Sun™ Crypto Accelerator 4000
보드 설치 및 사용 설명서

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

부품 번호: 817-2335-10
2003년 5월, 개정판 A

본 설명서에 대한 의견은 docfeedback@sun.com으로 보내 주십시오.

재활용
가능

Adobe PostScript

Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI
Product Family Name: Sun Crypto Accelerator 4000 - Fiber (X4012A)

EMC

USA - FCC Class B

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997 Class B

EN55024:1998 Required Limits:

EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass

EN61000-3-2:1995 + A1, A2, A14 Pass

EN61000-3-3:1995 Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition
IEC 60950:2000, 3rd Edition
Evaluated to all CB Countries
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Declaration of Conformity (Copper UTP)

Compliance Model Number: Venus-CU
Product Family Name: Sun Crypto Accelerator 4000 - Copper (X4011A)

EMC

USA - FCC Class B

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass

EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997	Class B
EN55024:1998 Required Limits:	
EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14	Pass
EN61000-3-3:1995	Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition

IEC 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者 會被要求採取某些適當的對策。

목차

표

머리말

*Sun Crypto Accelerator 4000 보드 설치 및 사용 설명서*는 Sun™ Crypto Accelerator 4000 보드의 기능, 프로토콜 및 인터페이스를 나열하고 시스템에 보드를 설치하고, 구성하고, 관리하는 방법을 설명합니다.

이 설명서는 사용자가 다음 중 하나 이상을 구성한 경험이 있는 네트워크 관리자라고 가정합니다: Solaris™ 운영 환경, PCI I/O 카드가 내장된 Sun 플랫폼, Sun™ ONE 및 Apache 웹 서버, IPsec, SunVTS™ 소프트웨어, 인증 기관 취득.

본 설명서의 구성

이 설명서는 다음과 같이 구성되어 있습니다.

- 1장은 Sun Crypto Accelerator 4000 보드의 제품 기능, 프로토콜, 인터페이스를 나열하며 하드웨어 및 소프트웨어 요구사항을 설명합니다.
- 2장은 Sun Crypto Accelerator 4000의 하드웨어 및 소프트웨어 설치 및 제거 방법을 설명합니다.
- 3장은 Sun Crypto Accelerator 4000 설정 가능한 드라이버 매개 변수를 정의하고 `ndd` 유틸리티와 `vca.conf` 파일을 통해 이를 구성하는 방법을 설명합니다. 또한 OpenBoot™ PROM 인터페이스에서 자동 교섭 또는 강제 모드를 활성화하는 방법과 네트워크 `hosts` 파일 구성 방법을 설명합니다.
- 4장은 `vcaadm` 및 `vcadiag` 유틸리티를 통한 Sun Crypto Accelerator 4000 보드 구성과 키스토어 관리 방법을 설명합니다.
- 5장은 Sun ONE 웹 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 구성 방법을 설명합니다.
- 6장은 Apache 웹 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 구성 방법을 설명합니다.

- 7장은 SunVTS 진단 응용 프로그램 및 보드 상의 FCode 자가 테스트를 통한 Sun Crypto Accelerator 4000 보드 테스트 방법을 설명합니다. 또한 OpenBoot PROM 명령을 사용한 문제 해결 기법도 설명합니다.
- 부록 A는 Sun Crypto Accelerator 4000 보드의 규격을 나열합니다.
- 부록 B는 Sun Crypto Accelerator 4000 소프트웨어를 사용하여 Apache 웹 서버에 대한 SSL 지원을 구성하는 데 필요한 지시어를 설명합니다.
- 부록 C는 Sun Crypto Accelerator 4000 보드와 함께 제공되는 소프트웨어와 본 보드의 암호화 가속 기능을 활용하여 OpenSSL 호환 응용 프로그램을 구축하는 방법을 설명합니다.
- 부록 D는 Sun Crypto Accelerator 4000 보드와 함께 사용되는 기타 소프트웨어의 사용에 대한 기타 업체 소프트웨어 제작사의 공지 사항 및 라이센스 조항을 설명합니다.
- 부록 E는 Sun Crypto Accelerator 4000 명령 설명과 각 명령에 대한 온라인 매뉴얼 페이지를 나열합니다.
- 부록 F는 Sun Crypto Accelerator 4000 보드를 보드의 `failsafe` 모드인 출고 상태로 초기화하는 방법을 설명합니다.
- 부록 G는 자주 재기되는 질문(FAQ)에 대한 답변을 제공합니다.

UNIX 명령 사용

이 설명서에는 시스템 종료, 시스템 부팅 및 장치 구성과 같은 기본 UNIX® 명령어 및 절차에 대한 정보는 나와 있지 않습니다.

이러한 정보는 다음을 참조하십시오.

- *Solaris 하드웨어 플랫폼 안내서*
- 다음 사이트에서 참조 가능한 Solaris 운영 환경용 온라인 설명서: `http://docs.sun.com`
- 시스템과 함께 제공된 기타 소프트웨어 설명서

활자체 규약

활자체	의미	예제
AaBbCc123	명령어, 파일 및 디렉토리의 이름과 컴퓨터 화면 상의 출력 내용	.login 파일을 편집하십시오. 모든 파일을 나열하려면 ls -a를 사용하십시오. % You have mail.
AaBbCc123	컴퓨터 화면 상의 출력 내용과 대조되는 사용자가 입력한 내용	% **su** Password:
AaBbCc123	문서 제목, 새로운 단어나 용어, 강조하는 단어	*사용 설명서*의 6장을 읽으십시오. 이들을 *클래스* 옵션이라고 합니다. 이 작업을 수행하려면 *반드시* 수퍼유저이어야 합니다.
	실제 이름이나 값으로 대체되는 명령행 변수	파일을 삭제하려면 rm *파일 이름*을 입력하십시오.

쉘 프롬프트

쉘	프롬프트
C 쉘	*machine_name*%
C 쉘 수퍼유저	*machine_name*#
Bourne 쉘 및 Korn 쉘	$
Bourne 쉘 및 Korn 쉘 수퍼유저	#

Sun 설명서 온라인 액세스

다음을 통해서 한글화된 버전을 비롯하여 Sun에서 제공하는 다양한 설명서를 보거나 인쇄 또는 구입할 수 있습니다.

`http://www.sun.com/documentation`

고객 의견

Sun은 설명서의 개선을 위해 항상 노력하고 있으며, 고객의 의견 및 제안을 언제나 환영합니다. 의견이 있으시면 다음 전자 우편 주소로 보내 주십시오.

`docfeedback@sun.com`

보내실 때는 해당 설명서의 부품 번호(817-2335-10)를 전자 메일 제목에 표기해 주십시오.

1 장

제품 개요

이 장에서는 Sun Crypto Accelerator 4000 보드의 개요를 설명하며 다음 항목으로 구성되어 있습니다.

제품 기능

Sun Crypto Accelerator 4000 보드는 Sun 서버에서 IPsec 및 SSL(대칭 및 비대칭 모두)에 대한 암호화 하드웨어 가속을 지원하는 기가비트 이더넷 기반의 네트워크 인터페이스입니다. 암호화되지 않은 네트워크 트래픽을 위한 표준 기가 비트 이더넷 네트워크 인터페이스로 운영될뿐만 아니라, 보드에는 표준 소프트웨어 솔루션보다 더 많은 암호화된 IPsec 트래픽 처리량을 지원하는 암호화 하드웨어가 내장되어 있습니다.

주요 프로토콜 및 인터페이스

Sun Crypto Accelerator 4000 보드는 표준 이더넷 최소/최대 프레임 크기(64~1,518바이트), 프레임 형식 및 다음의 표준과 프로토콜에 준수한다고 가정할 경우 기존의 이더넷 장비와 함께 운용할 수 있습니다.

- 전체 크기의 PCI 33/66Mhz, 32/64비트
- IEEE 802.3 CSMA/CD(이더넷)
- IEEE 802.2 논리적 연결 제어
- SNMP(국한된 MIB)
- 이중 및 반이중 기가비트 이더넷 인터페이스(IEEE 802.z)
- 일반 배전압 신호 방식(3.3V 및 5V)

주요 기능

- 구리 또는 섬유 인터페이스를 가진 기가비트 이더넷
- IPsec 및 SSL 암호화 기능 가속화
- 세션 설정율: 초 당 최대 연산 4,300번
- 대용량 암호화율: 최대 800Mbps
- 최대 2,048비트 RSA 암호화 제공
- 최대 10배 빠른 3DES 대용량 데이터 암호화 속도
- 보안 강화 및 키 관리 편의성을 위해 부정 조작 방지용 집중 보안 키와 Sun ONE 웹 서버용 인증서 관리
- FIPS 140-2 Level 3 인증서에 맞게 설계
- 낮은 CPU 사용률 — 서버 시스템 리소스 및 대역폭 소모량 감소
- 보안 개인 키 저장 및 관리
- Sun 미드프레임 및 고사양 서버 제품에 대해 동적 재구성(DR) 및 중복/장애 복구 지원
- 다중 CPU 간의 RX 패킷 부하 조절
- 완전한 흐름 제어 지원(IEEE 802.3x)

Sun Crypto Accelerator 4000 보드는 FIPS (Federal Information Processing Standard) 140-2, Level 3에서 설명한 암호화 모듈의 보안 요구 사항에 부응하도록 설계되었습니다.

지원되는 응용 프로그램

- Solaris 8 및 9 운영 환경(IPsec VPN)
- Sun ONE 웹 서버
- Apache 웹 서버

지원되는 암호화 프로토콜

이 보드는 다음 프로토콜을 지원합니다.

- IKE를 포함하여, IPv4 및 IPv6을 위한 IPsec
- SSLv2, SSLv3, TLSv1

이 보드는 다음 IPsec 기능을 가속화합니다.

- ESP (DES, 3DES) 암호화

이 보드는 다음 SSL 기능을 가속화 합니다.

- 클라이언트와 서버 간 보안 암호화 매개 변수 및 비밀 키 세트 설정
- 보드에 보안 비밀 키 — 보드를 떠날 경우 키 암호화

진단 지원

- OpenBoot™ PROM을 사용한 사용자가 실행하는 자가 테스트
- SunVTS™ 진단 테스트

암호화 알고리즘 가속화

Sun Crypto Accelerator 4000 보드는 하드웨어 및 소프트웨어 모두에 암호화 알고리즘을 가속화합니다. 이와 같은 복잡성의 이유는 암호화 알고리즘을 가속화하는 데 드는 비용이 모든 알고리즘에 대해 동일하지 않기 때문입니다. 일부 암호화 알고리즘은 하드웨어에서 구현되도록 특별히 설계된 반면 또다른 알고리즘은 소프트웨어에서 구현되도록 설계되었습니다. 하드웨어 가속화의 경우, 사용자 응용 프로그램에서 하드웨어 가속화 장치로 데이터를 이동하고 해당 결과를 다시 사용자 응용 프로그램으로 이동하는 데 추가 비용이 듭니다. 일부 암호화 알고리즘의 경우, 고도로 조정된 소프트웨어를 사용하면 전용 하드웨어의 수행 속도와 유사한 속도로 수행될 수 있습니다.

지원되는 암호화 알고리즘

Sun Crypto Accelerator 4000 드라이버(vca)는 각각의 암호화 요청을 검사하고 최대 처리량을 얻기 위해 가속화(호스트 프로세서 또는 Sun Crypto Accelerator 4000)를 위한 최적의 위치를 결정합니다. 부하 분산은 암호화 알고리즘, 현재 작업 부하 및 데이터 크기를 기반으로 이루어집니다.

Sun Crypto Accelerator 4000 보드는 다음 IPsec 알고리즘을 가속화합니다.

표 1-1 IPsec 암호화 알고리즘

유형	알고리즘
대칭형	DES, 3DES

Sun Crypto Accelerator 4000 보드는 다음 SSL 알고리즘을 가속화합니다.

표 1-2 SSL 암호화 알고리즘

유형	알고리즘
대칭형	DES, 3DES, ARCFOUR
비대칭형	Diffie-Hellman (Apache 전용) 및 RSA (최대 2,048비트 키), DSA
해시	MD5, SHA1

SSL 가속화

표 1-3은 하드웨어로 이동 가능한 SSL 가속 알고리즘과 Sun ONE 및 Apache 웹 서버에 제공되는 소프트웨어 알고리즘을 나타냅니다.

표 1-3 지원되는 SSL 알고리즘

	Sun ONE 웹 서버		Apache 웹 서버	
알고리즘	**하드웨어**	**소프트웨어**	**하드웨어**	**소프트웨어**
RSA	X	X	X	X
DSA	X	X	X	X
ARCFOUR		X		
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

대용량 암호화

Sun ONE 서버 소프트웨어를 위한 Sun Crypto Accelerator 4000 대용량 암호화 기능은 기본적으로 비활성화되어 있습니다. 파일을 생성하고 Sun ONE 서버 소프트웨어를 재시작하여 이 기능을 수동으로 활성화해야 합니다.

Sun Crypto Accelerator 4000 보드에서 Sun ONE 서버 소프트웨어가 대용량 암호화 기능을 사용할 수 있도록 하려면 `/etc/opt/SUNWconn/cryptov2/` 디렉토리에 `sslreg`이란 이름의 빈 파일을 생성한 후 서버 소프트웨어를 재시작합니다.

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

대용량 암호화 기능을 비활성화하려면 `sslreg` 파일을 삭제한 후 서버 소프트웨어를 재시작해야 합니다.

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

Apache 웹 서버 소프트웨어의 대용량 암호화 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

하드웨어 개요

Sun Crypto Accelerator 4000 하드웨어는 Sun 서버에서 IPsec 및 SSL의 성능을 향상시키는 전체 크기(10.668 × 31.198cm)의 암호화 가속기 PCI 기가비트 이더넷 어댑터입니다.

IPsec 하드웨어 가속화

Sun Crypto Accelerator 4000 보드는 하드웨어의 IPsec 패킷을 암호화하고 해독하여 SPARC™ 프로세서에서 이런 부하 높은 작업을 덜어줍니다. 암호화 하드웨어는 또한 기타 응응 프로그램에서 사용되는 일반 대칭 및 비대칭 암호화 작업을 지원하며 난수 하드웨어 소스를 포함하고 있습니다.

참고 – IPsec 가속화를 위해 Sun Crypto Accelerator 4000 보드를 실행할 경우 IPsec 설정이나 튜닝이 필요하지 않습니다. Sun Crypto Accelerator 4000 패키지를 설치하고 재부팅하기만 하면 됩니다.

Sun Crypto Accelerator 4000 보드 및 패키지가 설치되면 기존의 IPsec 설정과 향후 IPsec 설정은 핵심 Solaris 소프트웨어 대신 Sun Crypto Accelerator 4000 보드를 사용하게 됩니다. 보드는 표 1-1에 나열한 지원되는 모든 IPsec 알고리즘을 처리합니다. Sun Crypto Accelerator 4000 보드가 지원하지 않는 IPsec 알고리즘은 핵심 Solaris 암호화 소프트웨어가 계속 처리하게 됩니다. IPsec 설정에 대한 내용은 `http://docs.sun.com`에서 Solaris System Administrator Collection의 *System Administration Guide*를 참조하십시오.

Sun Crypto Accelerator 4000 MMF 어댑터

Sun Crypto Accelerator 4000 MMF 어댑터는 단일 포트 기가비트 이더넷 광섬유 PCI 버스 카드입니다. 1,000Mbps 이더넷 네트워크 상에서만 운용됩니다.

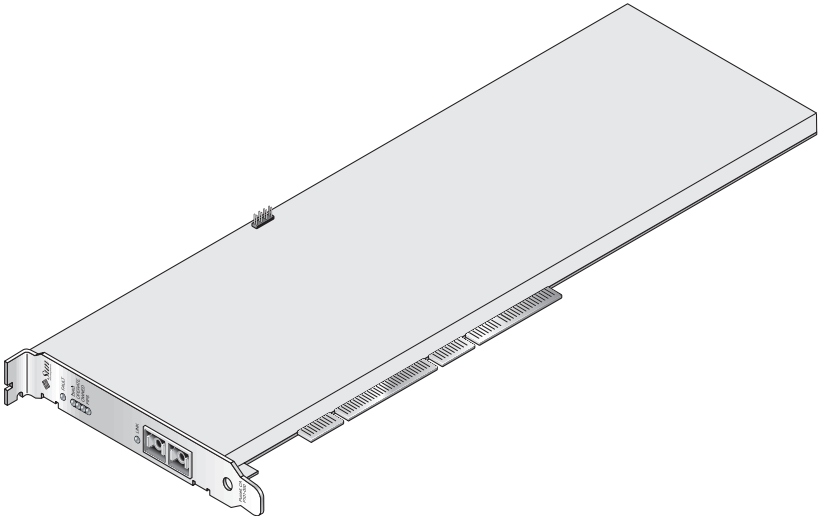

그림 1-1 Sun Crypto Accelerator 4000 MMF 어댑터

LED 디스플레이

표 1-4를 참조하십시오.

표 1-4 MMF 어댑터의 전면 패널 디스플레이 LED

레이블	점등 조건	색상
Fault	보드가 중단(치명적인 오류) 상태이거나 하위 수준 하드웨어 초기화에 실패한 경우 켜짐. 부팅 중 오류가 발생하면 깜빡거림.	적색
Diag	POST, 진단, 장애 시 안전(업그레이드 안된 펌웨어) 상태에서 켜짐. 진단 실행 중 깜빡림.	녹색
Operate	POST, 진단, 사용 불가(드라이버 없음) 상태에서 켜짐. 유휴, 작동, 장애 시 안전 상태에서 깜빡거림.	녹색

표 1-4 MMF 어댑터의 전면 패널 디스플레이 LED *(계속)*

레이블	점등 조건	색상
Init	보안 담당자가 `vcaadm`으로 보드를 초기화한 경우 켜짐. 61페이지의 "`vcaadm`을 통한 Sun Crypto Accelerator 4000 보드 초기화" 참조. ZEROIZE 점퍼 존재 시 깜빡거림.	녹색
FIPS Mode	FIPS 140-2 level 3 인증 모드에서 작동 시 켜짐. FIPS 모드가 아닌 경우 꺼짐.	녹색
Link	연결됨.	녹색

Sun Crypto Accelerator 4000 UTP 어댑터

Sun Crypto Accelerator 4000 UTP 어댑터는 단일 포트 기가비트 이더넷 구리 기반 PCI 버스입니다. 10, 100 및 1,000Mbps 이더넷 네트워크에서 작동하도록 설정할 수 있습니다.

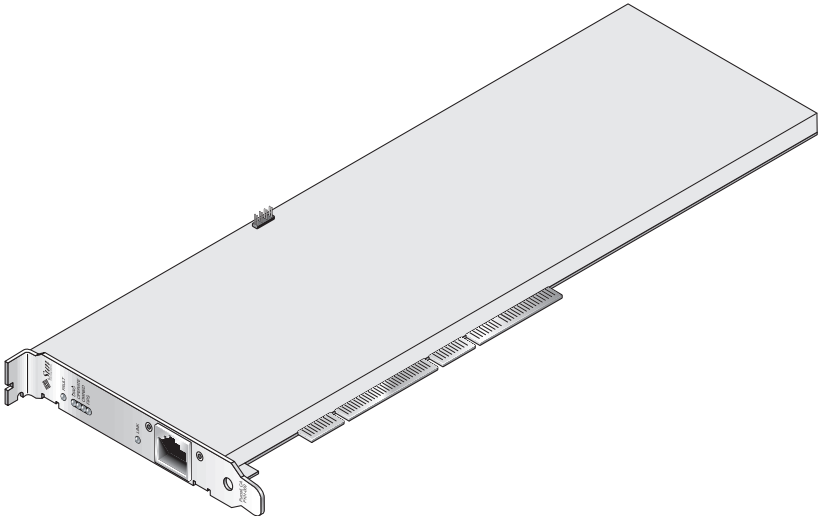

그림 1-2 Sun Crypto Accelerator 4000 UTP 어댑터

LED 디스플레이

표 1-5를 참조하십시오.

표 1-5 UTP 어댑터용 전면 패널 디스플레이 LED

레이블	점등 조건	색상
Fault	보드가 중단(치명적인 오류) 상태이거나 하위 수준 하드웨어 초기화에 실패한 경우 켜짐. 부팅 중 오류가 발생하면 깜빡거림.	적색
Diag	POST, 진단, 장애 시 안전(업그레이드 안된 펌웨어) 상태에서 켜짐. 진단 실행 중 깜빡림.	녹색
Operate	POST, 진단, 사용 불가(드라이버 없음) 상태에서 켜짐. 유휴, 작동, 장애 시 안전 상태에서 깜빡거림.	녹색
Init	보안 담당자가 `vcaadm`으로 보드를 초기화한 경우 켜짐. 61페이지의 "`vcaadm`을 통한 Sun Crypto Accelerator 4000 보드 초기화" 참조. ZEROIZE 점퍼 존재 시 깜빡거림	녹색
FIPS Mode	FIPS 140-2 level 3 인증 모드에서 작동 시 켜짐. FIPS 모드가 아닌 경우 꺼짐	녹색
1000	기가비트 이더넷 표시	녹색
활동(레이블 없음)	연결 송신 또는 수신 중	황색
Link	연결됨	녹색

참고 – 서비스 팩 번호(SP9 또는 SP1)는 iPlanet 웹 서버 4.1 또는 6.0이 언급될 경우 항상 포함됩니다.

동적 재구성 및 고가용성

Sun Crypto Accelerator 4000 하드웨어 및 관련 소프트웨어는 동적 재구성(DR)과 핫 플러깅을 지원하며 Sun 플랫폼에서 효과적으로 작동합니다. DR 또는 핫 플러그 작동 중에 Sun Crypto Accelerator 4000 소프트웨어 계층은 자동으로 보드의 추가나 제거를 감지하고 일정 알고리즘을 조정하여 하드웨어 리소스의 변경 사항을 수용합니다.

고가용성(HA) 구성을 수행하려면, 시스템 또는 도메인에 여러 개의 Sun Crypto Accelerator 4000 보드를 설치하여 하드웨어 가속을 계속적으로 사용할 수 있습니다. Sun Crypto Accelerator 4000 하드웨어 장애가 발생할 경우, 소프트웨어 계층은 장애를 감지하고 사용 가능한 하드웨어 암호화 가속기 목록에서 이를 제거합니다. Sun Crypto Accelerator 4000은 하드웨어 장애로 인한 리소스 감소를 일정 알고리즘을 조정하여 보완합니다. 그 이후의 암호와 요청은 나머지 보드로 넘어갑니다.

Sun Crypto Accelerator 4000 하드웨어는 장기 키 생성을 위한 고품질의 엔트로피 소스를 제공합니다. 도메인이나 시스템 내의 모든 Sun Crypto Accelerator 4000 보드가 제거된 경우 장기 키는 저품질 엔트로피로 생성됩니다.

부하 공유

Sun Crypto Accelerator 4000 소프트웨어는 Solaris 도메인 또는 시스템 내에 설치된 모든 보드로 부하를 분산시킵니다. 수신되는 암호화 요청은 정해진 길이의 작업 대기열에 기초하여 모든 보드에 걸쳐 분산됩니다. 암호화 요청은 첫 번째 보드로 전달되고, 해당 보드가 최대 용량으로 실행될 때까지 요청이 계속 전달됩니다. 첫 번째 보드가 최대 용량으로 실행되기 시작하면 추가 요청은 해당 유형의 요청을 수용 가능한 다음 보드의 대기열로 전달됩니다. 대기 메커니즘은 보드에서 요청의 결합을 통해 최적화하도록 설계되었습니다.

하드웨어 및 소프트웨어 요구 사항

표 1-6에는 Sun Crypto Accelerator 4000 어댑터에 대한 하드웨어 및 소프트웨어 요구 사항이 나와 있습니다.

표 1-6 하드웨어 및 소프트웨어 요구 사항

하드웨어 및 소프트웨어	요구 사항
하드웨어	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K; Netra™ 20 (lw4); Sun Blade™ 100, 150, 1000, 2000
운영 환경	Solaris 8 2/02 및 이후 호환 가능한 릴리스(IPsec 가속화에는 Solaris 9는 필수)

필요한 패치

자세한 내용은 *Sun Crypto Accelerator 4000 보드 릴리스 노트*를 참조하십시오.

다음은 시스템에서 Sun Crypto Accelerator 4000 보드를 실행하기 위해 필요한 패치입니다. Solaris 업데이트에는 이전 릴리스에 대한 패치가 포함되어 있습니다. `showrev -p` 명령을 사용하여 표시된 패치가 이미 설치되어 있는지 확인합니다.

다음 웹 사이트에서 다운로드할 수 있습니다. `http://sunsolve.sun.com`

패치의 최신 버전을 설치합니다. 대시 번호(예: -01)는 패치의 새 버전이 나올 때마다 증가됩니다. 웹 사이트에 있는 버전이 아래 표에 표시되어 있는 버전보다 높으면 최신 버전이 됩니다.

필요한 패치가 SunSolve℠에 없는 경우에는 지역 영업 센터 또는 서비스 대리점에 문의하십시오.

Apache 웹 서버 패치

Apache 웹 서버를 사용하려면 109234-09 패치를 설치해야 합니다. `SUNWkcl2a` 패키지가 추가되면 시스템은 Apache 웹 서버 mod_ssl 1.3.26로 구성됩니다.

Solaris 8 패치

다음 표에는 이 제품과 함께 사용 가능한 권장 및 필수 Solaris 8 패치가 나와 있습니다. 표 1-7은 필수 패치를 나열하고 설명합니다.

표 1-7 Sun Crypto Accelerator 4000 소프트웨어에 필요한 Solaris 8 패치

패치 ID	설명
110383-01	`libnvpair`
108528-05	`KU-05`(`nvpair` 지원)
112438-01	`/dev/random`

Solaris 9 패치

현재 필요한 Solaris 9 패치가 없습니다.

2 장

Sun Crypto Accelerator 4000 보드 설치

이 장에서는 Sun Crypto Accelerator 4000 하드웨어 및 소프트웨어 설치 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

보드 사용

각 보드는 특수 정전기 방지용 봉지에 포장되어 운반 또는 보관 기간 동안 보호됩니다. 보드에 내장된 정전기에 민감한 부품의 손상을 방지하려면 보드를 만지기 전에 다음 방법 중 한 가지를 사용하여 신체의 정전기를 감소시키십시오.

- 컴퓨터의 금속 프레임에 접촉합니다.
- 정전기 방지용 손목 띠를 손목 및 접지된 금속 표면에 부착합니다.

주의 – 보드에 내장된 민감한 부품의 손상을 방지하려면 보드를 다룰 때는 정전기 방지용 손목 띠를 착용하고, 보드를 들 때는 가장자리를 사용하며, 포장에 사용된 플라스틱 봉지와 같이 항상 정전기가 없는 장소에 놓아야 합니다.

보드 설치

Sun Crypto Accelerator 4000 보드 설치에는 시스템에 보드를 삽입하고 소프트웨어 도구를 로드하는 작업이 포함됩니다. 하드웨어 설치 지침에는 보드 설치에 대한 일반적인 단계만 포함됩니다. 특정 설치 지침에 대해서는 시스템과 함께 제공된 설명서를 참조하십시오.

▼ 하드웨어 설치

1. **수퍼유저로 로그인하고 시스템과 함께 제공된 지침에 따라 컴퓨터를 종료하고 전원을 끈 다음, 전원 코드를 분리하고 컴퓨터 덮개를 제거합니다.**
2. **사용하지 않은 PCI 슬롯(64비트, 66MHz 슬롯 권장)을 찾아봅니다.**
3. **정전기 방지용 손목 띠를 손목 및 접지된 금속 표면 끝에 부착합니다.**
4. **Phillips 헤드 나사 드라이버를 사용하여 PCI 슬롯 덮개에서 나사를 제거합니다.**

   5단계에서 브래킷을 고정할 수 있도록 나사를 보관합니다.
5. **Sun Crypto Accelerator 4000 보드의 가장자리를 잡고 플라스틱 봉지에서 꺼낸 다음 PCI 슬롯에 삽입하고 후면 브래킷의 나사를 고정시킵니다.**
6. **컴퓨터 덮개를 씌운 다음 전원 코드를 다시 연결하고 시스템 전원을 켭니다.**
7. **OpenBoot™ PROM** `ok` **프롬프트에서** `show-devs` **명령을 입력하여 보드가 올바르게 설치되었는지 확인합니다.**

```
ok show-devs
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
```

위 예제에서 `/pci@8,600000/network@1`은 Sun Crypto Accelerator 4000 보드에 대한 장치 경로를 확인합니다. 시스템의 각 보드에 대해 이런 행이 하나씩 있을 것입니다.

Sun Crypto Accelerator 4000 장치 속성이 올바르게 나열되었는지 판단하려면 ok 프롬프트에서 장치 경로까지 이동한 후 .properties를 입력하여 속성 목록을 확인합니다.

```
ok cd /pci@8,600000/network@1
ok .properties
assigned-addresses       82000810 00000000 00102000 00000000 00002000
                          81000814 00000000 00000400 00000000 00000100
                          82000818 00000000 00200000 00000000 00200000
                          82000830 00000000 00400000 00000000 00100000
d-fru-len                00 00 00 00
d-fru-off                00 00 e8 00
d-fru-dev                eeprom
s-fru-len                00 00 08 00
s-fru-off                00 00 e0 00
s-fru-dev                eeprom
compatible               70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                      00000800 00000000 00000000 00000000 00000000
                          02000810 00000000 00000000 00000000 00002000
                          02000814 00000000 00000000 00000000 00000100
                          02000818 00000000 00000000 00000000 00200000
                          02000830 00000000 00000000 00000000 00100000
address-bits             00 00 00 30
max-frame-size           00 00 40 00
network-interface-type   ethernet
device_type              network
name                     network
local-mac-address        08 00 20 aa bb cc
version                  Sun PCI Crypto Accelerator 4000 1000Base-T FCode
12.11.13 02/10/31
phy-type                 mif
board-model              501-6039
model                    SUNW,pci-vca
fcode-rom-offset         00000000
66mhz-capable
fast-back-to-back
devsel-speed             00000001
class-code               00100000
interrupts               00000001
latency-timer            00000040
cache-line-size          00000010
max-latency              00000040
min-grant                00000040
subsystem-id             00003de8
subsystem-vendor-id      0000108e
revision-id              00000002
device-id                0000b555
vendor-id                00008086
```

Sun Crypto Accelerator 4000 소프트웨어 설치

Sun Crypto Accelerator 4000 소프트웨어는 Sun Crypto Accelerator 4000 CD에 포함되어 있습니다. SunSolve 웹 사이트에서 패치를 다운로드해야 할 경우도 있습니다. 자세한 내용은 10페이지의 "필요한 패치"를 참조하십시오.

▼ 소프트웨어 설치

1. **시스템에 연결된 CD-ROM 드라이브에 Sun Crypto Accelerator 4000 CD를 넣습니다.**
   - 시스템이 Sun Enterprise Volume Manager™를 실행 중인 경우 CD-ROM이 `/cdrom/cdrom0` 디렉토리에 자동으로 설치됩니다.
   - 시스템에 Sun Enterprise Volume Manager가 실행 중이 아닌 경우 다음을 입력하여 CD-ROM을 마운트합니다.

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

`/cdrom/cdrom0` 디렉토리에 다음 파일과 디렉토리가 표시됩니다.

표 2-1 `/cdrom/cdrom0` 디렉토리의 파일

파일 또는 디렉토리	내용	
`Copyright`	미국 저작권 파일	
`FR_Copyright`	프랑스 저작권 파일	
`Docs`	*Sun Crypto Accelerator 4000 보드 설치 및 사용 설명서* *Sun Crypto Accelerator 4000 보드 릴리스 노트*	
`Packages`	다음 Sun Crypto Accelerator 4000 소프트웨어 패키지가 포함되어 있습니다.	
	`SUNWkcl2r`	암호화 커널 구성 요소
	`SUNWkcl2u`	암호화 관리 유틸리티 및 라이브러리
	`SUNWkcl2a`	Apache용 SSL 지원(*옵션*)
	`SUNWkcl2m`	암호화 관리 매뉴얼 페이지(*옵션*)
	`SUNWvcar`	VCA Crypto Accelerator(루트)
	`SUNWvcau`	VCA Crypto Accelerator(Usr)
	`SUNWvcaa`	VCA 관리

표 2-1 /cdrom/cdrom0 디렉토리의 파일 *(계속)*

파일 또는 디렉토리	내용	
	SUNWvcafw	VCA 펌웨어
	SUNWvcamn	VCA Crypto Accelerator 매뉴얼 페이지(*옵션*)
	SUNWvcav	VCA Crypto Accelerator의 SunVTS 테스트(*옵션*)
	SUNWkcl2o	SSL 개발 도구 및 라이브러리(*옵션*)
	SUNWkcl2i.u	KCLv2 Crypto를 통한 IPSec 가속화(*옵션*)

필수 패키지는 옵션 패키지 설치 전에 일정 순서에 따라 설치해야 합니다. 필수 패키지가 설치되면 순서에 상관없이 옵션 패키지를 설치하고 제거할 수 있습니다.

