지능형 콘솔 관리 서버

VTS II 시리즈

사용 설명서

버전 **1.1.2**

2007-05-07

VTS II 시리즈 사용 설명서

버전 v1.1.2

펌 웨어 버전 v1.1.1

Printed in Korea

등록 상표

Windows®는 Microsoft 사의 등록 상표입니다.

Ethernet®은 XEROX 사의 등록 상표입니다.

사용자 고지

시스템 결함으로 인한 손상, 사망 또는 재산상의 손해를 보호하기 위해, 적정한 백업 시스템과 필수 안전 장치는 필수적 입니다. 시스템 고장으로 인한 결과에 대한 보호는 사용자 책임입니다. 본 장치는 생명 유지 또는 의료 시스템으로서는 사용 승인을 받지 않은 제품입니다.

본 기기에 대하여 세나테크놀로지의 서면 허가 없이 이루어진 변경 또는 개조에 대해 세나테크놀로지는 책임을 지지 않습니다.

기술 지원

세나테크놀로지

서울시 서초구 양재동 210번지

137-130, 대한민국

전화: (02) 573-7772

팩스: (02) 573-7710

email: support.kr@sena.com

웹 사이트: http://www.sena.co.kr

개정 요약

Revision	Date	Name	Description
V1.0.1	**2006-09-30**		Initial Release
V1.1.0	**2007-03-02**	**M. W. Lee**	Firmware v1.1.0 update reflected
V1.1.1	**2007-03-08**	**JOJ**	Firmware v1.1.1 update reflected
V1.1.2	**2007-05-07**	**H.R. Zo**	오타 수정

목 차

1: 서론

1.1 개요

VTS II는 임베디드 Linux 기반 지능형 콘솔 관리 서버입니다. 이 제품은, Linux 상에서 구현된 각종 최신 프로토콜을 구비하고 있으며, 1개의 PC 카드 인터페이스 슬롯과 1개의 USB 인터페이스 슬롯을 지원하고 Perl 스크립트 엔진과 16M의 사용자 메모리 공간을 제공함으로써, 사용자가 원하는 각종 부가 기능을 구현할 수 있으므로, 보다 유연하고 효과적으로 콘솔 통합 관리를 할 수 있습니다.

IT 전문가, 네트워크 관리자 그리고 유틸리티 관리자들은 VTS II를 이용하여 네트워크를 통해 시리얼 콘솔 포트가 있는 서버, 라우터, 스위치 및 기타 랙 시스템과 같은 IT/Telco 장비를 원격 관리할 수 있습니다. 또한, VTS II는 Intel, HP, DELL, Sun 등의 다양한 서버 관리를 효과적으로 지원하기 위해 IPMI v2.0, iLO, ALOM, DRAC, SMASH 등 서버 자체적으로 내장된 관리 프로토콜을 지원합니다.

VTS II 장비는 콘솔 포트 접속을 위해, 4/8/16/32/48 개의 시리얼 포트를 가지고 있습니다. VTS II는 각 시리얼 포트에 RS232를 지원함으로써 거의 모든 RS232 시리얼 장치를 네트워크를 통해 접속할 수 있게 합니다.

VTS II는 TCP/IP, UDP 및 PPP와 같은 네트워크 프로토콜을 지원함으로써 10/100 Base-T Ethernet 네트워크를 사용하여 망내 (In-Band) 관리가 가능하며, 전화모뎀 접속(dial-in) 또는 ADSL 및 케이블 같은 초고속 인터넷 접속을 통해 망외 (Out-of-Band) 관리 기능도 제공되고 있습니다. 유동 IP 환경(Broadband 또는 동적 DNS)에서 도메인 네임으로 VTS II에 접근 가능하도록 하는 규약을 지원합니다.

VTS II는 Windows 원격 데스크탑 연결, 웹 기반의 원격 관리 소프트웨어 및 VNC 연결 기능을 지원하는 Free KVM 기능을 제공함으로써 한 서버 당 최대 8개의 Free KVM 콘솔 세션을 지원합니다.

VTS II는 다음 관리 기능들을 제공합니다.

- 시스템 상태 감시
- 원격 재설정
- 시스템 로그 기록 기능
- SNMP 또는 Email로 시스템 로그 알림 기능
- 웹, Telnet 또는 시스템 콘솔 포트를 이용하여 펌웨어 업그레이드 기능

- 포트 접속용 사용자 그룹 관리 기능
- IP 주소 필터링 보안 기능 (방화벽 기능)
- 안전한 데이터 통신을 보장하는 SSH(Secure shell) 기능
- 다양한 서버에 자체 내장된 관리 프로토콜을 지원
- 커스텀마이징 지원
- 원격 데스크탑 및 VNC 등의 Free KVM 콘솔 세션 지원

본 매뉴얼을 이해하려면 사용자는 인터넷 프로토콜 및 시리얼 통신에 대한 개념을 어느 정도 숙지하고 있어야 합니다.

1.2 패키지 체크 리스트

- VTS II 외장 박스
- 전원 케이블
- 19 인치 랙 설치용 브래킷
- 콘솔/Ethernet 케이블(RJ45-RJ45, 스트레이트 2m) 2 세트
- 케이블 키트는 다음을 포함합니다.

시리얼 RJ45 루프-백 커넥터	1 세트
RJ45-DB9 Female 어댑터(cross-over)	1 세트
RJ45-DB25 Female 어댑터(cross-over)	1 세트
RJ45-DB25 Male 어댑터(cross-over)	1 세트
RJ45-DB25 Male 어댑터(straight)	1 세트

- Quick Start Guide 하드 카피
- VTS Manager 및 매뉴얼이 포함된 CD-ROM

1.3 제품 사양

	VTS II 400	VTS II 800	VTS II 1600	VTS II 3200	VTS II 4800
시리얼 인터페이스	4-포트	8- 포트	16- 포트	32- 포트	48- 포트
	RJ45 커넥터 Sun Netra /Cisco 장비 관리에 CAT(Ethernet) 케이블 사용.				
	흐름 제어:Hardware RTS/CTS, Software XON/XOFF				
	신호: RS232 Rx, Tx, RTS, CTS, DTR, DSR, GND				
	모뎀 제어:DTR/DSR, RTS/CTS				
네트워크 인터페이스	듀얼 10/100 Base Ethernet, RJ45 커넥터				
	IP v4 및 v6 지원				
	동적 및 유동 IP 모드 지원				
프로토콜	Network Transfer Protocol : IP, ICMP, TCP, UDP, IPv4 and IPv6, ARP, RARP				
	Remote Management Protocol : Telnet, SSH v1/v2, HTTP, HTTPS, SMTP, FTP, SCP, SNMP v1/v2 and v3, NFS, DHCP, DNS, Dynamic DNS, SYSLOG, Samba, NTP, RIP, IPMI v2.0, iLO, ALOM, DRAC, SMASH				
PC 카드	Flash Memory, WiFi, Modem, Ethernet, GSM/CDMA				
USB 2.0 호스트	USB Memory, USB Wireless LAN				
내장 모뎀 인터페이스	V.92/56K, V.34/33.6K, V.32bis/14.4K and V.22bis/2400 bps data rate				
보안	시스템 및 포트 접근에 대한 다양한 보안 기능 지원				
	사용자 권한 관리: Root, Admin, Port Admin, User				
	SSH v1 & v2 (public key 지원)				
	RADIUS, LDAP, TACACS + 인증 지원 Custom PAM				
	SNMP v3 Encryption				
	시스템 및 각 포트별 IP 필터링				
로깅 및 이벤트 핸들링	시스템 로깅 : NFS, syslog server, ATA Flash memory, samba server, USB Memory				
	포트 버퍼링 : NFS, syslog server, ATA Flash memory, samba server, USB Memory				
	매체 및 장치에 따라 유연하게 버퍼 크기 설정 가능				
	E-mail 및 SNMP에 의한 알람 경보 기능				
Free KVM	Remote Desktop Access VNC 웹 기반 Remote Access 소프트웨어 지원				

클러스터링	NAT 기반의 효율적인 안전한 클러스터링 : 마스터/슬레이브 및 피어-투-피어(peer to peer) 방식				
	48개 슬레이브 및 48 개 피어 장치 관리 가능				
커스텀마이제이션	Perl 스크립트 엔진 및 16M의 내부 사용자 메모리 공간 지원 ELDK v4.0 지원				
관리	웹, Telnet/SSH, 시스템 콘솔 포트, VTS Manager				
	파워 유저를 위한 Linux 커맨드 라인 인터페이스 제공				
	풍부한 시스템 상태 및 통계치 표시 기능				
	펌웨어:Telnet, 웹이나 시스템 콘솔을 이용한 다운로드				
LED	Power (VTS II 400) or Power1/Power2 (VTS II 800/1600/3200/4800) Ready Ethernet 1/2 Link/Act, 100Mbps PC Card USB Find Modem DTR/DSR				
전원	5 VDC external power adapter 4A@5VDC	110 ~ 250 VAC, 50~60Hz, Max. 0.37A, 15W			
사용 환경	동작 온도 : 0C to 50C 저장 온도 : -20C to 66C 습 도 : 90% 이하(단, 결로 현상이 없을 것)				
치수 (LxWxH)	크기 203 mm 155 mm 29 mm	크기 443 mm 203 mm 44 mm 1U, 19 인치 랙에 탑재 가능	크기 443 mm 253 mm 44 mm 1U, 19 인치 랙에 탑재 가능		
	무게 : 0.98kg	무게 : 2.28kg	무게 : 2.8kg	무게 : 2.87kg	무게 : 2.87kg
MTBF	41.32 년	31.91 년	25.57 년	19.07 년	15.09 년
인증	CE, FCC, MIC, UL				
보증 기간	제한적 5년 보증				

1.4 용어 및 약어

이 섹션은 본 매뉴얼에서 일반적으로 사용되는 용어를 정의합니다. 이 용어들은 인터넷과 관련이 있으며 VTS II의 사용과 관련하여 정의되어 있습니다.

MAC 주소

LAN 또는 기타 네트워크상에서 MAC(Media Access Control) 주소는 컴퓨터의 고유한 하드웨어 번호를 나타냅니다. (Ethernet LAN 상에서 이는 Ethernet 주소와 동일합니다.)

MAC 주소는 6자리 OUI(Organization Unique Identifier) 번호와 6자리 하드웨어 식별 번호로 구성된 고유 12자리 하드웨어 번호입니다. VTS II의 MAC 주소는 00-01-95-xx-xx-xx이며, 외장 박스의 바닥면에 라벨이 붙어 있습니다.

호스트

네트워크에 연결된 사용자 컴퓨터.

인터넷 프로토콜 규격에서 “호스트”란 용어는 인터넷상에서 다른 컴퓨터와 완전 양방향 접속이 가능한 특정 컴퓨터를 뜻합니다. 호스트에는 네트워크 번호와 더불어 고유한 IP 주소를 구성하는 특정 “로컬” 또는 “호스트 번호”가 있습니다.

세션

단일 연결 기간 동안 두 개의 통신 종단점 사이에서 일어나는 일련의 상호 작용.

일반적으로 하나의 종단점은 다른 특정 종단점에 연결을 요청합니다. 만일 종단점이 응답하고 연결이 수락되는 경우 종단점은 서로 교대로 명령 및 데이터를 교환합니다("상호 대화"). 양쪽 종단점간에 연결이 이루어 질 때 세션이 시작되고 연결이 종료될 때 끝납니다.

클라이언트/서버

클라이언트/서버란 두개의 컴퓨터 프로그램, 즉 서비스를 요청하는 클라이언트 프로그램과 요청에 응답하여 이를 처리하는 서버 프로그램 사이의 관계를 말합니다.

서버는 하나 또는 여러 컴퓨터 상의 다른 컴퓨터 프로그램에 서비스를 제공하는 응용 프로그램입니다. 클라이언트는 클라이언트/서버 관계에 있는 요청 프로그램 또는 사용자입니다. 예를 들어, 웹 브라우저 사용자는 사실상 웹 페이지의 서버에 대하여 클라이언트 요청을 하고 있는 것입니다. 브라우저 자체는 컴퓨터와의 관계에서 요청한 HTML 파일을 받고 반환하는 클라이언트입니다. 요청을 처리하고 HTML 파일을 돌려주는 컴퓨터는 서버입니다.

표 1-1 약어표

ISP	**Internet Service Provider**
PC	**Personal Computer**
NIC	**Network Interface Card**
MAC	**Media Access Control**
LAN	**Local Area Network**
UTP	**Unshielded Twisted Pair**
ADSL	**Asymmetric Digital Subscriber Line**
ARP	**Address Resolution Protocol**
IP	**Internet Protocol**
ICMP	**Internet Control Message Protocol**
UDP	**User Datagram Protocol**
TCP	**Transmission Control Protocol**
DHCP	**Dynamic Host Configuration Protocol**
SMTP	**Simple Mail Transfer Protocol**
FTP	**File Transfer Protocol**
PPP	**Point-To-Point Protocol**
PPPoE	**Point-To-Point Protocol over Ethernet**
HTTP	**HyperText Transfer Protocol**
DNS	**Domain Name Service**
DDNS	**Dynamic Domain Name Service**
SNMP	**Simple Network Management Protocol**
RADIUS	**Remote Access for Dial-In User Service**
SSH	**Secure Shell**
NTP	**Network Time Protocol**
UART	**Universal Asynchronous Receiver/Transmitter**
Bps	**Bits per second (baud rate)**
DCE	**Data Communications Equipment**
DTE	**Data Terminal Equipment**
CTS	**Clear to Send**
DSR	**Data Set Ready**
DTR	**Data Terminal Ready**
RTS	**Request To Send**
DCD	**Data Carrier Detect**

2: 시작하기

본 장에서는 VTS II를 처음 설치하고 설정하는 방법에 대하여 설명합니다

- *2.1 패널 배치*에서는 패널 배치 및 LED 표시 등을 설명합니다.
- *2.2 하드웨어 연결하기*에서는 VTS II의 전원, 네트워크 및 장치 연결 방법을 설명합니다.
- *2.3 시스템 콘솔에 접속하기*는 시스템 콘솔 또는 Telnet 또는 웹 메뉴를 사용하여 VTS II의 콘솔 포트에 접속하는 방법을 설명합니다.

시작하려면 다음의 장치들이 필요합니다.

- 하나의 전원 케이블(패키지에 포함됨)
- 하나의 콘솔/Ethernet 케이블(패키지에 포함됨)
- 케이블 키트(패키지에 포함됨)
- 네트워크 인터페이스 카드(이하 NIC)가 있는 하나의 PC 또는 하나의 RS232 시리얼 포트

2.1 패널 배치

2.1.1 VTS II 400 패널 배치

VTS II 400 에는 그림 2-1과 같이 전면 패널에 상태 표시를 위한 LED 들이 위치해 있습니다. 모뎀이 장착된 모델의 경우에는 전면 좌측에 모뎀 소켓 및 2개의 상태 LED가 추가로 위치해 있습니다. 각 LED 의 기능은 표 2-1에 설명되어 있습니다. 패널 뒷부분은 2개의 Ethernet 포트, USB 포트, 팩토리 리셋 스위치, 전원 소켓 및 시리얼 포트들이 있습니다.

그림 2-1 VTS II 400의 패널 배치

2.1.2 VTS II 800/1600/3200 패널 배치

VTS II 800/1600/3200/4800의 전면 패널은 그림 그림 2-2와 같이 전면 패널에 상태 표시를 위한 LED 들이 위치해 있습니다. 모뎀이 장착된 모델의 경우에는 전면 좌측에 모뎀 소켓 및 2개의 상태 LED가 추가로 위치해 있으며 PC 카드 소켓 및 팩토리 리셋 스위치도 전면 판넬에 위치해

있습니다. 각 LED 의 기능은 표 2-1에 설명되어 있습니다. VTS II 800/1600/3200 의 전면 판넬 구성은 동일하며 (VTS II 4800 의 경우 전원 소켓이 전면에 위치) 패널 뒷부분은 2개의 Ethernet 포트, USB 포트, 전원 소켓 및 시리얼 포트들이 있습니다.

