Terminal Services assigns the User Mode to prevent the installation of any type of driver or application. To change to Install mode, type the following command at a DOS prompt:

```
C:\> change user /install
```

Control Panel Conflicts

If there is an exclamation mark next to the CryptoNetX accelerator card in the control panel, change the resource settings (such as IRQ or memory usage) and see if the conflict goes away.

Running the CryptoNetX Diagnostic

After installation of the CryptoNetX SSL Accelerator applications:

1. Double-click the **CryptoNetX Diagnostics** button in the desktop.
2. Run the self test on the adapter(s) that shows up in the panel (located in the right-side of the window).
3. Save the results to a file by clicking the **Save Log** button, and submit this file when contacting Support.

CryptoNetX Adapter Not Detected

Although there are no known issues with slot sensitivity at this time, try using different PCI slots if Windows fails to detect the card (such as there is no Plug and Play, and diags does not find the device). Also, try the pciconfig utility to see if it finds the card (pciconfig works on Windows NT/2000, but not on Windows 98). The pciconfig utility can be downloaded from the Compaq website at: ftp://ftp.compaq.com/pub/softpaq/alphant/pciiv132.zip.

CryptoNetX Adapter Detected, But Not Working

Interrupts from the CryptoNetX card are not recognized on some machines if the card is installed in a 64-bit slot, and Windows 2000 is installed with ACPI disabled. To check the status of ACPI, go to Device Manager and double-click the Computer button. ACPI should then display and work properly. If it is not installed, Windows needs to be reinstalled with the default setting for ACPI.

Linux

Tested Installations

The current version of the driver has only been tested on the following Linux distributions:

RedHat 6.2–2.2.14–6.1.1
RedHat 7.0–2.2.16–22
RedHat 7.1–2.4.2–2
RedHat 7.2–2.4.7–10

Mandrake 7.2–2.2.17–21
Mandrake 8.0–2.4.3–20
Mandrake 8.1–2.4.8–26

TurboLinux 6.5–2.2.18–2

SuSe 7.0–2.2.16
SuSe 7.1–2.4.0 and 2.2.18
SuSe 7.2–2.4.4

Caldera 2.4–2.2.14
Caldera 3.1–2.4.2

The driver has only been tested as a loadable module. Minor modifications may be required to install the driver on other Linux distributions.

Build Issues

Linux Distribution

Depending upon the Linux distribution that is being used for building and loading this module, some unresolved symbols for proc_net_ functions may be seen. Older kernel versions do not have these functions defined. If this is the case with the build, edit the cdevincl.h file to bump up the kernel version that defines UBSEC_SNMP_2_2 to the next available kernel version.

SuSe Linux

The driver may fail to compile in SuSe Linux distributions with kernel version 2.2.18. If this is the case, complete the following steps:

1. Ensure that the full 2.2.18 source tree is installed.
2. If not, install the lx_sus22.rpm package (provided on the CD or from SuSE's FTP site).
3. If the installation process did not automatically provide the source, load the 2.4.0 source by installing the lx_sus24.rpm package.

> **Note**
>
> **While installing these packages, dependency and package conflict issues may need to be resolved. The appropriate C compilers and binaries must be installed as usual.**

4. Once the source is installed, copy the following configuration files to the appropriate locations in the source tree:

```
/boot/vmlinuz.config, /boot/vmlinuz.version.h &
/boot/vmlinuz.autoconf.h
cp /boot/vmlinuz.config /usr/src/linux-2.2.18.SuSE/.config
cp /boot/vmlinuz.version.h /usr/src/linux-2.2.18.SuSE/include/linux/version.h
cp /boot/vmlinuz.autoconf.h /usr/src/linux-2.2.18.SuSE/include/linux/autoconf.h
```

5. Rebuild the source tree by typing the following:

```
make oldconfig
make dep
```

The b58diag Utility

The BCM58XX driver distribution provides the b58diag utility. This utility performs basic diagnostic testing using the BCM58XX driver, and verifies basic operation of the driver. The following table shows the b58diag usage.

```
b58diag [-v,-V,-s,-S,-h,-H,-x,-X]
```