옵션 SUNWkcl2a 패키지는 Apache를 웹 서버로 사용하려는 경우에만 설치합니다.

옵션 SUNWkcl2o 패키지는 Apache 웹 서버의 다른(지원되지 않는) 버전으로 다시 연결하려는 경우에만 설치합니다.

옵션 SUNWvcav 패키지는 SunVTS 테스트를 수행하려는 경우에만 설치합니다. SUNWvcav 패키지를 설치하려면 SunVTS 4.4 이상에서 5.x까지의 버전이 설치되어 있어야 합니다.

참고 – 옵션 SUNWkcl2i.u 패키지는 Sun Crypto Accelerator 4000 CD 상에서만 .u 확장자를 가지고 있습니다. 일단 패키지가 설치되면 이름이 SUNWkcl2로 변경됩니다. CD에 있는 본 패키지의 .u 확장자는 패키지를 sun4u 아키텍쳐 전용으로 정의합니다.

2. 다음을 입력하여 필수 소프트웨어를 설치합니다.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
```

3. (옵션) 소프트웨어가 올바르게 설치되었는지 확인하려면 pkginfo 명령을 실행합니다.

```
# pkginfo SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
system  SUNWkcl2r   Cryptography Kernel Components
system  SUNWkcl2u   Cryptographic Administration Utility and Libraries
system  SUNWvcar    VCA Crypto Accelerator (Root)
system  SUNWvcau    Crypto Accelerator/Gigabit Ethernet (Usr)
system  SUNWvcaa    VCA Administration
system  SUNWvcafw   VCA Firmware
```

4. **(옵션) 드라이버가 부착되었는지 확인하려면** prtconf **명령을 실행합니다.**
   prtdiag**(1m) 온라인 매뉴얼 페이지를 참조하십시오.**

```
# prtdiag -v
```

5. **(옵션)** modinfo **명령을 실행하여 모듈이 로드되었는지 확인합니다.**

```
# modinfo | grep Crypto
62   1317f62  20b1f 198   1  vca (VCA Crypto/Ethernet v1.102)
63   13360e9  12510 200   1  kcl2 (Kernel Crypto Library v1.148)
197  136d5d6   19b0 199   1  vcactl (VCA Crypto Control v1.19)
```

옵션 패키지 설치

Apache 웹 서버에 대한 SSL 지원과 암호화 관리 유틸리티 및 라이브러리를 제공하는 옵션 패키지만 설치하려면 다음을 입력하십시오.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2u
```

옵션 소프트웨어 패키지 모두 설치하려면 다음을 입력합니다.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

이전 예제의 옵션 패키지 내용에 대한 설명은 표 2-1을 참조하십시오.

디렉토리 및 파일

표 2-2는 Sun Crypto Accelerator 4000 소프트웨어의 기본 설치시 생성되는 디렉토리를 나타냅니다.

표 2-2 Sun Crypto Accelerator 4000 디렉토리

디렉토리	내용
/etc/opt/SUNWconn/vca/keydata	키스토어 데이터(암호화)
/opt/SUNWconn/cryptov2/bin	유틸리티
/opt/SUNWconn/cryptov2/lib	지원 라이브러리
/opt/SUNWconn/cryptov2/sbin	관리 명령

그림 2-1은 이런 디렉토리 및 파일의 계층 구조를 설명합니다.

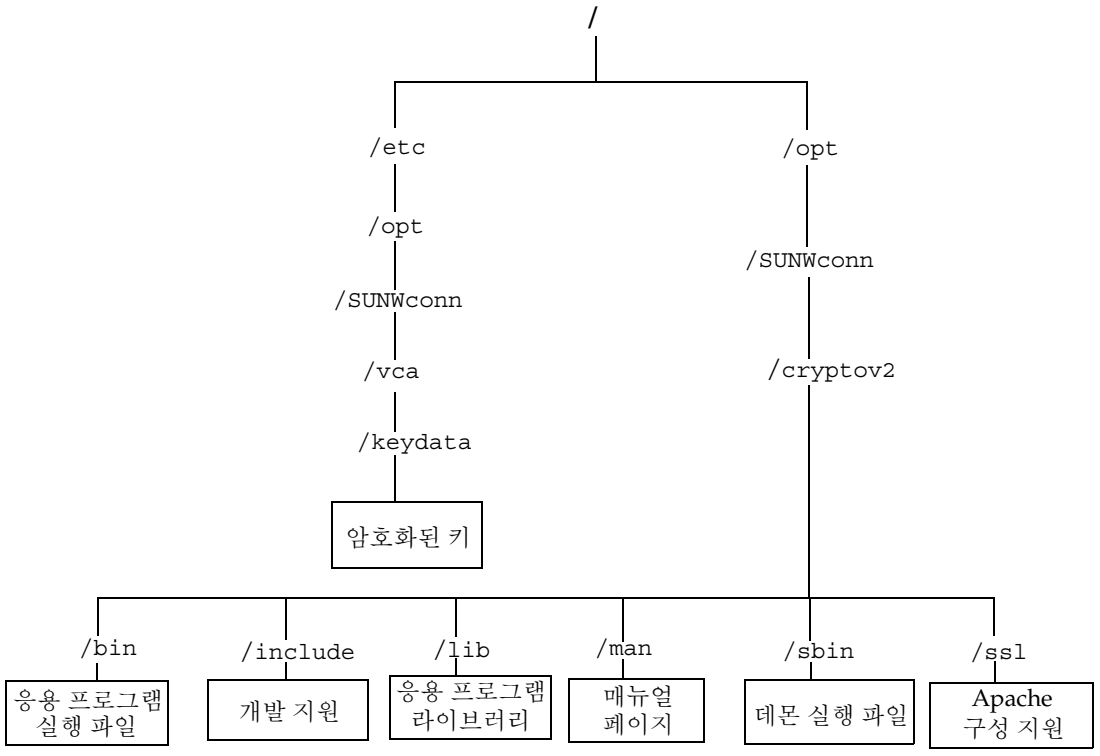

그림 2-1 Sun Crypto Accelerator 4000 디렉토리 및 파일

참고 – 보드의 하드웨어와 소프트웨어가 설치되면 구성 및 키스토어 정보로 보드를 초기화해야 합니다. 보드 초기화 방법에 대한 내용은 61페이지의 "`vcaadm`을 통한 Sun Crypto Accelerator 4000 보드 초기화"를 참조하십시오.

소프트웨어 제거

키스토어를 생성한 경우(65페이지의 "vcaadm를 통한 키스토어 관리" 참조) 소프트웨어를 삭제하기 전에 Sun Crypto Accelerator 4000 보드에 구성된 키스토어 정보를 삭제해야 합니다. `zeroize` 명령은 모든 키 요소를 제거하지만 Sun Crypto Accelerator 4000 보드가 설치된 물리적 호스트의 파일 시스템에 저장된 키스토어 파일을 삭제하지 않습니다. `zeroize` 명령에 대한 자세한 내용은 75페이지의 "Sun Crypto Accelerator 4000 보드 원상 복구"을 참조하십시오. 시스템에 저장된 키스토어 파일을 삭제하려면 수퍼유저 권한으로 이를 제거해야 합니다. 키스토어를 아직 생성하지 않은 경우 이 절차를 건너뛸 수 있습니다.

주의 – 현재 사용 중이거나 다른 사용자 또는 키스토어가 공유한 키스토어를 삭제하면 안됩니다. 키스토어에 대한 참조를 해제하려면 웹 서버 및/또는 관리 서버를 종료해야 할 수도 있습니다.

주의 – Sun Crypto Accelerator 4000 소프트웨어를 제거하기 전에 Sun Crypto Accelerator 4000 보드 사용을 위해 활성화한 모든 웹 서버를 비활성화해야 합니다. 그렇게 하지 않으면, 해당 웹 서버의 기능이 작동되지 않습니다.

▼ 소프트웨어 제거

- **수퍼유저인 상태에서 `pkgrm` 명령을 사용하여 본인이 설치한 소프트웨어 패키지만 제거합니다.**

주의 – 설치된 패키지는 반드시 아래에 표시된 순서대로 제거해야 합니다. 그렇지 않으면 종속 경고가 발생하고 커널 모듈이 로드된 채로 남아있을 수 있습니다.

패키지를 모두 설치한 경우에는 다음 방법으로 제거합니다.

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcafw SUNWvcau
```

참고 – Sun Crypto Accelerator 4000 보드를 위한 SunVTS 테스트(`SUNWdcav`)를 설치하거나 제거한 후에 SunVTS가 이미 실행 중인 경우에는 시스템을 재검사하여 사용 가능한 테스트를 업데이트해야 할 수 있습니다. 자세한 내용은 SunVTS 설명서를 참조하십시오.

3 장

드라이버 매개 변수 구성

이 장에서는 Sun Crypto Accelerator 4000 UTP 및 MMF 이더넷 어댑터 모두가 사용하는 vca 장치 드라이버 매개 변수의 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

Sun Crypto Accelerator 4000 이더넷 장치 드라이버(vca) 매개 변수

vca 장치 드라이버는 Sun Crypto Accelerator 4000 UTP 및 MMF 이더넷 장치를 제어합니다. vca 드라이버는 Sun Crypto Accelerator 4000의 UNIX pci 이름 속성 pci108e,3de8에 첨부되어 있습니다(108e는 벤더 ID, 3de8는 PCI 장치 ID입니다).

시스템의 각 Sun Crypto Accelerator 4000 장치를 사용자 정의하기 위해 vca 장치 드라이버 매개 변수를 수동으로 구성할 수 있습니다. 이 항목에서는 보드에 사용된 Sun Crypto Accelerator 4000 이더넷 장비의 기능에 대한 개요, 사용 가능한 vca 장치 드라이버 매개 변수 목록과 이런 매개 변수의 구성 방법을 설명합니다.

Sun Crypto Accelerator 4000 이더넷 UTP 및 MMF PCI 어댑터는 33페이지의 "자동 교섭 또는 강제 모드 설정"에서 나열한 운영 속도와 모드로 작동합니다. 기본적으로, vca 장치는 speed, duplex, link-clock 매개 변수에 대한 일반 작동 모드를 선택할 때는 링크(링크 파트너)의 원격 끝을 통해 자동 교섭 모드로 작동합니다. link-clock 매개 변수는 보드가 1,000Mbps로 작동한 경우에만 적용할 수 있습니다. vca 장치는 또한 각각의 이런 매개 변수에 대해 강제 모드로 구성될 수도 있습니다.

주의 – 올바른 링크를 설정하려면 두 링크 파트너 모두가 `speed`, `duplex`, `link-clock` (1,000Mbps에서만 가능) 매개 변수 각각에 대해 자동 교섭 모드 또는 강제 모드로 작동 중이어야 합니다. 링크 파트너 중 하나라도 각각의 이런 매개 변수에 대해 동일한 모드로 작동하지 않는 경우 네트워크 오류가 발생할 것입니다. 38페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조하십시오.

드라이버 매개 변수 값 및 정의

표 3-1은 `vca` 장치 드라이버의 매개 변수와 설정을 설명합니다.

표 3-1 `vca` 드라이버 매개 변수, 상태 및 설명

매개 변수	상태	설명
`instance`	읽기 및 쓰기	장치 인스턴스
`adv-autoneg-cap`	읽기 및 쓰기	작동 모드 매개 변수
`adv-1000fdx-cap`	읽기 및 쓰기	작동 모드 매개 변수(MMF 어댑터 전용)
`adv-1000hdx-cap`	읽기 및 쓰기	작동 모드 매개 변수
`adv-100fdx-cap`	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
`adv-100hdx-cap`	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
`adv-10fdx-cap`	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
`adv-10hdx-cap`	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
`adv-asmpause-cap`	읽기 및 쓰기	흐름 제어 매개 변수
`adv-pause-cap`	읽기 및 쓰기	흐름 제어 매개 변수
`pause-on-threshold`	읽기 및 쓰기	흐름 제어 매개 변수
`pause-off-threshold`	읽기 및 쓰기	흐름 제어 매개 변수
`link-master`	읽기 및 쓰기	1Gbps 속도 강제 모드 매개 변수
`enable-ipg0`	읽기 및 쓰기	패킷 전송 전 추가 지연 활성화
`ipg0`	읽기 및 쓰기	패킷 전송 전 추가 지연
`ipg1`	읽기 및 쓰기	인터패킷 갭 매개 변수
`ipg2`	읽기 및 쓰기	인터패킷 갭 매개 변수
`rx-intr-pkts`	읽기 및 쓰기	인터럽트 블랭킹 값 수신
`rx-intr-time`	읽기 및 쓰기	인터럽트 블랭킹 값 수신

표 3-1 vca 드라이버 매개 변수, 상태 및 설명 *(계속)*

매개 변수	상태	설명
red-dv4to6k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
red-dv6to8k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
red-dv8to10k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
red-dv10to12k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
tx-dma-weight	읽기 및 쓰기	PCI 인터페이스 매개 변수
rx-dma-weight	읽기 및 쓰기	PCI 인터페이스 매개 변수
infinit-burst	읽기 및 쓰기	PCI 인터페이스 매개 변수
disable-64bit	읽기 및 쓰기	PCI 인터페이스 매개 변수

통지 링크 매개 변수

다음 매개 변수는 vca 드라이버가 해당 링크 파트너에게 통지할 speed 및 duplex 링크 매개 변수의 송수신을 결정합니다. 표 3-2는 작동 모드 매개 변수 및 해당 기본값을 설명합니다.

참고 – 매개 변수의 초기 설정이 0으로 설정된 경우 이를 변경할 수 없습니다. 초기 설정이 0인 설정을 변경해도 다시 0으로 복귀됩니다. 기본적으로, 이러한 매개 변수들은 vca 장치의 기능에 맞춰 설정됩니다.

Sun Crypto Accelerator 4000 UTP 어댑터의 통지 링크 매개 변수는 표 3-2에서 설명한 것과 같이 Sun Crypto Accelerator 4000 MMF 어댑터의 통지 링크 매개 변수와는 다릅니다.

표 3-2 작동 모드 매개 변수

매개 변수	설명
다음 매개 변수는 Sun Crypto Accelerator 4000 UTP 및 MMF 어댑터 모두에 해당합니다.	
`adv-autoneg-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 강제 모드 1 = 자동 교섭(기본값)
다음 매개 변수는 Sun Crypto Accelerator 4000 MMF 어댑터에만 해당합니다.	
`adv-1000fdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 1,000Mbps 전이중 불가 1 = 1000Mbps 전이중 가능(기본값)
다음 매개 변수는 Sun Crypto Accelerator 4000 UTP 및 MMF 어댑터 모두에 해당합니다.	
`adv-1000hdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 1,000Mbps 반이중 불가 1 = 1,000Mbps 반이중 가능(기본값)
다음 매개 변수는 Sun Crypto Accelerator 4000 UTP 어댑터에만 해당합니다.	
`adv-100fdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 100Mbps 전이중 불가 1 = 100Mbps 전이중 가능(기본값)
`adv-100hdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 100Mbps 반이중 불가 1 = 100Mbps 반이중 가능(기본값)
`adv-10fdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 10Mbps 반이중 불가 1 = 10Mbps 반이중 가능(기본값)
`adv-10hdx-cap`	하드웨어가 통지한 로컬 인터페이스 기능 0 = 10Mbps 반이중 불가 1 = 10 Mbps 반이중 가능(기본값)

이전의 모든 매개 변수가 1로 설정된 경우 자동 교섭은 사용 가능한 최고 속도를 사용합니다. 이전의 모든 매개 변수가 0으로 설정된 경우 다음 오류 메시지가 표시됩니다.

```
NOTICE: Last setting will leave vca0 with no link capabilities.
WARNING: vca0: Restoring previous setting.
```

참고 – 위 예제에서 vca0은 모든 Sun Crypto Accelerator 4000 보드에 대해 문자열 vca가 사용되는 Sun Crypto Accelerator 4000 보드 장치 이름입니다. 이 문자열의 바로 다음에는 항상 보드의 장치 인스턴스 번호가 따릅니다. 그러므로, vca0 보드의 장치 인스턴스 번호는 0입니다.

흐름 제어 매개 변수

vca 장치는 IEEE 802.3x Frame Based Link Level Flow Control Protocol (프레임 기반 링크 수준 흐름 제어 프로토콜)에 부합하는 휴지 프레임 송신(전송) 및 착신(수신)이 가능합니다. vca 장치는 수신한 흐름 제어 프레임에 답하여 자신의 전송률을 낮출 수 있습니다. 또한, vca 장치는 흐름 제어 프레임을 송신할 수 있어 링크 파트너가 이 기능을 지원하는 경우 링크 파트너에게 전송률을 낮출 것을 요청합니다. 기본적으로, 드라이버는 자동 교섭 중 전송과 수신 휴지 기능 모두를 통지합니다.

표 3-3 은 흐름 제어 키워드와 기능을 설명합니다.

표 3-3 읽기-쓰기 흐름 제어 키워드 설명

키워드	설명		
adv-asmpause-cap	MMF 및 UTP 어댑터 모두가 비대칭 휴지를 지원하므로 vca 장치는 한 방향으로만 휴지할 수 있습니다. 0=끔(기본값) 1=켬		
adv-pause-cap	이 매개 변수는 adv-asmpause-cap 값에 따라 두 가지 의미를 갖게 됩니다. (기본값=0)		
	매개 변수 값 +	**매개 변수 값 =**	**설명**
	adv-asmpause-cap=	adv-pause-cap=	
	1	1 또는 0	adv-pause-cap은 휴지 진행 방향을 결정합니다.
	1	1	휴지는 수신되지만 송신되지는 않습니다.
	1	0	휴지는 송신되지만 수신되지는 않습니다.
	0	1	휴지는 송수신됩니다.
	0	1 또는 0	adv-pause-cap은 휴지 기능의 활성 여부를 결정합니다.

표 3-3 읽기-쓰기 흐름 제어 키워드 설명 *(계속)*

키워드	설명
pause-on-threshold	수신 (RX) FIFO에서 64바이트 블록의 수를 정의하여 보드가 XON-PAUSE 프레임을 생성하도록 합니다.
pause-off-threshold	RX FIFO에서 64바이트 블록의 수를 정의하여 보드가 XOFF-PAUSE 프레임을 생성하도록 합니다.

기가비트 강제 모드 매개 변수

기가비트 링크에 대해서는, 이 매개 변수는 link-master를 결정합니다. 일반적으로, 스위치는 link-master로 활성화되며 이런 경우에는 이 매개 변수가 변경되지 않습니다. 그렇지 않은 경우에는 link-master 매개 변수가 vca 장치를 link-master로 활성화하기 위해 사용될 수 있습니다.

표 3-4 기가비트 강제 모드 매개 변수

매개 변수	설명
link-master	1로 설정된 경우 이 매개 변수는 링크 파트너를 슬레이브로 간주하고 마스터 작업을 활성화합니다. 0으로 설정된 경우 이 매개 변수는 링크 파트너를 마스터로 간주하고 슬레이브 작업을 활성화합니다. (기본값)

인터패킷 갭 매개 변수

vca 장치는 enable-ipg0이란 프로그램 가능한 모드를 지원합니다.

활성화(기본값)된 enable-ipg0으로 패킷을 송신하기 전에, vca 장치는 추가 시간 지연을 설정합니다. ipg0 매개 변수가 설정한 이 지연은 ipg1 및 ipg2 매개 변수가 설정한 지연에 추가됩니다. 추가 ipg0 지연은 충돌을 줄입니다.

enable-ipg0이 비활성화된 경우, ipg0의 값은 무시되고 추가 지연은 설정되지 않습니다. ipg1 및 ipg2가 설정한 지연만 사용됩니다. 다른 시스템이 계속해서 대량의 연속 패킷을 전송하는 경우 enable-ipg0을 비활성화합니다. enable-ipg0이 활성화된 시스템은 네트워크 상에서 처리할 시간이 부족할 수도 있습니다. ipg0 매개 변수를 0에서 255까지 설정하여 지연을 추가할 수 있으며, 이는 매체 바이트 시간 지연입니다. 표 3-5는 enable-ipg0 및 ipg0 매개 변수를 정의합니다.

표 3-5 enable-ipg0 및 ipg0을 정의하는 매개 변수

매개 변수	값	설명
enable-ipg0	0 1	enable-ipg0 활성화 enable-ipg0 비활성화(기본값=1)
ipg0	0에서 255	패킷 전송전(패킷 수신후) 추가 시간 지연 (또는 갭)(기본값=8)

vca 장치는 프로그램 가능한 인터패킷 갭 매개 변수(IPG) ipg1 및 ipg2를 지원합니다. 총 IPG는 ipg1과 ipg2의 합계입니다. 1,000Mbps 링크 속도에 대한 총 IPG는 0.096 마이크로초입니다.

표 3-6은 IPG 매개 변수에 대한 기본값과 허용치를 나열합니다.

표 3-6 읽기-쓰기 인터패킷 갭 매개 변수 값 및 설명

매개 변수	값(바이트-시간)	설명
ipg1	0에서 255	인터패킷 갭 1(기본값=8)
ipg2	0에서 255	인터패킷 갭 2(기본값=4)

드라이버는 기본적으로 ipg1을 8바이트 시간으로, ipg2를 4바이트 시간으로 설정하며, 이는 표준값이 됩니다. (바이트 시간은 1,000Mbps의 링크 속도 설정에서 링크 상에 1바이트를 전송하는 데 소요되는 시간을 말합니다)

네트워크 상에 이보다 긴 IPG(ipg1 및 ipg2의 합)를 사용하는 시스템이 있고 이런 시스템에 대한 네트워크 액세스가 느린 경우 ipg1 및 ipg2의 값을 늘려 다른 시스템의 긴 IPG와 일치하도록 합니다.

인터럽트 매개 변수

표 3-7은 수신 인터럽트 블랭킹 값을 설명합니다.

표 3-7 RX 별칭 읽기용 블랭킹 레지스터

필드 이름	값	설명
rx-intr-pkts	0에서 511	최종 패킷 서비스 이후부터 해당 패킷 수가 도착한 후 인터럽트합니다. 0은 패킷 블랭킹이 없음을 의미합니다. (기본값=3)
rx-intr-time	0에서 524,287	최종 패킷 서비스 이후 4.5마이크로초(usecs)가 경과한 후 인터럽트합니다. 0은 패킷 블랭킹이 없음을 의미합니다. (기본값=3)

임의 조기 드롭 매개 변수

이 매개 변수는 수신 FIFO의 용량 상태에 따른 패킷 드롭 기능을 제공합니다. 이 기능은 기본적으로 비활성화되어 있습니다. FIFO 점유율이 일정 범위에 도달하면 패킷은 사전 설정된 확률에 따라 드롭됩니다. FIFO 수준이 증가할 때 확률도 증가해야 합니다. 제어 패킷은 드롭되지 않으며 통계에서 제외됩니다.

표 3-8 RX 임의 조기 감지 8비트 벡터

필드 이름	값	설명
red-dv4to6k	0에서 255	FIFO 임계값이 4,096바이트 이상, 6,144바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 0이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에 드롭됩니다. (기본값=0)
red-dv6to8k	0에서 255	FIFO 임계값이 6,144바이트 이상, 8,192바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 8이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에 드롭됩니다. (기본값=0)

표 3-8 RX 임의 조기 감지 8비트 벡터 *(계속)*

필드 이름	값	설명
red-dv8to10k	0에서 255	FIFO 임계값이 8,192바이트 이상, 10,240바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 16이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에 드롭됩니다. (기본값=0)
red-dv10to12k	0에서 255	FIFO 임계값이 10,240바이트 이상, 12,288바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 24가 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에 드롭됩니다. (기본값=0)

PCI 버스 인터페이스 매개 변수

이 매개 변수를 통해 PCI 인터페이스 특성을 수정하여 특정 응용 프로그램에 대해 보다 향상된 PCI 성능을 얻을 수 있습니다.

표 3-9 PCI 버스 인터페이스 매개 변수

매개 변수	설명
tx-dma-weight	가중된 라운드 로빈 조정이 실시되는 동안 전송(TX) 측에 크레디트를 부여하는 중복 계수를 결정합니다. 이 값은 0에서 3 사이입니다 (기본값=0). 0은 별도의 가중이 없음을 뜻합니다. 다른 값은 가중 트래픽에 대해 2의 지수를 사용합니다. 예를 들어, tx-dma-weight = 0 이고 rx-dma-weight = 3인 경우 RX 트래픽이 지속적으로 수신되는 동안 RX 트래픽의 우선 순위는 PCI에 접속하는 트래픽의 우선 순위보다 8배 더 큽니다.
rx-dma-weight	가중된 라운드 로빈 조정이 실시되는 동안 전송(TX) 측에 크레디트를 부여하는 중복 계수를 결정합니다. 0에서 3사이의 값입니다(기본값=0).
infinite-burst	활성화된 경우 이 매개 변수는 무한 버스트 기능을 지원하는 시스템에 대해 무한 버스트 기능을 사용할 수 있게 해줍니다. 어댑터는 버스를 통해 완전한 패킷이 전송될 때까지 버스를 계속 사용합니다. 값은 0 또는 1입니다(기본값=0).
disable-64bit	어댑터의 64비트 기능을 끕니다. 참고: UltraSPARC® III 기반 플랫폼에서 이 매개 변수는 기본적으로 1로 설정될 수 있습니다. UltraSPARC II 기반 플랫폼에서 기본값은 0입니다. 값은 0 또는 1입니다(기본값=0,64비트 기능 활성화).

vca 드라이버 매개 변수 설정

vca 장비 드라이버를 다음 두 가지 방법으로 설정할 수 있습니다.

- ndd 유틸리티 사용
- vca.conf 파일 사용

ndd 유틸리티를 사용한 경우 매개 변수는 시스템을 재부팅할 때까지만 유효합니다. 이 방법은 매개 변수 설정을 테스트할 때 적합합니다.

매개 변수 설정이 시스템 재부팅 후에도 유효하도록 하려면 /kernel/drv/vca.conf 파일을 생성하고 시스템 내 어떤 장치에 대한 특정 매개 변수를 설정할 필요가 있을 때 매개 변수값을 이 파일에 추가합니다. 자세한 내용은 35페이지의 "vca.conf 파일을 사용한 드라이버 매개 변수 설정"을 참조하십시오.

ndd 유틸리티를 사용한 매개 변수 설정

ndd 유틸리티를 사용하여 시스템 재부팅하기 전까지만 유효한 매개 변수를 설정합니다.

다음 항목은 vca 드라이버와 ndd 유틸리티를 사용하여 각 vca 장치의 매개 변수를 수정(-set 옵션으로) 또는 표시(-set 옵션 없이)하는 방법을 설명합니다.

▼ ndd 유틸리티용 장치 인스턴스 지정

vca 장치에 대한 매개 변수를 얻거나 설정하기 위해 ndd 유틸리티를 사용하기 전에는 유틸리티에 해당하는 장치 인스턴스를 지정해야 합니다.

1. **특정 장치와 관련된 인스턴스 번호를 확인하려면** /etc/path_to_inst **파일을 확인합니다.** path_to_inst**(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.**

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

위의 예제에서 세 가지 Sun Crypto Accelerator 4000 이더넷 인스턴스는 설치한 어댑터에서 기인합니다. 인스턴스 번호는 0과 1입니다.

2. 인스턴스 번호를 사용하여 장치를 선택합니다.

```
# ndd -set /dev/vcaN
```

참고 – 본 설명서에 포함된 예제에서는 *N*은 장치의 인스턴스 번호를 의미합니다.

선택을 변경할 때까지 장치는 선택된 상태로 남아있습니다.

비대화형 및 대화형 모드

ndd 유틸리티를 두 가지 모드로 사용할 수 있습니다:

- 비대화형
- 대화형

비대화형 모드에서 특정 명령을 실행하기 위해 유틸리티를 가동합니다. 일단 명령이 실행되면 유틸리티를 빠져 나갑니다. 대화형 모드에서는 유틸리티를 사용하여 하나 이상의 매개 변수 값을 얻거나 설정할 수 있습니다. 자세한 내용은 ndd(1M) 온라인 매뉴얼 페이지를 참조하십시오.

비대화형 모드에서 ndd *유틸리티 사용*

이 항목에서는 매개 변수값을 변경하고 표시하는 방법을 설명합니다.

● **매개 변수값을 수정하려면** -set **옵션을 사용합니다.**

ndd 유틸리티를 -set 옵션으로 호출한 경우 유틸리티는 *value*를 전달하여 이를 /dev/vca 드라이버 인스턴스에 지정되고 해당 값을 매개 변수에 할당합니다.

```
# ndd -set /dev/vcaN parameter value
```

adv 매개 변수를 변경하면 다음과 유사한 메시지가 나타납니다.

```
- link up 1000 Mbps half duplex
```

- **매개 변수값을 표시하려면 매개 변수 이름을 명시하고 값을 생략합니다.**

  -set 옵션을 생략하면 이를 질의 작업으로 간주하여 유틸리티는 지정된 드라이버 인스턴스를 질의한 후 지정된 매개 변수와 관련된 값을 검색하고 출력합니다.

```
# ndd /dev/vcaN parameter
```

대화형 모드에서 ndd *유틸리티 사용*

- **대화형 모드에서 매개 변수값을 수정하려면 다음과 같이** ndd /dev/vca**를 지정합니다.**

  그러면 ndd 유틸리티가 매개 변수 이름 입력을 위한 프롬프트를 표시합니다.

```
# ndd /dev/vcaN
name to get/set? (Enter the parameter name or ? to view all
parameters)
```

  매개 변수 이름이 입력되면 ndd 유틸리티는 매개 변수값을 묻는 프롬프트를 표시합니다 (표 3-1에서 표 3-9까지 참조).

- vca **드라이버가 지원하는 모든 매개 변수를 나열하려면** ndd /dev/vca**를 입력합니다.**
  (매개 변수 설명은 표 3-1에서 표 3-9까지 참조)

```
# ndd /dev/vca
name to get/set ? ?
?                               (read only)
instance                        (read and write)
adv-autoneg-cap                 (read and write)
adv-1000fdx-cap                 (read and write)
adv-1000hdx-cap                 (read and write)
adv-100fdx-cap                  (read and write)
adv-100hdx-cap                  (read and write)
adv-10fdx-cap                   (read and write)
adv-10hdx-cap                   (read and write)
adv-asmpause-cap                (read and write)
adv-pause-cap                   (read and write)
pause-on-threshold              (read and write)
pause-off-threshold             (read and write)
link-master                     (read and write)
enable-ipg0                     (read and write)
ipg0                            (read and write)
ipg1                            (read and write)
ipg2                            (read and write)
rx-intr-pkts                    (read and write)
rx-intr-time                    (read and write)
red-p4k-to-6k                   (read and write)
red-p6k-to-8k                   (read and write)
red-p8k-to-10k                  (read and write)
red-p10k-to-12k                 (read and write)
tx-dma-weight                   (read and write)
rx-dma-weight                   (read and write)
infinite-burst                  (read and write)
disable-64bit                   (read and write)
name to get/set ?
#
```

자동 교섭 또는 강제 모드 설정

다음 링크 매개 변수를 자동 교섭 또는 강제 모드로 작동하도록 설정할 수 있습니다.

- speed
- duplex
- link-clock

기본적으로, 이 링크 매개 변수에는 자동 교섭 모드가 활성화됩니다. 매개 변수 중 어느 하나가 자동 교섭 모드에 있는 경우 vca 장치는 호환값과 흐름 제어 기능을 협상하기 위해 링크 파트너와 통신합니다. 이런 매개 변수 중 어느 하나라도 auto이외의 값으로 설정된 경우 교섭은 수행되지 않고 링크 매개 변수가 강제 모드로 구성됩니다. 강제 모드에서는 speed 매개 변수값은 링크 파트너 간 일치해야 합니다. 38페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조하십시오.

▼ 자동 교섭 모드 비활성화

네트워크 장비가 자동 교섭을 지원하지 않거나 네트워크 speed, duplex 및 link-clock 매개 변수를 강제로 설정하려면 vca 장치 상에서 자동 교섭 모드를 비활성화할 수 있습니다.

1. **링크 파트너 장비와 함께 제공된 설명서에서 수록된 값으로 다음 드라이버 매개 변수를 설정합니다(예, 스위치).**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   이런 매개 변수에 대한 설명과 설정 가능한 값은 표 3-2를 참조하십시오.

2. adv-autoneg-cap **매개 변수를** 0**으로 설정합니다.**

```
# ndd -set /dev/vcaN adv-autoneg-cap 0
```

ndd 연결 매개 변수를 변경하면 다음과 유사한 메시지가 나타납니다.