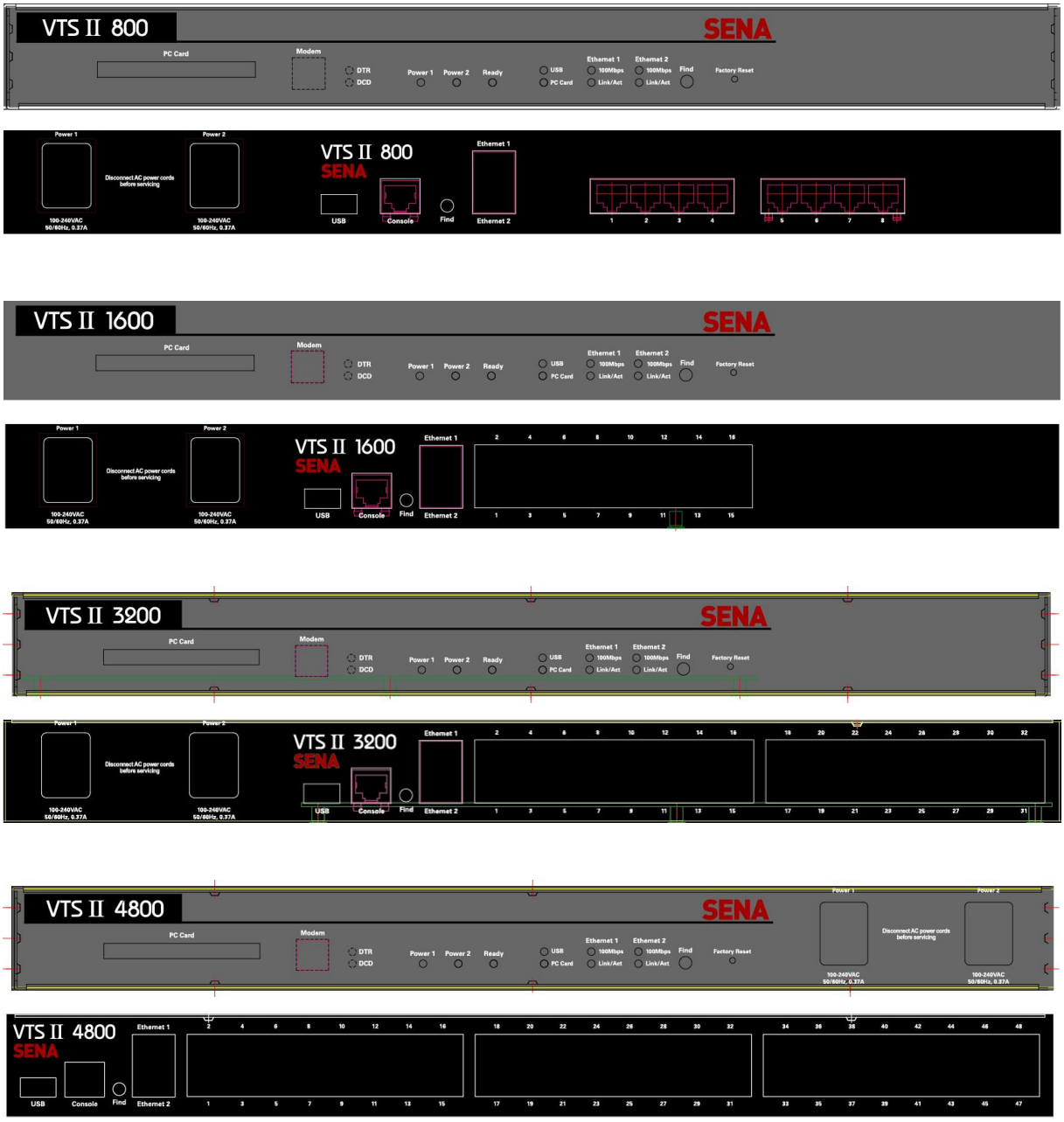


그림 2-2 VTS II 800/1600/3200/4800 의 패널 배치

표 2-1 VTS II3200의 LED 지시 램프

표시등		기능
시스템	**Power 1**	전원 소켓 1에 전원이 공급되는 경우 점등 됩니다.
	Power 2	전원 소켓 2에 전원이 공급되는 경우 점등 됩니다. (Dual Power 모델의 경우)
	Ready	시스템 작동이 준비되는 경우 점등 됩니다.
	FIND	해당 VTS II 의 위치를 찾기위한 용도로 사용됩니다.
Ethernet 1	**100Mbps**	Ethernet 1 포트가 100Base-TX 연결되는 경우 점등 됩니다..
	Link/Act	Ethernet 1 포트가 네트워크에 연결되는 경우 점등되며 Ethernet 1 포트를 통해 패킷이 들어오고 나가는 경우 깜박거립니다.
Ethernet 2	**100Mbps**	Ethernet 2 포트가 100Base-TX 연결되는 경우 점등 됩니다
	Link/Act	Ethernet 2 포트가 네트워크에 연결되는 경우 점등되며 Ethernet 2 포트를 통해 패킷이 들어오고 나가는 경우 깜박거립니다.
PC Card		PC Card 장치가 작동되는 경우 점등 됩니다. (PC Card 소켓이 장착되어 있는 모델의 경우)
USB		USB 장치가 작동되는 경우 점등 됩니다.
Modem	**DTR**	모뎀이 작동되는 경우 점등 됩니다.
	DCD	전화연결이 되어 있는 경우 점등 됩니다.

2.2 하드웨어 연결하기

본 절에서는 초기 테스트를 위해, VTS II를 장치에 연결하는 방법에 대하여 설명합니다.

- VTS II에 전원 공급 장치를 연결합니다.
- VTS II를 Ethernet 허브 또는 스위치에 연결합니다.
- 해당 장치에 연결합니다.

2.2.1 전원 연결하기

VTS II에 전원 케이블을 연결합니다. 다음에, 전원 스위치를 켭니다. 전원이 적절히 공급된 경우, [Power] 표시등이 초록색으로 점등 상태를 유지합니다.

그림 2-3 VTS II에 전원 연결하기

2.2.2 네트워크에 연결하기

Ethernet 케이블의 한쪽 끝을 VTS II Ethernet 포트 1 에 연결하고, 나머지 다른 Ethernet 케이블의 종단면을 네트워크 포트에 연결합니다. (Ethernet 포트 2를 동시에 사용하고자 할 경우에는

Ethernet 포트 2 에도 Ethernet 케이블의 연결하고 나머지 다른 Ethernet 케이블의 종단면을 네트워크 포트에 연결합니다). 케이블이 올바르게 연결된 경우, VTS II와 Ethernet 네트워크간의 연결표시는 다음과 같이 나타납니다.

- [Link/Act] 표시등은 녹색 점등 상태를 유지하면서 Ethernet 패킷이 있을 경우 깜박거리면서 Ethernet 패킷의 송수신이 여부를 나타냅니다.
- VTS II가 100Base-TX 네트워크에 연결되는 경우 [100Mbps] 표시등은 녹색 점등 상태를 유지합니다.
- 현재의 네트워크 연결이 10Base-T인 경우 [100Mbps] 표시등은 켜지지 않습니다.

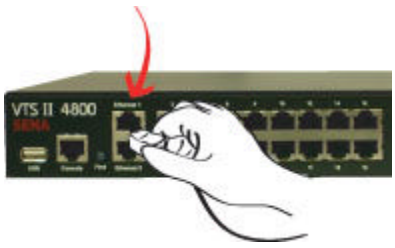


그림 2-4 VTS II에 네트워크 케이블 연결하기

2.2.3 해당 장치에 연결하기

VTS II의 시리얼 포트에 콘솔 케이블을 연결합니다. 사용자가 장치의 콘솔 포트에 연결하려면 장치 자체에서 제공한 콘솔 포트의 유형을 고려할 필요가 있습니다. VTS II 케이블 키트 패키지 내의 플러그-인 어댑터들은 사용자 장치에 맞는 케이블 형태를 지원하기 위해 제공됩니다. 자세한 내용은 ***부록 A.3 케이블 다이어그램***를 참조하십시오.

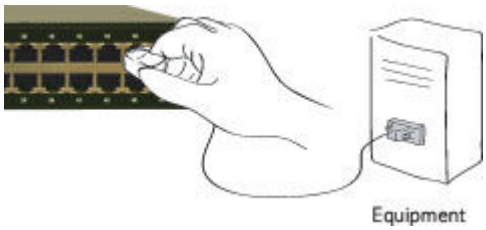


그림 2-5 장비를 VTS II에 연결하기

2.3 시스템 콘솔에 접속하기

VTS II에 접속하는 방법은 여러 가지가 있습니다. 이는, 사용자의 위치가 현지 또는 원격이냐 여부에 따라 달라집니다. 또한, VTS II는 텍스트 메뉴, GUI(Graphic User Interface) 메뉴 또는 CLI(Command Line Interface)를 제공하고 있습니다..

시스템 콘솔:

로컬 사용자는 해당되는 케이블 어댑터 및 콘솔/Ethernet 케이블을 사용해 VTS II의 시스템 콘솔

포트에 직접 연결할 수 있습니다.

원격 콘솔:

텍스트 메뉴 인터페이스를 요구하는 원격 사용자는 터미널 에뮬레이터를 사용해 VTS II의 Telnet(TCP 포트 23) 또는 SSH(TCP 포트 22)에 접속할 수 있습니다.

웹:

웹 브라우저를 사용하여 VTS II를 설정하려는 원격 사용자는 Internet Explorer 또는 Netscape Navigator와 같은 웹 브라우저를 사용하여 VTS II에 연결할 수 있습니다.

위의 방법들은 모두 VTS II 시스템으로의 로그인을 요구합니다.

참고 : 보안을 위하여 출고시 VTS II 의 기본 설정은 Telnet 콘솔과 HTTP 프로토콜을 이용한 웹 접속은 제한하고 있습니다. 초기 접속에는 SSH 콘솔 또는 HTTPS 프로토콜을 이용한 웹 접속만이 가능합니다. 이 설정은 ***9.7 Security Profile***에 설명된 바와 같이 **System Administration > Security Profile** 부분에서 변경이 가능합니다.

2.3.1 시스템 콘솔 사용하기

1) 콘솔/Ethernet 케이블의 한쪽 끝을 VTS II의 콘솔 포트에 연결합니다.

그림 2-6 VTS II에 시스템 콘솔 케이블을 연결하기

2) RJ45-DB9 어댑터(female adapter)를 사용자 컴퓨터에 연결합니다.
3) 사용자 컴퓨터의 시리얼 포트에 케이블의 한쪽 끝을 연결합니다.
4) 하이퍼터미널(HyperTerminal)과 같은 터미널 에뮬레이터 프로그램을 실행합니다. 다음과 같이 터미널 에뮬레이션 프로그램의 시리얼 설정 파라미터를 설정합니다.
   - **9600 baud rate**
   - **8 Data bits**
   - **Parity None**
   - **Stop bits 1**
   - **No flow control**
5) [ENTER] 키를 누릅니다.
6) 사용자 이름과 비밀 번호를 입력하고 VTS II에 로그인 합니다. 다음과 같이 디폴트 값 사용자 설정을 합니다.

Login: root **Password: root**

Login: admin **Password: admin**

```
Sena_VTSII login: root
Password:****
[root@Sena_VTSII ~]#
```

```
Sena_VTSII login: admin
Password: ****

--------------------------------------------------------------------------------
 Welcome to VTSII-4800 configuration page
 Current time   : 09/26/2006 11:06:12   Serial No.    : pp48-rev02
 F/W Rev.       : v1.0.1                Bios Ver.     : v1.0.0
 MAC addr.(eth0): 00-01-95-04-22-35     IP addr.(eth0) : 192.168.5.1
--------------------------------------------------------------------------------
```

7) 인증 시, 동일한 사용자 인터페이스가 나타납니다. 텍스트 메뉴 인터페이스 또는 CLI를 이용하여 초기 설정을 할 수 있습니다. 각 사용자 역할에서 사용할 수 있는 기본 사용자 인터페이스에 대한 자세한 내용은 ***9.1 사용자 관리***를 참조하십시오. CLI에 대한 자세한 내용은 ***11: CLI 안내서***를 참조하십시오.

기본 인터페이스가 텍스트 메뉴로 설정된 경우, 그림 2-7 에 있는 메뉴 화면이 나타납니다.

```
Sena_VTSII login: admin
Password: ****

--------------------------------------------------------------------------------
 Welcome to VTSII-4800 configuration page
 Current time   : 09/26/2006 11:06:12   Serial No.    : pp48-rev02
 F/W Rev.       : v1.0.1                Bios Ver.     : v1.0.0
 MAC addr.(eth0): 00-01-95-04-22-35     IP addr.(eth0) : 192.168.5.1
--------------------------------------------------------------------------------
 1. Network
 2. Serial port
 3. Clustering
 4. Power controller
 5. Peripherals
 6. System status & log
 7. System administration
 8. Activate Locator LED

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)>
```

그림 2-7 메인 메뉴 화면(VTS II 4800)

메인 메뉴 화면의 사용자는 메뉴 번호를 입력하여 VTS II 파라미터 설정에 필요한 메뉴 항목을 선택할 수 있습니다. 모든 파라미터는 VTS II의 비휘발성(Flash) 메모리 공간에 저장되며, 사용자는 메뉴상에서 [s] 키를 선택하여 변경된 파라미터 값을 Flash 메모리에 저장할 수

있습니다. 메뉴상에서 [a] 키를 선택하면 변경된 설정을 적용시킬 수 있으면 [x] 를 선택하면 메인 메뉴에서 빠져 나올 수 있습니다.

2.3.2 원격 콘솔 사용하기

사용자는 원격 콘솔을 사용하는 VTS II에 접속하기 전에 반드시 VTS II의 IP 주소를 알아야 합니다. (자세한 내용은 ***3: 네트워크 설정***을 참조하십시오). VTS II의 공장 출하시 기본 IP 주소는 **192.168.161.5**입니다.

원격 콘솔 기능은 원격 호스트 접속 옵션에서 Disable 될 수 있습니다.(자세한 내용은 ***3.5 IP 필터링***을 참조하십시오). VTS II는 원격 콘솔을 위한 Telnet 및 SSH 프로토콜 모두를 지원합니다. 단, 공장 출하시 Telnet 프로토콜 지원은 제한(Disable)되어 있습니다. Telnet 프로토콜을 이용하여 원격 콘솔 접속을 원하는 경우 ***9.7 Security Profile***에 설명된바와 같이 **System Administration > Security Profile** 부분에서 Telnet 프로토콜 지원을 Enable 하여야 합니다.

다음의 지침에 따라 VTS II 원격 콘솔에 연결합니다.

1) Telnet(또는 SSH)프로그램 또는 Telnet(또는 SSH) 기능(예, TeraTerm-Pro 또는 Hyper Terminal)을 지원하는 프로그램을 실행시킵니다. 목적지 IP 주소 및 Port Number는 VTS II와 동일해야 합니다. 필요한 경우, port number를 23(또는 22)으로 지정합니다.

   사용자 컴퓨터 명령 라인 인터페이스에 다음 명령어를 입력합니다.

   `telnet 192.168.161.5` (or `ssh admin@192.168.161.5`)

   또는 다음 파라미터를 갖는 Telnet 프로그램을 실행시킵니다.

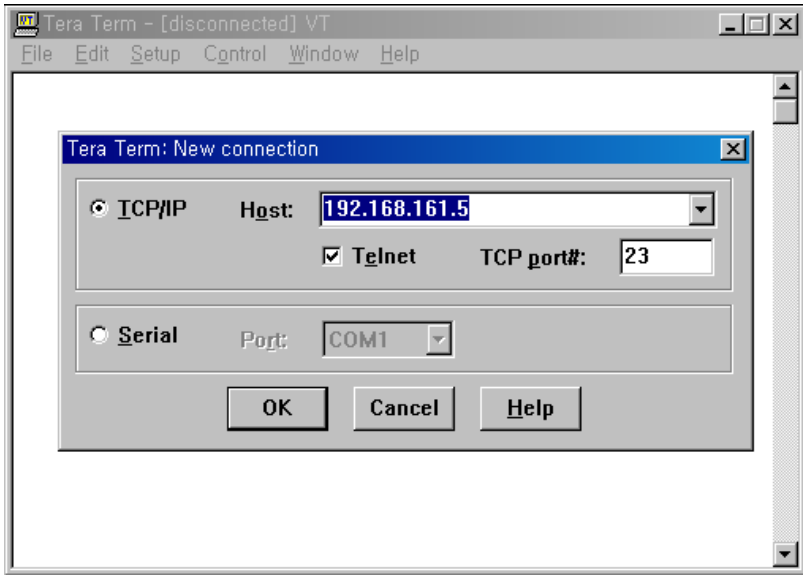


그림 2-8 Telnet 프로그램 설정 예제 (TeraTerm Pro)

2) 사용자는 반드시 VTS II로 로그인해야 하며, 이때 사용자 이름과 암호를 입력합니다. 사용자 이름 및 암호의 디폴트 설정은 시스템 root를 위한 **root** 및 시스템 관리자를 위한 **admin** 두 가지입니다(***9.1 사용자 관리***를 참조하십시오).
3) VTS II가 승인한 경우, CLI 프롬프트 또는 텍스트 메뉴 화면의 일부가 사용자 계정의 기본 shell 설정에 따라 사용자에게 나타납니다. 사용자가 CLI 프롬프트에 로그인하고자 하는 경우, 자세한 내용은 ***11: CLI 안내서***를 참조하십시오. 사용자는 텍스트 메뉴 인터페이스를 사용하여 메뉴 번호를 입력한 후, [ENTER]를 눌러 메뉴 항목을 선택할 수 있습니다. 사용자는 이와 동일한 화면을 통해 필요한 파라미터를 설정할 수 있습니다.

2.4 웹 브라우저 관리 인터페이스에 접속하기

VTS II는 HTTP 및 HTTPS(HTTP Over SSL) 프로토콜 모두를 지원합니다. 단, 공장 출하시 보안을 위하여 HTTP 프로토콜 지원은 제한(Disable)되어 있습니다. HTTP 프로토콜을 이용하여 VTS II 의 웹서버에 접속을 원하는 경우 ***9.7 Security Profile***에 설명된바와 같이 **System Administration > Security Profile** 부분에서 HTTP 프로토콜 지원을 Enable 하여야 합니다.
VTS II 에는 자체 웹 관리 페이지가 있습니다. VTS II 웹 관리 페이지에 접속하려면, VTS II의 IP 주소, 또는 유효한 호스트 이름을 웹 브라우저 URL/Location 필드에 입력해야 합니다. 이를 통해 사용자는 VTS II 로그인 화면으로 직접 이동할 수 있습니다. 사용자는 정확한 사용자 이름과 비밀 번호를 사용하여 로그인 함으로써 인증을 받아야 합니다. 기본 설정은 다음과 같습니다.