Table 1: b58diag Usage

Item	*Description*
`-v,-V`	Prints out the version of the driver.
`-s,-S<card number>`	The <card number> is between 1 and *n*, where *n* is the number of cards in the system. The crypto and key self test is performed on the specified card. If no card number (or a card number of 0) is specified, self test is performed on all the cards present in the system. The output for testing multiple cards does not specify all the cards tested in a system, but only gives the CryptoNet Device Selftest Passed message if tests passed for all installed cards. If any of the cards fail the tests, the output gives the CryptoNet Device Selftest Failed message without specifying which card is failed/passed. The failed card can be determined by -s (or -S)<card number> again for each installed card, until the failed card(s) is located. To perform self test on a specific card, do not put space between the s and <card number>. Otherwise, selftest is performed on all cards present in the system.
`-h,-H`	Displays a brief help message listing the available parameters.
`-x,-X`	Displays the version of this diagnostic utility.

Other Diagnostics

- lsmod—Used to list the installed modules. BCM5820 or BCM582X should be in the list.
- lspci—Used to list devices on the PCI bus. Use with the –x option to view CryptoNetX PCI configuration registers.

How can I tell if the driver is loaded?

Type the following:

```
b58diag –v
```

If b58diag returns with the No BCM582X Device Found error message, then run a make load from the directory where the .tar file is extracted.

How do I unload the driver?

In the directory where the .tar file is extracted, run make unload. Verify that the driver is unloaded with b58diag –v or lsmod.

Solaris

How can I tell if the driver is loaded?

To show the module name and the version, type:

```
modinfo | grep "bcm582x"
```

To show the version of the driver, type:

```
b58diag -v
```

Documentation for b58diag is found in the b58diag.txt file (and also in this document).

How do I manually load the driver?

For the BCM5821, type:

```
/usr/sbin/add_drv -m"* 0666 root root" -i'"pci14e4,5821"' -v bcm582x
```

For the BCM5820, type:

```
/usr/sbin/add_drv -m"* 0666 root root" -i'"pci14e4,5820"' -v bcm582x
```

How do I unload the driver?

To unload the driver from the O/S, type:

```
/usr/sbin/rem_drv bcm582x
```

How do I find out if any other driver is loaded for the same card?

To show the name of the driver module for the card, type:

```
grep "pci14e4,5820" /etc/driver_aliases
```

OPERATIONAL ISSUES

This section covers the issues relating to the operation of the adapter once it has been successfully installed.

PERFORMANCE ISSUES

SSL

If using a Windows machine, make sure that performance monitoring is set up correctly on the machine that the IPS or SSL card is installed in. For information on configuring the performance tool to monitor hardware security acceleration, refer to the HTML documentation in the Manuals directory on the CD.

Getting Half of the Expected Key Processing Performance

If using a BCM5821 based adapter, verify the SW1 setting. This switch is set to auto by default, which means that it samples the signal 66_EN from the PCI bus and sets the internal clock setting accordingly. Some motherboards may not properly drive this signal, and may require manual setting. If the CryptoNetX adapter is installed in a:

- 33-MHz bus, set SW1 to the 4x position
- 66-MHz bus, set SW1 to the 2x position

Performance Lower than Expected on Windows Platform

On most Windows 2000 systems, the bottleneck occurs in Windows before reaching the maximum performance of SSL800 (so greater performance is not achieved with SSL4000 or with multiple SSL800's). The Windows.NET Server (beta 3 or higher) gets much better performance.

Another factor affecting CryptoNetX acceleration under Windows is that the chips used on the SSL/IPS boards have multiple engines, so it is necessary to have multiple threads to keep the hardware busy to get maximum performance. This occurs when writing a test program that loops, and calls some accelerable function (such as a CAPI RSA encrypt function).