```
link up 1000 Mbps half duplex
```

참고 – 자동 교섭을 비활성화한 경우 speed, duplex 및 link-clock(1,00 Mbps에서만 가능) 매개 변수가 강제 모드에서 작동하도록 활성화해야 합니다. 해당 지침은 38페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조 하십시오.

---

vca.conf 파일을 사용한 매개 변수 설정

/kernel/drv 디렉토리의 vca.conf 파일에 항목을 추가하여 드라이버 매개 변수 속성을 지정할 수도 있습니다. 매개 변수 이름은 22페이지의 "드라이버 매개 변수 값 및 정의"에 나열된 이름과 같습니다.

주의 – /kernel/drv/vca.conf 파일의 그 어떠한 기본 항목을 삭제하지 마십시오.

prtconf(1) 및 driver.conf(4) 온라인 매뉴얼 페이지에는 이에 대한 추가 정보를 제공합니다. 다음 절차는 vca.conf 파일에서 매개 변수를 설정하는 예를 설명합니다.

이전 항목에서 정의된 변수는 시스템에서 이미 알려진 장치에 적용됩니다. vca.conf 파일로 Sun Crypto Accelerator 4000 보드에 대한 변수를 설정하려면 해당 장치에 대해 다음 세 가지 정보를 알고 있어야 합니다. 즉, 장치 이름, 장치 부모, 장치 단위 주소입니다.

▼ vca.conf 파일을 사용한 드라이버 매개 변수 설정

1. **장치 트리에서 해당** vca **장치에 대한 하드웨어 경로 이름을 획득합니다.**

   a. **특정 장치와 관련된 이름을 검색하려면** /etc/driver_aliases **파일을 확인합니다.**

```
# grep vca /etc/driver_aliases
vca "pci108e,3de8"
```

   위 예제에서 Sun Crypto Accelerator 4000 소프트웨어 드라이버(vca)와 관련된 장치 이름은 "pci108e,3de8"입니다.

   b. /etc/path_to_inst **파일에서 장치 부모 이름과 장치 단위 주소를 검색합니다.**

   path_to_inst(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

위 예제에서 장치 경로 이름, 인스턴스 번호, 소프트웨어 드라이브 이름이란 세 개의 열이 출력됩니다.

위 예제에서 첫 행의 장치 경로 이름은 "/pci@8,600000/network@1" 입니다. 장치 경로 이름은 장치 부모 이름, 장치 노드 이름, 장치 단위 주소란 세 부분으로 구성되어 있습니다. 표 3-10를 참조하십시오.

표 3-10 장치 경로 이름

전체 장치 경로 이름	부모 이름 부분	노드 이름 부분	단위 주소 부분
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

vca.conf 파일에서 PCI 장치를 명확하게 식별하려면 전체 장치 경로 이름을 사용합니다(부모 이름, 노드 이름, 단위 주소). PCI 장치 사양에 대한 자세한 내용은 pci(4) 온라인 매뉴얼 페이지를 참조하십시오.

2. /kernel/drv/vca.conf **파일에서 위 장치에 대한 매개 변수를 설정합니다.**

   다음 항목에서 특정 Sun Crypto Accelerator 4000 이더넷 장치에 대하여 adv-autoneg-cap 매개 변수가 비활성화됩니다.

```
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
```

3. vca.conf **파일을 저장합니다.**
4. **모든 파일과 프로그램을 저장하고 종료한 후 창 기능 시스템을 빠져 나갑니다.**
5. **시스템을 종료하고 재부팅합니다.**

vca.conf 파일로 모든 Sun Crypto Accelerator 4000 vca 장치의 매개 변수 설정

장치 경로 이름을 생략한 경우(부모 이름, 노드 이름, 단위 주소) 모든 Sun Crypto Accelerator 4000 이더넷 장치의 모든 인스턴스에 대한 변수가 설정됩니다.

▼ vca.conf 파일로 모든 Sun Crypto Accelerator 4000 vca 장치의 매개 변수 설정

1. **매개** *변수=값;***을 입력하여 모든 인스턴스에 대한 매개 변수 값을 변경할 수 있도록** vca.conf **파일에 행 하나를 추가합니다.**

   다음 예제에서는 모든 Sun Crypto Accelerator 4000 이더넷 장치의 모든 인스턴스에 대해 adv-autoneg-cap 매개 변수를 1로 설정합니다.

```
adv-autoneg-cap=1;
```

vca.conf 파일 예제

다음은 vca.conf 파일 예제입니다.

```
#
# Copyright 2002 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.2     02/06/26 SMI"

#
# Use the new Solaris 9 properties to ensure that the driver is attached
# on boot, to get us to register with KCL2.  This also prevents us from
# being unloaded by the cleanup modunload -i 0.
#
ddi-forceattach=1 ddi-no-autodetach=1;
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
adv-autoneg-cap=1;
```

OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화

OpenBoot PROM (OBP) 인터페이스에서 다음 매개 변수가 자동 교섭 또는 강제 모드에서 작동되도록 설정할 수 있습니다.

표 3-11 로컬 링크 네트워크 장치 매개 변수

매개 변수	설명
`speed`	이 매개 변수는 `auto`, `1000`, `100` 또는 `10`으로 설정할 수 있으며, 구문은 다음과 같습니다. • `speed=auto`(기본값) • `speed=1000` • `speed=100` • `speed=10`
`duplex`	이 매개 변수는 `auto`, `full` 또는 `half`으로 설정할 수 있으며, 구문은 다음과 같습니다. • `duplex=auto`(기본값) • `duplex=full` • `duplex=half`
`link-clock`	이 매개 변수는 `speed` 매개 변수가 `1000`으로 설정되어 있거나 1,000Mbps MMF Sun Crypto Accelerator 4000 보드를 사용하는 경우에만 적용할 수 있습니다. 이 매개 변수의 값은 링크 파트너의 값과 일치해야 합니다 — 예를 들어, 로컬 링크의 값이 `master`인 경우 링크 파트너는 `slave` 값을 가져야 합니다. 이 매개 변수는 `master`, `slave` 또는 `auto`로 설정할 수 있으며, 구문은 다음과 같습니다. • `link-clock=auto`(기본값) • `link-clock=master` • `link-clock=slave`

적절한 링크를 설정하려면 로컬 링크와 링크 파트너 간의 `speed`, `duplex` 및 `link-clock` (1,000Mbps에서만 가능) 매개 변수가 올바르게 구성되어야 합니다. 두 링크 파트너 모두가 `speed`, `duplex`, `link-clock` (1,000Mbps에서만 가능) 매개 변수 각각에 대해 자동 교섭 모드 또는 강제 모드로 작동 중이어야 합니다. 이 매개 변수 중 하나에 `auto` 값이 설정되면 해당 매개 변수의 링크가 자동 교섭 모드로 작동됩니다. OBP 프롬프트에서의 매개 변수 부재는 해당 매개 변수가 기본값으로 `auto`를 갖도록 구성합니다. `auto` 이외의 값은 해당 매개 변수에 대한 로컬 링크가 강제 모드에서 작동하도록 구성합니다.

로컬 링크가 100Mbps 미만의 속도로 speed 및 duplex 매개 변수에 대해 자동 교섭 모드에서 전이중 및 반이중 모두로 작동하게 되면 링크 파트너는 양쪽 이중 중 하나로 100Mps 또는 10Mbps 속도를 사용합니다.

speed 매개 변수가 강제 모드에서 작동하는 경우 이 값은 링크 파트너의 speed 값과 일치해야 합니다. 로컬 링크와 링크 파트너 간의 duplex 매개 변수가 일치하지 않은 경우 링크는 작동하지만 트래픽 충돌이 발생하게 됩니다.

로컬 링크 speed 매개 변수가 자동 교섭으로, 링크 파트너 speed 매개 변수가 강제로 설정되면 로컬 링크와 링크 파트너 간의 speed 값 교섭 가능 여부에 따라 링크가 활성화됩니다. 자동 교섭 모드의 인터페이스는 언제나 반이중으로 링크(일치하는 속도가 있는 경우) 활성화를 시도합니다. 두 인터페이스 중 하나가 자동 교섭 모드가 아니기 때문에 자동 교섭 모드의 인터페이스는 speed 매개 변수만을 감지합니다. 이중 매개 변수는 감지되지 않습니다. 이런 기법을 평행-감지라고 합니다.

주의 – 이중 충돌로 링크를 활성화하게 되면 항상 트래픽 충돌이 발생합니다.

로컬 링크 매개 변수가 강제 모드에서 작동하려면 매개 변수는 auto 이외의 값을 가져야 합니다. 예를 들어, 반이중으로 100Mbps 강제 모드 링크를 활성화하려면 OBP 프롬프트에서 다음을 입력합니다.

```
ok boot net:speed=100,duplex=half
```

참고 – 이 항목의 예제에서는 net은 기본적인 통합 네트워크 인터페이스 장치 경로의 별칭입니다. net 외의 장치 경로 이름을 지정하여 다른 네트워크 장치를 구성할 수 있습니다.

클럭 마스터인 반이중 1,000Mbps로 강제 모드를 활성화하려면 OBP 프롬프트에서 다음 명령을 입력합니다.

```
ok boot net:speed=1000,duplex=half,link-clock=master
```

참고 – link-clock 매개 변수의 값은 링크 파트너의 link-clock 값과 상응해야 합니다. 예를 들어, 로컬 링크의 link-clock 값이 master로 설정된 경우 링크 파트너의 link-clock 값을 slave로 설정되어 합니다.

10Mbps 속도의 이중 자동 교섭에 대한 강제 모드를 설정하려면 OBP 프롬프트에서 다음을 입력합니다.

```
ok boot net:speed=10,duplex=auto
```

또한 OBP 프롬프에서 다음을 입력하여 이전 예제와 동일한 로컬 링크 매개 변수를 설정할 수 있습니다.

```
ok boot net:speed=10
```

자세한 내용은 IEEE 802.3 설명사를 참조하십시오.

Sun Crypto Accelerator 4000 암호 및 이더넷 드라이버 운영 통계

이 항목은 kstat(1M) 명령이 제공하는 통계에 대해 설명합니다.

암호 드라이버 통계

표 3-12는 암호 드라이버 통계를 설명합니다.

표 3-12 암호 드라이버 통계

매개 변수	설명	안정 여부
vs-mode	값은 FIPS, standard 또는 unitialized입니다. FIPS는 보드가 FIPS 모드 있다는 것을 의미합니다. standard는 보드가 FIPS 모드에 있지 않다는 것을 의미합니다. unitialized는 보드가 초기화되지 않았다는 것을 의미합니다.	안정
vs-status	값은 ready, faulted 또는 failsafe입니다. ready는 보드가 정상적으로 작동하고 있다는 것을 의미합니다. faulted는 보드가 작동하지 않고 있다는 것을 의미합니다. failsafe는 보드의 출고 상태인 failsafe 모드를 의미합니다.	안정

이더넷 드라이버 통계

표 3-13은 이더넷 드라이버 통계를 설명합니다.

표 3-13 이더넷 드라이버 통계

매개 변수	설명	안정 여부
ipackets	내향 패킷 수	안정
ipackets64	ipackets의 64비트 버전	안정
ierrors	오류를 포함하고 있어 처리할 수 없는 총 수신 패킷(장기)	안정
opackets	인터페이스에 전송 요청된 총 패킷	안정
opackets64	인터페이스에 전송 요청된 총 패킷(64비트)	안정
oerrors	오류로 인해 성공적으로 전송할 수 없었던 총 패킷(장기)	안정
rbytes	인터페이스에서 성공적으로 수신한 총 바이트	안정
rbytes64	인터페이스에서 성공적으로 수신한 총 바이트(64비트)	안정
obytes	인터페이스에 전송 요청된 총 바이트	안정
obytes64	인터페이스에 전송 요청된 총 바이트(64비트)	안정
multircv	그룹 및 기능적 주소를 포함하여 성공적으로 수신된 멀티캐스트 패킷(장기)	안정
multixmt	그룹 및 기능적 주소를 포함하여 전송 요청된 멀티캐스트 패킷(장기)	안정
brdcstrcv	성공저긍로 수신된 동보 패킷(장기)	안정
brdcstxmt	전송 요청된 동보 패킷(장기)	안정
norcvbuf	수신용 패킷을 위한 버퍼가 할당되지 않아 유효한 수신 패킷이 폐기된 빈도수(장기)	안정
noxmtbuf	송신 버퍼가 작업 중이었거나 송신 버퍼가 할당되지 않아 출력 시 폐기된 패킷(장기)	안정

표 3-14는 송수신 MAC 카운터를 설명합니다.

표 3-14 TX 및 RX MAC 카운터

매개 변수	설명	안정 여부
tx-collisions	충돌을 일으킨 모든 프레임 전송 시도에 대한 16비트 로드 가능한 카운터 증분치	안정
tx-first-collisions	최초 시도에서 충돌이 있었지만 다음 시도에서 성공적으로 전송된 매 프레임에 대한 16비트 로드 가능한 카운터 증분치	불안정
tx-excessive-collisions	시도 수 제한값을 초과한 매 프레임 전송에 대한 16비트 로드 가능한 카운터 증분치	불안정
tx-late-collisions	충돌이 있었던 매 프레임 전송에 대한 16비트 로드 가능한 카운터 증분치. 적어도 최소 프레임 크기 바이트 수를 전송한 후 발생한 충돌로 인하여 TxMAC가 드롭한 프레임의 수를 표시합니다. 보통, 네트워크의 최대 허용 폭에 준수하지 않은 국이 네트워크 상에 적어도 하나가 있다는 것을 의미합니다.	불안정
tx-defer-timer	프레임 전송 시도 시 TxMAC가 네트워크의 트래픽으로 미루고 있는 16비트 로드 가능한 타이머 증분치. 타이머 기준 시간은 256으로 나눈 매체 바이트 시각입니다.	불안정
tx-peak-attempts	8비트 레지스터는 본 레지스터가 마지막으로 읽은 이후의 성공적으로 전송된 프레임 당 최대 연속 충돌 수를 표시합니다. 이 레지스터가 구할 수 있는 최대값은 255입니다. 성공적으로 전송된 프레임 당 연속 충돌 수가 255를 넘는 경우 소프트웨어에 마스크 가능한 인터럽트가 생성됩니다. 읽기가 완료되면 이 레지스터는 자동으로 0이 됩니다.	불안정
tx-underrun	네트워크에서 유효 프레임을 수신한 후의 16비트 로드 가능한 카운터 증분치	불안정
rx-length-err	네트워크에서 프로그램된 최대 프레임 크기 레지스터보다 긴 프레임을 수신한 후의 16비트 로드 가능한 카운터 증분치	불안정

표 3-14 TX 및 RX MAC 카운터 *(계속)*

매개 변수	설명	안정 여부
rx-alignment-err	수신 프레임에서 정렬 오류 감지 할 때 16비트 로드 가능한 카운터 증분치. 수신 프레임이 CRC (Cyclic Redundancy Checksum) 알고리즘에 실패하고 해당 프레임에 정수값이 아닌 바이트 수가 포함될 때(즉, 비트 단위의 프레임 크기가 0이 아닌 경우) 정렬 오류가 보고됩니다.	불안정
rx-crc-err	수신 프레임이 CRC 확인 알고리즘에 실패하고 해당 프레임에 정수값의 바이트 수가 포함되어 있을 때(즉, 8비트 모듈의 프레임 크기가 0인 경우) 16비트 로드 가능한 카운터 증분치	불안정
rx-code-violations	프레임을 수신하는 동안 MII 상에서 XCVR이 Rx_Err 지시를 생성할 때 16비트 로드 가능한 카운터 증분치. 이 지시는 송수신기가 수신한 데이터 스트림에서 부적절한 코드를 감지했을 때 생성됩니다. 수신 코드 위반은 FCS 또는 정렬 오류로 카운트되지 않습니다.	불안정
rx-overflows	자원 부족으로 드롭된 이더넷 프레임 수	불안정
rx-no-buf	수신 버퍼 공간이 부족하여 하드웨어가 데이터를 수신하지 못한 횟수	불안정
rx-no-comp-wb	하드웨어가 수신한 데이터에 대한 완료 항목 입력을 수행하지 못한 횟수	불안정
rx-len-mismatch	표시된 길이가 실제 프레임 길이와 맞지 않는 상태에서 수신된 프레임 수	불안정

다음 이더넷 속성(표 3-15)은 장치 특성과 링크 파트너 특성을 논리곱하여 도출된 것입니다.

표 3-15는 현재 이더넷 링크 속성을 설명합니다.

표 3-15 현재 이더넷 링크 속성

매개 변수	설명	안정 여부
ifspeed	1000, 100 또는 10Mbps	안정
link-duplex	0=반, 1=전	안정
link-pause	링크에 대한 현재 휴지 설정(25페이지의 "흐름 제어 매개 변수" 참조)	안정
link-asmpause	링크에 대한 현재 휴지 설정(25페이지의 "흐름 제어 매개 변수" 참조)	안정

표 3-15 현재 이더넷 링크 속성 *(계속)*

매개 변수	설명	안정 여부
link-up	1=활성, 0=비활성	안정
link-status	1=활성, 0=비활성	안정
xcvr-inuse	사용 중인 송수신기 종류: 1=내부 MII, 2=외부 MII, 3=외부 PCS	안정

표 3-16은 읽기 전용 매체 독립 인터페이스(MII)의 기능을 설명합니다. 이 매개 변수는 하드웨어의 기능을 정의합니다. 기가비트 매체 독립 인터페이스(GMII)는 다음 기능을 모두 지원합니다.

표 3-16 읽기 전용 vca 장치 기능

매개 변수	설명	안정 여부
cap-autoneg	0 = 자동 교섭 불가 1 = 자동 교섭 가능	안정
cap-1000fdx	로컬 인터페이스 전이중 가능 여부 0 = 1,000Mbps 전이중 불가 1 = 1,000Mbps 전이중 가능	안정
cap-1000hdx	로컬 인터페이스 반이중 가능 여부 0 = 1,000Mbps 반이중 불가 1 = 1,000Mbps 반이중 가능	안정
cap-100fdx	로컬 인터페이스 전이중 가능 여부 0 = 100Mbps 전이중 불가 1 = 100Mbps 전이중 가능	안정
cap-100hdx	로컬 인터페이스 반이중 가능 여부 0 = 100Mbps 반이중 불가 1 = 100Mbps 반이중 가능	안정
cap-10fdx	로컬 인터페이스 전이중 가능 여부 0 = 10Mbps 전이중 불가 1 = 10Mbps 전이중 가능	안정

표 3-16 읽기 전용 vca 장치 기능 *(계속)*

매개 변수	설명	안정 여부
cap-10hdx	로컬 인터페이스 반이중 가능 여부 0 = 10Mbps 반이중 불가 1 = 10Mbps 반이중 가능	안정
cap-asm-pause	로컬 인터페이스 흐름 제어 가능 여부 0 = 비대칭 휴지 불가 1 = 비대칭 휴지(로컬 장치로부터) 가능(25페이지의 "흐름 제어 매개 변수" 참조)	안정
cap-pause	로컬 인터페이스 흐름 제어 가능 여부 0 = 대칭 휴지 불가 1 = 대칭 휴지 가능(25페이지의 "흐름 제어 매개 변수" 참조)	안정

링크 파트너 기능 보고

표 3-17은 읽기 전용 링크 파트너의 기능을 설명합니다.

표 3-17 읽기 전용 링크 파트너 기능

매개 변수	설명	안정 여부
lp-cap-autoneg	0 = 자동 협상 불가 1 = 자동 협상	안정
lp-cap-1000fdx	0 = 1,000Mbps 전이중 전송 불가 1 = 1,000Mbps 전이중	안정
lp-cap-1000hdx	0 = 1,000Mbps 반이중 전송 불가 1 = 1,000Mbps 반이중	안정
lp-cap-100fdx	0 = 100Mbps 전이중 전송 불가 1 = 100Mbps 전이중	안정
lp-cap-100hdx	0 = 100Mbps 반이중 전송 불가 1 = 100Mbps 반이중 전송	안정
lp-cap-10fdx	0 = 10Mbps 전이중 전송 불가 1 = 10Mbps 전이중 전송	안정

표 3-17 읽기 전용 링크 파트너 기능 *(계속)*

매개 변수	설명	안정 여부
lp-cap-10hdx	0 = 10Mbps 반이중 전송 불가 1 = 10Mbps 반이중 전송	안정
lp-cap-asm-pause	0 = 비대칭 휴지 불가 1 = 링크 파트너 기능에 대한 비대칭 휴지 (25페이지의 "흐름 제어 매개 변수" 참조)	안정
lp-cap-pause	0 = 대칭 휴지 불가 1 = 대칭 휴지 가능(25페이지의 "흐름 제어 매개 변수" 참조)	안정

링크 파트너가 자동 교섭이 불가능한 경우(lp-cap-autoneg이 0일 때) 표 3-17에 설명된 나머지 내용은 이와 연관이 없어지며, 매개 변수 값은 0입니다.

링크 파트너가 자동 교섭이 가능한 경우(lp-cap-autoneg이 1일 때) 자동 교섭과 링크 파트너 기능을 사용하면 속도와 모드 정보가 표시됩니다.

표 3-18은 드라이버의 고유 매개 변수를 설명합니다.

표 3-18 드라이버 고유 매개 변수

매개 변수	설명	안정 여부
lb-mode	해당 경우, 장치가 속한 되돌림 모드 복사.	불안정
promisc	활성화된 경우, 장치는 자유 모드입니다. 비활성화된 경우, 장치는 자유 모드가 아닙니다.	불안정
이더넷 전송 카운터		
tx-wsrv	전송 링이 가득 찬 횟수 카운트.	불안정
tx-msgdup-fail	패킷 복제 시도 실패.	불안정
tx-allocb-fail	메모리 할당 시도 실패 .	불안정
tx-queue0	최초 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수.	불안정
tx-queue1	두 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수.	불안정
tx-queue2	세 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수.	불안정
tx-queue3	네 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수.	불안정

표 3-18 드라이버 고유 매개 변수 *(계속)*

매개 변수	설명	안정 여부
이더넷 수신 카운터		
rx-hdr-pkts	256바이트 이하로 수신된 패킷 수.	불안정
rx-mtu-pkts	256바이트 이상, 1,514바이트 이하로 수신된 패킷 수.	불안정
rx-split-pkts	두 페이지로 분할된 패킷 수 .	불안정
rx-nocanput	IP 스택으로의 전달 실패로 인해 드롭된 패킷 수.	불안정
rx-msgdup-fail	복제가 불가능했던 패킷 수.	불안정
rx-allocb-fail	불록 할당이 실패한 수.	불안정
rx-new-pages	수신 중 대체된 페이지 수.	불안정
rx-new-hdr-pages	수신 중 대체된 256바이트 이하의 패킷으로 채워진 페이지 수.	불안정
rx-new-mtu-pages	수신 중 대체된 256바이트 이상, 1,514 이하의 패킷으로 채워진 페이지 수.	불안정
rx-new-nxt-pages	수신 중 대체된 페이지 별로 분할된 패킷을 포함한 페이지 수.	불안정
rx-page-alloc-fail	페이지 할당이 실패한 수.	불안정
rx-mtu-drops	드라이버가 패킷을 대체하기 위해 신규 패킷을 맵하는 것이 불가능하여 256바이트보다 크고 1,514보다 작은 패킷의 전체 페이지가 드롭된 횟수.	불안정
rx-hdr-drops	드라이버가 패킷을 대체하기 위해 신규 패킷을 맵할 수가 없어 256바이트 이하인 페킷의 전체 페이지가 드롭된 횟수.	불안정
rx-nxt-drops	드라이버가 패킷을 대체하기 위해 신규 패킷을 맵할 수가 없어 분할 패킷이 담긴 페이지가 드롭된 횟수.	불안정
rx-rel-flow	드라이버가 흐름 해제를 요청받은 횟수.	불안정
이더넷 PCI 속성		
rev-id	Sun Crypto Accelerator 4000 이더넷 장치의 수정 ID는 해당 필드의 사용 장치 인식에 유용.	불안정
pci-err	모든 PCI 오류의 합.	불안정
pci-rta-err	수신된 대상 중단 수.	불안정
pci-rma-err	수신된 마스터 중단 수.	불안정

표 3-18 드라이버 고유 매개 변수 *(계속)*

매개 변수	설명	안정 여부
pci-parity-err	감지된 PCI 패리티 오류 수.	불안정
pci-drto-err	지연된 트랜잭션의 재시도 시간 초과 횟수.	불안정
dma-mode	Sun Crypto Accelerator 4000 드라이버에 의해 사용(vca).	불안정

▼ 링크 파트너 설정 확인

- **수퍼유저 권한으로** `kstat vca:`*N* **명령을 입력합니다.**

```
# kstat vca:N
module: vca                             instance: 0
name:   vca0                            class:    misc
```

참고 – 이전 예제에서 *N*은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 실행하는 보드의 인스턴스 번호를 반영해야 합니다.

네트워크 구성

이 항목은 시스템에 어댑터를 설치한 후 네트워크 호스트 파일을 편집하는 방법을 설명합니다.

네트워크 호스트 파일 구성

드라이버 소프트웨어를 설치한 후 어댑터의 이더넷 인터페이스를 위한 hostname.vca*N* 파일을 생성해야 합니다. 파일 이름 hostname.vca*N*에서 *N*은 사용할 vca 인터페이스의 인스턴스 번호에 해당합니다. 또한, /etc/hosts 파일에 해당 이더넷 인터페이스에 대해 IP 주소와 호스트 이름을 생성해야 합니다.

1. **/etc/path_to_inst 파일에서 적절한 vca 인터페이스와 인스턴스 번호를 검색합니다.**

   path_to_inst(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
```

   위 예제에서 인스턴스 번호는 0입니다.

2. **ifconfig(1M) 명령을 사용하여 어댑터의 vca 인터페이스를 설정합니다.**

   ifconfig 명령을 사용하여 네트워크 인터페이스에 IP 주소를 할당합니다. 명령행에서 다음을 입력하여 *ip_address*를 어댑터의 IP 주소로 대체합니다.

```
# ifconfig vcaN plumb ip_address up
```

참고 – 이 항목에 포함된 예제에서는 *N*은 장치의 인스턴스 번호를 말합니다.

   자세한 내용은 ifconfig(1M) 온라인 매뉴얼 페이지와 Solaris 설명서를 참조하십시오.

   - 재부팅 후에도 설정을 그대로 유지하려면 /etc/*hostname*.vca*N* 파일을 생성합니다. 여기서 *N*은 사용할 vca 인터페이스의 인스턴스 번호에 해당합니다.

     1단계에 있는 예제의 vca 인터페이스를 사용하려면 /etc/*hostname*.vca*N* 파일을 생성합니다. 여기서 *N*은 본 예제에서 0인 인스턴스 번호에 해당합니다. 인스턴스 번호가 1인 경우 파일 이름은 /etc/*hostname*.vca1가 됩니다.
   - 사용하지 않을 Sun Crypto Accelerator 4000 인터페이스를 위한 /etc/*hostname*.vca*N* 파일을 생성하지 마십시오.
   - /etc/*hostname*.vca*N* 파일은 적절한 vca 인터페이스에 대한 호스트 이름을 포함하고 있어야 합니다.
   - 호스트 이름은 IP 주소를 가지고 있어야 하며 /etc/hosts 파일에 나열되어 있어야 합니다.
   - 호스트 이름은 다른 어떤 인터페이스의 호스트 이름과 달라야 합니다. 예를 들어, /etc/*hostname*.vca0 및 /etc/*hostname*.vca는 동일한 호스트 이름을 공유할 수 없습니다.

   다음 예제는 Sun Crypto Accelerator 4000 보드를 가진 zardoz라는 시스템에 필요한 etc/*hostname*.vca*N* 파일을 보여줍니다(zardoz-11).

```
# cat /etc/hostname.hme0
zardoz
# cat /etc/hostname.vca0
zardoz-11
```

3. **각각의 활성화된** vca **인터페이스에 대해** /etc/hosts **파일에 적절한 항목을 생성합니다.**

예제:

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1     localhost
129.144.10.57 zardoz    loghost
129.144.11.83 zardoz-11
```

4 장

vcaadm 및 vcadiag 유틸리티를 통한 Sun Crypto Accelerator 4000 보드 관리

이 장에서는 vcaadm 및 vcadiag 유틸리티에 대한 개요를 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

vcaadm 사용

vcaadm 프로그램은 Sun Crypto Accelerator 4000 보드에 대한 명령행 인터페이스를 제공합니다. 보안 담당자로 지정된 사용자만이 vcaadm 유틸리티를 사용할 수 있습니다. vcaadm으로 처음 Sun Crypto Accelerator 4000 보드에 접속하게 되면 초기 보안 관리자와 암호를 만드는 화면이 나타납니다.

vcaadm 프로그램에 쉽게 액세스하려면 검색 경로 내에 다음 예제와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 넣습니다.

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

vcaadm 명령행 구문은 다음과 같습니다.

- vcaadm [-H]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-s *sec_officer*] *command*

참고 – -d 속성을 사용하는 경우, vca*N*은 보드의 장치 이름이며, 여기서 *N*은 Sun Crypto Accelerator 4000 장치 인스턴스 번호에 해당합니다.

표 4-1은 vcaadm 유틸리티의 옵션을 설명합니다.

표 4-1 vcaadm 옵션

옵션	의미
-H	vcaadm 명령어에 대한 도움말을 표시한 후 종료됩니다.
-d vca*N*	드라이버 인스턴스 번호가 *N*인 Sun Crypto Accelerator 4000 보드에 접속합니다. 예를 들어, -d vca1은 장치 vca1에 연결되며, 여기서 vca는 보드 장치 이름에 있는 문자열이고 1은 장치의 인스턴스 번호입니다. 이 값은 vca0으로 복귀되고 이는 반드시 vca*N* 형식여야 합니다. 여기서 *N*은 장치 인스턴스 번호에 해당합니다.
-f *filename*	*filename*에서 하나 이상의 명령을 해석한 후 종료됩니다.
-h *host*	*host*로 Sun Crypto Accelerator 4000 보드에 접속합니다. *host*의 값은 호스트 이름 또는 IP 주소가 될 수 있으며, 되돌림 주소로 복귀합니다.
-p *port*	*port*로 Sun Crypto Accelerator 4000 보드에 연결합니다. *port*의 값은 6870으로 복귀합니다.
-s *sec_officer*	이름이 *sec_officer*인 보안 관리자로 로그인합니다.
-y	확인이 필요한 모든 프롬프트에 대해 '예'라고 답합니다.

참고 – *sec_officer* 이름은 이 설명서 전체에서 보안 관리자 이름의 예제로 사용됩니다.

작동 모드

vcaadm은 다음 세 가지 모드에서 실행될 수 있습니다. 이런 모드는 vcaadm에 전달되는 명령의 방법에 따라 다릅니다. 세 가지 모드는 단일 명령 모드, 파일 모드 및 대화형 모드입니다.

참고 – vcaadm을 사용하려면 보안 관리자 인증을 받아야 합니다. 보안 관리자 인증을 받아야 하는 필요 횟수는 사용 중인 운영 모드에 따라 결정됩니다.

단일 명령 모드

단일 명령 모드에서는 모든 명령에 대해 보안 담당자 인증을 받아야 합니다. 명령이 실행되면 vcaadm에서 로그 아웃하게 됩니다.

단일 명령 모드에서 명령을 입력하는 경우 모든 명령행 스위치가 지정된 후 실행할 명령을 지정하게 됩니다. 예를 들어, 단일 명령 모드에서 다음 명령은 주어진 키스토어 내의 모든 사용자를 표시하고 사용자를 명령 쉘 프롬프트로 복귀합니다.

```
$ vcaadm show user
Security Officer Name: sec_officer
Security Officer Password:
```

다음 명령은 보안 관리자 *sec_officer*로 로그인을 수행하고 키스토어에 사용자 *web_admin*을 생성합니다.