Login: root Password: root
Login: admin Password: admin

***참고**: VTS II 웹 관리 페이지에 접속하기 전, 사용자는 VTS II의 IP 주소(또는 적합한 호스트 이름), 그리고 서브넷 마스크 설정을 검사해야 합니다.*

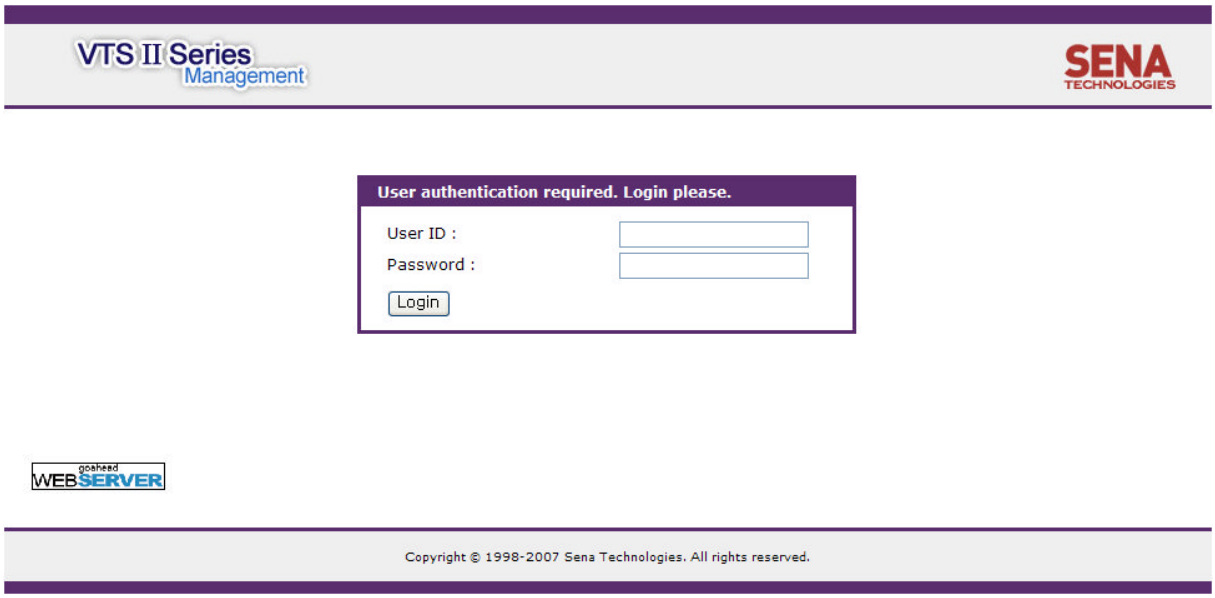


그림 2-9 VTS II 웹 관리 페이지 로그인 화면

그림 2-10은 VTS II 웹 관리 인터페이스에 대한 사용자 홈페이지를 보여줍니다. 메뉴 바는 화면 왼쪽에 있습니다. 메뉴 바는 가장 최상위의 설정 메뉴 그룹을 포함하고 있습니다. 메뉴 바의 항목을 선택하여 각 그룹에서 사용 가능한 모든 하위 메뉴의 상세 보기를 엽니다. 사용자는 하위 메뉴 항목을 선택하여 해당 항목에 대한 파라미터 설정을 수정할 수 있습니다.

사용자가 해당 페이지의 경로를 쉽게 파악하고 해당페이지의 상위 메뉴나 해당 경로의 다른 항목으로 쉽게 이동할 수 있도록, VTS II는 페이지 제목 아래에 경로를 표시하고 각 경로마다 다른 페이지로 링크를 제공합니다. 그림 2-10의 경우 **IP configuration** 제목 아래에 **/network/ip** 라는 경로가 표시되고 사용자가 경로 내의 network 또는 ip 링크를 선택하면 해당 페이지로 연결할 수 있습니다.

사용자는 모든 페이지에서 **[Save to flash]**, **[Save & apply]** 또는 **[Cancel]** 기능을 조작할 수 있습니다. 사용자는 설정 파라미터 값을 변경한 후 **[Save to flash]**를 선택하여 비휘발성 메모리에 변경된 파라미터 값을 저장해야 합니다. 모든 변경 사항을 적용하려면, 사용자는 **[Apply changes]** 메뉴를 선택해야 합니다. 이 옵션은 메뉴 바 하단에서 사용할 수 있습니다. 사용자가 **[Apply changes]**를 선택한 경우에 한해, 새로운 파라미터 값이 VTS II 설정에 적용됩니다. 사용자는 **[Save & apply]**를 선택하여 동시에 변경 사항을 저장하고 적용할 수도 있고, **[Save to flash]**를 선택하여 저장한 후 **[Apply changes]**를 선택하여 변경된 내용을 적용할 수 있습니다. 사용자가 새로운 파라미터 값을 저장하지 않고자 하는 경우, **[Cancel]**을 선택합니다. 모든 변경 사항은 취소가 되며 이전 값이 보존됩니다.

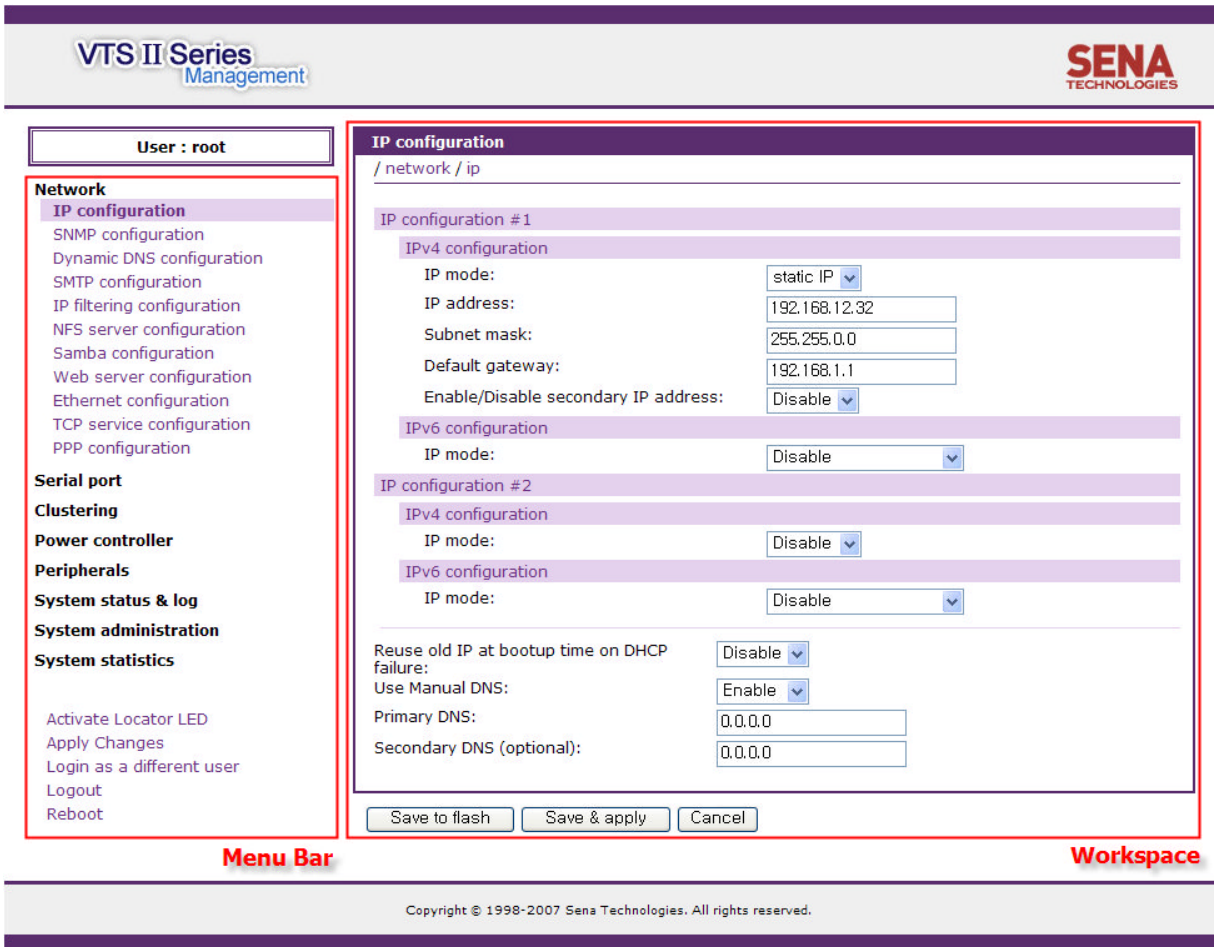


그림 2-10 VTS II 웹 관리 화면

3: 네트워크 설정

3.1 IP 설정

사용자 네트워크 환경에서 VTS II를 사용하려면, 유효한 IP 주소가 필요합니다. IP 주소가 준비되지 않은 경우, 시스템 관리자에게 문의하여 VTS II를 위한 유효한 IP 주소를 할당 받습니다. 네트워크에 VTS II를 연결하려면, 고유 IP 주소가 있어야 합니다.
VTS II는 두개의 Ethernet interface를 제공합니다. 아래의 내용은 두 Interface에 똑같이 적용됩니다.

3.1.1 IPv4 address 설정

VTS II IP 주소 설정 시, 사용자는 다음과 같은 2개의 인터넷 프로토콜 중의 하나를 선택할 수 있습니다.

- **Static IP**
- **DHCP** (Dynamic Host Configuration Protocol)

VTS II는 초기 기본값을 **192.168.161.5**의 IP 주소를 갖는 **Static IP** 모드로 설정되어 있습니다. 표 3-1은 2개의 모든 IP 설정 파라미터를 보여줍니다. 그림 3-1은 사용자 IP 설정을 변경하기 위한 실제 웹 기반 GUI를 보여줍니다.

표 3-1 IPv4 설정 파라미터

Static IP	IP address
	Subnet mask
	Default gateway
	Use manual DNS (Enable only) / Primary DNS / Secondary DNS (Optional)
	Enable/Disable secondary IP/Secondary IP address/Secondary subnet mask
DHCP	Reuse old IP at bootup time on DHCP failure
	Use manual DNS/Primary DNS/Secondary DNS (Optional)
	Enable/Disable secondary IP/Secondary IP address/Secondary subnet mask

사용자는 또한 **IP mode**를 **Disable**로 설정하여 네트워크에 VTS II를 연결하지 않을 수도 있습니다.

Enable/Disable secondary IP가 **Enable**로 설정되고, **Secondary IP address**와 **Secondary subnet mask**가 Static IP 프로토콜의 유효한 IP 주소가 설정되면, 사용자는 이 2차 IP 주소를 통하여 VTS II로 연결할 수 있습니다. 2차 IP 주소를 설정하는 방법은 ***3.1.2 Static IP 주소 사용하기***를 참조하시기 바랍니다.

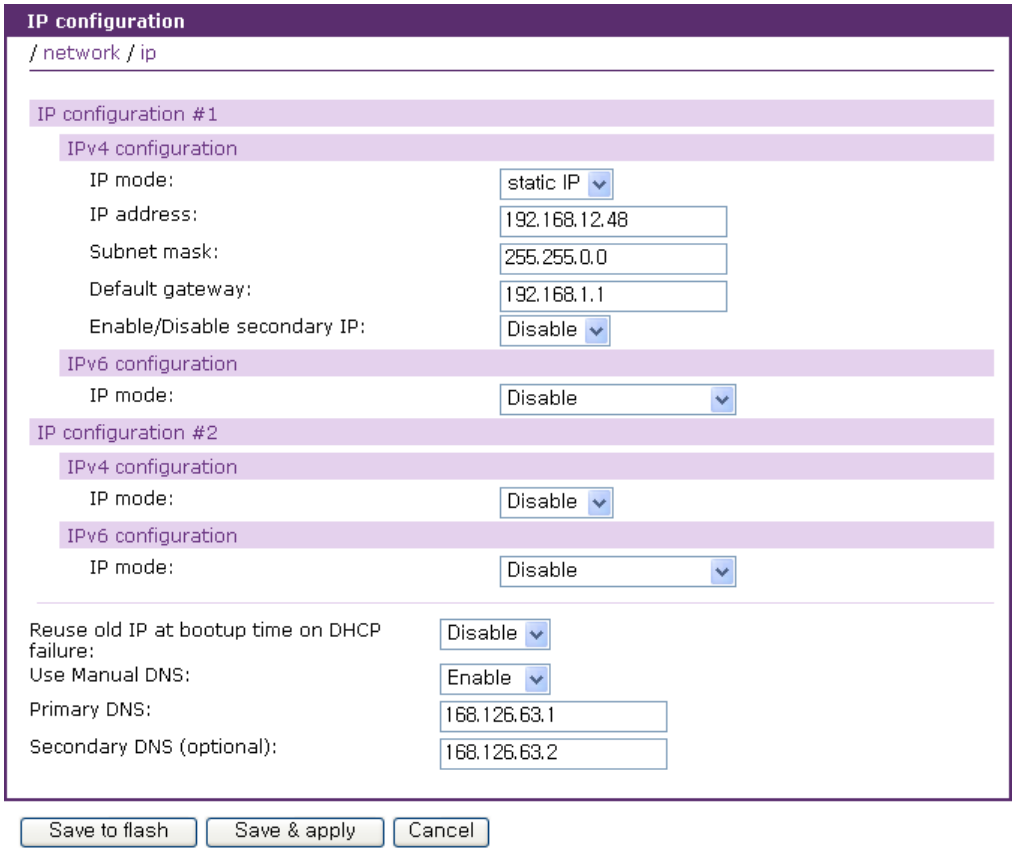


그림 3-1 IPv4 설정

3.1.2 Static IP 주소 사용하기

사용자가 **Static IP** 주소를 사용할 경우, VTS II의 IP 주소와 관련 있는 모든 설정 파라미터를 수동으로 지정해야 합니다. 이러한 파라미터에는 IP 주소, Subnet mask, gateway와 DNS server가 포함됩니다. 이 섹션에서는 이를 보다 자세하게 다룰 것입니다.

***참고**: VTS II는 활성될 때 마다 설정된 정보를 이용하여 네트워크를 검색하려고 합니다.*

IP address

Static IP는 "고정" 또는 영구적인 식별 번호의 역할을 합니다. 이 번호는 컴퓨터에 할당되어 네트워크 상의 위치 주소로서의 역할을 합니다. 컴퓨터는 이러한 IP 주소를 사용하여 네트워크 상에서 상호 식별하고 대화할 수 있습니다. 따라서, 선택된 IP 주소는 네트워크 환경에서 절대적으로 고유하고 유효해야만 합니다.

***참고**: 192.168.1.x 형식의 IP 주소는 ISP (Internet Service Provider)가 배정하지 않는다는 점에서 사설(private) 주소입니다. VTS II 시리즈를 적용하려면 경우에 따라 인터넷과 같은 공중망을 통해 데이터를 주고 받을 수 있어야 하며, 이 경우 유효한 공인 IP 주소를 할당해야 합니다. 공인 IP 주소는 일반적으로 지역 ISP로부터 구입하거나 임대할 수 있습니다.*

Subnet Mask

서브넷은 같은 지리적 위치, 한 건물 또는 동일한 LAN상에 있는 모든 네트워크 호스트를 뜻합니다. 네트워크를 통해 나가는 패킷이 있는 경우 VTS II 시리즈는 패킷이 지정한 TCP/IP 호스트가 로컬 네트워크 영역에 있는지 서브넷 마스크를 통해 확인합니다. 주소가 VTS II 시리즈와 동일한 네트워크 영역에 있다면 VTS II 시리즈로부터 직접 연결됩니다. 그렇지 않으면 주어진 기본 게이트웨이를 통해 연결됩니다.

Default Gateway(기본 게이트웨이)

게이트웨이는 다른 네트워크로 들어가는 입구 역할을 하는 네트워크 접점입니다. 일반적으로 네트워크 내에서 또는 지역 ISP에서 트래픽을 제어하는 컴퓨터는 게이트웨이 노드입니다. 로컬 네트워크 환경 밖의 호스트와 통신하기 위해서는 VTS II 시리즈가 기본 게이트웨이 컴퓨터의 IP 주소를 알아야 합니다. 게이트웨이 IP 주소에 대한 정확한 정보는 네트워크 관리자에게 문의하십시오.

Primary / Secondary DNS (기본 및 보조 DNS)

사용자가 특정 웹사이트를 방문하고자 하면, 컴퓨터는 웹사이트의 정확한 IP 주소에 대하여 DNS(Domain Name System) 서버에게 묻고, 그 답을 이용하여 웹 서버에 접속합니다. DNS는 인터넷 도메인 네임을 식별하여 IP 주소로 변환시켜주는 방식입니다. 도메인 네임은 **sena.com**과 같은 영문자와 숫자를 조합한 형식의 이름이며 일반적으로 기억하기가 더 쉽습니다. DNS 서버는 그러한 텍스트 기반의 도메인 네임을 TCP/IP에 연결하기 위해 숫자 IP 주소로 변환시켜주는 호스트입니다.