When configuring the server certificate, the selected key length affects acceleration (such as 512-bit faster and 2048-bit slower).

No Performance Improvement with Apache/OpenSSL

Enable the hardware acceleration by doing the following:

1 Edit the Httpd.conf file, and add the SSLCryptoDevice ubsec directive at the beginning of the file.

2 Stop and then restart the web server again by typing:
   - apachectl stop
   - apachectl startssl

3 Check all logs in the <install path>/Apache/Logs file to make sure the web server is running and has accepted the directives.

4 Test again using a web browser.

Can I offload bulk crypto under Windows?

The acceleration support for Windows 2000/XP/.NET is limited to OffloadModExpo(), which offloads modular exponentiation for Microsoft CAPI. Bulk encryption acceleration is not supported by Windows. For IPSec and other bulk encryption capabilities of the 582X, a proprietary kernel level crypto API is supported by the driver (Windows NT4/98/ME/2000/XP/.NET). No SSL hardware acceleration is supported for Windows NT4/98/ME.

The Simple Cryptographic API is not supported on Windows (such as no OpenSSL, PKCS11, and so on support).

Performance Issues

Use a minimal httpd file, and not the default that comes up with apache/mod_ssl. Build one up from scratch defining just what is needed (such as server and document root).

- Do not enable logging, because this avoids file writes and other logging overhead. The ability to track statistics and access audit trails is lost.
- Do not turn on directory access controls and disable default checking, because this avoids directory opens looking for the non-existent .htaccess file. The ability to do fine-grained access controls on directories and files is lost.
- Do not enable session caching (that is, do not define parameters, no session re-use, and new RSA per connection).
- Disable keepalive, which is on by default. Do a new TCP connection for every handshake (new RSA).

IPSec (Bulk Encryption)

Getting Half of the Expected Bulk Crypto Processing Performance

If using the BCM5821 based adapter, verify the SW1 setting. If the CryptoNetX adapter is installed in a:

- 33-MHz bus, set SW1 to the 4x position
- 66-MHz bus, set SW1 to the 2x position

For best bulk cryptographic performance, make sure the CryptoNetX adapter is installed in a 64-bit PCI slot. This doubles the amount of available PCI bandwidth.

Effects of Packet Size Performance

As packet size decreases, the bulk cryptographic performance of the CryptoNetX family of adapters decreases. Performance on small packets (64 bytes) can be as low as 20% of quoted performance on larger packets. For more information, refer to the data sheets on respective adapters.

PCI Bandwidth Issues

A 32-bit/33-MHz bus has a theoretical maximum bandwidth of 1 GB. Devices installed on the PCI bus have to share this bandwidth. As more devices are installed on the bus, there is less bandwidth available for the CryptoNetX adapter. Move the CryptoNetX to a wider/faster PCI bus if higher performance is required, such as a 64-bit/66MHz bus that has a maximum bandwidth of 4 GB.

STRONG ENCRYPTION NOT WORKING

The SSL boards come in different versions. The BCM9582XSSL board is configured to disable both 3DES and RC4 processing for export reasons. Check the paperwork that came with the CryptoNetX adapter to see which version it is.

SELF-TEST FAILS

Some motherboards (specifically ASUS boards with the Intel 440BX chipset) require leaving the PCI signal REQ64# floating on the 32-bit PCI slots. This is a violation of the PCI specification and causes intermittent behavior, as that signal moves between logic levels.

THE RC4 IS NOT WORKING

The SSL800 boards are unable to perform any RC4 processing due to an issue with the chip used on those boards. If RC4 processing is required, use an SSL4000.

SNMP ISSUES (LINUX ONLY)

For SNMP issues, make sure the:

- snmpd daemon is installed in the system
- BCM58XX driver is installed and then stop the snmpd daemon and then restart it again with /usr/sbin/snmpd

Broadcom Corporation

16215 Alton Parkway
P.O. Box 57013
Irvine, California 92619-7013
Phone: 949-450-8700
Fax: 949-450-8710