```
$ vcaadm -s sec_officer create user web_admin
Security Officer Password:
Enter new user password:
Confirm password:
User web_admin created successfully.
```

참고 – 첫 번째 암호는 보안 관리자용이고 그 다음은 신규 사용자 *web_admin*의 암호 및 암호 확인입니다.

단일 명령 모드의 모든 출력은 표준 출력 스트림으로 흐릅니다. 표준 UNIX 쉘 기반 방법으로 이 출력을 재지정할 수 있습니다.

파일 모드

파일 모드에서는 실행되는 각 파일에 대해 보안 관리자 인증을 받아야 합니다. 명령 파일의 명령이 실행된 후 vcaadm에서 로그아웃합니다.

파일 모드에 명령을 입력하려면 vcaadm이 하나 이상의 명령을 읽어오는 파일을 지정합니다. 파일은 각 행마다 하나의 명령으로 구성된 ASCII 코드의 텍스트여야 합니다. 각 코멘트는 "#" 문자로 시작됩니다. 파일 모드 옵션이 설정된 경우 vcaadm은 최종 옵션 이후의 모든 명령행 인수를 무시합니다. 다음 예제는 deluser.scr 파일에 있는 명령을 실행하고 모든 프롬프트에 긍정적으로 응답합니다.

```
$ vcaadm -f deluser.scr -y
```

대화형 모드

대화형 모드에서는 보드에 접속할 때마다 보안 관리자 인증을 받아야 합니다. 이것은 vcaadm의 기본적인 운영 모드입니다. 대화형 모드의 vcaadm에서 로그아웃하려면 logout명령을 사용합니다. 54페이지의 "vcaadm을 통한 로그인 및 로그아웃"을 참조하십시오.

대화형 모드는 사용자에게 한 번에 하나의 명령을 입력할 수 있는 ftp(1)와 유사한 인터페이스를 제공합니다. 대화식 모드에서는 -y 옵션이 지원되지 않습니다.

vcaadm을 통한 로그인 및 로그아웃

명령행에서 vcaadm을 사용하여 각각 -h, -p, -d 속성으로 *호스트*, *포트*, *장치*를 지정하게 되면, 네트워크 접속이 올바르게 수행된 경우 즉시 보안 관리자로 로그인하는 프롬프트가 나타납니다.

vcaadm 프로그램은 특정 보드에 실행 중인 vcaadm 응용 프로그램과 Sun Crypto Accelerator 4000 펌웨어 간에 암호화된 네트워크 접속(채널)을 활성화합니다.

암호화된 채널을 설정하는 동안 보드는 하드웨어 이더넷 주소와 RSA 공용키를 통해 서로 식별합니다. vcaadm이 처음 보드에 연결되면 트러스트 데이터베이스 ($HOME/.vcaadm/trustdb)가 생성됩니다. 이 파일에는 현재 보안 관리자가 신뢰하는 모든 보드가 포함되어 있습니다.

vcaadm을 통한 보드 로그인

보안 관리자가 새 보드에 연결한 경우 vcaadm은 보안 관리자에게 이를 통보하고 다음 옵션을 표시합니다.

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Trust this board forever (adds the hardware ethernet address
   and RSA public key to the trust database).
```

보안 관리자가 변경된 원격 접근 키가 있는 보드에 연결한 경우 vcaadm은 보안 관리자에게 이를 통지하고 다음과 같이 세 가지 옵션을 표시합니다.

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Replace the old public key bound to this hardware ethernet
   address with the new public key.
```

새 보드에 로그인

참고 – 이 장의 나머지 예제들은 vcaadm의 대화형 모드로 생성되었습니다.

새 보드에 로그인하는 경우 vcaadm은 트러스트 데이터베이스에 새 항목을 생성해야 합니다. 다음은 새 보드에 로그인하는 예제입니다.

```
# vcaadm -h hostname
Warning: MAC ID and Public Key Not Found
-----------------------------------------------------
The MAC ID and public key presented by this board were
not found in your trust database.

MAC ID: 08:00:20:EE:EE:EE
Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Trust the board for all future sessions.

Your Choice -->
```

변경된 원격 액세스 키를 통한 보드 로그인

변경된 원격 액세스 키가 있는 보드에 접속하는 경우, vcaadm은 트러스트 데이터베이스의 보드에 해당하는 항목을 변경해야 합니다. 다음은 변경된 원격 액세스 키가 있는 보드에 로그인하는 예제입니다.

```
# vcaadm -h hostname
Warning: Public Key Conflict
-----------------------------------------------------
The public key presented by the board you are connecting
to is different than the public key that is trusted for
this MAC ID.

MAC ID: 08:00:20:EE:EE:EE
New Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
Trusted Key Fingerprint: A508-38D1-FED8-8103-7ACC-0D19-C9C9-11F2
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the current trusted key with the new key.

Your Choice -->
```

vcaadm 프롬프트

대화형 모드에서 vcaadm 프롬프트는 다음과 같이 나타납니다.

```
vcaadm{vcaN@hostname, sec_officer}> command
```

다음 표는 vcaadm 프롬프트 변수를 설명합니다.

표 4-2 vcaadm 프롬프트 변수 정의

프롬프트 변수	정의
vca*N*	vca는 Sun Crypto Accelerator 4000 보드를 표시하는 문자열입니다. *N*은 보드의 장치 경로 이름에 속한 장치 인스턴스 번호(단위 주소)입니다. 장치의 인스턴스 번호 회수에 대한 자세한 내용은 35페이지의 "vca.conf 파일을 사용한 드라이버 매개 변수 설정"을 참조하십시오.
hostname	Sun Crypto Accelerator 4000 보드가 물리적으로 연결된 호스트 이름입니다. *hostname*을 물리적 호스트의 IP 주소로 대체할 수 있습니다.
sec_officer	현재 보드에 로그인된 보안 관리자의 이름입니다.

vcaadm으로 보드에서 로그아웃

대화형 모드에서 작업하는 경우, vcaadm을 완전히 빠져나오지 않은 상태에서 한 보드의 연결을 끊고 다른 보드에 연결할 수 있습니다. 보드 연결을 종료하고 로그아웃하지만 대화형 모드를 지속하려면 logout 명령을 사용합니다.

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm>
```

위 예제에서 vcaadm> 프롬프트가 더 이상 장치 인스턴스 번호, 호스트 이름, 보안 관리자 이름을 표시하지 않는다는 것을 주의하십시오. 다른 장치에 로그인하려면 다음 매개 변수 옵션과 함께 connect 명령을 입력합니다.

표 4-3 connect 명령 매개 변수 옵션

매개 변수	의미
dev vca*N*	드라이버 인스턴스 번호가 *N*인 Sun Crypto Accelerator 4000 보드에 연결합니다. 예를 들어, -d vca1은 장치 vca1에 연결하며, 이는 장치 vca0으로 복귀합니다.
host *hostname*	*hostname*의 Sun Crypto Accelerator 4000 보드에 연결합니다(되돌림 주소로 복귀). *hostname*을 물리적 호스트의 IP 주소로 대체할 수 있습니다.
port *port*	*port* 포트의 Sun Crypto Accelerator 4000 보드에 연결합니다. (6870으로 복귀).

예제

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm> connect host hostname dev vca2
Security Officer Login: sec_officer
Security Officer Password:
vcaadm{vcaN@hostname, sec_officer}>
```

이미 Sun Crypto Accelerator 4000 보드에 연결된 경우 vcaadm으로 connect 명령을 실행할 수 없습니다. 먼저 로그아웃한 후 connect 명령을 실행해야 합니다.

새 연결이 활성화될 때마다 vcaadm과 대상 Sun Crypto Accelerator 4000 펌웨어는 전송된 관리 데이터를 보호하기 위해 새로운 세션 키 재교섭을 수행합니다.

vcaadm을 통한 명령 입력

vcaadm 프로그램에는 Sun Crypto Accelerator 4000 보드와 대화하는 데 사용해야 하는 명령 언어가 내포되어 있습니다. 명령은 단어의 전체 또는 일부(확실한 식별이 가능할 정도)를 사용하여 입력합니다. show 대신 sh를 사용하여 입력할 수 있으나, re만 입력할 경우에는 reset 또는 rekey에 모두 해당될 수 있으므로 의미가 모호합니다.

다음은 전체 단어를 사용하여 명령을 입력하는 예제입니다.

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                          Status
-----------------------------------------------------
web_admin                                    enabled
Tom                                           enabled
-----------------------------------------------------
```

sh, us와 같이 단어의 일부를 명령으로 사용해도 위 예제와 동일한 정보를 얻을 수 있습니다.

모호한 명령을 입력하면 다음과 같이 설명 메시지가 표시됩니다.

```
vcaadm{vcaN@hostname, sec_officer}> re
Ambiguous command: re
```

명령어에 대한 도움말 보기

vcaadm에는 도움말 기능이 내장되어 있습니다. 도움말을 보려면 도움말이 필요한 명령어 다음에 물음표(?) 문자를 입력합니다. 전체 명령어가 입력되고 해당 행에 "?"가 있는 경우, 아래 예제와 같이 명령어에 대한 구문이 표시됩니다.

```
vcaadm{vcaN@hostname, sec_officer}> create ?
Sub-Command                         Description
-----------------------------------------------------
so                                  Create a new security officer
user                                Create a new user

vcaadm{vcaN@hostname, sec_officer}> create user ?
Usage: create user [<username>]

vcaadm{vcaN@hostname, sec_officer}> set ?
Sub-Command                         Description
-----------------------------------------------------
passreq                             Set password requirements
password                            Change an existing security officer password
timeout                             Set the auto-logout time
```

vcaadm 프롬프트에서 물음표를 입력하여 다음 예제와 같이 모든 vcaadm 명령의 목록과 설명을 표시할 수 있습니다.

```
vcaadm{vcaN@hostname, sec_officer}> ?
Sub-Command                         Description
-----------------------------------------------------
backup                              Backup master key
connect                             Begin admin session with firmware
create                              Create users and accounts
delete                              Delete users and accounts
diagnostics                         Run diagnostic tests
disable                             Disable a user
enable                              Enable a user
exit                                Exit vcaadm
loadfw                              Load new firmware
logout                              Logout current session
quit                                Exit vcaadm
rekey                               Generate new system keys
reset                               Reset the hardware
set                                 Set operating parameters
show                                Show system settings
zeroize                             Delete all keys and reset board
```

vcaadm 대화형 모드가 아닌 경우 "?" 문자는 현재 작업 중인 쉘에 의해 해석될 수 있습니다. 이런 경우에는 물음표를 입력하기 전에 반드시 명령 쉘 이스케이프 문자를 입력해야 합니다.

대화형 모드에서 vcaadm 프로그램 종료

quit 및 exit란 두 명령을 통해 vcaadm을 종료할 수 있습니다. Ctrl-D 키를 눌러도 vcaadm이 종료됩니다.

vcaadm을 통한 Sun Crypto Accelerator 4000 보드 초기화

Sun Crypto Accelerator 4000 보드 구성의 첫 번째 단계는 이를 초기화하는 것입니다. 보드를 초기화할 때는 키스토어를 생성해야 합니다. 80페이지의 "개념 및 용어"를 참조하십시오. Sun Crypto Accelerator 4000 보드를 신규 키스토어로 초기화하거나 백업 파일을 활용하여 기존 키스토어로 초기화할 수 있습니다.

vcaadm으로 처음 Sun Crypto Accelerator 4000 보드에 연결하면 신규 키스토어로 보드를 초기화하거나 백업 파일에 저장된 기존 키스토어로 초기화하라는 메시지가 표시됩니다. vcaadm은 보드 초기화 형태와 상관없이 이에 필요한 모든 정보를 묻습니다.

▼ 새 키스토어로 Sun Crypto Accelerator 4000 보드 초기화

1. Sun Crypto Accelerator 4000 보드가 설치된 시스템의 명령 프롬프트에서 `vcaadm`을 입력하거나 원격 시스템인 경우 `vcaadm -h` *hostname*을 입력한 후 1을 선택하여 보드를 초기화합니다.

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 1
```

2. 초기 보안 관리자 이름과 암호를 생성합니다(65페이지의 "명명 요구 사항" 참조).

```
Initial Security Officer Name: sec_officer
Initial Security Officer Password:
Confirm Password:
```

3. 키스토어 이름을 생성합니다(65페이지의 "명명 요구 사항" 참조).

```
Keystore Name: keystore_name
```

4. FIPS 140-2 모드 또는 비 FIPS 모드를 선택합니다.

FIPS 모드에서는 Sun Crypto Accelerator 4000 보드가 FIPS 140-2, 레벨 3을 준수합니다. FIPS 140-2는 사용자 조작 방지 및 고도의 데이터 무결성과 보안을 요구하는 미국 정보 처리 표준입니다. 다음 웹 사이트에서 FIPS 140-2 관련 문서를 참조하십시오. `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`

```
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
```

참고 – 필수 매개 변수를 삭제하거나 변경하거나 예상치 못한 결과를 가져올 수도 있는 명령을 실행하기 전에 vcaadm은 사용자에게 Y, Yes, N 또는 No를 입력하여 확인하도록 합니다. 이런 값은 대/소문자를 구분하지 않으며, 기본값은 No입니다.

5. 구성 정보를 확인합니다.

```
Board initialization parameters:
-----------------------------------------------------
Initial Security Officer Name: sec_officer
Keystore name: keystore_name
Run in FIPS 140-2 Mode: Yes
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board...
```

기존 키스토어를 통한 Sun Crypto Accelerator 4000 보드 초기화

단일 키스토어에 여러 보드를 추가할 경우 모든 보드가 동일한 키스토어 정보를 사용하도록 초기화할 수 있습니다. 또한, Sun Crypto Accelerator 4000 보드를 원래 키스토어 구성으로 복원할 수도 있습니다. 이 항목은 백업 파일에 저장된 기존 키스토어로 보드를 초기화하는 방법을 설명합니다.

이 절차를 실행하기에 앞서 기존 보드 구성의 백업 파일을 먼저 생성해야 합니다. 백업 파일을 생성하고 복원하려면 백업 파일의 데이터를 암호화하고 해독할 암호가 필요합니다. 70페이지의 "마스터 키 백업"을 참조하십시오.

▼ 기존 키스토어 사용을 위한 Sun Crypto Accelerator 4000 보드 초기화

1. **Sun Crypto Accelerator 4000 보드가 설치된 시스템의 명령 프롬프트에서** `vcaadm`**을 입력하거나 원격 시스템인 경우** `vcaadm -h` *hostname*을 **입력한 후 2를 선택하여 백업에서 보드를 복원합니다.**

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 2
```

2. **백업 파일의 경로와 암호를 입력합니다.**

```
Enter the path to the backup file: /tmp/board-backup
Password for restore file:
```

3. **구성 정보를 확인합니다.**

```
Board restore parameters:
-----------------------------------------------------
Path to backup file: /tmp/board-backup
Keystore name: keystore_name
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Restoring data to crypto accelerator board...
```

vcaadm를 통한 키스토어 관리

키스토어는 키 요소에 대한 리포지터리입니다. 키스토어는 보안 관리자 및 사용자와 연관되어 있습니다. 키스토어는 스토리지를 제공할 뿐만 아니라 사용자 계정이 키 객체를 소유할 수 있는 수단을 제공합니다. 그러면 소유자로 인증되지 않은 응용 프로그램에서 키를 숨길 수 있습니다. 키스토어에는 세 가지 구성 요소가 있습니다.

- **키 객체 —** Sun ONE 웹 서버와 같은 응용 프로그램을 위해 저장된 장기 키
- **사용자 계정 —** 응용 프로그램이 특정 키를 인증하고 액세스하는 수단 제공
- **보안 관리자 계정 —** 이런 계정은 vcaadm을 통해 키 관리 기능에 액세스 제공

참고 – 단일 Sun Crypto Accelerator 4000 보드는 정확히 하나의 키스토어를 갖고 있어야 합니다. 추가 성능과 장애 허용 기능을 위해 여러 Sun Crypto Accelerator 4000 보드가 동일한 키스토어를 함께 사용하도록 구성할 수 있습니다.

명명 요구 사항

보안 관리자 이름,사용자 이름, 키스토어 이름은 다음 요구 사항을 만족해야 합니다.

표 4-4 보안 관리자 이름, 사용자 이름 및 키스토어 이름 요구 사항

이름 요구 사항	설명
최소 길이	최소 1자
최대 길이	사용자 이름 63자, 키스토어 이름 32자
유효 문자	영숫자, 밑줄(_), 대시(-), 마침표(.)
시작 문자	반드시 알파벳이어야 함

암호 요구 사항

암호 요구 사항은 현재 `set passreq` 설정(`low`, `med`, `high`)에 따라 다릅니다.

암호 요구 사항 설정

`set passreq` 명령을 사용하여 Sun Crypto Accelerator 4000 보드에 대한 암호 요구 사항을 설정합니다. 이 명령은 `vcaadm`이 표시하는 모든 암호 프롬프트의 암호 문자 요구 사항을 설정합니다. 암호 요구 사항 설정에는 세 가지가 있습니다.

표 4-5 암호 요구 사항 설정

암호 설정	요구 사항
`low`	암호 제한이 없습니다. 보드가 FIPS 모드에 있지 않은 경우의 기본값입니다.
`med`	최소 6개의 문자가 필요하며 한 문자는 알파벳이 아니어야 합니다. 이것은 보드가 FIPS 140-2 모드인 경우의 기본값으로, FIPS 140-2 모드에서 허용하는 최소 암호 요구 사항입니다.
`high`	최소 8개의 문자가 필요하며, 이 중 3개의 문자는 반드시 알파벳이고 하나의 문자는 알파벳이 아니어야 합니다. 이 값은 기본값이 아니므로 직접 구성해야 합니다.

암호 요구 사항을 변경하려면 `set passreq` 명령과 `low`, `med` 또는 `high`를 이어서 입력합니다. 다음 명령은 Sun Crypto Accelerator 4000 보드에 대한 암호 요구 사항을 `high`로 설정합니다.

```
vcaadm{vcaN@hostname, sec_officer}> set passreq high

vcaadm{vcaN@hostname, sec_officer}> set passreq
Password security level (low/med/high): high
```

키스토어에 보안 관리자 배치

하나의 키스토어에 대해 하나 이상의 보안 관리자가 있을 수 있습니다. 보안 관리자 이름은 Sun Crypto Accelerator 4000 보드 도메인 내에서만 알 수 있으며 호스트 시스템의 사용자 이름과 같을 필요는 없습니다.

보안 관리자를 생성할 때는 명령행에서 이름은 옵션 매개 변수입니다. 보안 관리자 이름이 생략된 경우, vcaadm은 이름 입력을 위한 프롬프트를 표시합니다(65페이지의 "명명 요구 사항" 참조).

```
vcaadm{vcaN@hostname, sec_officer}> create so Alice
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@hostname, sec_officer}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

키스토어에 사용자 배치

이 사용자 이름은 Sun Crypto Accelerator 4000 보드의 도메인 내에서만 알려져 있으며 웹 서버가 프로세스를 실제로 실행할 UNIX 사용자 이름과 같을 필요는 없습니다.

사용자를 생성할 때는 명령행에서 사용자 이름은 옵션 매개 변수입니다. 사용자 이름이 생략된 경우, vcaadm은 사용자 이름 입력을 위한 프롬프트를 표시합니다(65페이지의 "명명 요구 사항" 참조).

```
vcaadm{vcaN@hostname, sec_officer}> create user web_admin
Enter new user password:
Confirm password:
User web_admin created successfully.

vcaadm{vcaN@hostname, sec_officer}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

사용자는 웹 서버 시작 시 인증할 때는 이 암호를 사용해야 합니다.

주의 – 사용자는 이 암호를 기억하고 있어야 합니다. 암호가 없으면 해당 키에 액세스할 수 없습니다. 분실된 암호는 회수될 수 없습니다.

참고 – 5분 이상 명령 입력이 없으면 사용자 계정은 로그아웃됩니다. 이것은 변경이 가능한 옵션입니다. 자세한 내용은 72페이지의 "자동 로그아웃 시간 설정"을 참조하십시오.

사용자 및 보안 관리자 목록

키스토어와 연관된 사용자나 보안 관리자를 나열하려면 `show user` 또는 `show so` 명령을 입력합니다.

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                          Status
-----------------------------------------------------
web_admin                                     Enabled
Tom                                           Enabled
-----------------------------------------------------


vcaadm{vcaN@hostname, sec_officer}> show so
Security Officer
-----------------------------------------------------
sec_officer
Alice
Bob
-----------------------------------------------------
```

암호 변경

`vcaadm`으로는 보안 관리자 암호만 변경할 수 있으며 보안 관리자는 자신의 암호만 변경할 수 있습니다. `set password` 명령을 사용하여 보안 관리자 암호를 변경합니다.

```
vcaadm{vcaN@hostname, sec_officer}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

Sun ONE 웹 서버 `modutil` 유틸리티로 PKCS#11 인터페이스를 통해 암호를 변경할 수 있습니다. 자세한 내용은 Sun ONE 웹 서버 설명서에서 `modutil`을 참조하십시오.

사용자 활성화 또는 비활성화

참고 – 보안 관리자는 비활성화될 수 없습니다. 일단 보안 관리자가 생성되면 삭제될 때까지 활성화된 상태를 유지합니다.

모든 사용자는 기본적으로 활성화 상태로 생성됩니다. 사용자는 비활성화될 수 있습니다. 비활성화된 사용자는 PKCS#11 인터페이스로 키 요소에 액세스할 수 없습니다. 비활성화된 사용자를 활성화하면 해당 사용자의 모든 키 요소에 대한 액세스가 복원됩니다.

사용자를 활성화하거나 비활성화할 때는 명령행에서 사용자 이름은 옵션 매개 변수입니다. 사용자 이름이 생략된 경우, vcaadm은 사용자 이름 입력을 위한 프롬프트를 표시합니다. 사용자 계정을 비활성화하려면 `disable` 명령을 입력합니다.

```
vcaadm{vcaN@hostname, sec_officer}> disable user Tom
User Tom disabled.
vcaadm{vcaN@hostname, sec_officer}> disable user
User name: web_admin
User web_admin disabled.
```

계정을 활성화하려면 `enable user` 명령을 입력합니다.

```
vcaadm{vcaN@hostname, sec_officer}> enable user Tom
User Tom enabled.

vcaadm{vcaN@hostname, sec_officer}> enable user
User name: web_admin
User web_admin enabled.
```

사용자 삭제

delete user 명령을 실행하고 삭제할 사용자를 지정합니다. 사용자를 삭제할 때는 명령행에서 사용자 이름은 옵션 매개 변수입니다. 사용자 이름이 생략된 경우, vcaadm은 사용자 이름 입력을 위한 프롬프트를 표시합니다.

```
vcaadm{vcaN@hostname, sec_officer}> delete user web_admin
Delete user web_admin? (Y/Yes/N/No) [No]: y
User web_admin deleted successfully.

vcaadm{vcaN@hostname, sec_officer}> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

보안 관리자 삭제

delete so 명령을 실행하고 삭제할 보안 관리자를 지정합니다. 보안 관리자를 삭제할 때는 명령행에서 보안 관리자 이름은 옵션 매개 변수입니다. 보안 관리자 이름이 생략된 경우 vcaadm은 보안 관리자 이름 입력을 위한 프롬프트를 표시합니다.

```
vcaadm{vcaN@hostname, sec_officer}> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@hostname, sec_officer}> delete so
Security Officer name: Alice
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

마스터 키 백업

키스토어는 디스크에 저장되고 마스터 키에 암호화됩니다. 마스터 키는 Sun Crypto Accelerator 4000 펌웨어에 저장되어 보안 관리자는 이를 백업할 수 있습니다.

마스터 키를 백업하려면 backup 명령을 사용합니다. backup 명령에는 백업을 저장할 백업 파일의 경로 이름이 있어야 합니다. 이 경로 이름은 명령행에 넣을 수 있으며, 생략된 경우 vcaadm은 경로 이름 입력을 위한 프롬프트를 표시합니다.

백업 데이터에 대한 암호를 설정해야 합니다. 이 암호는 백업 파일에 있는 마스터 키를 암호화하기 위해 사용됩니다.

```
vcaadm{vcaN@hostname, sec_officer}> backup /opt/SUNWconn/vca/backups/bkup.data
Enter a password to protect the data:
Confirm password:
Backup to /opt/SUNWconn/vca/backups/bkup.data successful.
```

주의 – 이 암호는 키스토어를 위한 마스터 키를 보호하므로 백업 파일을 만들 때는 짐작하기 어려운 암호를 선택하는 것이 좋습니다. 입력한 암호도 반드시 기억해야 합니다. 암호가 없으면 마스터 키 백업 파일에 액세스할 수 없습니다. 분실된 암호로 보호된 데이터를 회수할 수 없습니다.

백업 방지를 위한 키스토어 잠금

보안 방침이 엄격한 사이트는 Sun Crypto Accelerator 4000 보드의 마스터 키가 하드웨어에서 추출되지 못하도록 할 수 있습니다. `set lock` 명령을 통해 이를 강화할 수 있습니다.

주의 – 이 명령을 실행한 후에는 모든 마스터 키 백업 시도가 실패하게 됩니다. 마스터 키를 다시 입력해도 잠금 상태가 지속됩니다. 이 설정을 지우는 유일한 방법은 `zeroize` 명령으로 Sun Crypto Accelerator 4000 보드를 원상 복구화하는 것입니다. 75페이지의 "Sun Crypto Accelerator 4000 보드 원상 복구"을 참조하십시오.

```
vcaadm{vcaN@hostname, sec_officer}> set lock
WARNING: Issuing this command will lock the
         master key.  You will be unable to back
         up your master key once this command
         is issued.  Once set, the only way to
         remove this lock is to zeroize the board.
Do you wish to lock the master key? (Y/Yes/N/No) [No]: y
The master key is now locked.
```

vcaadm을 통한 보드 관리

이 항목은 vcaadm 유틸리티로 Sun Crypto Accelerator 4000 보드를 관리하는 방법을 설명합니다.

자동 로그아웃 시간 설정

보안 관리자가 자동으로 보드에서 로그아웃되는 시간을 사용자 정의하려면 set timeout 명령을 사용합니다. 자동 로그아웃 시간을 변경하려면 set timeout 명령과 함께 보안 관리자가 자동으로 로그아웃되는 시간을 분 단위로 환산한 숫자를 입력합니다. 값이 0인 경우 자동 로그아웃 기능이 비활성되며, 최대 대기값은 1,440분(1일)입니다. 새롭게 초기화된 Sun Crypto Accelerator 4000 보드는 기본값인 5분으로 복귀합니다.

다음 명령은 보안 관리자의 자동 로그아웃 시간을 10분으로 변경합니다.

```
vcaadm{vcaN@hostname, sec_officer}> set timeout 10
```

보드 상태 표시

Sun Crypto Accelerator 4000 보드의 현재 상태를 알려면 show status 명령을 실행합니다. 이 명령은 보드의 하드웨어 및 펌웨어 버전, 네트워크 인터페이스의 MAC 주소 및 상태(활성/비활성, 속도, 이중 및 기타) 및 키스토어 이름과 ID를 표시합니다.

```
vcaadm{vcaN@hostname, sec_officer}> show status
Board Status
----------------------------------------------------------------
Hardware Version: 1.0
Firmware Version: 1.0
Bootstrap Firmware Version: VCA Crypto Accelerator 1.0  March 2003
Current Firmware Version: VCA Crypto Accelerator 1.0  March 2003
MAC Address: 00:03:ba:0e:96:aa
Interface information: Link up, 1000Mbps, Full Duplex
Keystore Name: keystore_name
Keystore ID: 832aece03e654790
Login Session Timeout (in minutes): 10
Password policy security level: HIGH
Number of master key backups: 0
* Device is in FIPS 140-2 Mode
----------------------------------------------------------------
```

FIPS 140-2 모드에서의 보드 작동 여부 판단

Sun Crypto Accelerator 4000 보드가 FIPS 140-2 모드에서 작동하고 있는 경우 `show status` 명령을 실행하면 다음 메시지가 표시될 것입니다.

```
* Device is in FIPS 140-2 Mode
```

보드가 FIPS 140-2 모드에서 작동하고 있지 않은 경우 `show status` 명령은 FIPS 140-2 모드를 명시하는 메시지를 표시하지 않을 것입니다.

또한, `kstat`(1M) 유틸리티를 사용하여 보드가 FIPS 140-2 모드에서 작동 중인지 판단할 수 있습니다. 보드가 FIPS 140-2 모드에서 작동 중인 경우 `kstat`(1M) 매개 변수인 `vs-mode`는 `FIPS` 값을 반환합니다. 40페이지의 "Sun Crypto Accelerator 4000 암호 및 이더넷 드라이버 운영 통계" 및 온라인 매뉴얼 페이지에서 `kstat`(1M)를 참조하십시오.

새 펌웨어 로드

새 기능이 추가되면 Sun Crypto Accelerator 4000 보드의 펌웨어를 업데이트하여 이를 반영할 수 있습니다. 펌웨어를 로드하려면 `loadfw` 명령을 실행하고 펌웨어 파일에 대한 경로를 입력합니다.

펌웨어를 올바르게 업데이트하려면 `reset` 명령으로 보드를 직접 재설정해야 합니다. 보드를 재설정하게 되면 현재 로그인한 보안 관리자는 로그아웃 됩니다.

```
vcaadm{vcaN@hostname, sec_officer}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: sec_officer
Security Officer Password:
WARNING: This command will load new firmware onto the
          the target device.  You must issue a reset
          command and log back into the target device in
          order to use the new firmware.

Proceed with firmware update? (Y/Yes/N/No) [No]: y
```

Sun Crypto Accelerator 4000 보드 재설정

특정 상황에서는 보드를 재설정해야 할 수도 있습니다. 이런 경우에는 reset 명령을 실행해야 합니다. 컴퓨터는 정말 이 명령을 실행할 것인지 묻게 될것입니다. Sun Crypto Accelerator 4000 보드를 재설정하게 되면, 해당 보드의 작업을 대신 수행할 다른 활성화된 Sun Crypto Accelerator 4000 보드가 없으면 시스템의 암호 가속화가 일시적으로 중단될 수 있습니다. 또한, 이 명령이 실행되면 vcaadm에서 자동으로 로그아웃되기 때문에 장치 관리를 계속 하려면 vcaadm에 다시 로그인하고 해당 장치에 다시 연결해야 합니다.

```
vcaadm{vcaN@hostname, sec_officer}> reset
WARNING: Issuing this command will reset the
         the board and close this connection.

Proceed with reset? (Y/Yes/N/No) [No]: y
Reset successful.
```

Sun Crypto Accelerator 4000 보드 키 재생성

보안 방침상 일정 기간이 경과하면 마스터 키 또는 원격 액세스 키에 대해 새 키를 사용해야 하기 때문에 이 기능이 필요할 수 있습니다. rekey 명령을 통해 이러한 키 중 하나 또는 두 개 모두를 재생성할 수 있습니다.

마스터 키를 재생성하면 키스토어가 새 키로 재암호화되어 새 키스토어 파일로 이전의 백업 마스터 키 파일을 무효화시킵니다. 재생성 시마다 마스터 키를 백업해 두는 것이 좋습니다. 여러 Sun Crypto Accelerator 4000 보드가 동일한 키스토어를 사용하고 있는 경우 새 마스터 키를 백업하고 이를 다른 보드에 복원해야 합니다.

원격 액세스 키를 재생성하면 보안 관리자는 로그아웃되고 새 원격 엑세스 키로 다시 연결해야 합니다.

rekey 명령을 실행할 때 세 가지 키 종류 중 하나를 지정할 수 있습니다.

표 4-6 키 유형

키 유형	작업
master	마스터 키를 재생성합니다.
remote	원격 액세스 키를 재생성합니다. 보안 관리자는 로그아웃됩니다.
all	마스터 키와 원격 액세스 키 모두를 재생성합니다.