VTS II 시리즈의 DNS 기능을 사용하려면 도메인 네임으로 호스트에 접속할 수 있도록 이 DNS 서버의 IP 주소를 설정해야 합니다. VTS II 시리즈는 **Primary DNS** 와 **Secondary DNS** 같은 DNS 서버의 IP 주소를 설정하는 방법을 제공합니다. Secondary DNS 서버는 Primary DNS 서버를 사용할 수 없을 때 사용하기 위해 지정합니다.

3.1.3 DHCP 사용하기

동적 호스트 설정 통신 규약(DHCP)은 네트워크 관리자가 IP 주소의 할당을 조직의 네트워크에서 중앙 관리하고 자동화할 수 있게 하는 통신 프로토콜입니다. DHCP는 네트워크 관리자가 IP 주소를 중심점에서 감독하고 분배하도록 하며 컴퓨터가 다른 네트워크 위치에 플러그인 된 경우 새로운 IP 주소를 자동으로 전송되도록 합니다.

Static IP 모드의 경우, IP 주소는 각 컴퓨터에 수동으로 입력되어야 합니다. 만일 컴퓨터가 다른 네트워크 위치로 이동되는 경우, 새로운 IP 주소가 반드시 할당되어야 합니다. IP 주소가 DHCP 모드에서 할당되면 IP 주소, 서브넷 마스크, 게이트웨이, DNS 서버를 포함하는 모든 파라미터가 자동으로 설정됩니다. DHCP는 임의의 IP 주소가 하나의 컴퓨터에 대하여 유효한 시간 즉, “대여(lease)” 개념을 사용합니다. IP 주소를 할당하는데 필요한 모든 파라미터는 DHCP 서버

측면에서 자동으로 설정되며 IP 주소가 시동되는 경우 DHCP 클라이언트 컴퓨터는 이러한 정보를 수신합니다.
VTS II가 재설정될 때마다 VTS II는 네트워크 상에서 DHCP 요청을 발송합니다. DHCP 서버의 응답에는 IP 주소를 비롯하여 서브넷 마스크, 게이트웨이 주소, DNS 서버 및 "대여" 시간이 포함되어 있습니다. VTS II는 즉시 이런 정보를 자체 메모리에 저장합니다. "대여"가 만료되는 경우, VTS II는 DHCP 서버로부터 "대여" 시간의 연장을 요청합니다. DHCP 서버가 대여 연장을 승인할 경우, VTS II는 계속해서 현재 IP 주소로 작동할 수 있습니다. DHCP 서버가 대여 연장을 승인하지 않는 경우, VTS II는 DHCP 서버로부터 새로운 IP 주소 요청 절차를 시작합니다.

***참고**: DHCP 모드에서 DNS 서버를 포함한 모든 네트워크 관련 VTS II 파라미터는 자동으로 설정됩니다. DNS 서버가 자동으로 설정되지 않은 경우, 사용자는 Primary 및 Secondary DNS 주소를 입력함으로써 수동으로 설정할 수 있습니다. DNS 주소를 자동 설정하려면, Primary 및 Secondary DNS 주소를 0.0.0.0 (권장됨)으로 설정합니다.*

DHCP 서버는 네트워크 관리자가 관리하고 있는 IP 주소 풀에서 IP 주소를 동적으로 할당합니다. 이는 VTS II와 같은 DHCP 클라이언트가 작동될 때마다 다른 IP 주소를 수신합니다. DHCP 서버에서 IP 주소를 예약하여 사용자가 새롭게 할당된 VTS II 주소를 항상 인식할 수 있도록 보장해야 합니다. DHCP 네트워크에서 IP 주소를 예약하려면 관리자는 VTS II의 하단 부분에 있는 라벨 스티커에 있는 VTS II의 MAC 주소를 알아야 합니다.

Reuse old IP at bootup time on DHCP failure을 **Enable**로 설정하면, VTS II가 부팅될 때 DHCP 서버에서 VTS II의 IP 주소를 할당 받지 못 한 경우, 부팅 전에 사용하던 IP 주소를 이용하여 IP 설정하여 네트워크에 연결합니다. 이 후 "대여" 시간이 만료되면 DHCP 서버에 IP 주소를 요청합니다.

3.1.4 IPv6 주소 설정

IPv6는 IPv4의 주소 고갈 문제를 해결하고자 제안되었으며, 이 제안이 차세대 IP 체계로 인정받게 되었습니다. IPv6의 주소 공간 확대로 모든 호스트에 정적으로 공인 주소를 부여할 수 있게 되었습니다. IPv6에서는 라우터와 호스트가 통신하여 자동으로 IPv6 주소를 생성 할 수 있습니다. 또한 IPv6에서는 인증과 암호화가 가능합니다. IP층의 기능이므로 TCP나 UDP, ICMP등 어플리케이션에 상관없이 이 기능을 적용할 수 있도록 고안되어 있습니다.
VTS II는 IPv6를 지원하며, IPv6 주소를 설정할 수 있는 방법을 제공합니다. VTS II에서 IPv6 주소 설정시, 사용자는 다음과 같은 3개의 인터넷 프로토콜 중의 하나를 선택할 수 있습니다.

- **Auto confiuration**
- **Manual configuration**
- **DHCPv6 (Dynamic Host Configuration Protocol version 6)**

표 3-2는 각 프로토콜별 설정 파라미터를 보여줍니다. 그림 3-2는 사용자 IPv6 설정을 변경하기 위한 셀제 웹 기반 GUI를 보여줍니다.

표 3-2 IPv6 설정 파라미터

Auto configuration	Secondary IP Address
	6to4 tunneling Enable/Disable / IPv4 address of the remote 6to4 relay / Overwrite local IPv4 address
Manual configuration	IP address
	Default gateway
	Secondary IP Address
	6to4 tunneling Enable/Disable / IPv4 address of the remote 6to4 relay / Overwrite local IPv4 address
DHCPv6	Secondary IP Address
	6to4 tunneling Enable/Disable / IPv4 address of the remote 6to4 relay / Overwrite local IPv4 address

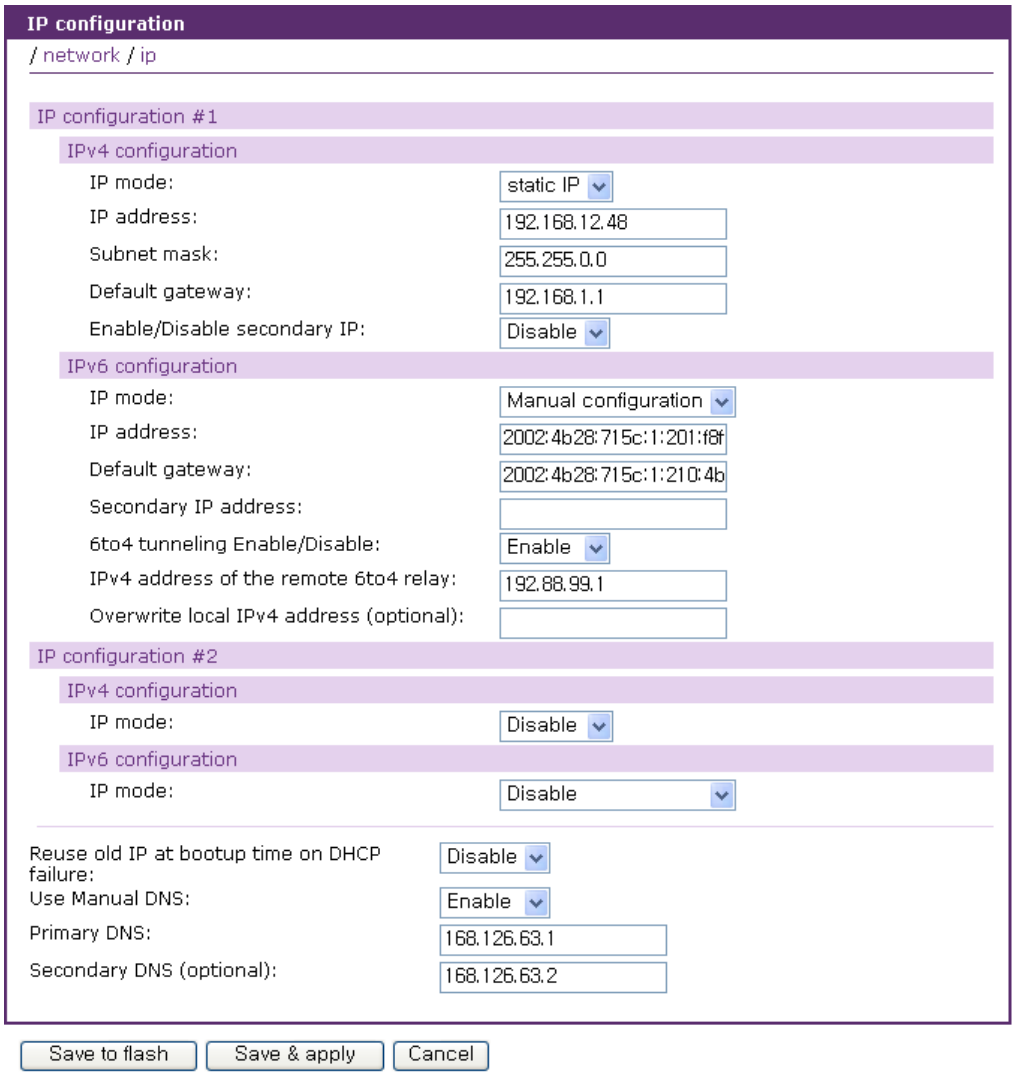


그림 3-2 IPv6 address 설정

사용자는 또한 **IP mode**를 **Disable**로 설정하여 IPv6 네트워크에 VTS II를 연결하지 않을 수도 있습니다.

3.1.5 IPv6 주소 자동 설정

사용자가 **Auto configuration** 모드를 사용할 경우, VTS II는 RA(Router Advertisement) 메시지를 받아 VTS II의 Mac address와 조합하여 IPv6 주소를 생성합니다.
RA 메시지는 라우터가 정기적으로 송신하거나 RS(Router Solicitation) 메시지를 수신했을 때 송신합니다. 호스트는 이 메시지로부터 prefix를 알수 있고, 이 prefix를 사용하여 자동으로 주소를 설정할 수 있습니다.
RS 메시지는 라우터에 RA 메시지를 요청하는 메시지입니다.

***참고**: IP mode를 Manual configuration이나 DHCPv6으로 설정하여도, 네트워크에 RA를 보내는 Router가 존재한다면 VTS II는 RA를 사용하여 IPv6 주소를 생성합니다.*

3.1.6 IPv6 주소 수동 설정

사용자가 **Manual configuration** 모드를 사용할 경우, VTS II의 IPv6 주소와 관련 있는 모든 설정 파라미터를 수동으로 지정해야 합니다. 이러한 파라미터에는 **IP address, Default gateway, Secondary IP address** 등이 포함됩니다.

IP address
IPv4에서의 IP address와 마찬가지로 “고정” 또는 영구적인 식별 번호의 역할을 합니다. 여기에는 IPv4에서의 subnet mask와 같은 역할을 하는 prefix 또한 포함하여 입력할 수 있습니다. 만약 prefix가 생략된다면 그 값은 64를 의미합니다.

Default gateway(기본 게이트웨이)
IPv4에서의 gateway와 같은 역할을 수행합니다.

Secondary IP address
추가적으로 IPv6 address를 입력하여 사용할 수 있습니다.

3.1.7 DHCPv6 사용

IPv4에서의 DHCP와 마찬가지로 IPv6에서도 DHCPv6를 사용하여 IP를 할당 받을 수 있습니다.

3.1.8 6to4 Tunneling

IPv6 네트워크를 구성해도 IPv6 네트워크들을 연결해주는 IPv6 네트워크가 존재하지 않을 수도 있고, 라우터가 IPv4 밖에 라우팅하지 않을 수도 있습니다. 이와 같은 문제를 해결하기 위해 IPv6 over IPv4 터널이라는 기술을 사용합니다.
6to4는 RFC3056에 기술되어 있는 것으로, IPv4 환경에서 IPv6 사이트끼리 통신하는 경우 이들 사이트가 특별한 주소를 이용해서 자동으로 터널을 구축하도록 하는 것입니다. 6to4를 이용하는 사이트에서 사용하는 주소의 2002:V4ADDR::/48 와 같은 형식을 가집니다. 여기서 V4ADDR은 6to4를 이용하고 있는 사이트에서 터널의 끝점이 되는 6to4라우터가 갖는 글로벌 IPv4주소를 말합니다. 따라서 사설 IP를 사용하는 경우 6to4를 사용할 수 없습니다.

IPv4 address of the remote 6to4 relay
Relay 서버의 IPv4 address입니다. 이 relay 서버를 통해 IPv4환경에서 IPv6를 사용할 수 있습니다. 192.88.99.1로 relay 서버를 지정하며, 현재 VTS II의 네트워크 위치에서 가장 가까운 relay 서버를 찾아 그것을 사용합니다. 그러나 이러한 방법은 가끔 해외의 relay 서버를 찾는 경우가 있으므로, 한국전산원(203.254.38.130) 라우터를 사용하거나 네트워크 관리자에게 문의하십시오.

Overwrite local IPv4 address
사용할 공인 IPv4 주소입니다. 이 주소가 없을 경우 자동으로 현재 VTS II의 IP 주소를 사용합니다. 만약 IP 주소가 사설 IP 주소라면 6to4 tunnel이 구성되지 않을 수 있습니다.

3.2 SNMP 설정

VTS II는 SNMP v1, v2 및 v3 프로토콜을 지원하는 SNMP(Simple Network Management Protocol) 에이전트가 있습니다. NMS 또는 SNMP 브라우저와 같은 네트워크 관리자는 VTS II로 필수 기능에 접속 할 수 있을 뿐만 아니라 정보를 교환할 수 있습니다.
SNMP 프로토콜은 GET, SET, GET-Next, 그리고 TRAP을 포함합니다. 이런 기능을 통해서 관리자는 중대한 이벤트 발생 통지를 받을 수 있고(TRAPs), 자세한 정보를 위한 장치를 조회할 수 있으며(GET) 장치 상태를 변경할 수 있습니다(SET). SNMP v2에는 정보 및 보안 기능을 복구할 수 있는 GET-Bulk 기능이 추가되어 있습니다. SNMP v3에는 보안 기능이 강화되고 관리 능력이 추가되었습니다.
SNMP 설정 패널을 통해 사용자는 MIB-II 시스템 개체, 접속 제어 설정 및 TRAP 수신기 설정에 대해 설정을 할 수 있습니다. 이 메뉴에서 설정된 관리자는 정보 교환 및 작동 제어를 모두 수행할 수 있습니다. 그림 3-3는 웹 인터페이스를 통한 SNMP 설정 화면을 보여줍니다.

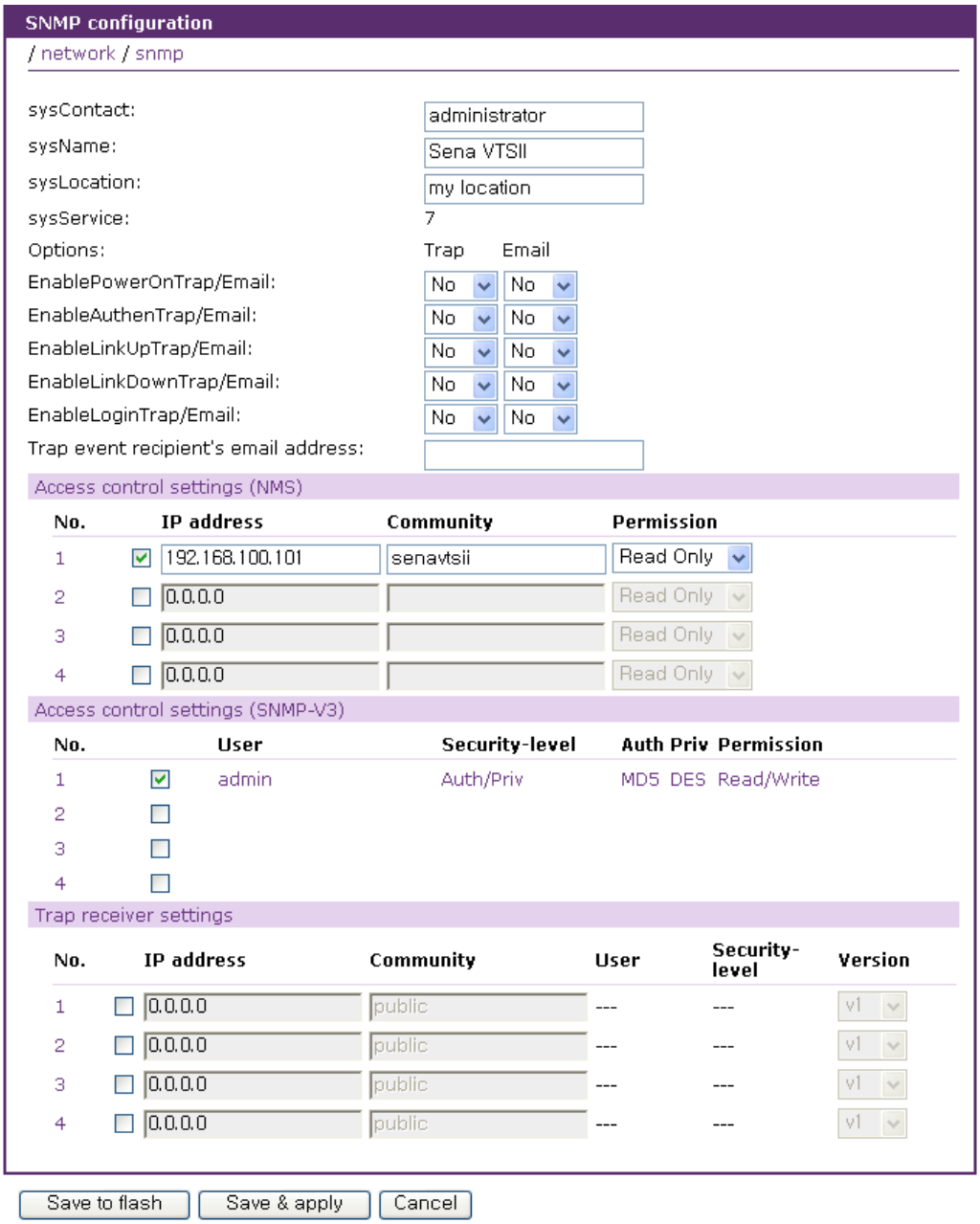


그림 3-3 SNMP 설정

3.2.1 MIB-II 시스템 객체(MIB-II system objects) 설정

MIB-II 시스템 객체 설정을 통해 시스템연락, 이름, 위치 및 VTS II의 SNMP 에이전트가 사용하는 인증 실패 정보(Authentication-failure traps)를 설정할 수 있습니다. 이러한 설정은 MIB-II **sysName**, **sysContact**, **sysLocation** 객체 식별정보(OID)가 사용하는 값을 제공해 줍니다. **EnablePowerOnTrap/Email**, **EnableAuthenTrap/Email**, **EnableLinkUpTrap/Email**, **EnableLinkDownTrap/Email**과 **EnableLoginTrap/Email**이 발생할 경우 **Trap event recipient's email address**로 이메일을 전송하게 할 수도 있습니다.

각 OID의 간단한 설명은 다음과 같습니다.

- **sysContact**: 관리 시스템(VTS II)에 대한 담당자 신분 및 해당 관리자에 연락을 취하는 방법을 설명합니다.
- **sysName**: 시스템 식별에 사용되는 이름으로 일반적으로 노드의 FQDN(Fully Qualified Domain Name) 입니다.
- **sysLocation**: 시스템의 실제 물리적 위치 (예, 방 384호, 실험실, 등등)
- **sysService**(읽기전용) : 콤마로 분리된 일련의 값들로서 시스템이 제공하는 서비스 세트들을 나타냅니다. 기본값으로 VTS II는 응용 프로그램(7) 레벨만을 지원합니다.
- **EnablePowerOnTrap/Email**: SNMP 에이전트 프로세스가 시스템이 시작되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.
- **EnableAuthenTrap/Email**: SNMP 에이전트 프로세스가 인증 실패에 관련된 정보 생성을 허용할 것인지 여부를 나타냅니다. 이 객체 값은 특정 설정 정보를 덮어 씁니다; 이것으로 모든 인증 실패와 관련된 정보를 비활성 시킬 수 있는 방법을 제공합니다.
- **EnableLinkUpTrap/Email**: SNMP 에이전트 프로세스가 Ethernet 연결이 되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.
- **EnableLinkDownTrap/Email**: SNMP 에이전트 프로세스가 Ethernet 연결이 단절 되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.
- **EnableLoginTrap/Email**: SNMP 에이전트 프로세스가 시스템에 로그인 했는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.

사용자가 MIB 추가 또는 수정에 대한 지원이 필요한 경우, 세나 기술 지원부서로 연락하시기 바랍니다. MIB와 SNMP의 자세한 정보는 RFC의 1066, 1067, 1098, 117, 1318 그리고 1213 문서를 참조하십시오.

3.2.2 액세스 제어 설정(Access control settings)

액세스 제어는 VTS II SNMP 에이전트에 대한 관리자의 접속 가능성을 정의하고 있습니다. 이 메뉴 상에 설정된 관리자만이 VTS II SNMP 에이전트에 접속하여 정보를 교환하고 작동을 제어할 수 있습니다. 지정된 IP 주소가 없는 경우(모든 IP 주소는 0.0.0.0 이 기본값), 모든 호스트 관리자가 VTS II SNMP 에이전트에 접속할 수 있습니다.

3.2.3 SNMP v3 액세스 제어 설정(Access control settings for SNMP v3)

SNMP v3 액세스 제어는 VTS II SNMP 에이전트에 대한 접속 정보을 정의하고 있습니다. 이 메뉴 상에 설정된 정보를 사용하여 VTS II SNMP 에이전트에 접속하여 정보를 교환하고 작동을 제어할 수 있습니다.

3.2.4 트랩 수신기 설정(Trap receiver settings)

트랩 수신기는 VTS II SNMP 에이전트로부터 중요한 이벤트(TRAP) 발생 상황을 관리자에게 통보할 수 있도록 정의합니다.

3.2.5 SNMP를 이용한 관리

NMS(네트워크 관리 시스템) 또는 SNMP 브라우저를 사용하는 SNMP 프로토콜을 통해 VTS II를 관리할 수 있습니다. VTS II가 NMS 또는 SNMP 브라우저가 실행되고 있는 호스트에 접속을 허용하려면 NMS 또는 SNMP 브라우저를 사용하기 전에, 액세스 제어 설정을 적절히 설정해야 합니다. 그림 3-4은 VTS II SNMP 에이전트의 MIB-II OID를 브라우징 하고 있는 일반적인 SNMP 브라우저 화면을 보여줍니다.

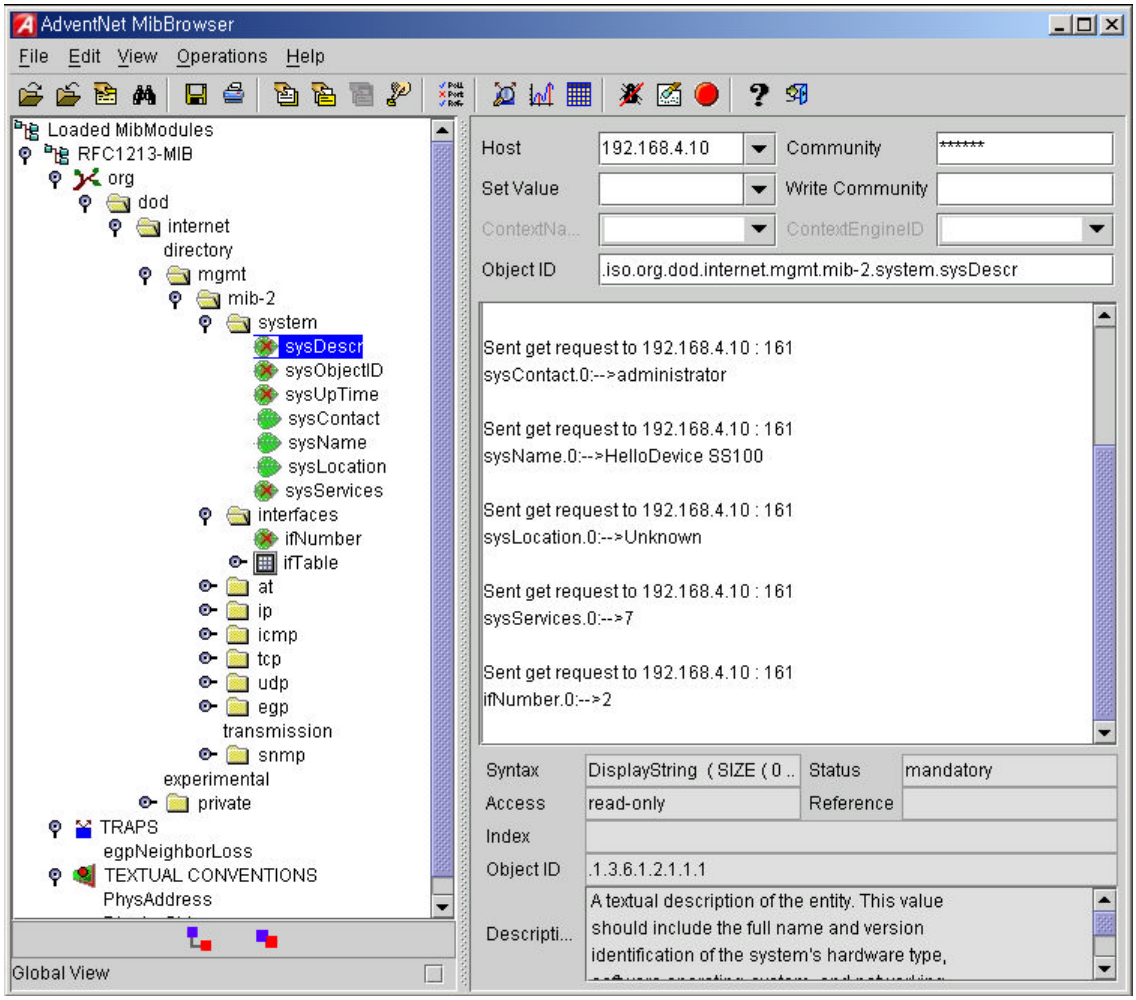


그림 3-4 SNMP 브라우저를 사용한 VTS II SNMP 에이전트의 MIB-II OID 브라우징 (AdventNet MIB 브라우저)

3.3 동적 DNS(Dynamic DNS) 설정

사용자가 VTS II를 DSL 라인에 연결하거나 DHCP 설정을 사용할 경우, 대여 시간이 경과하면, IP 주소가 변경되게 됩니다. 이러한 변경된 IP 주소에 대한 정보를 항상 보유하고 있는 것은 매우 어려운 일입니다. 또한, 관리자가 Telnet 등의 원격 콘솔만을 통해 그 호스트에 접속하려는 경우, IP 주소가 변경되었으면 접속할 방법을 찾기 어렵습니다.

동적 DNS 서비스는 위에서 언급한 문제점을 해결하기 위한 프로토콜이며, 여러 ISP 또는 단체에서 제공합니다. 동적 DNS 서비스를 사용함으로써, 사용자는 IP 주소의 변경에 상관없이 동적 DNS 서버에 등록된 호스트 이름을 통해 VTS II에 접속할 수 있습니다.

일반적으로, VTS II는 Dynamic DNS Network Services (www.dyndns.org)에서 제공하고 있는 동적 DNS 서비스만을 지원합니다. 기타 동적 DNS 서비스 제공업자와 관련 있는 문제점은 세나 기술 지원 부서에 연락하시기 바랍니다.

Dynamic DNS Network Services가 제공하는 동적 DNS 서비스를 사용하려면, 사용자는 그들의 회원 NIC(Network Information Center-http://members.dyndns.org)에 계정을 설정해야 합니다. 사용자는 Dynamic DNS Network Services Members NIC에 로그인 한 후 새로운 동적 DNS 호스트 링크를 추가할 수 있습니다.

동적 DNS 설정 메뉴에서, 동적 DNS 서비스가 가능하도록 한 후, 사용자는 등록된 Domain name, User name 및 Password를 입력해야 합니다. 설정 변경 사항을 적용한 후, 사용자는 Domain name만을 사용하여 VTS II에 접속할 수 있습니다.

그림 3-5는 동적 DNS 설정 웹 인터페이스를 보여줍니다.

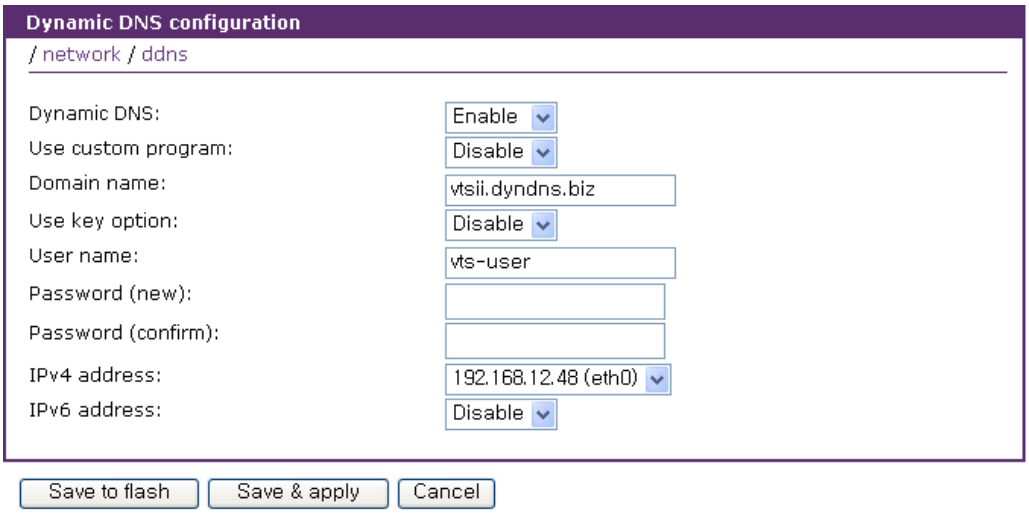


그림 3-5 동적 DNS 설정

3.4 SMTP 설정

시스템 로그 메시지가 특정 개수 만큼 쌓였거나 장비의 경고 메시지가 발생된 경우 VTS II는 Email 통보를 통해 이를 관리자에게 알려 줄 수 있습니다. 이를 위해서는, 유효한 SMTP 서버의 설정이 중요합니다. VTS II는 다음과 같은 3가지 SMTP 서버 유형을 지원합니다.

- **SMTP without authentication**
- **SMTP with authentication**
- **POP before SMTP**

각 SMTP 설정에서 필요한 파라미터는 다음과 같습니다.

- **Primary / Secondary SMTP server name**
- **Primary / Secondary SMTP mode**
- **Primary / Secondary SMTP user name**
- **Primary / Secondary SMTP password**
- **Device mail address**

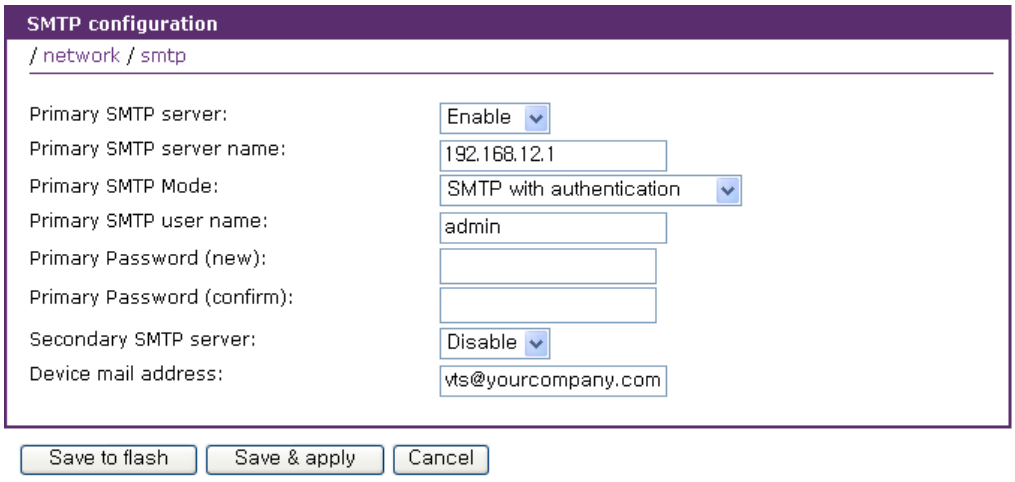


그림 3-6 SMTP 설정

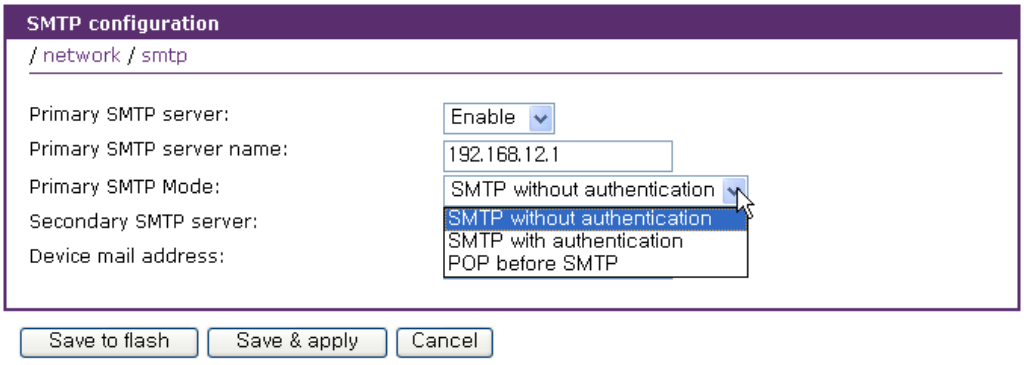


그림 3-7 SMTP Mode 선택

Device mail address는 모든 로그 및 경고 전달 Email을 위한 발신자, 즉, VTS II의 메일 주소를 지정합니다. SMTP Server는 유효성을 위해 Email 주소의 호스트 도메인 이름만을 확인합니다. 따라서, 장치에 대한 Email 주소 설정은 등록된 호스트 이름 (i.e. arbitrary_user@yahoo.com or anybody @sena.com)을 갖는 임의의 User name을 사용할 수 있습니다.