다음 예제는 rekey 명령에 all 키 유형이 입력됩니다.

```
vcaadm{vcaN@hostname, sec_officer}> rekey

Key type (master/remote/all): all
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file. If other boards use this
         keystore, they will need to have this new key backed up and
         restored to those boards. Rekeying the remote access key will
         terminate this session and force you to log in again.

Rekey board? (Y/Yes/N/No) [No]: y
Rekey of master key successful.
Rekey of remote access key successful.  Logging out.
```

Sun Crypto Accelerator 4000 보드 원상 복구

때로는 보드의 모든 키 요소를 삭제해야 하는 상황도 발생할 수 있습니다. 다음 두 방법을 통해 이를 수행할 수 있습니다. 첫 번째 방법은 하드웨어 점퍼를 사용합니다. 이런 원상 복구 방법은 Sun Crypto Accelerator 4000 보드를 원래 출고 상태로 복구하게 됩니다 (failsafe 모드). 155페이지의 "Sun Crypto Accelerator 4000 하드웨어를 출고 상태로 초기화"를 참조하십시오. 두 번째 방법은 zeroize 명령을 사용합니다.

참고 – zeroize 명령은 키 요소만을 삭제하고 업데이트된 펌웨어를 보존합니다. 이 명령은 또한 작업이 성공적으로 완료되면 보안 관리자를 로그아웃합니다.

---

zeroize 명령으로 보드를 원상 복구하려면 다음을 입력합니다.

```
vcaadm{vcaN@hostname, sec_officer}> zeroize
WARNING: Issuing this command will zeroize all keys
         on the board.  Once zeroized, these keys
         cannot be recovered unless you have
         previously backed up your master key.

Proceed with zeroize? (Y/Yes/N/No) [No]: y
All keys zeroized successfully.
```

vcaadm diagnostics 명령 사용

SunVTS 외에도 vcaadm 유틸리티에서 진단을 실행할 수 있습니다. vcaadm에 있는 diagnostics 명령은 Sun Crypto Accelerator 4000 하드웨어의 세 가지 주요 항목인 일반 하드웨어, 암호화 하위 시스템 및 네트워크 하위 시스템을 진단합니다. 일반 하드웨어 테스트는 DRAM, 플래시 메모리, PCI 버스, DMA 컨트롤러 및 기타 내장 하드웨어를 테스트합니다. 암호화 하위 시스템 테스트는 난수 발생기와 암호화 가속기를 테스트합니다. 네트워크 하위 시스템 테스트는 vca 장치를 테스트합니다.

```
vcaadm{vcaN@hostname, sec_officer}> diagnostics
Performing diagnostic tests...Done.
Diagnostic Results
------------------------------------------------------
General Hardware:                PASS
Cryptographic Subsystem:         PASS
Network Subsystem:               PASS
------------------------------------------------------
```

vcadiag 사용

vcadiag 프로그램은 루트 사용자가 보안 관리자 인증을 받지 않고 관리 업무를 수행할 수 있도록 Sun Crypto Accelerator 4000 보드와의 명령행 인터페이스를 제공합니다. 명령행 옵션은 vcadiag가 수행하는 작업을 결정합니다.

vcadiag 프로그램에 쉽게 액세스하려면 다음 예제와 같이 검색 경로 내에 Sun Crypto Accelerator 4000 도구 디렉토리를 넣습니다.

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

vcadiag 명령행 구문은 다음과 같습니다.

- vcadiag [-D] vca*N*
- vcadiag [-F] vca*N*
- vcadiag [-K] vca*N*
- vcadiag [-Q]
- vcadiag [-R] vca*N*
- vcadiag [-Z] vca*N*

참고 – [-DFKRZ] 속성을 사용할 때는 vca*N*은 보드의 장치 이름이며, 여기서 *N*은 Sun Crypto Accelerator 4000 장치 인스턴스 번호에 해당합니다.

표 4-7은 vcadiag 유틸리티의 옵션을 설명합니다.

표 4-7 vcadiag 옵션

옵션	의미
-D vca*N*	Sun Crypto Accelerator 4000 보드에 진단을 수행합니다.
-F vca*N*	관리 세션을 보호하기 위해 Sun Crypto Accelerator 4000 보드가 사용하는 공용 키 지문을 표시합니다.
-K vca*N*	관리 세션을 보호하기 위해 Sun Crypto Accelerator 4000 보드가 사용하는 공용 키 및 공용 키 지문을 표시합니다.
-Q	Sun Crypto Accelerator 4000 장치 및 소프트웨어 구성 요소에 대한 정보를 제공합니다. 콜론으로 구분한 목록 형식으로 다음 정보를 출력합니다: 장치, 내부 기능, 키스토어 이름, 키스토어 일련 번호, 키스토어 참조 카운트이 명령을 사용하여 장치와 키스토어 간의 관계를 확인할 수 있습니다.
-R vca*N*	Sun Crypto Accelerator 4000 보드를 재설정합니다.
-Z vca*N*	Sun Crypto Accelerator 4000 보드를 원상 복구합니다.

다음은 -D 옵션의 예제입니다.

```
# vcadiag -D vca0
Running vca0 on-board diagnostics.
Diagnostics on vca0 PASSED.
```

다음은 -F 옵션의 예제입니다.

```
# vcadiag -F vca0
5f26-b516-83b4-d254-a75f-c70d-0544-4de6
```

다음은 -K 옵션의 예제입니다.

```
# vcadiag -K vca0
Device: vca0
Key Length: 1024 bits
Key Fingerprint: 5f26-b516-83b4-d254-a75f-c70d-0544-4de6
Modulus:
        b7215a99 8bb0dfe9 389363a0 44dac2b0 7c884161
        20ee8c8b d751437d 4e6a5cdb 76fdcb2a ad353c0b
        248edc1d 3c76591d dbca5997 f6ee8022 e8bb5a6d
        465a4f8c 601d46be 573e8681 506e5d8d f240a0db
        11d5c095 2d237061 df27b2de c353900f f531092b
        7d9a755b c5d79782 95a1180b e17303bb aca939ef
        006c73f7 74469031
Public Exponent:
        00010001
```

다음은 -Q 옵션의 예제입니다.

```
# vcadiag -Q
vca0:cb
vca0:cb:keystore_name:83097c2b3e35ef5b:1
vca0:ca
vca0:ca:keystore_name:83097c2b3e35ef5b:1
kcl2pseudo
vca0:om
vca0:om:keystore_name:83097c2b3e35ef5b:1
libkcl
```

다음은 -R 옵션의 예제입니다.

```
# vcadiag -R vca0
Resetting device vca0, this may take a minute.
Please be patient.
Device vca0 reset ok.
```

다음은 -Z 옵션의 예제입니다.

```
# vcadiag -Z vca0
Zeroizing device vca0, this may take a few minutes.
Please be patient.
Device vca0 zeroized.
```

5 장

Sun Crypto Accelerator 4000 보드와 함께 사용할 Sun ONE 서버 소프트웨어 구성

이 장에서는 Sun One 웹 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드의 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

참고 – 본 설명서에서 설명하는 Sun ONE 웹 서버의 이전 이름은 iPlanet™ 웹 서버였습니다.

Sun ONE 웹 서버를 위한 보안 관리

이 단원에서는 Sun One 웹 서버로 관리할 경우 Sun Crypto Accelerator 4000 보드의 보안 기능에 대한 개요를 설명합니다.

참고 – 키스토어를 관리하려면 해당 시스템의 관리자 계정에 액세스할 수가 있어야합니다.

개념 및 용어

Sun One 웹 서버와 같은 PKCS#11 인터페이스를 통해 Sun Crypto Accelerator 4000 보드와 통신하는 응용 프로그램을 위한 키스토어와 사용자를 생성해야 합니다.

사용자는 Sun Crypto Accelerator 4000의 정의에 따라 암호화를 위한 키 자료를 소유합니다. 키는 한 사용자만이 소유할 수 있습니다. 각 사용자는 다수의 키를 소유할 수 있습니다. 사용자는 `production` 키와 `development` 키와 같은 서로 다른 구성을 지원하기 위해 다양한 키를 소유할 수 있습니다(사용자가 지원하는 조직을 반영하기 위해).

참고 – *사용자* 또는 *사용자 계정*이라는 용어는 `vcaadm`에서 생성된 Sun Crypto Accelerator 4000 사용자를 말하며,일반 UNIX 사용자 계정을 의미하지 않습니다. UNIX 사용자 이름과 Sun Crypto Accelerator 4000 사용자 이름은 간의 상호 연관이 없습니다.

키스토어는 키 요소에 대한 리포지터리입니다. 키스토어는 보안 관리자 및 사용자와 연관되어 있습니다. 키스토어는 스토리지를 제공할 뿐만 아니라 사용자 계정이 키 객체를 소유할 수 있는 수단을 제공합니다. 이로 인해 소유자로 인증되지 않은 응용 프로그램에서 키를 숨길 수 있습니다. 키스토어에는 세 가지 구성 요소가 있습니다.

- **키 객체 —** Sun ONE 웹 서버와 같은 응용 프로그램을 위해 저장된 장기 키
- **사용자 계정 —** 응용 프로그램이 특정 키를 인증하고 액세스하는 수단 제공
- **보안 관리자 계정 —** 이런 계정은 `vcaadm`을 통해 키 관리 기능에 액세스 제공

참고 – 단일 Sun Crypto Accelerator 4000 보드는 정확히 하나의 키스토어를 갖고 있어야 합니다. 추가 성능과 장애 허용 기능을 위해 여러 Sun Crypto Accelerator 4000 보드가 동일한 키스토어를 함께 사용하도록 구성할 수 있습니다.

일반적인 설치는 단일 사용자를 가진 단일 키스토어를 포함하고 있습니다. 예를 들어, 이와 같은 구성은 *web_server*라는 키스토어와 해당 키스토어 내에 *web_admin*이라는 단일 사용자로 구성될 수 있습니다. 이러한 구성으로 사용자 *web_admin*은 단일 키스토어 내에서 서버 키의 액세스 제어를 소유하고 관리할 수 있습니다.

관리 도구인 `vcaadm`은 Sun Crypto Accelerator 4000 키스토어와 사용자를 관리하기 위해 사용됩니다. 65페이지의 "`vcaadm`를 통한 키스토어 관리"를 참조하십시오.

토큰 및 토큰 파일

Sun ONE 웹 서버에서는 *키스토어*가 토큰으로 나타납니다. 토큰 파일은 Sun Crypto Accelerator 4000 관리자가 해당 응용 프로그램에 특정 토큰을 선택적으로 제공하는 기술입니다.

예제

engineering, *finance*, *legal*로 구성된 세 개의 키스토어가 있습니다. Sun ONE 웹 서버에 다음 토큰이 제시됩니다.

- `engineering`
- `finance`
- `legal`

토큰 파일

기본 설정을 덮어쓰려면 토큰 파일이 있어야 합니다. 일부 응용 프로그램은 여러 토큰을 취급할 수 없습니다. 토큰 파일은 행 당 하나 이상의 토큰 이름을 포함한 텍스트 파일입니다.

참고 – 토큰 이름과 키스토어 이름은 같습니다.

Sun ONE 웹 서버는 토큰 파일에 나열된 토큰만 제공합니다. 토큰 파일을 지정하는 방법은 다음과 같습니다(순서대로).

1. 환경 변수 `SUNW_PKCS11_TOKEN_FILE`이 명명한 파일

   일부 응용 프로그램 소프트웨어는 환경 변수를 억제합니다. 이런 경우에는 이 방법을 사용할 수 없습니다.

2. `$HOME/.SUNWconn_cryptov2/tokens` 파일

   이 파일은 Sun ONE 웹 서버를 해당 사용자로 실행하고 있는 UNIX 사용자의 홈 디렉토리에 있어야 합니다. Sun ONE 웹 서버가 홈 디렉토리가 없는 UNIX 사용자로 실행되는 경우에는 이 방법을 사용할 수 없습니다.

3. `/etc/opt/SUNWconn/cryptov2/tokens` 파일

토큰 파일이 없는 경우 Sun Crypto Accelerator 4000 소프트웨어는 Sun ONE 웹 서버에 모든 토큰을 제공합니다.

다음은 토큰 파일 내용에 대한 예제입니다.

```
================================
# This is an example token file

engineering # Comments are acceptable on the same line

legal

# Because the finance keystore is not listed, the Sun Crypto
# Accelerator will not present it to the Sun ONE Web Server.

...
================================
```

참고 – 주석은 샵(#) 표시로 시작되며 빈 행도 가능합니다.

상기 파일이 없는 경우 80페이지의 "토큰 및 토큰 파일"에 설명된 기본 방법이 사용됩니다.

대용량 암호 활성화 및 비활성화

SunONE 소프트웨어의 대용량 암호화 기능은 기본적으로 비활성화되어 있습니다. 대용량 파일을 안전하게 전송하기 위해 이 기능을 활성화할 수도 있습니다.

Sun Crypto Accelerator 4000 보드에서 Sun ONE 서버 소프트웨어가 대용량 암호화 기능을 사용할 수 있도록 하려면 `/etc/opt/SUNWconn/cryptov2/` 디렉토리에 `sslreg`이란 이름의 빈 파일을 생성한 후 서버 소프트웨어를 재시작합니다.

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

대용량 암호 기능을 비활성화하려면 `sslreg` 파일을 삭제한 후 서버 소프트웨어를 다시 시작해야 합니다.

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

Sun ONE 웹 서버 구성

이 항목은 다음을 설명합니다.

암호

Sun ONE 웹 서버를 작동하는 과정에서 여러 암호 입력에 대한 요청을 받게 됩니다. 표 5-1은 각 암호에 대해 설명합니다. 이러한 암호는 장 전체에서 언급됩니다. 사용할 암호를 모르는 경우에는 표 5-1을 참조하십시오.

표 5-1 Sun ONE 웹 서버에 필요한 암호

암호 유형	설명
Sun ONE 웹 서버 관리 서버	Sun ONE 웹 서버 관리 서버를 시작하는 데 필요합니다. 이 암호는 Sun ONE 웹 서버를 설정하는 동안 할당됩니다.
웹 서버 트러스트 데이터베이스	보안 모드에서 실행할 경우 내부 암호화 모듈 시작에 필요합니다. 이 암호는 Sun ONE 웹 서버 관리 서버를 통해 트러스트 데이터베이스를 작성할 때 할당됩니다. 또한 인증서를 요청하고 이를 내부 암호화 모듈에 설치할 경우에도 필요합니다.
보안 관리자	`vcaadm` 권한을 부여받은 작업 수행 시 필요합니다.
사용자 이름:암호	안전 모드에서 실행할 경우 Sun Crypto Accelerator 4000 모듈 시작에 필요합니다. 암호는 또한 인증서를 요청하고 이를 내부 암호화 모듈에 설치할 경우에도 필요합니다(*keystore_name*). 암호는 `vcaadm`에서 생성된 키스토어 사용자의 *사용자 이름*과 *암호*로 구성됩니다. 키스토어 *사용자 이름*과 *암호*는 콜론(:)으로 구분합니다.

키스토어 배치

Sun ONE 웹 서버와 함께 사용하기 위해 보드를 활성화하기 전에 먼저 보드를 초기화하고 보드의 키스토어에 적어도 한 사용자를 배치해야 합니다. 보드의 키스토어는 초기화 과정 중 생성됩니다. 기존 키스토어를 사용하도록 Sun Crypto Accelerator 4000 보드를 초기화할 수도 있습니다. 61페이지의 "vcaadm을 통한 Sun Crypto Accelerator 4000 보드 초기화"를 참조하십시오.

참고 – Sun Crypto Accelerator 4000 보드 당 하나의 키스토어만 구성할 수 있으며 보드 당 하나의 키스토어를 구성해야 합니다. 추가 성능과 장애 허용 능력 향상을 위해 여러 Sun Crypto Accelerator 4000 보드가 같은 키스토어를 함께 사용하도록 구성할 수 있습니다.

▼ 키스토어 배치

1. **이미 그렇게 하지 않은 경우, 다음 예와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 검색 경로에 위치시킵니다.**

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

2. **vcaadm 명령으로 vcaadm 유틸리티에 액세스하거나 vcaadm -h *hostname*을 입력하여 vcaadm을 원격 호스트에 있는 보드에 연결합니다.**

   51페이지의 "vcaadm 사용"을 참조하십시오.

```
$ vcaadm -h hostname
```

3. **보드 키스토어에 사용자를 배치합니다.**

   이런 사용자 이름은 Sun Crypto Accelerator 4000 보드의 도메인 내에서만 알려져 있으며 웹 서버 프로세스가 실제로 사용하는 UNIX 사용자 이름과 동일할 필요는 없습니다. 사용자를 생성하기 전에 반드시 vcaadm 보안 관리자로 로그인해야 합니다.

4. `create user` **명령으로 사용자를 생성합니다.**

```
vcaadm{vcaN@hostname, sec_officer}> create user username
Initial password:
Confirm password:
User username created successfully.
```

여기서 생성된 *사용자 이름*과 *암호*는 *사용자 이름:암호*를 구성합니다(표 5-1 참조). 웹 서버 시작 시 인증할 때는 이 암호를 사용해야 합니다. 단일 사용자의 키스토어 암호입니다.

주의 – 사용자는 반드시 이 *사용자 이름:암호*를 기억해야 합니다. 이 암호가 없으면 사용자는 해당 키에 액세스할 수 없습니다. 분실된 암호는 회수될 수 없습니다.

5. `vcaadm`**을 빠져나옵니다.**

```
vcaadm{vcaN@hostname, sec_officer}> exit
```

Sun ONE 웹 서버 활성화 개요

Sun ONE 웹 서버를 활성화하려면 다음 절차를 완료해야 합니다. 이에 대한 자세한 내용은 다음 항목에 설명됩니다.

- Sun ONE 웹 서버 설치
- 트러스트 데이터베이스 생성
- 인증서 요청
- 인증서 설치
- Sun ONE 웹 서버 구성

주의 – 상기 절차는 반드시 순서대로 수행해야 합니다. 그렇게 하지 않으면 구성이 잘못될 수 있습니다.

- Sun ONE 웹 서버 4.1을 사용하는 경우 86페이지의 "Sun ONE 웹 서버 4.1 설치 및 구성"을 참조하십시오.
- Sun ONE 웹 서버 6.0을 사용하는 경우 95페이지의 "Sun ONE 웹 서버 6.0 설치 및 구성"을 참조하십시오.

Sun ONE 웹 서버 4.1 설치 및 구성

이 항목은 Sun ONE 웹 서버 4.1 설치 및 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

Sun ONE 웹 서버 4.1 설치

절차는 반드시 순서대로 수행해야 합니다. Sun ONE 웹 서버 사용법에 대한 자세한 내용은 Sun ONE 웹 서버 설명서를 참조하십시오.

▼ Sun ONE 웹 서버 4.1 설치

1. **Sun ONE 웹 서버 4.1 소프트웨어를 다운로드합니다.**

   웹 서버 소프트웨어는 다음 URL에 있습니다. `http://www.sun.com/`

2. **웹 서버를 설치합니다.**

   이 항목에 포함된 지침은 하나의 예제에 대한 것이므로, 원할 경우 Sun ONE 웹 서버를 다르게 구성할 수도 있습니다. 이 서버의 기본 작업 경로 이름은 다음과 같습니다. `/usr/netscape/server4`

   Sun ONE 웹 서버가 설치되는 동안 기본 경로를 승인합니다. 이 설명서는 기본 경로를 참조합니다. 웹 서버 소프트웨어를 다른 위치에 설치하려면 설치한 위치를 기록해 두는 것이 좋습니다.

3. 설치 **프로그램을 실행합니다.**

4. **설치 스크립트의 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 편리상 기본값을 승인할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 조건에 동의합니다.**

   b. **정식** ***hostname.domain*****을 입력합니다.**

   c. **Sun ONE 웹 서버 4.1 관리 서버 암호를 두 번 입력합니다.**

   d. **프롬프트가 나오면 [Return]을 누릅니다.**

▼ 트러스트 데이터베이스 생성

1. **Sun ONE 웹 서버 4.1 관리 서버를 시작합니다.**

   setup 요청에 따라 startconsole을 실행하지 않고 다음 명령을 사용하여 Sun ONE 웹 서버 4.1 관리 서버를 시작합니다.

   ```
   # /usr/netscape/server4/https-admserv/start
   SunONE-WebServer-Enterprise/4.1SP9 BB1-08/23/2001 05:50
   startup: listening to http://hostname.domain, port 8888 as root
   ```

   서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 GUI (Graphical User Interface)를 시작합니다.**

   ```
   http://hostname.domain:admin_port
   ```

   인증 대화 상자에서 setup 실행 중 선택한 Sun ONE 웹 서버 4.1 관리 서버의 사용자 이름과 암호를 입력합니다.

   참고 – Sun ONE 웹 서버 설치 시 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE 웹 서버 4.1 관리 서버 사용자 이름에 admin을 입력합니다.

3. **[OK(확인)]를 선택합니다.**

   Sun ONE 웹 서버 4.1 관리 서버의 서버 창이 나타납니다.

4. **웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성합니다.**

   a. **Sun ONE 웹 서버 4.1관리 서버 창에서 [Servers(서버)] 탭을 선택합니다.**

   b. **서버를 선택한 다음 [Manage(관리)] 단추를 선택합니다.**

   c. **페이지의 상단 부분에 있는 [Security(보안)] 탭을 누르고 [Create Database(데이터베이스 생성)] 링크를 선택합니다.**

   d. **두 개의 대화 상자에 암호(웹 서버 트러스트 데이터베이스;** 표 5-1 **참조)를 입력하고 [OK(확인)]를 선택합니다.**

      8개 이상의 문자로 된 암호를 선택합니다. Sun ONE 웹 서버를 보안 모드로 실행할 경우 이 암호를 사용하여 내부 암호화 모듈을 시작합니다.

      하나 이상의 웹 서버 인스턴스에서 보안을 활성화할 수 있습니다. 이 경우에는 각 웹 서버 인스턴스에 대해 1단계 ~ 4단계를 반복합니다.

참고 – Sun ONE 웹 서버 4.1 관리 서버에서 SSL (Secure Socket Layer)을 실행하고 싶은 경우에도 트러스트 데이터베이스의 설정 절차는 유사합니다. 자세한 내용은 `http://docs.sun.com`에서 *iPlanet Web Server, Enterprise Edition Administrator's Guide*를 참조하십시오.

5. **다음 스크립트를 실행하여 Sun Crypto Accelerator 4000 보드를 활성화합니다.**

```
# /opt/SUNWconn/bin/iplsslcfg
```

이 스크립트에서 웹 서버를 선택할 것을 지시합니다. Sun ONE 웹 서버를 위한 Sun Crypto Accelerator 4000 암호화 모듈을 설치합니다. 그러면 스크립트가 구성 파일을 업데이트하여 Sun Crypto Accelerator 4000 보드를 활성화합니다.

6. **`1`을 입력하여 Sun ONE 웹 서버가 SSL을 사용할 수 있도록 구성한 다음 [Return]을 누릅니다.**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. **프롬프트가 나타나면 웹 서버 루트 디렉토리의 경로를 입력한 다음 [Return]을 누릅니다.**

```
Please enter the full path of the web server
root directory [/usr/netscape/server4]: /usr/netscape/server4
```

8. **계속 진행하려면 프롬프트에 y를 입력하고 [Return]을 누릅니다.**

```
This script will update your Sun ONE Web Server installation
in /usr/netscape/server4 to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **0을 입력하여 종료합니다.**

▼ 서버 인증서 작성

1. **다음 명령을 입력하여 Sun ONE웹 서버 4.1 관리 서버를 재시작합니다.**

```
# /usr/netscape/server4/https-admserv/stop
# /usr/netscape/server4/https-admserv/start
```

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.**

```
http://hostname.domain:admin_port
```

인증 대화 상자에서 setup 실행 중 선택한 Sun ONE 웹 서버 4.1 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE 웹 서버 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE 웹 서버 4.1 관리 서버 사용자 이름에 admin을 입력합니다.

---

3. **[OK(확인)]를 선택합니다.**

Sun ONE 웹 서버 4.1관리 서버 창이 나타납니다.

4. **서버 인증서를 요청하려면 Sun ONE 웹 서버 4.1 관리 서버 창 상단에 있는 [Security (보안)] 탭을 선택합니다(**그림 5-1**).**

   [Create Trust Database(트러스트 데이터베이스 생성)] 페이지가 표시됩니다.

5. **왼쪽 프레임에서 [Request a Certificate(인증서 요청)] 링크를 선택합니다(**그림 5-1**).**

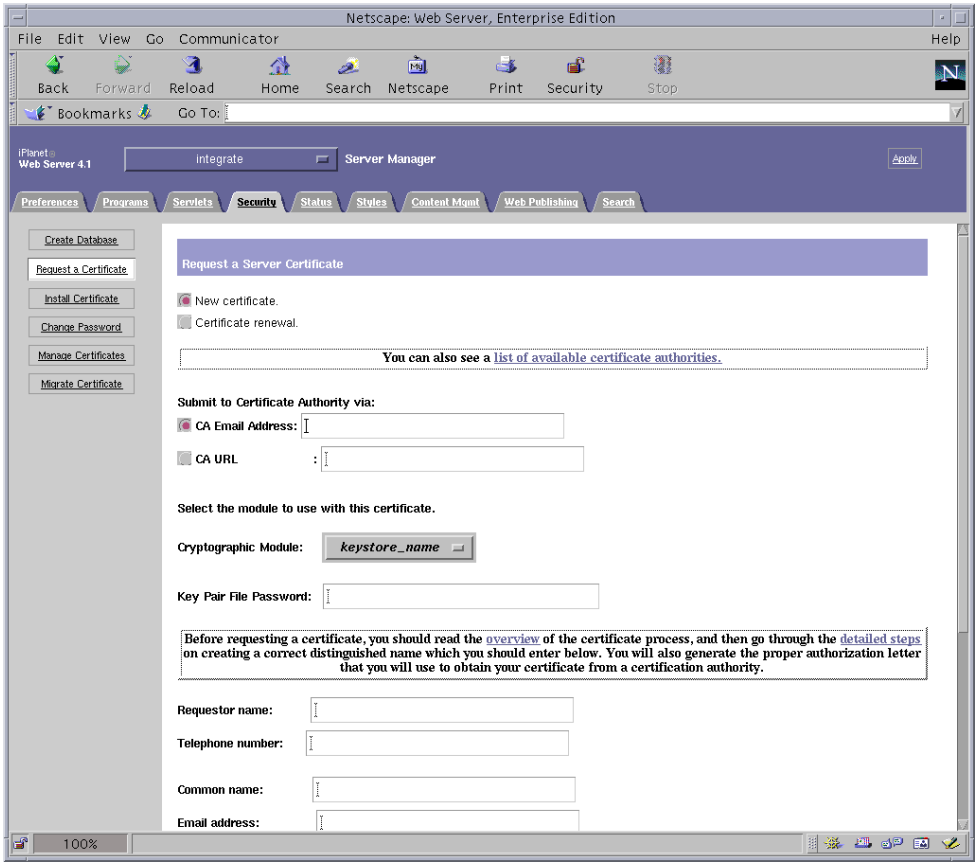

그림 5-1 Sun ONE 웹 서버 4.1 관리 서버의 서버 인증서 요청 페이지

6. **다음 정보를 사용하여 인증서 요청을 작성합니다.**

   a. **새 인증서를 선택합니다.**

      웹 기능이 가능한 인증 기관 또는 등록 기관에 인증서 요청을 직접 보낼 수 있는 경우 CA URL 링크를 선택합니다. 그렇지 않은 경우 [CA Email Address(CA 전자 우편 주소]를 선택하고 인증서 요청을 수신할 전자 우편 주소를 입력합니다.

b. 사용할 암호화 모듈을 선택합니다.

풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어가 선택되었는지 확인합니다. SUNW 가속만 선택하지 마십시오.

c. [Key Pair File Password(키 쌍 파일 암호)] 대화 상자에서 키를 소유할 사용자의 암호를 입력합니다.

이 암호의 형식은 *사용자 이름:암호*(표 5-1)입니다.

d. 다음 요청자 정보 필드에 적절한 정보를 입력합니다.

표 5-2 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name (공용 이름):	방문자 브라우저에 입력되는 웹 사이트 도메인 *hostname.domain*
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	인증서에 표시될 소속 기관 값
Organizational Unit (소속 기관 단위):	(선택 사항) 인증서에 표시될 소속 기관 단위 값
Locality(지방):	(선택 사항) 제공될 경우 인증서에 표시될 도시, 국가
State(주):	(선택 사항) 전체 주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

e. [OK(확인)] 단추를 선택하여 해당 정보를 전송합니다.

7. 인증 기관을 이용하여 인증서를 작성합니다.

- 인증서를 CA URL에 보내도록 선택하면 인증서 요청이 CA URL에 자동으로 전송됩니다.
- [CA Email Address(CA 전자 우편 주소)]를 선택할 경우 헤더와 함께 전자 우편으로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

8. 인증서가 작성되면 헤더와 함께 클립보드에 복사합니다.

참고 – 인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다. 다음 항목의 5단계를 위해 이 데이터를 클립보드에 보관합니다.

▼ 서버 인증서 설치

1. **Sun ONE 웹 서버 4.1관리 서버 창 왼쪽의 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

   인증 기관의 승인을 받고 인증서가 발급되면 Sun ONE 웹 서버에 인증서를 설치해야 합니다.

2. **[Security(보안)] 탭을 선택합니다.**

3. **왼쪽 프레임에서 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

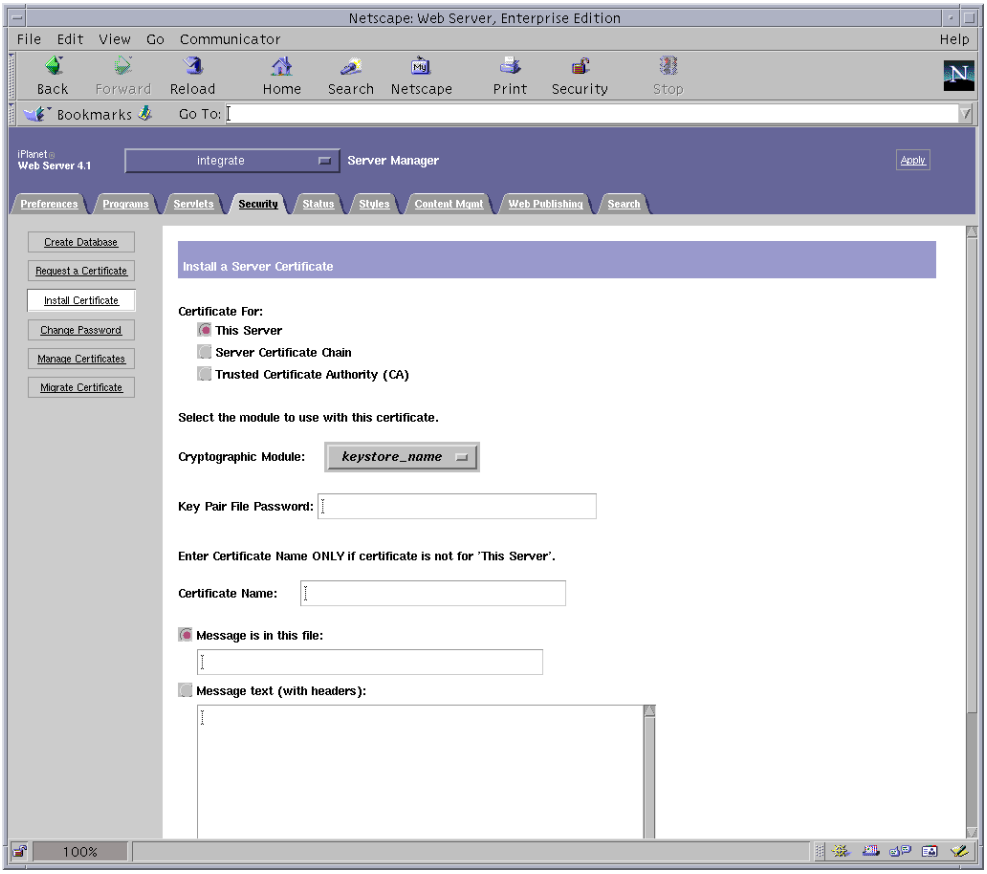

그림 5-2 Sun ONE 웹 서버 4.1 관리 서버의 서버 인증 설치 페이지

4. **양식을 작성하여 인증서를 설치합니다.**

표 5-3 인증서 설치에 필요한 필드

필드	설명
[Certificate For (인증 대상)]	해당 서버
[Cryptographic Module (암호화 모듈)]	풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 반드시 정확한 키스토어 이름을 선택해야 합니다. Sun Crypto Accelerator 4000을 사용하려면 키스토어에 할당한 이름과 같은 이름을 가진 모듈을 선택해야 합니다.
[Key Pair File Password (키 쌍 파일 암호)]	이 암호의 형식은 *사용자 이름:암호*(표 5-1)입니다.
[Certificate Name (인증서 이름)]	대부분의 경우 공백으로 둡니다. 이름을 제공할 경우 SSL 지원으로 실행하게 되면 웹 서버가 인증서와 키에 액세스할 때 사용하는 이름을 변경합니다. 이 필드의 기본값은 `Server-Cert`입니다.

5. **인증 기관에서 복사한 인증서(89페이지의 "서버 인증서 작성"의 8단계)를 [Message box(메시지 상자)]에 붙여넣습니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

6. **페이지 하단에 있는 [OK(확인)] 단추를 선택합니다.**

7. **모두 올바르게 입력되었는지 확인한 다음 [Add Server Certificate(서버 인증서 추가)] 단추를 선택합니다.**

   화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스는 절차가 진행되는 동안 계속 종료되어 있었기 때문에 이 메시지에 따르지 않아도 됩니다.

   또한 웹 서버가 SSL을 사용하려면 웹 서버를 구성해야 한다는 메시지가 표시됩니다. 다음 절차를 따라하여 웹 서버를 구성합니다.

SSL을 위한 Sun ONE 웹 서버 4.1 구성

웹 서버 및 서버 인증서 설치가 완료되면 SSL을 위해 웹 서버를 구성해야 합니다.

▼ Sun ONE 웹 서버 4.1 구성

1. **기본 Sun ONE 웹 서버 4.1 관리 서버 페이지에서 작업할 웹 서버 인스턴스 선택한 후 [Manage(관리)]를 선택합니다.**

2. **페이지 상단의 [Preferences(환경 설정)] 탭이 선택되어 있지 않은 경우 [Preferences (환경 설정)] 탭을 선택합니다.**

3. **페이지 왼쪽에 있는 [Encryption On/Off(암호 설정/해제)] 링크를 선택합니다.**

4. **암호화를 [On(설정)]으로 설정합니다.**

   대화 상자의 [Port(포트)] 필드가 기본 SSL 포트 번호인 443으로 업데이트되어야 합니다. 필요한 경우 포트 번호를 변경합니다.

5. **[OK(확인)] 단추를 선택합니다.**

6. **[Save(저장)] 단추를 선택하여 변경 사항을 적용합니다.**

   웹 서버가 보안 모드에서 실행되도록 구성되었습니다.

7. **다음 행을 추가하여** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **(***hostname***은 웹 서버 이름)파일을 편집합니다.**

   ```
   CERTDefaultNickname keystore_name:Server-Cert
   ```

   작성된 인증서는 기본적으로 `Server-Cert`로 이름이 지정됩니다. 인증서 이름이 다른 경우 `Server-Cert` 대신 선택한 이름을 사용해야 합니다.

8. **관리할 서버를 선택한 다음 페이지의 오른쪽 상단 모서리에 있는 [Apply(적용)] 단추를 선택합니다.**

   이것을 선택하면 Sun ONE 웹 서버 4.1 관리 서버를 통해 변경 사항을 적용할 수 있습니다.

9. **[Load Configuration Files(구성 파일 로드)] 단추를 선택하여 방금** `magnus.conf` **파일에 수행한 변경 사항을 적용합니다.**

   웹 서버 인스턴스를 시작할 수 있는 페이지로 다시 돌아갑니다.

   서버가 꺼져있을 때 [Apply Changes(변경 사항 저장)]을 선택할 경우 인증 대화 상자가 나타나 *사용자 이름:암호* 입력을 요청합니다. 이 창은 크기를 조정할 수 없으며, 변경 사항을 전송하는 데 문제가 생길 수 있습니다.

   이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

   - [Load Configuration Files(구성 파일 로드)]을 대신 선택합니다.
   - 웹 서버를 먼저 시작한 다음 [Apply Changes(변경 사항 적용)] 단추를 선택합니다.

10. **Sun ONE 웹 서버 4.1 관리 서버 창에서 창 좌측의 [On/Off(설정/해제)] 링크를 선택합니다.**

11. **서버의 암호를 입력한 다음 [OK(확인)] 단추를 선택합니다.**

    하나 이상의 암호를 입력하게 됩니다. [Module Internal(모듈 내부)] 프롬프트에서 웹 서버 트러스트 데이터베이스에 대한 암호를 입력합니다.

    모듈 *keystore_name* 프롬프트에서 해당 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

    나타난 다른 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

12. **다음 웹 사이트에서 새로운 SSL 작동 웹 서버를 확인합니다.**

    `https://`*hostname.domain*`:`*server_port*`/`

참고 – 기본 *server_port*는 443입니다.

Sun ONE 웹 서버 6.0 설치 및 구성

이 장은 Sun ONE 웹 서버 6.0과 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 활성화 방법을 설명합니다. 이 항목은 다음을 설명합니다.

Sun ONE 웹 서버 6.0 설치

절차는 반드시 순서대로 수행해야 합니다. Sun ONE 웹 서버 사용법에 대한 자세한 내용은 Sun ONE 웹 서버 설명서를 참조하십시오.

▼ Sun ONE 웹 서버 6.0 설치

1. **Sun ONE 웹 서버 6.0 소프트웨어를 다운로드합니다.**

   웹 서버 소프트웨어는 다음 URL에 있습니다. `http://www.sun.com/`

2. **웹 서버를 설치합니다.**

   이 항목에 포함된 지침은 하나의 예제에 대한 것이므로, 원할 경우 Sun ONE 웹 서버를 다르게 구성할 수도 있습니다. 이 서버의 기본 작업 경로 이름은 다음과 같습니다: `/usr/iplanet/servers`

   Sun ONE 웹 서버가 설치되는 동안 기본 경로를 승인합니다. 이 설명서는 기본 경로를 참조합니다. 소프트웨어를 다른 위치에 설치하려면 설치한 위치를 기록해 두는 것이 좋습니다.

3. 설치 **프로그램을 실행합니다.**

4. **설치 스크립트의 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 편리상 기본값을 허용할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 조건에 동의합니다.**

   b. **정식** *hostname.domain***을 입력합니다.**

   c. **Sun ONE 웹 서버 6.0 관리 서버 암호를 두 번 입력합니다.**

   d. **프롬프트가 나오면 [Return]을 누릅니다.**

▼ 트러스트 데이터베이스 생성

1. Sun ONE 웹 서버 6.0 관리 서버를 시작합니다.

Sun ONE 웹 서버 6.0 관리 서버를 시작하려면 다음 명령을 사용합니다(`setup` 요청에 따라 `startconsole`을 실행하지 않고).