SMTP with authentication 또는 **POP before SMTP** mode가 선택되는 경우, SMTP 사용자 이름 및 SMTP password가 필요합니다.
Secondary SMTP 설정은 첫 번째 SMTP 서버를 통한 메일 전송이 실패할 경우에 이용하기 위해 필요합니다. 즉, 첫 번째 SMTP 서버를 통한 메일 전송이 실패할 경우에만 Secondary SMTP 서버를 통하여 메일 전송을 시도하게 됩니다.

3.5 IP 필터링

VTS II는 IP 주소 기반의 필터링 규칙을 사용하여 승인 권한이 없는 호스트가 VTS II에 접속하는 것을 막는 기능이 있습니다. IP 필터링 규칙을 설정하기 위한 항목에는 **Interface**, **Option**, **IP address/Mask**, **Protocol**, **Port**와 **Chain rule**등이 있습니다.

Interface
데이터를 받는 네트워크 인터페이스의 이름을 설정하는 항목입니다. 다음 세 가지의 인터페이스 중 하나를 선택합니다.

- **eth0** : VTS II 기본 인터페이스
- **eth1** : VTS II 기본 인터페이스
- **all** : eth0와 eth1 인터페이스 모두 적용

Option
해당 IP 필터링 규칙이 **IP address/Mask**에서 설정된 호스트 범위에 포함된 호스트에 적용될지 포함되지 않은 호스트에 적용될지를 결정합니다. 다음 두 가지의 **Option** 중에서 선택합니다.

- **Normal** : 호스트 범위에 포함된 호스트에 적용
- **Invert** : 호스트 범위에 포함되지 않은 호스트에 적용

IP address/Mask
주 호스트 IP 주소 / 서브넷 마스크의 형식으로 입력하여 해당 IP 필터링 규칙이 적용될 호스트의 범위를 설정합니다. 사용자는 파라미터 설정을 변경함으로써 호스트 범위를 다음 시나리오 중의 하나로 설정할 수 있습니다.

- 특정 IP 주소를 갖는 단일 호스트
- 특정 서브넷에 있는 호스트
- 모든 호스트

표 3-3 IPv4 Address/Mask 입력 예제

적용 호스트 범위	입력 포맷	
	주 호스트 IP 주소	서브넷 마스크
모든 호스트	0.0.0.0	0.0.0.0
	anywhere	
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128	255.255.255.128

표 3-4 IPv6 Address/Mask 입력 예제

적용 호스트 범위	입력 포맷	
	주 호스트 IP 주소	서브넷 마스크
모든 호스트	0::0	0
	anywhere	
2002:1234:5678:90ab:cdef:1234:5678:90ab	2002:1234:5678:90ab:cdef:1234:5678:90ab	128
2002:1234:5678:90ab:0:0:0:0 ~ 2002:1234:5678:90ab:ffff:ffff:ffff:ffff	2002:1234:5678:90ab::	64
2002:1234:0:0:0:0:0:0 ~ 2002:1234:ffff:ffff:ffff:ffff:ffff:ffff	2002:1234::	32
2002:0:0:0:0:0:0:0 ~ 2002:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2002::	16

Protocol

호스트와 VTS II의 통신에 사용되는 프로토콜을 지정합니다. **TCP**, **UDP**, **ICMP**, **HTTP**, **HTTPS**, **Telnet**, **SSH**, **PORT**, **Cluster** 등의 항목 중에 선택할 수 있습니다.

Port

호스트가 접속하려는 VTS II의 포트번호를 설정합니다. **Protocol**이 **HTTP**, **HTTPS**, **Telnet**, **SSH** 인 경우에 대한 Port는 자동으로 지정되며, **PORT**를 선택할 경우 시리얼포트를 선택할 수 있습니다. **Cluster**를 선택하면 All ports에 대한 설정으로 자동 설정됩니다.

Chain rule

호스트의 접속이 허용될지 또는 거부될지를 표시합니다. 다음 두 가지 항목 중에 선택할 수 있습니다.

- **ACCEPT** : 접근 허용
- **DROP** : 접근 거부

그림 3-8은 IP 필터링 설정 웹 인터페이스를 보여줍니다.

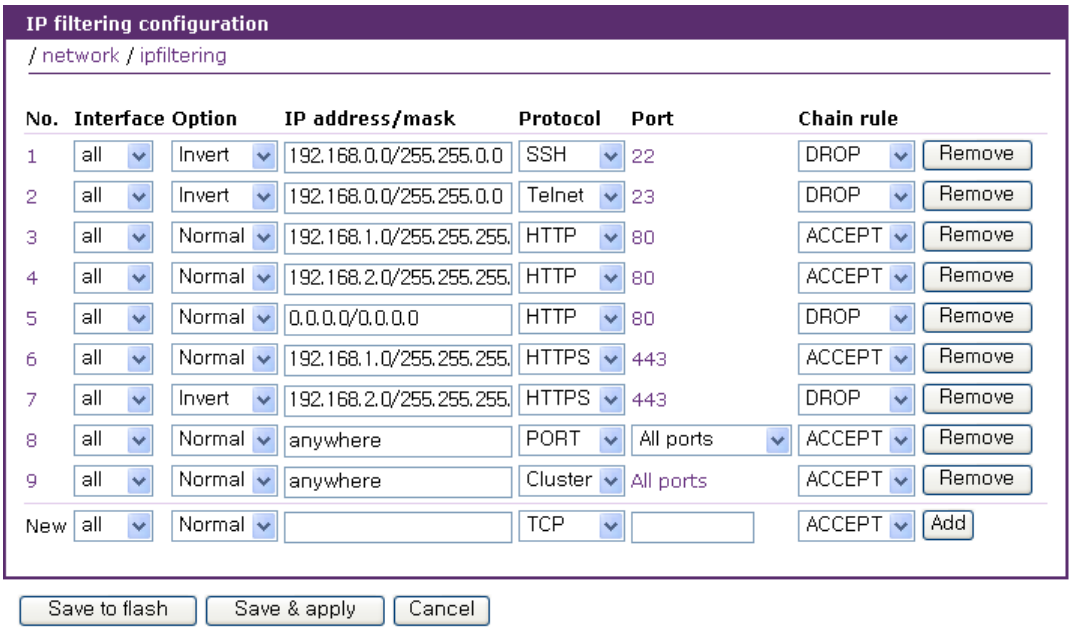


그림 3-8 IP 필터링 설정

그림 3-8에서 1번 IP 필터링 규칙은 192.168.0.1에서 192.168.255.254 사이의 호스트 범위(IP address/Mask : 192.168.0.0/255.255.0.0)에 있는 호스트를 제외(Option : invert)한 호스트가 eth0 또는 eth1 인터페이스(Interface : all)를 통하여 SSH 프로토콜(port : 22)로 VTS II에 접속을 시도할 때 접속이 거부된다는 것을 의미합니다. 즉, 1번 규칙은 192.168.x.x 서브넷에 속한 호스트만 SSH 프로토콜로 VTS II에 접속할 수 있도록 허용합니다. 2번 규칙은 192.168.x.x 서브넷에 속한 호스트의 eth0나 eth1 인터페이스를 통해 VTS II로 텔넷 접속을 허용함을 의미합니다.

5번 규칙에 의해 어떠한 호스트도 HTTP 프로토콜(Port : 80)로 VTS II에 접속할 수 없습니다. 그러나, 3번 규칙에 의해 192.168.1.x 서브넷 호스트의 접근이 허용되고, 4번 규칙에 따라 192.168.2.x 서브넷 호스트의 접속이 가능합니다. 따라서, 3번에서 5번까지의 규칙에 의해 192.168.1.x와 192.168.2.x 서브넷에 속한 호스트만이 HTTP로 VTS II에 접속할 수 있게 됩니다.
7번 규칙은 192.168.2.x 서브넷에 속한 호스트를 제외한 모든 호스트의 HTTPS(Port : 443) 접속을 제한합니다. 6번 규칙은 192.168.1.x 서브넷에 속한 호스트의 접근을 허용합니다. 따라서, 192.168.1.x와 192.168.2.x 서브넷에 속한 호스트만이 HTTPS로 VTS II에 접속할 수 있게 됩니다.

8, 9번 규칙에서 anywhere는 0.0.0.0/0.0.0.0 과 같은 의미를 가집니다. 8번 규칙에 의해 모든 호스트는 모든 시리얼 포트에 대한 접근을 허용됩니다. 9번 규치에 의해 모든 호스트는 모든 Clustering 포트에 접근 가능합니다.

사용자는 IP 필터링 규칙을 설정하고 **[Add]** 버튼을 클릭하여 새로운 IP 필터링 규칙을 추가합니다. **[Remove]** 버튼을 클릭하면 등록된 IP 필터링 규칙을 제거할 수 있습니다. 등록된 규칙들의 설정을 변경한 후 **[Save to flash]** 또는 **[Save & apply]** 버튼을 클릭하여 IP 필터링 규칙을 편집 수정할 수 있습니다. **[Save & apply]** 버튼을 누르거나 **Apply changes** 메뉴를 선택하여 변경 사항을 적용하기 전까지는 IP 필터링 규칙이 VTS II에 적용되지 않습니다.

3.6 NFS 서버 설정

VTS II는 시스템 로그 또는 포트 데이터를 NFS(Network File System) 서비스를 통해 NFS 서버에 저장할 수 있게 하는 기능을 지원합니다. 이를 사용하려는 사용자는 NFS 서버의 IP 주소 및 NFS 서버의 설치 경로를 반드시 지정해야 합니다. 그림 3-9는 NFS 서버 설정 페이지를 보여줍니다.
VTS II 로그 데이터를 NFS 서버에 저장하려면, VTS II 설정에 지정된 NFS 서버를 "read and write allowed"으로 설정해야 합니다. VTS II 및 NFS 서버 사이에 방화벽이 있는 경우, 사용자는 나가고 들어오는 UDP 패킷이 자유롭게 이동할 수 있는 규칙을 반드시 추가해야 합니다.
NFS 서비스가 사용 가능 상태이고 NFS 서버 설정이 적절한 경우이만, 사용자는 VTS II의 시스템 로그 또는 포트 데이터 로그를 NFS 서버로 저장할 수 있습니다. 또, 보조 NFS 서버가 설정된 경우, VTS II는 동일한 LOG 메시지를 보조 NFS 서버에도 저장합니다. 포트/시스템 로그 저장 위치에 대한 자세한 정보는 ***4.5.8 Port Logging*** 및 ***8.2 시스템 로그 설정*** 섹션을 참조하십시오.

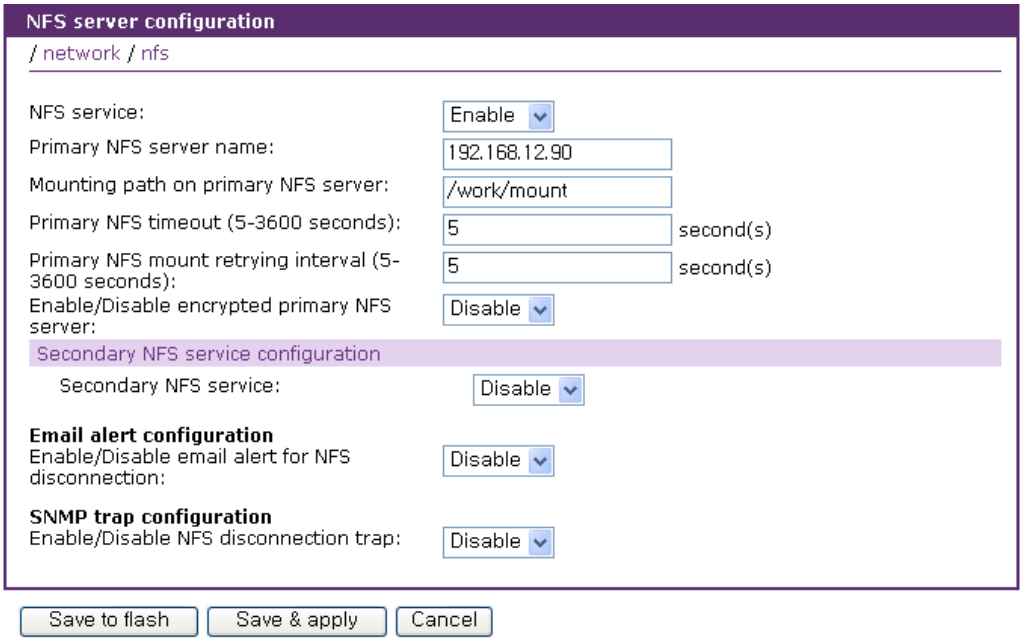


그림 3-9 NFS 서버 설정

각 NFS 서버 설정에서 필요한 파라미터는 다음과 같습니다.

- **Primary / Secondary NFS server IP address**
- **Mounting path on primary / secondary NFS server**
- **Primary / Secondary NFS timeout**
- **Primary / Secondary NFS mount retrying interval**
- **Enable/Disable encrypted primary / secondary NFS server**
- **Encrypted primary / secondary NFS server user**
- **Encrypted primary / secondary NFS server password**
- **Email alert configuration**
- **SNMP trap configuration**

NFS timeout

NFS server가 응답이 없을 경우, VTS II가 NFS의 응답을 얼마 동안 기다릴지를 지정합니다. 이 시간 동안 NFS server의 응답이 없으면 NFS server의 지정된 디렉토리(NFS server의 mounting path)를 언마운트 합니다.

NFS mount retrying interval

VTS II가 NFS server로의 연결이 가능한지를 점검하는 주기를 설정합니다. 설정된 주기마다 VTS II는 NFS server로 연결이 가능한지를 점검합니다. 가능하다면, VTS II는 VTS II의 디렉토리로 NFS server의 mounting path를 다시 마운트하고, 필요하다면 자동으로 데이터 로깅 위치를 NFS server로 변경합니다.

Encrypted NFS

NFS는 네트워크를 통하여 파일들을 공유하는데 널리 사용되는 프로토콜입니다. 그러나, 일반적으로 NFS는 UDP 프로토콜을 사용하므로 다음과 같은 보안상의 문제점을 가지고 있습니다.

- NFS server 와 client 사이의 data는 암호화 되기 어렵다.
- NFS server에 접속하려는 사용자의 ID에 따른 인증 방법을 마련하기가 어렵다.
- NFS server 와 client 사이의 방화벽이 있는 경우 NFS 기능을 사용하기가 어렵다.

그러나, SSH 터널링을 이용한 암호화된 NFS(Encrypted NFS) 기능을 이용하면 위와 같은 문제를 해결 할 수 있습니다. 암호화된 NFS 기능을 사용하려면, 사용자는 TCP 프로토콜을 지원하는 NFS server를 사용해야 합니다. 대부분의 마이크로소프트 윈도즈용 NFS server는 TCP 프로토콜을 지원합니다. 또한, 암호화된 NFS server로 사용될 호스트에는 SSH 데몬이 실행되고 있어야 합니다. 마지막으로, VTS II 제품과 함께 제공되는 pause.exe 라는 유틸리티 프로그램을 SSH 데몬 프로그램이 위치한 디렉토리로 복사해야 합니다. 이 기능의 보다 자세한 설명은 ***부록 G: 암호화된 NFS 기능 안내***를 참고하시기 바랍니다.

Email alert configuration

Enable/Disable email alert for NFS disconnection option이 **Enable**로 설정되면 NFS server의

연결이 끊어질 때마다 VTS II는 **이메일 경보 설정(Email alert configuration)**에 따라 이메일을 전송합니다.

SNMP trap configuration

Enable/Disable NFS disconnection trap option이 **Enable**로 설정되고, 트랩 수신기 설정(Trap receiver settings)에서 IP 주소가 트랩 수신기로 바르게 설정되면, NFS server의 연결이 단절될 때마다 VTS II는 트랩 수신기 설정에 맞추어 트랩을 보냅니다. **Use global SNMP configuration**이 **Enable**로 설정되면 **SNMP Configuration**에서 설정된 트랩 수신기 설정이 SNMP 트랩의 목적지로 사용됩니다. 자세한 내용은 ***3.2 SNMP 설정***을 참조하시기 바랍니다.

3.7 Samba 설정

VTS II는 시스템 로그 또는 포트 데이터를 Samba 서비스를 통해 Samba 서버에 저장할 수 있게 하는 기능을 지원합니다. 이를 사용하려는 사용자는 Samba 서버의 IP 주소 및 Samba 서버의 설치 경로를 반드시 지정해야 합니다. 그림 3-10는 Samba 서버 설정 페이지를 보여줍니다.

VTS II 로그 데이터를 Samba 서버에 저장하려면, VTS II 설정에 지정된 Samba 서버를 "read and write allowed"으로 설정해야 합니다. VTS II 및 Samba 서버 사이에 방화벽이 있는 경우, 사용자는 나가고 들어오는 UDP 패킷이 자유롭게 이동할 수 있는 규칙을 반드시 추가해야 합니다.

Samba 서비스가 사용 가능 상태이고 Samba 서버 설정이 적절한 경우에만, 사용자는 VTS II의 시스템 로그 또는 포트 데이터 로그로 Samba 서버로 저장할 수 있습니다. 포트/시스템 로그 저장 위치에 대한 자세한 정보는 ***4.5.8 Port Logging*** 및 ***8.2 시스템 로그 설정*** 섹션을 참조하십시오.

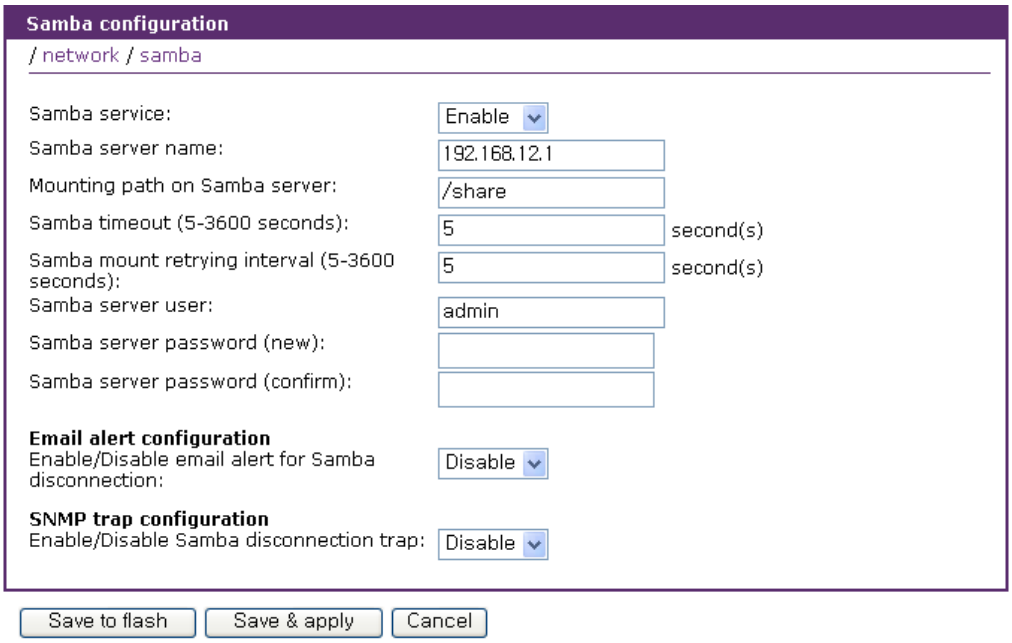


그림 3-10 Samba 설정

각 Samba 서버 설정에서 필요한 파라미터는 다음과 같습니다.

- **Samba server name**
- **Mounting path on Samba server**
- **Samba timeout**
- **Samba mount retrying interval**
- **Samba server user**
- **Samba server password**
- **Email alert configuration**
- **SNMP trap configuration**

Samba timeout

Samba server가 응답이 없을 경우, VTS II가 Samba의 응답을 얼마 동안 기다릴지를 지정합니다. 이 시간 동안 Samba server의 응답이 없으면 Samba server의 지정된 디렉토리(Samba server의 mounting path)를 언마운트 합니다.

Samba mount retrying interval

VTS II가 Samba server로의 연결이 가능한지를 점검하는 주기를 설정합니다. 설정된 주기마다 VTS II는 Samba server로 연결이 가능한지를 점검합니다. 가능하다면, VTS II는 VTS II의 디렉토리로 Samba server의 mounting path를 다시 마운트하고, 필요하다면 자동으로 데이터 로깅 위치를 Samba server로 변경합니다.

Email alert configuration

Enable/Disable email alert for Samba disconnection option이 **Enable**로 설정되면 Samba server의 연결이 끊어질 때마다 VTS II는 이메일 경보 설정(Email alert configuration)에 따라 이메일을 전송합니다.

SNMP trap configuration

Enable/Disable Samba disconnection trap option이 **Enable**로 설정되고, 트랩 수신기 설정(Trap receiver settings)에서 IP 주소가 트랩 수신기로 바르게 설정되면, Samba server의 연결이 단절될 때마다 VTS II는 트랩 수신기 설정에 맞추어 트랩을 보냅니다. **Use global SNMP configuration**이 **Enable**로 설정되면 **SNMP Configuration**에서 설정된 트랩 수신기 설정이 SNMP 트랩의 목적지로 사용됩니다. 자세한 내용은 ***3.2 SNMP 설정***을 참조하시기 바랍니다.

3.8 웹 서버 설정

VTS II의 웹 서버는 HTTP 및 HTTPS(HTTP Over SSL) 서비스를 모두 지원합니다. 사용자는 시큐리티 프로파일에서 각각의 서비스를 개별적으로 제공할 지 여부를 설정할 수 있습니다.

자세한 내용은 ***9.7 Security Profile***을 참조하시기 바랍니다. 그림 3-11은 웹 서버 설정 페이지를 보여줍니다.

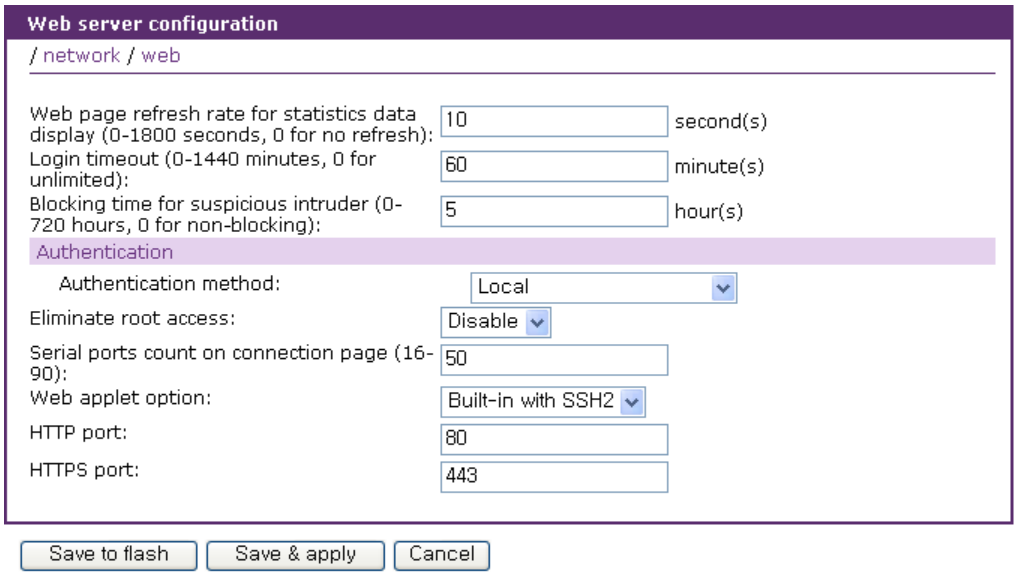


그림 3-11 웹 서버 설정

본 설정 페이지에서 **웹 페이지 업데이트 주기(Web page refresh rate)**는 조정될 수 있습니다. 업데이트 주기는 Serial port 연결 페이지와 네트워크 인터페이스, 시리얼 포트, IP, ICMP, TCP 및 UDP와 같은 시스템 통계 등을 나타내는 페이지 및 파워 컨트롤러 관리 페이지등에 적용됩니다. 그 외의 웹 페이지에서는 자동으로 새로 고침(Refresh)이 적용 되지 않습니다. 포트 연결에 대한 자세한 내용은 ***4.7 Serial port 연결***을 참조하시고, 시스템 통계에 대한 자세한 내용은 ***10: 시스템 통계***를 참조하십시오.

웹인터페이스를 일정 시간이 경과할 동안 사용하지 않다가 다시 사용할 경우 재로그인하도록 하는 시간을 **Login timeout**에서 설정합니다. 0으로 설정되면 재로그인을 요구하지 않습니다.

VTS II는 웹으로 공격하려는 호스트의 접근을 막고 있습니다. 이러한 공격자의 접근이 막히고 다음 접근이 가능하도록 하는 시간을 접근 제한 시간(**Blocking time for suspicious intruder**)으로 설정할 수 있습니다. 0으로 설정되면 접근을 제한하지 않습니다.

Authentication method 선택 메뉴에서는 웹에 로그인할 때 사용자 인증 방법을 선택할 수 있습니다. 현재 VTS II의 웹서버는 **Local**, **RADIUS server**, **RADIUS server - Local**, **Local - RADIUS server**, **RADIUS down - Local**, **TACACS+ server**, **TACACS+ server - Local**, **Local - TACACS+ server**, **TACACS+ down - Local**, **LDAP server**, **LDAP server - Local**, **Local - LDAP server**, **LDAP down - Local**, **Kerberos server**, **Kerberos server - Local**, **Local - Kerberos server**, **Custom PAM**등의 인증 방법을 지원합니다. 인증 방법에 대한 자세한 내용은 ***4.5.10 Authentication 설정***을 참조하시기 바랍니다.

Remote authentication을 통해 웹에 로그인 할 경우 사용자의 다음의 조건에 따라 각기 다른 사용자 권한을 갖습니다.

- **사용자가 VTS II 에도 등록되어 있는 경우**
  사용자를 등록할 때 지정한 사용자 그룹에 따른 접속 권한을 갖습니다. 사용자 그룹별 접속 권한은 9.1 사용자 관리를 참조하시기 바랍니다.
- **사용자가 VTS II 의 web_admin 액세스 리스트에 포함되어 있는 경우**
  사용자는 System admin 그룹 접속 권한을 갖습니다. 자세한 내용은 9.2 액세스 리스트를 참조하시기 바랍니다.
- **사용자가 VTS II 의 web_padmin 액세스 리스트에 포함되어 있는 경우**
  사용자는 Port admin 그룹 접속 권한을 갖습니다. 자세한 내용은 9.2 액세스 리스트를 참조하시기 바랍니다.
- **사용자가 Remote authentication server에만 등록되어 있는 경우**
  사용자는 User 그룹 접속 권한을 갖습니다.

Eliminate root access 항목을 **Enabled**로 설정하여 VTS II의 root 사용자의 웹 인터페이스 접근을 제한할 수 있습니다. VTS II의 root 사용자의 텔넷/SSH 프로토콜의 원격 또는 시리얼 콘솔 접근을 제한하려면 ***11: CLI 안내서***의 ***11.1 서론***을 참조하십시오.

참고: *웹 서버의 인증 방법은 시리얼 포트의 인증 방법과 달리 항상 **local** 데이터베이스를 참조하게 되어 있습니다. 즉, 웹서버의 인증 방법을 원격 인증 방법인 **RDAIUS, TACAS+, LDAP, Kerberos** 등으로 설정 하더러도 **local** 데이터베이스에 해당 사용자가 없을 경우에는 인증이 실패하게 됩니다. 단, 해당 사용자가 원격 인증 서버에서 인증이된 경우에는 **local** 데이터베이스에 기록되어 있는 암호는 무시되게 됩니다. 시리얼 포트의 인증 방법은 **4.5.10 Authentication 설정** 을 참고하시기 바랍니다. 또한 **local** 데이터베이스에서의 사용자 관리는 **9.1 사용자 관리**를 참고 하시기 바랍니다.*

시리얼 포트 연결 페이지에서 한 페이지 표시할 포트수를 **Serial ports count on connection page** 항목에서 설정할 수 있습니다. 이 수보다 많은 포트를 표시해야 할 경우 시리얼 포트 연결 페이지의 우측 상단에 다른 페이지로 직접 이동할 수 있도록 하는 리스트 박스를 제공합니다. 자세한 내용은 ***4.7 Serial port 연결***을 참조하십시오.

시리얼 포트, 원격 포트 또는 슬레이브 장치의 시리얼 포트로 연결할 Java applet의 종류를 **Web applet option**에서 설정할 수 있습니다. VTS II가 제공하는 Java applet을 사용하는 경우, Telnet 프로토콜은 차이가 없고 SSH 프로토콜인 경우 SSH 버전1(**Built-in with SSH1**)을 사용할 지 SSH 버전2(**Built-in with SSH2**)를 사용할 지를 결정해야 합니다. VTS II가 제공하는 SSH 버전1를 지원하는 Java applet을 선택한 경우, 시큐리티 프로파일의 SSH 버전1을 사용 불가능하도록 설정(***9.7 Security Profile***을 참조)하면 Java applet으로 SSH 프로토콜의 포트에 접근할 수 없게 되므로 주의하시기 바랍니다. 사용자가 만든 Java applet을 사용할 수도 있습니다. 사용자가 만든

Java applet을 /usr2/jta.jar로 복사하면 **Web applet option**에 **User-defined**라는 항목이 추가됩니다. 이 항목을 선택하면 사용자가 만든 /usr2/jta.jar가 Java applet으로 사용됩니다.

HTTP port와 **HTTPS port**를 변경하여 웹 서비스 포트를 변경할 수 있습니다.

3.9 Ethernet 설정

VTS II는 다음과 같은 여러 유형의 Ethernet mode를 지원합니다.

- Auto Negotiation
- 100 BaseT Half Duplex
- 100 BaseT Full Duplex
- 10 BaseT Half Duplex
- 10 BaseT Full Duplex

Ethernet mode를 변경한 후, 사용자는 시스템을 재부팅해야 합니다. Ethernet mode의 공장 출하시 기본값은 Auto Negotiation으로 설정되어 있습니다. 대부분의 네트워크 환경에서, Auto Negotiation 모드는 가장 무난하며 권장되는 모드입니다. Ethernet mode설정을 실제와 다르게 설정하면, VTS II가 네트워크 환경에서 동작하지 않을 수 있습니다.

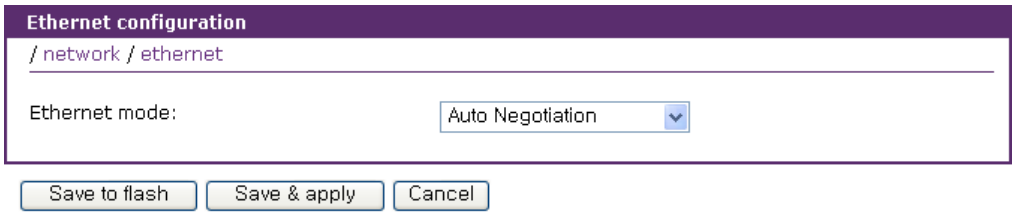


그림 3-12 Ethernet 모드 설정

3.10 TCP 서비스 설정

TCP 세션이 두 호스트 상에서 생성되는 경우, 호스트 TCP 포트의 lock-up을 방지하기 위해서, 정상적으로 종료되어야 합니다. 이러한 lock-up은 프로그램의 비정상적인 종료 등으로 인해 발생하며, 이러한 lock-up을 방지하기 위해서, VTS II는 TCP keep-alive 기능을 제공합니다. VTS II는 네트워크가 여전히 keep alive되어 있는지 확인하기 위해 주기적으로 상대 호스트에 패킷을 전송합니다. 반응이 없으면 상대 호스트에 이상이 있는 것으로 간주하고, 세션을 종료하게 됩니다.

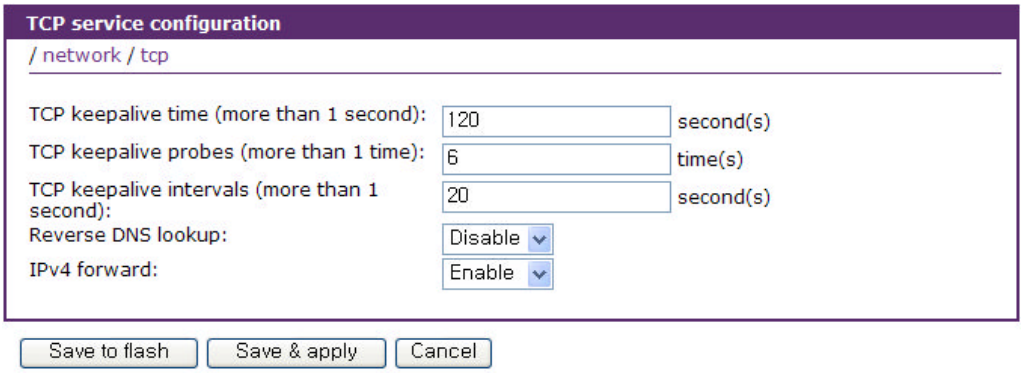


그림 3-13 TCP service 설정

VTS II로 TCP "keepalive" 기능을 사용하려면, 사용자는 다음과 같이 3개의 파라미터를 설정해야 합니다.

- **TCP keepalive time (sec)**:
  세션 간의 통신이 없는 상태에서 얼마나 경과하면 keepalive 패킷 전송을 시작할 것인지 여부를 결정합니다. 기본값은 120 초로 설정되어 있습니다.
- **TCP keepalive probes (times)**:
  연결을 종료할 때까지 정상 상태인지 여부를 확인하기 위해 원격 호스트에 keepalive 패킷을 몇 번이나 전송하는 가를 나타냅니다. 기본값은 6 회로 설정되어 있습니다.
- **TCP keepalive intervals (sec)**:
  Keepalive 패킷 전송의 시간 간격을 나타냅니다. 기본값은 20 초로 설정되어 있습니다.