```
# /usr/iplanet/servers/https-admserv/start
SunONE-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
warning: daemon is running as super-user
[LS ls1] http://hostname.domain/port 8888 ready to accept requests
startup: server started successfully
```

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. 웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.

```
http://hostname.domain:admin_port
```

인증 대화 상자에서 `setup` 실행 중 선택한 Sun ONE 웹 서버 6.0 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE 웹 서버 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE 웹 서버 6.0 관리 서버 사용자 이름에 `admin`을 입력합니다.

---

3. [OK(확인)]를 선택합니다.

Sun ONE 웹 서버 6.0 관리 서버 창이 나타납니다.

4. 웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성합니다.

하나 이상의 웹 서버 인스턴스에 대해 보안을 활성화할 수 있습니다. 이 경우에는 각 웹 서버 인스턴스에 대해 1단계 ~ 4단계를 반복합니다.

참고 – Sun ONE 웹 서버 6.0 관리 서버에서 SSL을 실행하고 싶은 경우에도 트러스트 데이터베이스의 설정 절차는 유사합니다. 자세한 내용은 `http://docs.sun.com`에서 *iPlanet Web Server, Enterprise Edition Administrator's Guide*를 참조하십시오.

---

a. Sun ONE 웹 서버 6.0 관리 서버 창에서 [Servers(서버)] 탭을 선택합니다.

b. 서버를 선택한 다음 [Manage(관리)] 단추를 선택합니다.

c. 페이지의 상단 부분에 있는 [Security(보안)] 탭을 누르고 [Create Database(데이터베이스 생성)] 링크를 선택합니다.

d. 두 개의 대화 상자에 암호(웹 서버 트러스트 데이터베이스[표 5-1])를 입력하고 [OK (확인)]를 누릅니다.

8개 이상의 문자로 된 암호를 선택합니다. Sun ONE 웹 서버를 보안 모드로 실행할 경우 이 암호를 사용하여 내부 암호화 모듈을 시작합니다.

5. 다음 스크립트를 실행하여 Sun Crypto Accelerator 4000 보드를 활성화합니다.

```
# /opt/SUNWconn/crypto/bin/iplsslcfg
```

이 스크립트에서 웹 서버를 선택할 것을 지시합니다. Sun ONE 웹 서버를 위한 Sun Crypto Accelerator 4000 암호화 모듈을 설치합니다. 그러면 스크립트가 구성 파일을 업데이트하여 Sun Crypto Accelerator 4000 보드를 활성화합니다.

6. 1을 입력하여 Sun ONE 웹 서버가 SSL을 사용할 수 있도록 구성한 다음 [Return]을 누릅니다.

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. 프롬프트가 나타나면 웹 서버 루트 디렉토리의 경로를 입력한 다음 [Return]을 누릅니다.

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

8. **계속 진행하려면 프롬프트에 y를 입력하고 [Return]을 누릅니다.**

```
This script will update your Sun ONE Web Server installation
in /usr/iplanet/servers to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **0을 입력하여 종료합니다.**

▼ 서버 인증서 작성

1. **다음 명령을 입력하여 Sun ONE 웹 서버 6.0 관리 서버를 재시작합니다.**

```
# /usr/iplanet/servers/https-admserv/stop
# /usr/iplanet/servers/https-admserv/start
```

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.**

```
http://hostname.domain:admin_port
```

인증 대화 상자에서 setup 실행 중 선택한 Sun ONE 웹 서버 6.0 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE 웹 서버 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE 웹 서버 6.0 관리 서버 사용자 이름에 admin을 입력합니다.

---

3. **[OK(확인)]를 선택합니다.**

Sun ONE 웹 서버 6.0 관리 서버 창이 나타납니다.

4. **서버 인증서를 요청하려면 Sun ONE 웹 서버 6.0 관리 서버 창 상단에 있는 [Security (보안)] 탭을 선택합니다.**

   [Create Trust Database(트러스트 데이터베이스 작성)] 창이 표시됩니다.

5. **Sun ONE 웹 서버 6.0 관리 서버 창의 왼쪽 프레임에서 [Request a Certificate (인증서 요청)] 링크를 선택합니다.**

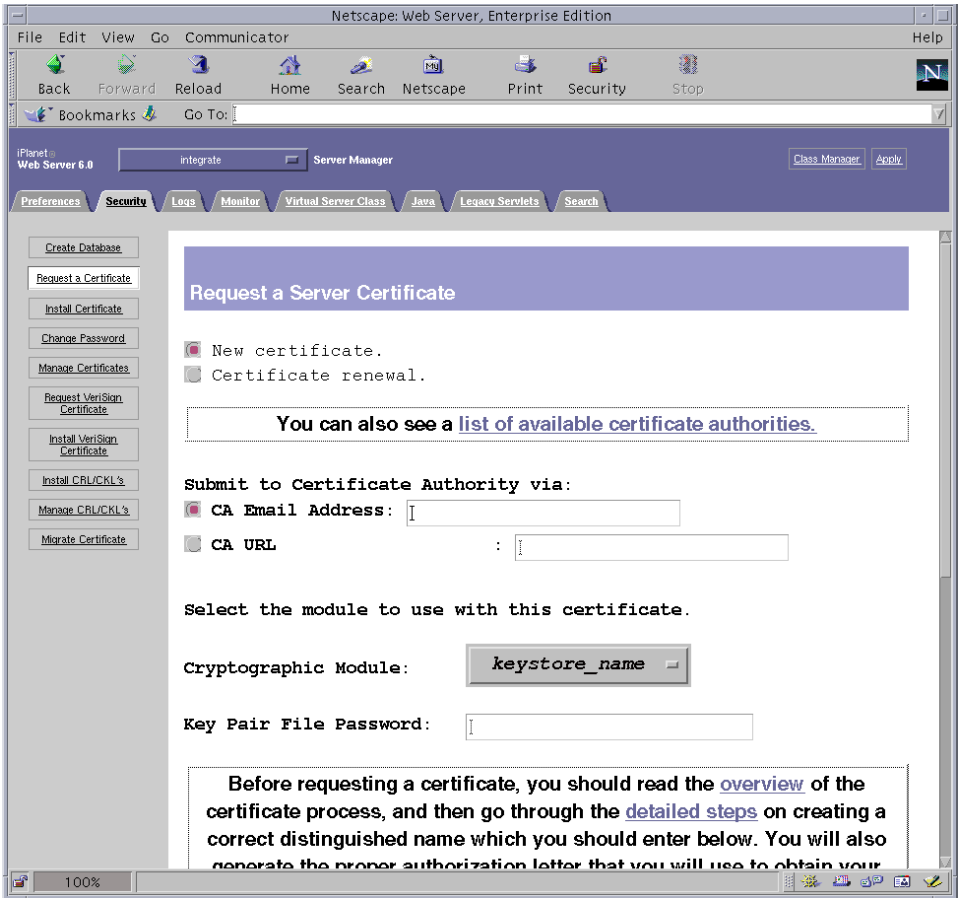

그림 5-3 Sun ONE 웹 서버 6.0 관리 서버의 서버 인증서 요청 페이지

6. **다음 정보를 기입하여 인증서 요청을 작성합니다.**

   a. **새 인증서를 선택합니다.**

      웹 기능이 가능한 인증 기관 또는 등록 기관에 인증서 요청을 직접 보낼 수 있는 경우 CA URL 링크를 선택합니다. 그렇지 않은 경우 [CA Email Address(CA 전자 우편 주소]를 선택하고 인증서 요청을 수신할 전자 우편 주소를 입력합니다.

b. 사용할 암호화 모듈을 선택합니다.

풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어가 선택되었는지 확인합니다. SUNW 가속만 선택하지 마십시오.

c. [Key Pair File Password(키 쌍 파일 암호)] 대화 상자에서 키를 소유할 사용자의 암호를 입력합니다.

이 암호의 형식은 *사용자 이름:암호*(표 5-1)입니다.

d. 다음 요청자 정보 필드에 적절한 정보를 입력합니다.

표 5-4 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name (공용 이름):	방문자 브라우저에 입력되는 웹 사이트 도메인 *hostname.domain*
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	인증서에 표시될 소속 기관 값
Organizational Unit (소속 기관 단위):	(선택 사항) 인증서에 표시될 소속 기관 단위 값
Locality(지방):	(선택 사항) 제공된 경우 인증서에 표시된 도시, 국가
State(주):	(선택사항) 전체 주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

e. [OK(확인)] 단추를 선택하여 해당 정보를 전송합니다.

7. 인증 기관을 이용하여 인증서를 작성합니다.

- 인증서를 CA URL에 보내도록 선택하면 인증서 요청이 CA URL에 자동으로 전송됩니다.
- [CA Email Address(CA 전자 우편 주소)]를 선택할 경우 헤더와 함께 전자 우편으로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

8. 인증서가 작성되면 헤더와 함께 클립보드에 복사합니다.

참고 – 인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다. 101페이지의 "서버 인증서 설치"의 5단계를 위해 이 데이터를 클립보드에 보관합니다.

▼ 서버 인증서 설치

1. **Sun ONE 웹 서버 6.0 관리 서버 창 왼쪽의 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

   인증 기관의 승인을 받고 인증서가 발급되면 Sun ONE 웹 서버에 인증서를 설치해야 합니다.

2. **[Security(보안)] 탭을 선택합니다.**

3. **왼쪽 프레임에서 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

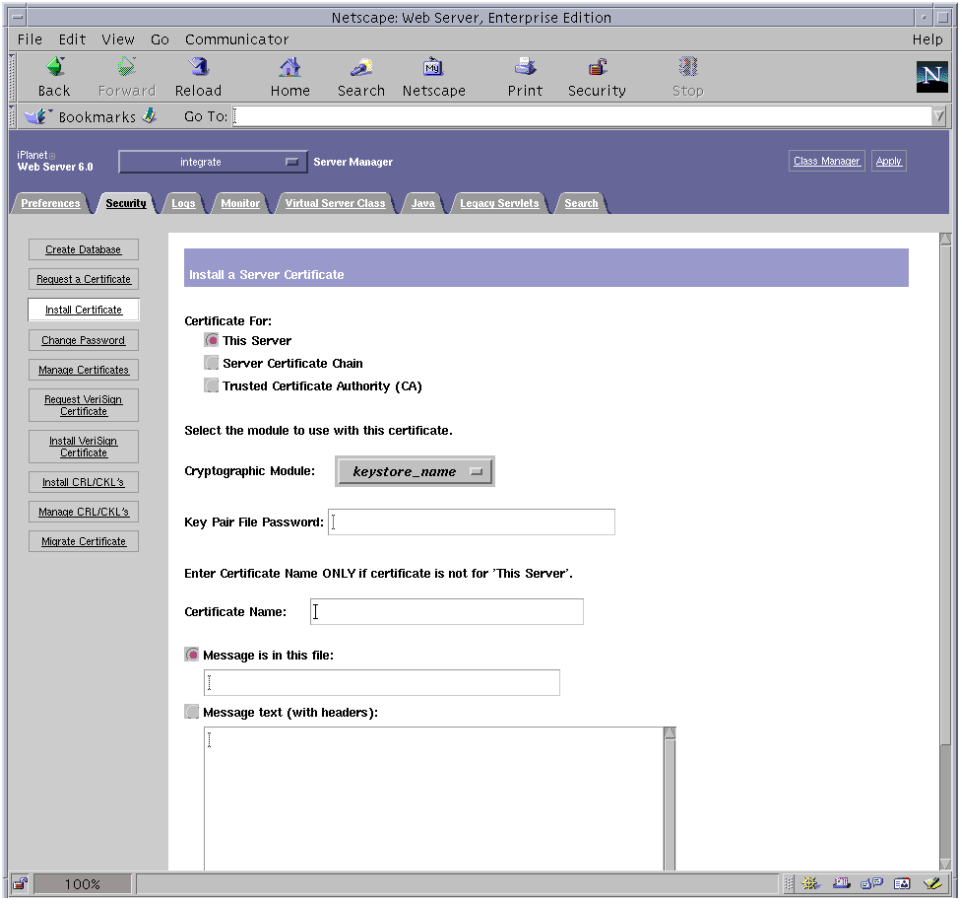

그림 5-4 Sun ONE 웹 서버 6.0 관리 서버의 서버 인증서 설치 페이지

4. 양식을 작성하여 인증서를 설치합니다.

표 5-5 인증서 설치에 필요한 필드

필드	설명
[Certificate For (인증 대상)]	해당 서버
[Cryptographic Module (암호화 모듈)]	풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어 이름이 선택되었는지 확인합니다. Sun Crypto Accelerator 4000을 사용하려면 반드시 *keystore_name* 형식의 모듈을 선택해야 합니다.
[Key Pair File Password (키 쌍 파일 암호)]	이 암호의 형식은 *사용자 이름:암호*(표 5-1)입니다.
[Certificate Name (인증서 이름)]	대부분의 경우 공백으로 둡니다. 이름을 제공할 경우 SSL 지원으로 실행하게 되면 웹 서버가 인증서와 키에 액세스할 때 사용하는 이름을 변경합니다. 이 필드의 기본값은 `Server-Cert`입니다.

5. 인증 기관에서 복사한 인증서(98페이지의 "서버 인증서 작성"의 8단계)를 [Message (메시지)] 텍스트 상자에 붙여넣습니다.

인증서에 대한 일부 기본 정보가 표시됩니다.

6. 페이지 하단에 있는 [OK(확인)] 단추를 선택합니다.

7. 모두 올바르게 입력되었는지 확인한 다음 [Add Server Certificate(서버 인증서 추가)] 단추를 선택합니다.

화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스는 절차가 진행되는 동안 계속 종료되어 있었기 때문에 이 메시지에 따르지 않아도 됩니다.

또한 웹 서버가 SSL을 사용하려면 웹 서버를 구성해야 한다는 메시지가 표시됩니다. 다음 절차를 따라하여 웹 서버를 구성합니다.

SSL을 위한 Sun ONE 웹 서버 6.0 구성

웹 서버 및 서버 인증서 설치가 완료되면 SSL을 위해 웹 서버를 구성해야 합니다.

▼ Sun ONE 웹 서버 6.0 구성

1. **페이지 상단 부분의 [Preferences(환경 설정)] 탭을 선택합니다.**
2. **왼쪽 프레임에 있는 [Edit Listen Sockets(수신 대기 소켓 편집)] 링크를 선택합니다.**
   기본 프레임은 웹 서버 인스턴스에 대해 설정된 모든 수신 대기 소켓이 나열합니다.
   a. **다음 필드를 수정합니다.**
      - **Port(포트)**: SSL 작동 웹 서버를 실행할 포트로 설정합니다(주로 443 포트).
      - **Security(보안)**: [On(설정)]으로 설정합니다.
   b. **[OK(확인)] 단추를 선택하여 변경 사항을 적용합니다.**
      이제 [Edit Listen Sockets(수신 대기 소켓 편집)] 페이지의 보안 필드에 [Attributes (속성)] 링크가 표시됩니다.
3. **[Attributes(속성)] 링크를 선택합니다.**
4. **시스템의 키스토어에 대한 인증을 받으려면 사용자 이름:암호를 입력합니다.**
5. **암호의 기본 설정을 변경하려면 [Ciphers(암호)]의 표제에서 해당 암호 모음을 선택합니다.**
   암호 설정 변경을 위한 대화 상자가 나타납니다. [Cipher Default(암호 기본값)] 설정, [SSL2] 또는 [SSL3/TLS (Transmission Layer Security)]를 선택할 수 있습니다. [Ciipher Default(암호 기본값)]를 선택한 경우 기본 설정이 표시되지 않습니다. 다른 두 옵션을 선택하려면 팝업 대화 상자에서 활성화할 알고리즘을 선택해야 합니다. 암호 선택에 대한 내용은 Sun ONE 설명서를 참조하십시오.
6. **키스토어를 위한 인증서를 선택하고 그 뒤에 :** `Server-Cert` **다음에 나오는 키스토어에 대한 인증서를 선택합니다(또는 이와 다른 경우 선택한 이름**).
   [Certificate Name(인증서 이름)] 필드에는 적절한 키스토어 사용자가 소유하는 키만 나타납니다. 키스토어 사용자는 *사용자 이름:암호*로 인증한 사용자입니다.
7. **인증서를 선택하고 보안 설정을 모두 확인했으면 [OK(확인)] 단추를 선택합니다.**
8. **오른쪽 상단 모서리에 있는 [Apply(적용)] 링크를 선택하여 서버를 시작하기 전에 변경 사항을 적용합니다.**

9. **[Load Configuration Files(구성 파일 로드)] 링크를 선택하여 변경 사항을 적용합니다.**

   웹 서버 인스턴스를 시작할 수 있는 페이지로 다시 돌아갑니다.

   서버가 꺼져있을 때 [Apply Changes(변경 사항 저장)]을 선택할 경우 인증 대화 상자가 나타나 *사용자 이름:암호* 입력을 요청합니다. 이 창은 크기를 조정할 수 없으며, 변경 사항을 전송하는 데 문제가 생길 수 있습니다.

   이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

   - [Load Configuration Files(구성 파일 로드)]을 대신 선택합니다.
   - 웹 서버를 먼저 시작한 다음 [Apply Changes(변경 사항 적용)] 단추를 선택합니다.

10. **Sun ONE 웹 서버 6.0 관리 서버 창에서 창 좌측의 [On/Off(설정/해제)] 링크를 선택합니다.**

11. **서버의 암호를 입력한 다음 [OK(확인)] 단추를 선택합니다.**

    하나 이상의 암호를 입력하게 됩니다. [Module Internal(모듈 내부)] 프롬프트에서 웹 서버 트러스트 데이터베이스에 대한 암호를 입력합니다.

    keystore_name 모듈 프롬프트에서 *사용자 이름:암호*를 입력합니다.

    나타난 다른 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

12. **다음 웹 사이트에서 새로운 SSL 작동 웹 서버를 확인합니다.**

    `https://hostname.domain:server_port/`

참고 – 기본 *server_port*는 443입니다.

---

6 장

Sun Crypto Accelerator 4000 보드와 함께 사용할 Apache 웹 서버 구성

이 장에서는 Apache 웹 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

주의 – Apache 웹 서버로 Sun Crypto Accelerator 1000 보드와 Sun Crypto Accelerator 4000을 동시에 사용하도록 구성하지 마십시오. 두 보드 모두가 Apache 웹 서버를 동시에 사용하도록 구성될 경우 Apache는 올바르게 작동하지 않을 것입니다.

Apache 웹 서버를 사용하려면 109234-09 패치를 설치해야 합니다. `SUNWkcl2a` 패키지가 추가되면 시스템은 Apache 웹 서버 mod_ssl 1.3.26로 구성됩니다.

참고 – Apache 웹 서버 소프트웨어의 대용량 암호화 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

Apache 웹 서버를 위한 보드 활성화

이 항목은 Apache 웹 서버와의 사용을 위한 Sun Crypto Accelerator 4000 보드 활성화 방법에 대한 개요를 제공합니다.

Apache 웹 서버 활성화

Sun Crypto Accelerator 4000 보드와 함께 사용하려면 Apache 웹 서버 1.3.26 이상이 필요합니다. 다음 지침은 Apache 웹 서버 1.3.26 릴리스에 해당합니다. Apache 웹 서버 사용에 대한 자세한 내용은 Apache 웹 서버 설명서를 참조하십시오.

▼ Apache 웹 서버 활성화

1. `httpd` 구성 파일을 생성합니다.

Solaris 시스템인 경우 `httpd.conf-example` 파일은 일반적으로 `/etc/apache` 안에 있습니다. 이 파일을 템플릿으로 사용하여 다음 방법으로 복사할 수 있습니다.

```
# cp /etc/apache/httpd.conf-example /etc/apache/httpd.conf
```

2. `ServerName`을 `http.conf` 파일의 서버 이름으로 대체합니다.

3. `apsslcfg`를 시작합니다.

```
# /opt/SUNWconn/cryptov2/bin/apsslcfg
```

4. `1`을 선택하여 SSL을 사용할 Apache 웹 서버를 구성합니다.

```
Sun Crypto Accelerator Apache Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Apache.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Apache for SSL
2. Work with Apache keys

Your selection (0 to quit): 1
```

5. Apache 바이너리가 포함된 디렉토리를 제공합니다.

Solaris 시스템에서 일반적으로 `/usr/apache`가 사용됩니다.

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache
```

6. **Apache 구성 파일의 위치를 제공합니다.**

   Solaris 시스템에서 일반적으로 /etc/apache가 사용됩니다.

```
Please enter the directory where the Apache configuration files exist
[/etc/apache]: /etc/apache
```

7. **시스템에 RSA 키 쌍을 생성합니다.**

   키 쌍 생성을 선택하지 않은 경우 나중에는 뒤로 이동하여 sslconfig를 사용하여 키를 생성해야 합니다.

```
Do you wish to create a new RSA keypair and certificate request? [Y/N]:
```

   [No]로 응답한 경우 108페이지의 "인증서 작성"으로 건너뜁니다.

8. **키를 저장할 디렉토리를 제공합니다.**

   이 디렉토리가 존재하지 않을 경우에는 새로 생성됩니다.

```
Where would you like the keys stored? [/etc/apache/keys]: /etc/apache/keys
```

9. **키 요소의 기본 이름을 선택합니다.**

   이 이름에는 키 파일, 인증서 요청 파일, 그리고 이후에는 인증서 파일과 서로 구별되도록 다른 접미사가 추가됩니다.

```
Please choose a base name for the key and request file: base_name
```

10. **키의 길이는 512비트에서 2,048비트 사이로 제공합니다.**

    대부분의 웹 서버 응용 프로그램에는 1,024비트 정도면 충분하지만 필요한 경우 더 강력한 키를 사용할 수 있습니다.

```
What size would you like the RSA key to be [1024]? 1024
Using configuration from /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
........++++++
.....................................................++++++
writing new private key to /etc/apache/keys/base_name
```

11. PEM 패스 문구를 생성합니다.

패스 문구는 키 요소를 보호합니다. 안전적이지만 기억할 수 있는 패스 문구를 선택해야 합니다. 패스 문구를 잊을 경우 해당 키에 액세스할 수 없습니다.

```
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

주의 – 입력한 패스 문구는 반드시 기억해야 합니다. 패스 문구가 없으면 해당 키에 액세스할 수 없습니다. 분실된 패스 문구를 회수할 방법이 없습니다.

인증서 작성

다음 절차는 Sun Crypto Accelerator 4000 보드와 함께 Apache 웹 서버를 작동하는 데 필요한 인증서 작성 방법에 대해 설명합니다.

▼ 인증서 작성

1. 106페이지의 "Apache 웹 서버 활성화"에서 생성한 키를 사용하여 인증서 요청을 작성합니다.

키에 액세스하려면 먼저 암호를 입력해야 합니다. 그 다음, 아래 필드에 적합한 정보를 입력합니다.

- Country Name(국가): 두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)이며, 인증서에 표시될 필수 필드
- State or Province Name(주/도 이름): (선택 사항) 정확한 주/도 이름(또는 마침표(.)를 입력한 다음 [Return]을 누름)
- Locality(지방): (선택 사항) 제공될 경우 인증서에 표시될 도시, 군, 국가 등의 정보
- Organization Name(소속 기관): 인증서에 표시될 소속 기관 값
- Organizational Unit Name(소속 기관 단위): (선택 사항) 인증서에 표시될 소속 기관 단위 값
- SSL Server Name(SSL 서버 이름): 방문자의 브라우저에 입력되는 웹 사이트 도메인
- Email Address(전자 우편 주소): 요청자의 연락처 정보

다음은 인증서 필드의 입력 방식에 대한 예제입니다.

```
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) []: Fictional Company, Inc.
Organizational Unit Name (eg, section) []: Online Sales Division
SSL Server Name (eg, www.company.com) []:www.fictional-company.com
Email Address []:admin@fictional-company.com
```

2. **/etc/apache/httpd.conf 파일을 지침에 따라 수정합니다.**

   키 및 인증서 파일에 대한 정보가 표시됩니다. 또한 Sun Crypto Accelerator 4000 소프트웨어와 함께 사용하기 위한 /etc/apache/httpd.conf 파일의 수정 방법에 대한 지침이 표시되어 있습니다.

```
The keyfile is stored in /etc/apache/keys/base_name-key.pem.
The certificate request is in /etc/apache/keys/base_name-certreq.pem.

You will need to edit /etc/apache/httpd.conf for the following items:

You must specify the ports that Apache will listen to for
SSL connections, as well as for non-SSL connections.  One
way to accomplish this is to add the following lines in
the Listen section:

Listen 80
Listen 443

In the LoadModule section, add the following:

LoadModule ssl_module /usr/apache/libexec/mod_ssl.so.version-number

In the AddModule section, add the following:

AddModule mod_ssl.c
```

참고 – 해당 구성에 대한 정확한 *버전 번호*가 표시됩니다.

3. **VirtualHost 설정을 선택하지 않은 경우, httpd.conf 파일의 SSLEngine, SSLCertificateFile 및 SSLCertificateKeyFile 지시어를 SSLPassPhraseDialog 지시어 바로 위에 위치해야 합니다.**

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/base_name-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/base_name-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass

Other SSL-related directives and their explanations
can be found in the Sun Crypto Accelerator documentation.

Other Apache-related directives may need to be configured
in order to start your Apache Web Server.  Please refer
to your Apache documentation.

<Press ENTER to continue>
```

106페이지의 "Apache 웹 서버 활성화"의 7단계 질문에 응답하지 않은 경우 키 요소 작성 방법에 대한 추가 정보를 받게 됩니다.

```
Since you did not create keys, you will need to
make sure that you have a key file and a certificate
file in place before enabling SSL for Apache.

You can create a new key file and certificate request
by selecting the "Generate a keypair and request a
certificate for Apache" option after choosing
"Work with Sun ONE and Apache keys" from the
apsslcfg main menu.
```

4. **sslconfig 작업이 완료되면 0을 선택하여 이를 종료합니다.**

5. **/etc/apache/keys/*base_name*-certreq.pem(*base_name*은 106페이지의 "Apache 웹 서버 활성화"의 9단계에서 설정됨)에서 헤더와 함께 인증서 요청을 복사한 다음 해당 인증 기관으로 전송합니다.**

6. **인증서가 작성되면 인증서 파일** `/etc/apache/keys/`*base_name*`-cert.pem`**을 작성한 후 이를 해당 파일에 붙여 넣습니다.**

7. **Apache 웹 서버를 시작합니다.**

   Apache 바이너리 디렉토리를 `/usr/apache/bin`으로 가정합니다. 바이너리 디렉토리가 아닌 경우 올바른 디렉토리를 입력합니다.

```
# /usr/apache/bin/apachectl start
```

8. **프롬프트가 나타나면 PEM 패스 문구를 입력합니다.**

9. **다음 웹 사이트에서 새로운 SSL 작동 웹 서버를 확인합니다:**

   `https://`*server_name*`:`*server_port*`/`

   기본 *server_port*는 443입니다.

7 장

진단 및 문제 해결

이 장에서는 Sun Crypto Accelerator 4000 소프트웨어에 대한 진단 테스트 및 문제 해결에 대해 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

SunVTS 진단 소프트웨어

핵심 SunVTS 래퍼는 테스트 제어 및 일련의 테스트에 대한 사용자 인터페이스를 제공합니다. 일부 테스트는 Solaris 8/9 Software Supplement CD안에 번들로 구성된 핵심과 함께 SUNWvts 및 SUNWvtsx 패키지로 제공됩니다. 번들에 포함되지 않고 SunVTS 핵심을 사용하는 기타 테스트는 테스트되는 드라이버 소프트웨어 패키지와 함께 제공됩니다.

Sun Crypto Accelerator 4000 보드를 세 종류의 SunVTS 테스트로 테스트할 수 있습니다. 이 테스트 중 nettest 및 netlbtest 두 가지는 SunVTS 5.1 Patch Set (PS) 2 릴리스부터 핵심 SunVTS 소프트웨어와 번들로 제공됩니다. 이 테스트는 보드의 이더넷 회로에서 실행됩니다.

세 번째 SunVTS 테스트인 vcatest는 Sun Crypto Accelerator 4000 CD의 SUNWvcav 패키지에 제공되어 핵심 SunVTS 래퍼와 함께 작동하여 보드의 암호화 회로를 진단합니다.

SunVTS netlbtest 및 nettest 설치vca 드라이버 지원

표 7-1은 설치된 SunVTS 소프트웨어를 업데이트하여 vca 드라이버에 대한 SunVTS netlbtest 및 nettest 지원을 제공하는 방법을 설명합니다.

표 7-1 vca 드라이버를 위한 SunVTS netlbtest 및 nettest 필수 소프트웨어

기본 Solaris 소프트웨어	기본 SunVTS 소프트웨어	필수 교체 패키지	필수 오버레이 패치
Solaris 8 7/01	SunVTS4.4		111854-04
Solaris 8 10/01	SunVTS4.5		112250-04
Solaris 8 2/02	SunVTS4.6	SunVTS5.1ps2	
Solaris 9 5/02	SunVTS5.0	SunVTS5.1ps2	
Solaris 9 9/02	SunVTS5.1		113614-11
Solaris 8 HW 12/02	SunVTS5.1ps1		113614-11
Solaris 9 12/02	SunVTS5.1ps1		113614-11
Solaris 8 HW 5/03	SunVTS5.1ps2		
Solaris 9 4/03	SunVTS5.1ps2		

SunVTS 소프트웨어는 각 Solaris 릴리즈와 함께 배포되는 Solaris Software Supplement CD에 담겨 전달됩니다. 표 7-1의 기본 SunVTS 소프트웨어 열에 나열된 SunVTS 소프트웨어 버전은 같은 행에 명시된 Solaris 릴리즈와 함께 제공되는 Solaris Software Supplement CD를 통해 배포됩니다.

표 7-1에서 "SunVTS"로 시작되는 항목은 SunVTS 패키지 세트의 버전을 식별합니다. 각 SunVTS 패키지 세트에 포함된 SUNWvts 및 SUNWvtsx 패키지는 반드시 설치해야 합니다.

표 7-1의 필수 교체 패키지 열은 이전에 설치한 SunVTS 패키지 세트를 대체해야 하는 SunVTS 패키지 세트를 나열합니다. SunVTS 교체 패키지를 설치하기 전에 이전에 설치한 SunVTS 패키지를 제거해야 합니다. 이전에 설치한 SunVTS 패키지는 설치 시와 같은 방법으로 제거해야 합니다. 예를 들어, 패키지를 설치할 때 pkgadd 명령을 사용한 경우 이를 제거할 때는 pkgrm 명령을 사용해야 합니다.

표 7-1의 필수 오버레이 패치 열에 항목이 있는 경우 patchadd 명령을 사용하여 기본 SunVTS 열에 표시된 SunVTS 패키지 위에 패치를 설치해야 합니다. 필수 패치를 추가하기 전에 이전에 설치한 SunVTS 패키지를 제거하지 마십시오.

patchadd 명령으로 패치 113614-11를 설치하는 것은 이전에 설치한 SunVTS 패키지를 SunVTS5.1ps2 패키지로 대체하는 것과 같습니다.

교체 패키지를 다음 사이트에서 얻을 수 있습니다.
http://www.sun.com/oem/products/vts/

오버레이 패치는 다음 사이트에서 얻을 수 있습니다.
http://sunsolve.sun.com/

참고 – SUNWvcav 패키지를 설치하기 전에 필수 SunVTS 패키지 및 기타 필수 패치를 설치해야 합니다. SUNWvcav 패키지에는 SunVTS 테스트 vcatest가 포함되어 있습니다.

SunVTS 소프트웨어를 통한 vcatest, nettest 및 netlbtest 실행

이러한 진단 테스트의 수행 및 감시 지침은 SunVTS 테스트 참조 설명서, 사용 설명서 및 빠른 참조 안내서를 참조하십시오. 해당 설명서를 http://docs.sun.com에서 Sun Hardware Documentation Set의 Solaris 항목에서 얻을 수 있습니다. 또한 시스템의 Solaris와 함께 배포되는 Solaris Software Supplement CD에도 제공됩니다.

참고 – 필수SunVTS 패키지와 기타 필수 SunVTS 패치를 설치한 경우에만 SunVTS를 사용할 수 있습니다.

▼ vcatest 실행

1. **수퍼유저로 로그인하고 SunVTS를 시작합니다.**

```
# /opt/SUNWvts/bin/sunvts
```

SunVTS 시작에 대한 자세한 지침은 SunVTS 설명서를 참조하십시오.

다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드가 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**

4. **[Cryptography(암호화)]의 확인 상자를 선택하고 Cryptography의 플러스 상자를 선택하여 Cryptography 그룹의 모든 테스트를 표시합니다.**

5. **[Cryptography(암호화)] 그룹에서 `vcatest` 이름이 지정되지 않은 확인 상자를 해제합니다.**

   - `vcatest`가 표시된 경우 6단계로 이동합니다.
   - `vcatest`가 표시되지 않은 경우 [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하고 시스템을 검색하여 vcatest를 찾습니다.

   정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 `vcatest`가 표시되면 6단계로 이동합니다.

6. **`vcatest`의 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

   이 옵션은 `vcatest`에만 해당되며, 117페이지의 "`vcatest`에 대한 테스트 매개 변수 옵션"에서 설명됩니다.

7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한 `vcatest`의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든 `vcatest`의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.

8. **`vcatest`의 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)]을 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.

9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거하고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**

10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**

11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

vcatest에 대한 테스트 매개 변수 옵션

표 7-2는 vcatest 하위 테스트를 설명합니다.

표 7-2 vcatest 하위 테스트

테스트 이름	설명
CDMF	[CDMF bulk encryption(CDMF 대용량 암호)]을 테스트합니다.
DES	[DES bulk encryption(DES 대용량 암호)]을 테스트합니다.
3DES	[3DES Bulk Encryption(3DES 대용량 암호)]을 테스트합니다.
RSA	[RSA Public and Private Keys(RSA 공용 및 개인 키)]를 테스트합니다.
DSA	[DSA Signature Verification(DSA 서명 인증)]을 테스트합니다.
MD5	[MD5 Message Digest/Digital Signature(메시지 요약/디지털 서명)]를 테스트합니다.
SHA1	[SHA1 Digest Key Creation(SHA1 요약 키 생성)]을 테스트합니다.
RNG	난수 생성을 테스트합니다.

vcatest 명령행 구문

CDE 인터페이스 대신 명령행에서 vcatest 실행을 선택할 경우 명령행 문자열에 모든 인수가 지정되어야 합니다.

32비트 모드인 경우 vcatest 경로는 /opt/SUNWvts/bin/입니다. 64비트 모드인 경우 vcatest 경로는 /opt/SUNWvts/bin/sparcv9/입니다.

vcatest에 대한 명령행 인터페이스에서 모든 SunVTS 표준 옵션이 지원됩니다. 테스트와 관련된 옵션은 -o 인수로 지정됩니다.

표준 명령행 인수에 대한 정의는 SunVTS 테스트 참조 설명서를 참조하십시오. vcatest는 [Functional Mode(기능 모드)] 테스트이므로 -f가 포함되어야 합니다. 용도 메시지를 표시하려면 -u를, 자세한 메시지를 표시하려면 -v를 포함합니다. 대괄호 안에 있는 항목은 옵션 항목을 나타냅니다.

다음은 32비트 모드에서 vcatest를 독립형 프로그램으로 호출하는 예제입니다. 다음 명령은 vca0에서 모든 하위 테스트를 수행합니다.

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,tl=all
```

다음은 SunVTS 인프라에서 64비트 모드로 vcatest를 호출하는 예제입니다. 다음 명령은 vca2에서 RSA, DSA 및 MD5를 테스트합니다.

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=RSA+DSA+MD5
```

명령행에서 vcatest를 실행할 때 옵션을 생략하게 되면 표 7-3에 설명된 대로 해당 옵션의 기본 작동이 수행됩니다.

표 7-3 vcatest 명령행 구문

옵션	설명
dev=vca*N*	vca0 또는 vca2와 같이 테스트할 장치의 인스턴스를 지정합니다. 지정되지 않은 경우 기본값인 vca0로 지정됩니다. *N*은 테스트할 장치의 인스턴스 번호 배치를 나타냅니다.
tl=*testlist*	실행할 하위 테스트 목록을 지정합니다. tl의 하위 테스트는 +(플러스) 문자로 구분됩니다. 지원되는 하위 테스트는 CDMF, DES, 3DES, DSA, RSA, MD5, SHA1 및 RNG이기 때문에 tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 명령은 모든 하위 테스트를 활성화합니다. 또는 모든 테스트를 실행하는 tl=all을 입력해도 됩니다. 하위 테스트가 지정되지 않은 경우 기본값인 all이 지정됩니다.

▼ netlbtest 실행

1. 수퍼유저로 로그인하고 SunVTS를 시작합니다.

```
# /opt/SUNWvts/bin/sunvts
```

자세한 시작 지침은 SunVTS 설명서를 참조하십시오.

다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드가 또한 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**
4. **[Network(네트워크)]의 확인 상자를 선택하고 Network의 플러스 상자를 선택하여 Network 그룹의 모든 테스트를 표시합니다.**
5. **[Network(네트워크)] 그룹에서** `vca`*N*`(netlbtest)` **이름이 지정되지 않은 확인 상자를 해제합니다.** *N***은 테스트 중인 장치의 인스턴스 번호 배치를 나타냅니다.**
   - `vca`*N*`(netlbtest)`가 표시된 경우 6단계로 이동합니다.
   - `vca`*N*`(netlbtest)`가 표시되지 않은 경우, [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하고 시스템을 검사하여 vcatest를 찾습니다.

   정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 `vca`*N*`(netlbtest)`가 표시되면 6단계로 이동합니다.
6. **[Intervention Mode(중재 모드)] 단추를 선택합니다.** `vca`*N*`(netlbtest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

   이 옵션은 `netlbtest`에만 해당되며, SunVTS 테스트 참조 설명서에서 설명됩니다.
7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한** `vca`*N*`(netlbtest)`**의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든** `vca`*N*`(netlbtest)`**의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.
8. `vca`*N*`(netlbtest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.
9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거하고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**
10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**
11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

▼ nettest 수행

1. **수퍼유저로 로그인하고 SunVTS를 시작합니다.**

```
# /opt/SUNWvts/bin/sunvts
```

자세한 시작 지침은 SunVTS 사용 설명서를 참조하십시오.

다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드가 또한 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**
4. **[Network(네암호화)]의 확인 상자를 선택하고 Network의 플러스 상자를 선택하여 Network 그룹의 모든 테스트를 표시합니다.**
5. **[Network(네트워크)] 그룹에서** `vca`*N*`(nettest)` **이름이 지정되지 않은 확인 상자를 해제합니다.** *N***은 테스트 중인 장치의 인스턴스 번호 배치를 나타냅니다.**
   - `vca`*N*`(nettest)`이 표시된 경우 6단계로 이동합니다.
   - `vca`*N*`(nettest)`이 표시되지 않은 경우 `vca`*N* 보드를 가진 다른 서버에서 창을 열고 `ifconfig -a`를 입력합니다. 다음과 같은 항목이 나열되어 있어야 합니다.

```
vcaN up inet ip-address plumb
```

앞의 `ifconfig` 항목이 나열되어 있지 않은 경우 `nettest` 검색은 장치를 테스트 부적합으로 간주하기 때문에 인터페이스를 온라인 상태로 전환하려면 `ifconfig` 온라인 매뉴얼 페이지의 지침을 따라야 합니다.

`ifconfig -a`가 위 항목을 생성하면 [SunVTS Diagnostic(SunVTS 진단)] 기본 창으로 돌아간 후 [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하여 `vca`를 찾습니다.

정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 `vca0(nettest)`가 표시되면 6단계로 이동합니다.

6. `vca`*N*`(nettest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

이 옵션은 `nettest`에만 해당되며, SunVTS 테스트 참조 설명서에서 설명됩니다.

7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한** `vca`*N*`(nettest)`**의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든** `vca`*N*`(nettest)`**의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.

8. `vca`*N*`(nettest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.

9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거한 후 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**

10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**

11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

참고 – `nettest`와 `netlbtest` 을 동시에 수행하도록 선택하지 마십시오.

---

kstat를 통한 암호화 작업 결정

Sun Crypto Accelerator 4000 보드에는 보드에서 수행되는 암호화 작업을 나타내는 신호나 기타 표시등이 없습니다. 암호화 작업 요청이 보드에서 실제로 수행되고 있는지를 확인하려면 kstat(1M) 명령을 사용하여 장치 사용 내역을 표시합니다.

```
# kstat vca:0
module: vca                     instance: 0
name:   vca0                    class:    misc
        3desbytes               3040
        3desjobs                5
        crtime                  65.342725895
        dsasign                 0
        dsaverify               0
        rngbytes                10592
        rngjobs                 187
        rngsha1bytes            16328
        rngsha1jobs             327
        rsaprivate              9
        rsapublic               0
        snaptime                106956.467004482
```

참고 – 위 예제에서 0은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 수행하는 보드의 인스턴스 번호를 반영해야 합니다.

kstat 정보 표시는 암호화 요청 또는 "작업"이 Sun Crypto Accelerator 4000 보드로 전송되고 있는지의 여부를 나타냅니다. 시간 경과에 따라 "*작업*" 값이 변하면, 보드가 Sun Crypto Accelerator 4000 보드에 전송된 암호화 작업 요청을 가속화하고 있는 것입니다. 암호화 작업 요청이 보드로 전송되지 않을 경우, 웹 서버의 각 특정 구성별로 웹 서버 구성을 확인하십시오.

kstat(1M)가 반환하는 커널/드라이버 정적 값을 해석하려고 시도하지 마십시오. 이 값은 드라이버 내에 유지되어 필드 지원을 도와 줍니다. 의미와 실제 이름은 시간에 따라 변경됩니다.

참고 – nostats 속성이 /kernel/drv/vca.conf 파일에 정의된 경우 통계의 캡처와 표시는 비활성화됩니다. 이 속성은 트래픽 분석을 방지하는 데 사용될 수 있습니다.

OpenBoot PROM FCode 자가 테스트 사용

시스템이 부팅되지 않은 경우 다음 테스트를 통해 어댑터의 문제를 식별할 수 있습니다.

OpenBoot PROM (OBP) `test` 또는 `test-all` 명령을 사용하여 FCode 자가 테스트 진단을 호출할 수 있습니다. 진단 수행 중 오류가 발생한 경우 이에 대한 적절한 메시지가 나타납니다. `test` 및 `test-all` 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

FCode 자가 테스트는 대부분의 기능을 하위 항목별로 실행하여 다음을 확인합니다.

- 어댑터 보드 설치 중 연결성
- 시스템 부팅에 필요한 모든 구성 요소의 기능 여부 확인

▼ 이더넷 FCode 자가 테스트 진단 수행

이더넷 진단을 수행하려면 우선 재설정을 실행한 후 OBP 프롬프트에서 시스템을 멈추어야 합니다. 시스템을 재설정하지 않은 경우 진단 테스트로 인해 시스템이 중지될 수도 있습니다.

이 항목에서 설명하는 OpenBoot 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

1. **시스템을 종료합니다.**

   *Solaris Handbook for Sun Peripherals*에 설명된 표준 종료 절차를 따릅니다.

2. **OBP 프롬프트에서** `auto-boot?` **구성 변수를** `false`**로 설정합니다.**

```
ok setenv auto-boot? false
```

3. **시스템을 재설정합니다.**

```
ok reset-all
```

4. **show-nets를 입력하여 장치 목록을 표시하고 선택을 입력합니다.**

   어댑터 고유의 장치 목록이 아래 예제와 유사한 형식으로 보일 것입니다.

```
ok show-nets
a) /pci@8,600000/network@1
b) /pci@8,700000/network@5,1
q) NO SELECTION
Enter Selection, q to quit: a
/pci@8,600000/network@1 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y for creating devalias mydev for
/pci@8,600000/network@1
```

참고 – test 명령으로 다음의 자가 테스트를 수행하려면 이더넷 포트가 네트워크에 연결되어 있어야 합니다.

5. **test 명령으로 자가 테스트를 수행합니다.**

   test 명령이 실행되면 다음 테스트가 수행됩니다.

   - vca 레지스터 테스트(diag-switch?가 true인 경우에만 수행됨)
   - 내부 되돌림 테스트
   - 링크 활성화/비활성화 테스트

참고 – 외부 되돌림 케이블을 사용하는 1,000Mbps 연결에 대한 Sun Crypto Accelerator 4000 UTP 어댑터 자가 테스트는 지원되지 않으며, 이것은 링크 클럭을 재조정할 수 없기 때문입니다. 이 테스트를 수행하려면 로컬 및 원격 포트를 클럭 마스터와 클럭 슬레이브로 재조정해야 합니다. 외부 되돌림 케이블이 사용된 경우 로컬 및 원격 포트 모두가 동일합니다. 따라서, 단일 포트가 클럭 마스터와 클럭 슬레이브 모두가 될 수 없어 PHY 연결이 항상 실패하게 됩니다. 1,000Mbps 연결에 대한 Sun Crypto Accelerator 4000 UTP 어댑터 자가 테스트가 수행되려면 원격 1000Base-T 포트를 연결해야 합니다.

다음을 입력합니다.

```
ok test device_path
```

test를 통과하면 다음 메시지가 표시됩니다.

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: 100 Mbps half duplex link up
```

보드가 네트워크에 연결되어 있지 않은 경우, 다음 메시지가 표시됩니다.

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: link down
```

6. 어댑터 테스트 후, 다음을 입력하여 OBP 인터페이스를 표준 운영 모드로 되돌립니다.

```
ok setenv diag-switch? false
```

7. auto-boot? **구성 매개 변수를** true**로 설정합니다.**

```
ok setenv auto-boot? true
```

8. 시스템을 재설정하고 재부팅합니다.

Sun Crypto Accelerator 4000 보드 문제 해결

이 항목은 보드의 문제 해결을 위해 OBP 수준에서 실행 가능한 명령을 설명합니다. 다음 하위 항목에서 설명하는 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

show-devs

Sun Crypto Accelerator 4000 장치가 시스템에 나열되어 있는지 확인하려면 OBP 프롬프트에서 `show-devs`를 입력하여 장치 목록을 표시합니다. 장치 목록에는 Sun Crypto Accelerator 4000 보드와 관련된 행이 아래 예제와 유사하게 표시되어야 합니다.

```
ok show-devs
.
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
.
```

위 예제에서 `/pci@8,600000/network@1` 항목은 Sun Crypto Accelerator 4000 보드로의 장치 경로를 식별합니다. 시스템의 각 보드에 대해 이런 행이 하나씩 있을 것입니다.

.properties

Sun Crypto Accelerator 4000 장치 속성이 정확하게 나열되었는지 확인하려면 OBP 프롬프트에서 .properties를 입력하여 속성 목록을 표시합니다.

```
ok .properties
assigned-addresses        82000810 00000000 00102000 00000000 00002000
                           81000814 00000000 00000400 00000000 00000100
                           82000818 00000000 00200000 00000000 00200000
                           82000830 00000000 00400000 00000000 00100000
d-fru-len                 00 00 00 00
d-fru-off                 00 00 e8 00
d-fru-dev                 eeprom
s-fru-len                 00 00 08 00
s-fru-off                 00 00 e0 00
s-fru-dev                 eeprom
compatible                70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                       00000800 00000000 00000000 00000000 00000000
                           02000810 00000000 00000000 00000000 00002000
                           02000814 00000000 00000000 00000000 00000100
                           02000818 00000000 00000000 00000000 00200000
                           02000830 00000000 00000000 00000000 00100000
address-bits              00 00 00 30
max-frame-size            00 00 40 00
network-interface-type    ethernet
device_type               network
name                      network
local-mac-address         08 00 20 aa bb cc
version                   Sun PCI Crypto Accelerator 4000 1000Base-T Code
2.11 02/10/31
phy-type                  mif
board-model               501-6039
model                     SUNW,pci-vca
fcode-rom-offset          00000000
66mhz-capable
fast-back-to-back
devsel-speed              00000001
class-code                00100000
interrupts                00000001
latency-timer             00000040
cache-line-size           00000010
max-latency               00000040
min-grant                 00000040
subsystem-id              00003de8
subsystem-vendor-id       0000108e
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

watch-net

네트워크 연결을 감시하려면 OBP 프롬프트에서 `apply watch-net` 명령과 장치 경로를 함께 입력합니다.

```
ok apply watch-net /pci@8,600000/network@1
/pci@8,600000/network@1: 1000 Mbps full duplex link up
Watch ethernet packets
'.' is a good packet and 'X' is a bad packet
Press any key to stop
.....X...X......X.....
```

시스템은 오류 없는 패킷을 전송받으면 "."를, 네트워크 하드웨어 인터페이스가 감지할 수 있는 오류를 가진 패킷을 받을 때는 "X"를 표시하여 네트워크 트래픽을 감시합니다.

부록 **A**

사양

본 부록에서는 Sun Crypto Accelerator 4000 MMF 및 UTP 어댑터의 사양을 설명합니다. 다음 항목으로 구성되어 있습니다.

Sun Crypto Accelerator 4000 MMF 어댑터

이 항목은 Sun Crypto Accelerator 4000 MMF 어댑터의 사양을 설명합니다.

커넥터

그림 A-1은 Sun Crypto Accelerator 4000 MMF 어댑터의 커넥터를 설명합니다.

그림 A-1 Sun Crypto Accelerator 4000 MMF 어댑터 커넥터

표 A-1은 SC 커넥터의 특성을 설명합니다(850nm).

표 A-1 SC 커넥터 링크 특성(IEEE P802.3z)

특성	62.5마이크론 MMF	50마이크론 MMF
동작 범위	최대 260m	최대 550m

물리적 크기

표 A-2 물리적 크기

크기	치수	미터 치수
길이	12.283인치	312.00 mm
너비	4.200인치	106.68 mm

성능 사양

표 A-3 성능 사양

기능	사양
PCI 클럭	최대 33/66 MHz
PCI 데이터 버스트 전송률	최대 64바이트 버스트
PCI 데이터/주소 폭	32/64비트
PCI 모드	마스터/슬레이브
1 Gbps, 850 nm	1000 Mbps(전이중)

전력 요구 사항

표 A-4 전력 요구 사항

사양	치수
최대 전력 소모량	6.25 W @ 5V 12.75 W @ 3.3V
전압 안정도	5V +/- 5% 3.3V +/- 5%

인터페이스 사양

표 A-5 인터페이스 사양

기능	사양
PCI 클럭	33 MHz 또는 66 MHz
호스트 인터페이스	33 MHz 또는 66 MHz의 클럭 속도 및 3.3V 또는 5V 전력을 지원하는 PCI 2.1
PCI 버스 너비	32비트 또는 64비트

환경 사양

표 A-6 환경 사양

조건	동작 사양	보관 사양
온도	0° ~+55°C(+32° ~+131°F)	-40° ~+75°C(-40° ~+167°F)
상대 습도	5~85%, 비응축	0~95%, 비응축

Sun Crypto Accelerator 4000 UTP 어댑터

이 항목은 Sun Crypto Accelerator 4000 UTP 어댑터의 사양을 설명합니다.

커넥터

그림 A-2은 Sun Crypto Accelerator 4000 UTP 어댑터에 대한 커넥터를 설명합니다.

그림 A-2 Sun Crypto Accelerator 4000 UTP 어댑터 커넥터

표 A-7은 Sun Crypto Accelerator 4000 UTP 어댑터가 사용하는 Cat-5 커넥터의 특성을 설명합니다.

표 A-7 Cat-5 커넥터 링크 특성

특성	설명
동작 범위	최대 100 m

물리적 크기

표 A-8 물리적 크기

크기	치수	미터 치수
길이	12.283인치	312.00 mm
너비	4.200인치	106.68 mm

성능 사양

표 A-9 성능 사양

기능	사양
PCI 클럭	최대 33/66 MHz
PCI 데이터 버스트 전송률	최대 64바이트 버스트
PCI 데이터/주소 폭	32/64비트
PCI 모드	마스터/슬레이브
1 Gbps, 850 nm	1000 Mbps(전이중)

전력 요구 사항

표 A-10 전력 요구 사항

사양	치수
최대 전력 소모량	6.25 W @ 5V 12.75 W @ 3.3V
전압 안정도	5V +/- 5% 3.3V +/- 5%

인터페이스 사양

표 A-11 인터페이스 사양

기능	사양
PCI 클럭	33 MHz 또는 66 MHz
호스트 인터페이스	33 MHz 또는 66 MHz의 클럭 속도 및 3.3V 또는 5V 전력을 지원하는 PCI 2.1
PCI 버스 너비	32비트 또는 64비트

환경 사양

표 A-12 환경 사양

조건	동작 사양	보관 사양
온도	0° ~+55°C(+32° ~+131°F)	-40° ~+75°C(-40° ~+167°F)
상대 습도	5~85%, 비응축	0~95%, 비응축

부록 **B**

Apache 웹 서버를 위한 SSL 구성 명령

본 부록에서는 Sun Crypto Accelerator 4000 소프트웨어를 사용하여 Apache 웹 서버를 위해 SSL 지원을 구성하는 데 필요한 명령을 설명합니다. 명령을 `http.conf` 파일에 구성합니다. 자세한 내용은 Apache 웹 서버 설명서를 참조하십시오.

1. `SSLPassPhraseDialog exec:`*program*

   컨텍스트: 전역

   이 명령은 Apache 웹 서버에게 키 파일의 암호를 수집하기 위해서 지정된 *program*을 실행하도록 알립니다. *program*은 수집된 암호를 표준 출력으로 인쇄해야 합니다.

   다수의 키 파일이 표시되고 공통 암호가 있을 경우, *program*은 한 번만 실행됩니다 (각각의 수집된 암호는 *program*을 다시 실행하기 전에 이를 사용하여 시도함).

   *program*은 두 개의 인수로 실행되며, 그 첫번째 인수는 서버 이름으로 *서버 이름*:포트의 형식으로 실행됩니다. 예를 들어, `www.fictional-company.com:443` (포트 443은 SSL 기반 웹 서버의 일반 포트)과 같습니다. 두 번째 인수는 키 파일의 키 유형입니다(*keytype*). *keytype*은 RSA 또는 DSA가 될 수 있습니다.

참고 – 이 프로그램은 시스템을 시작하는 동안 실행될 수 있으므로, 콘솔이 `tty` 장치가 아닐 경우(즉, `tty`(3c)가 false를 반환하는 경우)에 대처하도록 설계되었는지 확인하십시오.

   제공된 프로그램인 `/opt/SUNWconn/cryptov2/bin/apgetpass`는 *program* 실행용으로 사용할 수 있습니다. 이 프로그램은 암호 입력 프롬프트를 자동으로 표시하고 입력된 암호가 표시되지 않도록 합니다.

   제공된 `sslpassword` 프로그램은 또한 파일 내에서 암호를 자동으로 검색하여 웹 서버 시작 시 사용자가 관여하지 않은 상태에서 수행될 수 있습니다. 키 파일의 암호는 이름이 `/etc/apache/`*servername*:*port*.*keytype*`.pass`인 파일에서 검색됩니다. 이 파일이 없는 경우 `/etc/apache/default.pass` 파일이 사용됩니다. 이 암호 파일은 암호화되지 않은 암호 자체를 한 행에 담고 있습니다.

참고 – 암호 파일은 웹 서버가 실행하는 UNIX 사용자만이 읽을 수 있도록 권한을 부여하여 보호해야 합니다. 이 사용자는 표준 Apache `User` 명령으로 구성된 사용자와 동일해야 합니다.

지정되지 않은 경우는 기본 작동은 내부 프롬프트 메커니즘을 사용합니다. 시스템 시작 시 상호 작용 문제를 방지하려면 이를 대신 `sslpassword` 프로그램을 사용하십시오.

2. `SSLEngine` (`on`|`off`)

   컨텍스트: 전역, 가상 호스트

   이 명령은 SSL 프로토콜을 활성화합니다. 일반적으로 가상 호스트에서 서버의 하위 집합에 SSL을 활성화하는 데 사용됩니다. 공통적으로 사용되는 형식은 다음과 같습니다.

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

위 구문은 443 포트를 수신하는 모든 서버에 대한 SSL 사용을 구성합니다(표준 HTTPS 포트). 표시되지 않을 경우, 기본적으로 비활성화됩니다.

3. `SSLProtocol [+-]`*protocol*

   컨텍스트: 전역, 가상 호스트

   이 명령은 SSL 트랜잭션을 위해 사용할 프로토콜을 구성합니다. 사용 가능한 프로토콜은 표 B-1에서 나열되어 설명됩니다.

표 B-1 SSL 프로토콜

프로토콜	설명
`SSLv2`	Netscape의 원본 표준 SSL 프로토콜
`SSLv3`	대부분의 웹 브라우저에서 지원되는 SSL 프로토콜의 업데이트 버전
`TLSv1`	최소 브라우저 지원을 통해 현재 IETF 표준화를 수행 중인 `SSLv3`로 업데이트
`all`	모든 프로토콜 활성화

플러스(+) 또는 마이너스(-) 기호를 사용하여 프로토콜을 추가하거나 제거할 수 있습니다. 예를 들어, SSLv2에 대한 지원을 비활성화하려면 다음 명령을 사용할 수 있습니다.

```
SSLProtocol all -SSLv2
```

위 구문은 다음과 동일합니다.

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

   SSLCipherSuite 명령은 사용 가능한 SSL 암호와 이들의 선호 설정을 구성할 때 사용됩니다. 전체 컨텍스트 또는 가상 호스트 컨텍스트에서는 이 명령은 초기 SSL 핸드셰이크 중 사용됩니다. 디렉토리별 컨텍스트에서는 SSL 재교섭을 강제로 수행하여 이름이 지정된 암호를 사용합니다. 재교섭은 요청을 읽고 응답을 보내기 전 사이에 이루어집니다.

   *cipher-spec*은 표 B-2에 설명되어 있는 콜론으로 구분된 암호 목록입니다. 표 B-2에서 DH는 Diffie-Hellman을 의미하며, DSS는 Digital Signature Standard를 의미합니다.

표 B-2 사용 가능한 SSL 암호

암호-태그	프로토콜	키 교환	승인	암호화	MAC	유형
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168비트)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168비트)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR(128비트)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR(128비트)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR(128비트)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO(128비트)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56비트)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR(64비트)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56비트)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA(512비트)	RSA	DES(40비트)	SHA1	내보내기
EXP-RC2-CBC-MD5	SSLv2	RSA(512비트)	RSA	ARCTWO(40비트)	SHA1	내보내기
EXP-RC2-CBC-MD5	SSLv3	RSA(512비트)	RSA	ARCTWO(40비트)	SHA1	내보내기
EXP-RC4-MD5	SSLv3	RSA(512비트)	RSA	ARCFOUR(40비트)	MD5	내보내기
EXP-RC4-MD5	SSLv2	RSA(512비트)	RSA	ARCFOUR(40비트)	MD5	내보내기

표 B-2 사용 가능한 SSL 암호*(계속)*

암호-태그	프로토콜	키 교환	승인	암호화	MAC	유형
NULL-SHA	SSLv3	RSA	RSA	없음	SHA1	
NULL-MD5	SSLv3	RSA	RSA	없음	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	없음	3DES(168비트)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	없음	DES(56비트)	SHA1	
ADH-RC4-MD5	SSLv3	DH	없음	ARCFOUR(128비트)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168비트)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168비트)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES(56비트)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES(56비트)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH(512비트)	RSA	DES(40비트)	SHA1	내보내기
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH(512비트)	DSS	DES(40비트)	SHA1	내보내기
EXP-ADH-DES-CBC-SHA	SSLv3	DH(512비트)	없음	DES(40비트)	SHA1	내보내기
EXP-ADH-RC4-MD5	SSLv3	DH(512비트)	없음	ARCFOUR(40비트)	MD5	내보내기

표 B-3에서는 매크로와 유사한 그룹화를 제공하는 별칭을 설명합니다.

표 B-3 SSL 별칭

별칭	설명
SSLv2	모든 SSL 버전 2.0 암호
SSLv3	모든 SSL 버전 3.0 암호
EXP	모든 내보내기 수준의 암호
EXPORT40	모든 40비트의 내보내기 암호
EXPORT56	모든 56비트의 내보내기 암호
LOW	강도가 낮은 암호(DES, 40비트 RC4)
MEDIUM	모든 128비트 암호
HIGH	3중 DES를 사용하는 모든 암호
RSA	RSA 키 교환을 사용하는 모든 암호
DH	Diffie-Hellman 키 교환을 사용하는 모든 암호

표 B-3 SSL 별칭 *(계속)*

별칭	설명
EDH	Ephemeral Diffie-Hellman 키 교환을 사용하는 모든 암호
ADH	익명의 Diffie-Hellman 키 교환을 사용하는 모든 암호
DSS	DSS 인증을 사용하는 모든 암호
NULL	암호화를 사용하지 않는 모든 암호

암호의 선호도는 표 B-4에 나열하고 설명한 특수 문자를 사용하여 구성할 수 있습니다.

표 B-4 암호 선호도를 구성하기 위한 특수 문자

문자	설명
<없음>	목록에 암호 추가
!	전체 목록에서 암호 제거 — 다시 추가할 수 없음
+	암호를 목록에 추가하고 현재 위치로 끌어냄(암호 강등)
-	목록에서 암호 제거(나중에 추가 가능)

cipher-spec 의 기본값은 다음과 같습니다.

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

기본값은 익명(인증되지 않은) Diffie-Hellman을 제외한 모든 암호를 구성하고 ARCFOUR 및 RSA에 선호도를 부여하여 낮은 수준에 대해 더 높은 수준의 암호화를 제공합니다.

5. `SSLCertificateFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 명령는 서버에 대한 PEM 암호화 X.509 인증 파일의 위치를 지정합니다.

6. `SSLCertificateKeyFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 명령는 서버에 대한 PEM 암호화 개인 키 파일을 지정하며, 이는 `SSLCertificateFile` 명령으로 구성된 인증서에 해당합니다.

7. `SSLCertificateChainFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 명령은 서버의 인증 경로를 만드는 PEM 암호화 인증서를 포함하는 파일의 위치를 지정합니다. 서버 인증서가 클라이언트가 인식하는 기관에 의해 직접 서명되지 않은 경우, 명령을 사용하여 클라이언트가 서버 인증서를 확인하도록 도울 수 있습니다.

   클라이언트 인증(`SSLVerifyClient`)을 사용할 때 체인에 있는 인증서 역시 클라이언트 인증에 유효합니다.

8. `SSLCACertificateFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 명령은 클라이언트 인증에 사용된 인증 기관(CA)에 대해 일련의 인증서를 포함하는 파일의 위치를 지정합니다.

9. `SSLCARevocationFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 명령은 클라이언트 인증에 사용된 일련의 CA 인증 거부 목록을 포함하는 파일의 위치를 지정합니다.

10. `SSLVerifyClient` *level*

    컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

    이 명령은 서버에 클라이언트 인증을 구성합니다(일반적으로 전자상거래 응용 프로그램에 꼭 필요하지는 않지만 기타 응용 프로그램에서 사용됨).

    *level*에 대한 값은 표 B-5에서 나열하고 설명합니다.

표 B-5 SSL 검증 클라이언트 레벨

레벨	설명
`none`	클라이언트 인증서 필요 없음
`optional`	클라이언트는 유효한 인증서 제공 가능
`require`	클라이언트는 *반드시* 유효한 인증서를 제공해야 함
`optional_no_ca`	클라이언트가 인증서를 제공할 수 있으나 유효할 필요 없음

일반적으로 `none` 또는 `require`가 사용됩니다. 기본값은 `none`입니다.

11. `SSLVerifyDepth` *depth*

    컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

    이 명령은 클라이언트 인증에 대해 서버가 허용하는 인증서 체인의 최대 깊이를 지정합니다. 값이 0인 경우 자체 서명된 인증서가 적합함을 의미하며, 값이 1인 경우 클라이언트 인증서가 서버에 직접 알려진 CA에 의해 서명되어야 함을 의미합니다 (`SSLCACertificateFile`을 통해서). 그 이상의 값은 CA의 위임을 허용합니다.

12. `SSLLog` *filename*

    컨텍스트: 전역, 가상 호스트

    이 명령은 SSL 관련 정보가 기록될 로그 파일을 지정합니다. 지정(기본값)되지 않을 경우, SSL 관련 정보가 기록되지 않습니다.

13. `SSLLogLevel` *level*

    컨텍스트: 전역, 가상 호스트

    이 명령은 SSL 로그 파일에 기록된 정보의 상세 정도를 지정합니다. *level*에 대한 값은 표 B-6에서 나열하고 설명합니다.

표 B-6 SSL 로그 레벨 값

값	설명
`none`	기록되지는 않지만 오류 메시지는 표준 Apache 오류 로그로 전송됩니다.
`warn`	경고 메시지를 포함합니다.
`info`	정보 메시지를 포함합니다.
`trace`	추적 메시지를 포함합니다.
`debug`	디버그 메시지를 포함합니다.

14. `SSLOptions` [`+-`] *option*

    컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

    이 명령은 디렉토리를 기준으로 SSL 실행 시간 옵션을 구성합니다. 플러스 기호(+)를 앞에 붙여 현재 구성에 옵션을 추가하거나 마이너스 기호(-)를 사용하여 제거할 수 있습니다. 여러 옵션을 디렉토리에 적용할 수 있는 경우 가장 제한적인 옵션이 사용되며, 옵션은 결합되지 않습니다.

표 B-7에서 옵션을 나열하고 설명합니다.

표 B-7 사용 가능한 SSL 옵션

옵션	설명
`StdEnvVars`	SSL 관련 CGI/SSI 환경 변수의 표준 집합을 생성합니다. 이에 따라 성능이 저하될 수 있습니다.
`ExportCertData`	`SSL_SERVER_CERT`, `SSL_CLIENT_CERT` 및 `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) 환경 변수를 내보냅니다. 이 변수는 클라이언트 및 서버에 대하 PEM 암호화 인증서를 포함합니다.
`FakeBasicAuth`	클라이언트 인증서의 고유 이름(DN)은 HTTP 기본 인증 사용자 이름으로 전환되며 인증된 것처럼 "가장"합니다. 이로 인해 암호에 대한 사용자 입력 없이 SSL 클라이언트 인증으로 표준 Apache 액세스 제어 메커니즘을 사용할 수 있습니다. Apache 암호 파일에서 사용자 항목으로 암호화된 암호 `xxj31ZMTZzkVA`를 사용해야 합니다. 이 암호는 단지 "password"라는 단어의 암호화된 형식(`crypt`(3c))입니다.
`StrictRequire`	`Satisfy Any`와 같은 SSLRequireSSL을 무시하는 명령이 있다 하더라도 `SSLRequireSSL`로 인해 강제로 금지된 액세스가 거부되도록 합니다.

15. `SSLRequireSSL`

컨텍스트: 디렉토리, `.htaccess`

이 명령은 HTTPS를 사용하지 않으면 해당 디렉토리에 액세스하는 것을 금지합니다. 이 명령을 사용하여 디렉토리의 내용이 인증되지 않고 암호화되지 않은 액세스에 노출될 수 있는 잘못된 구성으로부터 보호하는 데 사용합니다.

부록 **C**

Sun Crypto Accelerator 4000 보드와 함께 사용할 응용 프로그램 구축

본 부록은 Sun Crypto Accelerator 4000과 함께 제공된 소포트웨어를 설명하며, 이를 Sun Crypto Accelerator 4000 보드의 암호 가속화 기능을 활용하기 위해 OpenSSL 호환 응용 프로그램을 구축하는 데 사용할 수 있습니다. 모든 OpenSSL 응용 프로그램을 이러한 방식(`www.openssl.org`에서 다운로드할 수 있는 OpenSSL 라이브러리로 구축하는 방법과는 달리)으로 컴파일할 수 있는 것은 아닙니다.

참고 – Sun Crypto Accelerator 4000 소프트웨어 및 하드웨어를 사용하기 위한 응용 프로그램의 구축에 대한 정보는 오직 있는 그대로 제공되며 이 제품에서 공식적으로 지원받은 부분이 아닙니다. 이 정보는 고객의 편리를 위한 목적으로 보증 없이 제공됩니다. Sun이 지원하는 솔루션이 필요할 경우, Sun Professional Services에 문의하여 옵션에 대한 정보를 받으십시오.

먼저 필요한 헤더 파일 및 라이브러리가 포함된 `SUNWkcl2o` 패키지를 설치해야 합니다.

다음과 같이 `/opt/SUNWconn/crypto/include`에서 컴파일러 플래그와 함께 OpenSSL 헤더를 포함하도록 응용 프로그램을 구성해야 합니다.

```
-I/opt/SUNWconn/cryptov2/include
```

또한, 적절한 라이브러리에 참조 파일이 포함되도록 링커를 지정해야 합니다. 대부분의 OpenSSL 호환 응용 프로그램은 `libcrypto.a` 및 `libssl.a` 라이브러리 중 하나 또는 두 가지 모두 참조합니다. Sun 암호화 라이브러리도 반드시 포함되야 합니다. 다음 링커 속성은 이를 수행합니다.

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \
-lcrypto -lssl -lkcl
```

부록 **D**

소프트웨어 라이센스

본 부록에서는 Sun 이진 코드 라이센스 계약서와 타사 소프트웨어 통지 및 라이센스 조항을 설명합니다.

참고 – 본 부록에서 제공하는 타사 라이센스 및 통지는 해당 소프트웨어 라이센스 및 통지 소유업체가 제공하는 바와 일치합니다.

Sun Microsystems, Inc.

이진 코드 라이센스 계약서

본 소프트웨어 매체의 포장을 개봉하기 전에 본 계약서 및 별도로 제공되는 '라이센스 약정서 추록'(이하 양자를 통칭하여 "본 계약"이라고 합니다.)의 모든 조항을 자세히 읽으십시오. 사용자인 귀하(이하 "귀하")께서 소프트웨어 매체의 포장을 개봉하면 본 계약의 모든 조항에 동의하는 것으로 간주됩니다. 귀하가 본 소프트웨어에 전자적으로 접근하고 있는 경우에는 본 계약서 문구의 최하단에 있는 "동의" 단추를 눌러 본 계약에 대한 승인을 표시해야 합니다. 귀하께서 본 계약에 동의하지 않는다면, 본 소프트웨어를 사용하지 않은 채로 구입처에 즉시 반환하여 환불을 받으시고, 만약 본 소프트웨어에 전자적으로 접근하고 있는 경우에는 이 계약서 문구의 최하단에 있는 "동의 안함" 단추를 누르십시오.

1. 사용허락의 범위. Sun은 귀하에게 Sun이 제공하는 본 소프트웨어와 설명서 및 모든 오류 수정 프로그램(이하 "소프트웨어")에 대해 내부 전용으로만 사용할 수 있는 독점적이고 양도 불가능한 라이센스를 부여하되, 이는 해당요금을 지불한 만큼의 사용자 수와 컴퓨터 하드웨어 등급에 국한된 것입니다.

2. 제한 사항. 본 소프트웨어의 내용은 기밀이며 저작권의 보호를 받습니다. 본 소프트웨어에 대한 권리 및 이에 관련된 모든 지적재산권은 'Sun'과 'Sun'에 대한 해당 라이센스 제공자가 보유합니다. '라이센스 약정서 추록'에서 특별히 승인된 경우를 제외하고는, (비상)보관용 복사본 1부를 만드는 경우 이외에 본 소프트웨어의 복사본을 제작해서는 안됩니다. 관련 법령에 의해 허용되는 경우를 제외하고는 본 소프트웨어를 수정하거나, 역 컴파일(Decompiling) 또는 역설계(Reverse Engineering)하여서는 안됩니다. 귀하는 본 소프트웨어가 핵 시설의 설계나 건설, 작동, 유지 보수 등에 사용할 목적으로 의도되거나 고안 또는 사용허락 되지 않았음을 알고 있습니다. 따라서 Sun은 본 소프트웨어가 이러한 용도에 적합하다는 점에 대해서는 어떠한 명시적 또는 묵시적 보증을 하지 않습

니다. 본 계약의 체결로 인하여, Sun과 Sun에 대한 라이센스 제공자의 어떠한 상표, 서비스 마크, 로고 또는 상호 등에 대한 권리나 권한 기타 권익도 귀하에게 허용되거나 부여되는 것이 아니라는 점을 유의하십시오.

3. 제한 보증. Sun은 영수증 사본으로 증명되는 제품 구매일로부터 90일 동안, 정상적인 사용조건 하에서는 본 소프트웨어를 장착한 매체가 재료 및 제조기술과 관련하여서는 결함이 없음을 보증합니다. 이를 제외하고는 본 소프트웨어는 "있는 그대로" 제공됩니다. 이렇듯 제한적인 보증 하에서 귀하가 받을 수 있는 보상의 한도, 즉 Sun이 부담하여야 할 책임의 전부는 Sun의 선택에 따라 귀하에게 본 소프트웨어의 매체를 교환하여 드리거나 또는 귀하가 본 소프트웨어를 구매할 때 지급한 비용을 귀하에게 환불하여 드리는 것에 국한됩니다.

4. 보증의 부인. SUN은 본 계약서에 명시하지 않은 경우, 상품성의 묵시적 보증 및 특정 목적 또는비침해성에 대한 적합성을 포함한 일체의 명시적 또는 묵시적 조건, 진술 및 보증에 대해책임을 지지 않습니다. 이러한 보증의 부인은 법적으로 허용된 범위 내에서만 적용됩니다.

5. 책임의 제한. SUN 또는 그에 대한 라이센스 제공자는 법이 허용하는 한도 내에서는, 어떠한 경우에도, 설사 SUN이 그러한 손해의 발생 가능성을 사전에 고지받았다고 할지라도, '법적 책임'에 관한 여하한 이론에 상관없이, 본 소프트웨어의 사용 또는 사용 불가능으로부터 비롯되거나 관련되어 발생하는 데이터나 금전적 수익의 손실 또는 특정손해, 간접손해, 결과적 손해, 부수적 손해, 또는 징벌적 손해 등에 관한 배상책임을 지지 않습니다. 귀하에 대한 Sun의 책임은 계약이나 불법행위(과실 포함) 등 기타 어떠한 것에 근거한 것인지에 관계 없이, 어떠한 경우라도 본 계약에 따라 귀하가 본 소프트웨어에 대해 지불한 금액을 초과할 수는 없습니다. 이와 같은 제한은 앞에서 규정한 보증에 관한 사항들이 그 본질적인 목적을 달성하지 못하는 경우에도 적용됩니다.

6. 계약의 종료. 본 계약은 종료될 때까지 유효합니다. 귀하는 언제라도 본 소프트웨어의 모든 사본을 폐기함으로써 본 계약을 종료할 수 있습니다. 귀하가 본 계약의 제반 규정을 준수하지 않는 경우, Sun의 통지가 없더라도 즉각 본 계약은 종료됩니다. 본 계약이 종료되는 경우, 귀하는 본 소프트웨어의 모든 사본을 폐기해야 합니다.

7. 수출의 제한. 본 계약에 의해 제공되는 모든 소프트웨어 및 기술 데이터는 미국의 수출 제한 관련 법규의 적용을 받으며, 기타 다른 국가로부터 수출 및 수입의 규제를 받을 수 있습니다. 귀하는 이러한 모든 해당 법규 및 제한 규정을 엄격히 준수할 것에 동의하며, 본 제품이 귀하에게 인도된 이후 필요한 수출, 재수출 또는 수입과 관련한 허가의 취득은 귀하의 책임임을 인정합니다.

8. 미 정부의 권리제한. 미국 정부 또는 미국 정부의 주계약자나 그 하도급업체(하도급의 단계는 불문함)가 본 소프트웨어를 구입한 경우에도, 본 소프트웨어 및 관련 설명서에 대한 정부의 권리는 본 계약에 규정되어 있는 조건 및 규정에 국한됩니다. 이는 48 C.F.R.227.7201부터 227.7202-4에 나와 있는 규정(미국 국방성(DOD) 취득물에 관한 규정)과 48 C.F.R.2.101 및 12.212 규정(미국 국방성(DOD) 이외의 취득에 관한 규정)에 의거한 것입니다.

9. 적용법규. 본 계약과 관련된 모든 소송은 캘리포니아주 법령과 미 연방 법령의 적용을 받습니다. 기타 사법권의 여하한 섭외사법 규정은 적용되지 않습니다.

10. 규정의 분리성. 본 계약의 어떤 규정이 실행될 수 없는 경우, 당해 조항을 제외한 본 계약의 나머지 규정은 그대로 유효합니다. 당해 조항의 제외로 인해 본 계약의 목적을 달성하지 못하게 되는 경우에는 본 계약이 즉시 종료됩니다.

11. 통합. 본 계약은 귀하와 Sun 사이의 본 제품에 관한 합의 사항의 전부입니다. 본 계약은 양 당사자 사이에서 현재 혹은 그 이전에 구두 또는 서면으로 이루어진 의사교류, 제안, 진술 및 보증사항 등에 우선하며, 본 계약 기간 중 본 제품에 대하여 양 당사자 사이에 발생하는 인용, 명령, 인지 또는 기타 의사교류에 관한 분쟁이나 추가적인 규정에 우선합니다. 양 계약 당사자의 공인된 대표자에 의한 서면 합의와 서명이 없는 한, 본 계약의 수정은 법적 구속력이 없습니다.

의문 사항이 있으면 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054로 문의하시기 바랍니다.

(양식 ID#011801)

Sun Microsystems, Inc.

Sun Crypto Accelerator 4000에 대한 추가 조항

Sun Crypto Accelerator 4000에 대한 본 추가 조항은 Binary Code 라이센스 계약("BCL")을 보충합니다. 여기서 정의되지 않은 대문자로 시작하는 조항은 BCL의 해당 의미로 간주합니다. 이 추가 조항은 BCL의 불일치되거나 모순되는 조항보다 우선합니다. 소프트웨어의 사용은 여기서 보충하는 BCL의 수용을 의미합니다.

1. 타사 라이센스 조항. 소프트웨어의 일부는 사용을 관할하는 타사로부터 통지 및/또는 라이센스를 제공받습니다.

Third Party License Terms

OPENSSL LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

``Ian Fleming was a UNIX fan!
How do I know? Well, James Bond
had the (license to kill) number 007,
i.e. he could execute anyone.''
-- Unknown

MOD_SSL LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

부록 **E**

매뉴얼 페이지

본 부록에서는 Sun Crypto Accelerator 4000 보드 명령을 설명하고 각 명령에 대한 온라인 매뉴얼 페이지를 나열합니다. 본 부록에 수록된 명령은 Sun Crypto Accelerator 4000 소프트웨어에 포함되어 있습니다.

다음 명령을 입력하여 온라인 매뉴얼 페이지를 볼 수 있습니다.

```
man -M /opt/SUNWconn/man page
```

표 E-1은 사용 가능한 온라인 매뉴얼 페이지를 설명합니다.

표 E-1 Sun Crypto Accelerator 4000 온라인 매뉴얼 페이지

man 페이지	설명
vca(7d)	vca 장치 드라이버는 내장된 하드웨어 암호 가속기에 액세스 제어를 제공하는 리프 드라이버입니다. vca 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어가 필요합니다.
vcad(1m)	vcad 데몬은 키스토어 서비스를 제공합니다.
vcaadm(1m)	vcaadm은 Sun Crypto Accelerator 4000의 관리 프로그램입니다. vcaadm 명령은 Sun Crypto Accelerator 4000 보드과 관련된 구성, 계정 및 키 데이터베이스를 수동으로 관리하는 데 사용됩니다. vcaadm은 민감한 암호화 키 정보를 처리합니다.
vcadiag(1m)	vcadiag를 통해 루트 사용자는 Sun Crypto Accelerator 4000 보드를 재설정하고 키 요소를 초기 상태로 복원합니다. 또한, 루트 사용자는 이를 사용하여 기본 진단을 수행할 수도 있습니다.
kcl2(7d)	kcl2은 암호화 하드웨어 드라이버를 지원하는 커널 모듈입니다.

표 E-1 Sun Crypto Accelerator 4000 온라인 매뉴얼 페이지 *(계속)*

man 페이지	설명
kcl2(7d)	kcl2 장치 드라이버는 Sun 암호화 프로바이더 드라이버를 지원하는 대량의 스레드를 갖춘 로드 가능 커널 모듈입니다. kcl2 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어가 필요합니다.
apsslcfg(1m)	apsslcfg는 Apache 웹 서버용 구성 유틸리티입니다.
iplsslcfg(1m)	iplsslcfg는 Sun ONE 웹 서버용 구성 유틸리티입니다.

부록 **F**

하드웨어 원상 복구

본 부록에서는 Sun Crypto Accelerator 4000 보드를 보드의 `failsafe` 모드인 출고 상태로 복구하는 방법을 설명합니다.

주의 – 본 부록에서 설명하는 절차는 반드시 필요한 경우에만 사용해야 합니다. `vcaadm`의 `zeroize` 명령은 모든 키 요소를 제거해야 하는 경우에 적합합니다. `zeroize` 명령에 대한 자세한 내용은 75페이지의 "Sun Crypto Accelerator 4000 보드 원상 복구"를 참조하십시오. 또한 모든 키 요소 삭제에 대해서는 `vcadiag`(4)의 온라인 매뉴얼 페이지를 참조하십시오.

참고 – 본 부록에서 설명하는 절차는 Sun Crypto Accelerator 4000 펌웨어를 제거합니다. Sun Crypto Accelerator 4000 소프트웨어와 함께 제공된 펌웨어를 다시 설치해야 합니다.

Sun Crypto Accelerator 4000 하드웨어를 출고 상태로 초기화

어떤 경우에는 보드를 `failsafe` 모드로 복구하고 모든 키 요소와 구성 정보를 삭제해야 할 때가 있습니다. 이 작업은 보드에 달린 하드웨어 점퍼를 통해서만 수행할 수 있습니다.

참고 – `vcaadm` 유틸리티와 `zeroize` 명령을 사용하여 Sun Crypto Accelerator 4000 보드에서 모든 키 요소를 제거할 수 있습니다. 그러나 `zeroize` 명령은 업데이트된 펌웨어를 보존합니다. 75페이지의 "Sun Crypto Accelerator 4000 보드 원상 복구"를 참조하십시오. 또한 `vcadiag` 온라인 매뉴얼 페이지도 참조하십시오.

▼ 하드웨어 점퍼를 통한 Sun Crypto Accelerator 4000 보드 원상 복구

1. **시스템 전원을 끕니다.**

참고 – 일부 시스템에서는 본 절차에 대해 전원을 끄는 대신에 동적 재구성(DR)을 통해 필요한 보드를 제거하고 교체할 수 있습니다. 적절한 DR 절차는 시스템과 함께 제공된 설명서를 참조하십시오.

주의 – 점퍼를 조정하는 동안 보드에 전력이 공급되면 안됩니다.

---

2. **컴퓨터 덮개를 제거하여 보드의 상단 중앙에 있는 점퍼에 접근합니다.**

3. **점퍼를 점퍼 블록의 0 및 1 핀에 끼웁니다.**

   0과 1 핀은 브래킷에서 가장 가까운 핀이며 "Z"로 표시되어 있습니다. 2핀씩 4조로 구성되어 있으며 점퍼는 그림 F-1에서처럼 0과 1에 끼워야 합니다.

주의 – 0과 1 핀에 점퍼를 끼우면 Sun Crypto Accelerator 4000 보드를 사용할 수 없습니다.

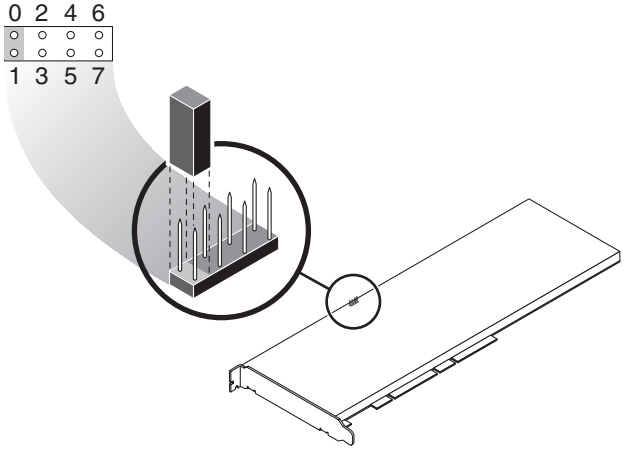

그림 F-1 Sun Crypto Accelerator 4000 보드 점퍼 블록 핀

4. **시스템을 켭니다.**

주의 – Sun Crypto Accelerator 4000 보드 점퍼를 조정한 후 시스템의 전원을 켜면 모든 펌웨어, 키 요소 및 구성 정보가 삭제됩니다. 이 절차를 통해 보드는 출고 상태로 복구되고 `failsafe` 모드로 전환됩니다.

5. **시스템 전원을 끕니다.**
6. **점퍼 블록의 0과 1핀에서 점퍼를 제거하고 점퍼를 원래 위치에 보관합니다.**
7. **시스템을 켭니다.**
8. **`vcaadm`으로 Sun Crypto Accelerator 4000 보드에 연결합니다.**

   `vcaadm` 프롬프트가 나타나면 펌웨어 업그레이드 경로를 입력합니다.
9. **펌웨어 설치 경로로 `/opt/SUNWconn/cryptov2/firmware/sca4000fw`를 입력합니다.**

   펌웨어가 자동 설치되고 `vcaadm`에서 로그아웃됩니다.
10. **`vcaadm`으로 Sun Crypto Accelerator 4000 보드에 다시 연결합니다.**

    `vcaadm` 프롬프트는 새 키스토어로 보드를 초기화할 것인지, 기존 키스토어로 초기화할 것인지를 묻습니다. 61페이지의 "`vcaadm`을 통한 Sun Crypto Accelerator 4000 보드 초기화"를 참조하십시오.

부록 **G**

자주 재기되는 질문(FAQ)

재부팅할 때 사용자 상호 작용없이 시작하게 하려면 웹 서버를 어떻게 구성해야 합니까?

암호화된 키를 통해 Sun ONE 및 Apache 웹 서버가 재부팅 시 사용자 입력없이 시작할 수 있도록 활성화할 수 있습니다.

▼ 재부팅 시 Apache 웹 서버의 자동 시작을 위한 암호화 키 생성

1. **`httpd.conf` 파일에 다음 항목이 있는지 확인합니다.**

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

이 명령은 `/etc/apache` 디렉토리에서 암호로 보호된 파일을 검색하여 암호를 회수합니다.

2. **다음 파일 이름 규칙에 따라 `/etc/apache` 디렉토리의 암호만을 담은 암호 파일을 생성합니다.**

```
server_name:port.KEYTYPE.pass
```

- *server_name* — `httpd.conf` 파일의 "ServerName" 명령에 입력한 값.
- *port* — 해당 SSL 서버가 실행될 포트(예: 443)
- *KEYTYPE* — `RSA` 또는 `DSA`

예제: 이름이 `webserv101`이고 `RSA` 키로 443 포트에서 SSL을 실행하는 서버에 대해서는 `/etc/apache`에 다음 파일을 생성합니다.

```
webserv101:443.RSA.pass
```

암호 파일의 권한과 소유를 다음과 같이 변경하는 것이 좋습니다.

```
# chmod 400 server_name:port.KEYTYPE.pass
# chown root server_name:port.KEYTYPE.pass
```

자세한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

▼ 재부팅 시 Sun ONE 웹 서버의 자동 시작을 위한 암호 키 생성

1. **Sun ONE 웹 서버 인스턴스의** `config` **하위 디렉토리로 이동합니다. 예:** `/usr/iplanet/servers/https-`***webserver_instance_name***`/config`**.**

2. **다음 행만을 포함한** `password.conf` **파일을 생성합니다(암호 정의는** 표 5-1**을 참조하십시오):**

```
internal:trust_db_password
keystore_name:username:password
```

3. **암호 파일의 파일 소유를 서버가 운영하는 UNIX 사용자 ID로 설정하고 파일 소유자만이 읽을 수 있도록 권한을 설정합니다.**

```
# chown web_server_UNIX_user_ID password.conf
# chmod 400 password.conf
```

같은 서버에 설치한 여러 보드에 다른 MAC 주소를 할당하는 방법은 무엇입니까?

한 서버의 여러 보드에 다른 MAC 주소를 할당하는 두 가지 방법이 있습니다. 첫 번째 방법은 운영 환경 수준에서, 두 번째 방법은 OpenBoot PROM (OBP) 수준에서 수행됩니다.

▼ 터미널 창에서 다른 MAC 주소 할당

1. **다음 명령을 입력합니다.**

```
# eeprom "local-mac-address?"=true
```

참고 – local-mac-address? 매개 변수를 true로 설정된 경우 모든 비통합 네트워크 인터페이스 장치는 제조 설비에서 제품에 할당된 로컬 MAC 주소를 사용합니다.

2. **시스템을 재부팅합니다.**

▼ OpenBoot PROM 수준에서 다른 MAC 주소 할당

1. **OBP 프롬프트에서 다음 명령을 입력합니다.**

```
ok setenv local-mac-address? true
```

참고 – local-mac-address? 매개 변수를 true로 설정된 경우 모든 비통합 네트워크 인터페이스 장치는 제조 설비에서 제품에 할당된 로컬 MAC 주소를 사용합니다.

2. **운영 환경을 부팅합니다.**

Sun Crypto Accelerator 4000 소프트웨어를 설치한 후 Apache와 함께 사용하도록 Sun Crypto Accelerator 1000을 구성하는 방법은 무엇입니까?

SUNWkcl2a 소프트웨어 패키지가 설치되면 시스템은 Apache 웹 서버 mod_ssl 1.3.26로 구성됩니다.

Apache로 Sun Crypto Accelerator 1000을 구성하려면 다음 패치를 설치해야 합니다.

SUNWkcl2a 패키지가 설치된 Solaris 8 시스템에서 Apache 1.3.26을 Sun Crypto Accelerator 1000과 함께 구성하려면 다음 패치가 필요합니다.

- Apache 1.3.26 — 패치 ID 109234-09 이상
- Sun Crypto Accelerator 1000 버전 1.0 소프트웨어 — 패치 ID 112869-02
- Sun Crypto Accelerator 1000 버전 1.1 소프트웨어 — 패치 ID 113355-01

SUNWkcl2a 패키지가 설치된 Solaris 9 시스템에서 Apache 1.3.26을 Sun Crypto Accelerator 1000과 함께 구성하려면 다음 패치가 필요합니다.

- Apache 1.3.26 — 패치 ID 113146-01 이상
- Sun Crypto Accelerator 1000 버전 1.1 소프트웨어 — 패치 ID 113355-01

테스트를 위해 인증서에 자가 서명하는 방법은 무엇입니까?

이 절차에 대해서는 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

색인

심볼

숫자

A

P

R

S

T

U

V

W

ㅂ

ㅅ