공장 초기 설정일 때, VTS II 는 데이터가 통신이 없는 상태부터 120 초가 지난 후 20 초 간격으로 6 회 keepalive 패킷을 전송합니다.

Reverse DNS lookup을 Enable로 설정하면, VTS II는 xxx.xxx.xxx.xxx 형식의 IP 주소를 도메인 이름으로 변경하여 표시합니다.

IPv4 forward를 Disable로 설정하면, VTS II는 IPv4 패킷을 더 이상 전송하지 않습니다.

3.11 PPP 설정

PPP는 두 대의 컴퓨터가 직렬 인터페이스를 통해 통신할 때 필요한 프로토콜로 전화회선을 통해 서버에 연결하는 PC에서 사용됩니다. PPP는 IP를 사용하며, TCP/IP 패킷을 포장해서 실제 인터넷으로 보내어 질 수 있도록 통신합니다.
VTS II는 PC에서 Modem를 통해 VTS II로 연결할 수 있도록 아래와 같은 인터페이스를 제공합니다.

PPP를 통한 IP할당은 직접 지정 혹은 IP pool을 이용하여 동적으로 할당이 가능합니다. 그림 3-14는 동적 IP 할당을 위한 IP pool 설정 화면입니다.

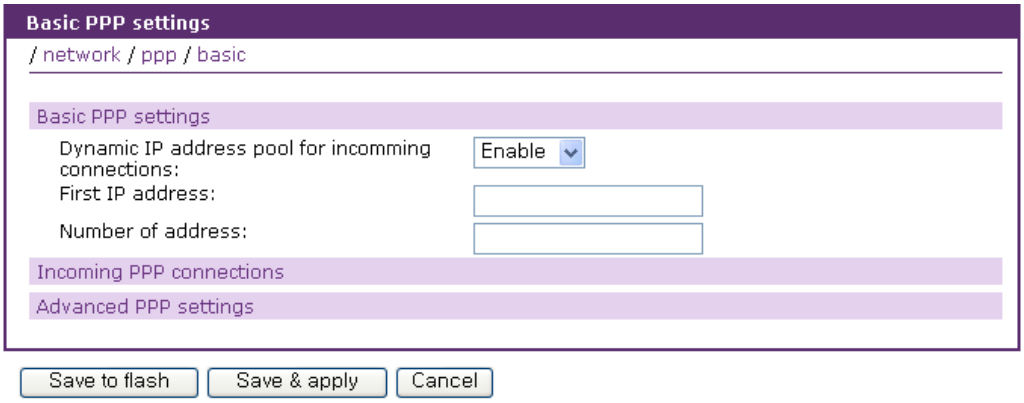


그림 3-14. Basic PPP 설정

PPP 연결을 위한 설정은 그림 3-15에서와 같이 사용자 별로 각기 다르게 설정이 가능합니다.

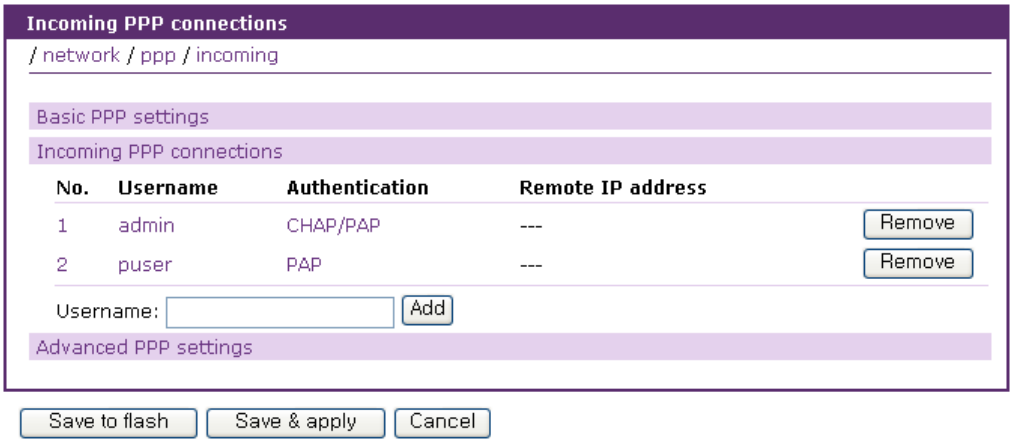


그림 3-15. Incomming PPP connections 설정

사용자별 설정은 그림 3-16과 같이, 사용자 이름, 패스워드, Authentication method, peer와 local IP설정, idle 상태 즉 주고 받는 데이터가 일정 시간 동안 없는 경우 접속을 끝는 idle timeout 을 설정합니다.

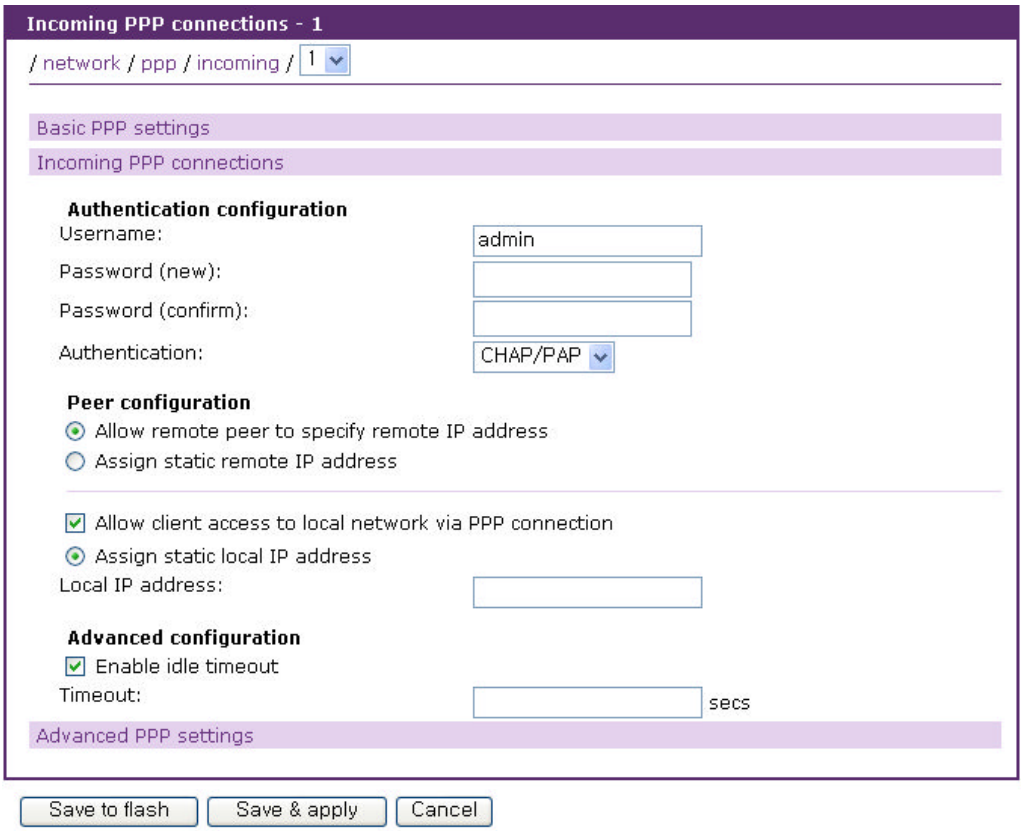


그림 3-16. 사용자별 PPP 설정 화면

그림 3-17은 Advanced PPP 설정 화면을 보여줍니다. Proxy ARP 설정은 peer의 IP와 system의 IP를 ARP table에 추가하도록 하는 옵션으로, peer쪽으로의 패킷이 라우팅 되도록 합니다.

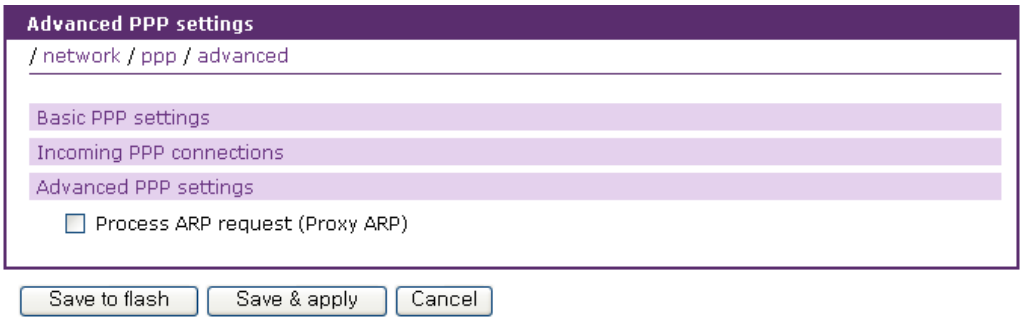


그림 3-17. Advanced PPP 설정

주의 :

1. PPP를 지원하기 위해선 모뎀을 통한 VTS II 연결이 PPP로 설정이 되어야 합니다.

2. 모뎀을 통한 PPP 연결을은 포트에 외장 모뎀을 연결하여 PPP를 지원하게 하거나 PC Modem Card() 혹은 내장 모뎀()을 이용하여 설정이 가능합니다.

4: 시리얼 포트 설정

4.1 개요

시리얼 포트 설정 기능을 통해 사용자는 각 포트의 Host mode, 시리얼 통신 파라미터, 포트 로깅 및 기타 관련 파라미터를 설정할 수 있습니다.

시리얼 포트의 Host mode는 다음과 같이 설정할 수 있습니다.

- **Console server mode**: 연결 요청은 원격 호스트로부터 전송됩니다. 이를 통해 원격지의 호스트는 VTS II의 시리얼 포트에 접속할 수 있습니다.
- **Terminal server mode**: 연결 요청은 시리얼 포트로부터 전송됩니다. 이를 통해 네트워크 상의 원격 호스트에 접속하거나 VTS II의 쉘 프로그램을 실행할 수 있습니다.
- **Dial-in modem mode**: 모뎀 연결을 통해 VTS II에 접속할 수 있습니다.
- **Dial-in terminal server mode**: 모뎀 연결을 통해 네트워크 상의 원격 호스트에 접속할 수 있습니다.

VTS II는 원격 호스트로부터 연결 요청이 오면 네트워크상의 원격 호스트로 접속하는 원격 포트(remote port) 기능도 지원합니다. 원격 포트는 시리얼 포트의 Console server mode처럼 원격 호스트로부터 연결 요청을 받지만 VTS II의 시리얼 포트로 접속하는 시리얼 포트의 Console server mode와는 달리 원격 호스트로 접속합니다. 그래서, 원격 포트에서는 시리얼 포트의 Serial port parameters 설정 대신 접속할 원격 호스트의 속성을 설정하는 Remote port parameters 설정이 사용됩니다.

VTS II는 또한 Port access menu를 제공합니다. 이 메뉴는 모든 시리얼 포트를 한번에 표시함으로써, 포트 접속을 용이하게 합니다. 사용자는 포트 번호를 나타내는 메뉴만 선택하여 모든 시리얼 포트에 접속할 수 있습니다.

콘솔 서버 모드에서 Port group으로 설정되어 있는 포트들은 그룹에 포함되어 있는 포트중 하나에 접속해서 다른 모든 포트들로 같은 명령어를 전송할 수 있습니다. 그리고, 특정 포트에 연결되어 있는 상태에서 같은 Port group 내의 다른 포트로의 전환이 가능합니다. 또한, Port group을 관리할 수 있는 설정 화면을 통해 그룹에 속할 포트들을 한꺼번에 설정할 수 있습니다.

VTS II는 시리얼 포트에 연결된 장치를 자동으로 검색할 수 있습니다. Port automatic detection configuration 설정 화면에서는 시리얼 포트에 연결된 장치의 baud rate를 검색하는 룰을 정의합니다. 또한 Automatic detection 설정을 이용 인식된 장치 정보의 활용을 정의합니다.

콘솔 서버 모드에서 Port logging 기능 상태에서, 시리얼 포트를 통해 전송되는 데이터는

MEMORY, NFS server storage, Sambe server storage, PC 카드 슬롯을 사용하는 ATA/IDE fixed disk card 또는 USB 슬롯을 사용하는 USB 메모리로 전달됩니다. 위에서 열거한 저장매체에 데이터를 저장하는 것과 동시에 SYSLOG server로 데이터를 전송하도록 설정할 수도 있습니다. 사용자는 포트 별로 키워드 메시지들을 등록할 수 있으며, 이때 VTS II는 등록된 메시지들이 도착되면 Email 또는 SNMP trap 을 통해 관리자에게 통보할 수 있습니다. 이를 통해 사용자는 연결된 장치로부터의 메시지를 감시할 수 있습니다.
MEMORY 에 저장된 데이터는 VTS II에 전원이 들어와 동작할 경우에만 유효합니다. 시리얼 포트 로그 데이터를 보존하려면 SYSLOG server, NFS server, ATA/IDE fixed disk card 또는 USB 메모리를 사용합니다.
VTS ||는 Multiple session 기능을 제공합니다. 즉, 여러 사람이 동시에 한 포트에 접속하여, 협업을 통해 교육 또는 Troubleshooting을 수행할 수 있는데, 포트당 최대 16명까지의 Multiple session 사용자를 등록할 수 있습니다.

콘솔 서버 모드의 시리얼 포트에 연결된 호스트나 리모트 포트로 연결되는 원격 호스트가 KVM 기능을 제공할 경우, VTS II는 사용자가 KVM 클라이언트 프로그램을 이용하여 호스트에 연결할 수 있는 수단을 제공합니다.

VTS II는 원격 감시/제어를 지원합니다. 시리얼 포트에 연결된 호스트나 리모트 포트로 연결되는 원격 호스트가 Intelligent Platform Management Interface(IPMI), Intergrated Lights-Out(iLO), Dell Remote Assistant Card(DRAC)를 지원하는 경우, VTS II는 IPMI, iLO, DRAC을 통해 호스트를 감시하거나 제어할 수 있습니다.

시리얼 포트와 원격 포트는 개별적으로 또는 한꺼번에 모두 설정할 수 있습니다. 표 4-1에 시리얼 포트 설정과 관련한 설정 파라미터를 요약하였습니다.

표 4-1. 시리얼 포트 설정 파라미터

Port Access Menu	Port Access Menu Enable/Disable
	Enable/Disable assigned IP
	Assigned IP
	Listening TCP port
	Protocol (Telnet or SSH)
	Inactivity timeout (seconds)
	Quick connect via (Web applet, Local client, User defined)
	Client program path
	Web applet encoding – Web applet only (English (latin1), Korean (KSC5601), Japanese (eucjp), Unicode (UTF8)
	Web applet size - Columns, Rows
	Login on port access Enable/Disable
	Authentication method (None, Local, RADIUS, TACAS+, LDAP…)
	Enable/Disable email alert for port login
	Title of email
	Recipient's email address
	Enable/Disable port login trap
	User global SNMP configuration

	First / Second Trap receiver settings	IP Address	
		Community	
		User name	
		Security level (NoAuth/NoPriv, Auth/NoPriv, Auth/Priv)	
		Engine ID	
		Version (v1, v2c, v3)	
Port group configuration	Group name		
	Login on each port (Enable/Disable)		
	Ports		
Port automatic detection configuration	Baudrate		
	Data bit		
	Paraty bit		
	Stop bit		
	Probe string		
	Wait time		
All ports setting Or Individual serial port setting #1~#5 (4, 8,16,32,48) Or Remote port	**Port Management**	Enable/Disable this port	
		Group	
		Reset this port (except all ports setting)	
		Set this port as factory default (except all ports setting)	
	Apply all port settings	Apply all port settings Enable/Disable (except all ports setting)	
	Automatic detection	Automatic detection Method (Off, Active, Passive)	
		Initial delay	
		Recheck interval	
		Start time	
		Probe string	
		Detected OS (Read only)	
		Use detected port title (Enable/Disable)	
		Use detected type of console server (Enable/Disable)	
		Use detected freeKVM (Enable/Disable)	
		Use detected serial parameters (Enable/Disable)	
		Automatic detection : Start Now	
	Port title	Port naming rule	
		Port title	
	Host mode configuration	**Console server**	Type of console server
			Service processor (NONE/IPMI/iLO/DRAC)
			Enable/Disable assigned IP
			Assigned IP
			Listening TCP port
			Protocol (Telnet/SSH/RawTCP)
			Inactivity timeout (0 for unlimited)
			Enable/Disable port escape sequence
			Port escape sequence
			Port break sequence
			Use comment
			Quick connect via
			Client program path
			Web applet encoding (same as Port access menu web applet encoding)
			Web applet size - Columns, Rows
		Terminal server (except remote port)	Terminal server option (Remote connection / Shell program)
			Terminal server shell program path
			Destination IP
			Destination port
			Protocol (Telnet/SSH/RawTCP)
			Inactivity timeout (0 for unlimited)

		Dial-in modem (except remote port))	Modem init string
			Enable/Disable dial-in modem callback
			Dial-in modem callback phone number
			Enable/Disable dial-in modem test
			Dial-in modem test phone number
			Dial-in modem test interval
		Dial-in terminal server (except remote port)	Terminal server option (Remote connection only)
			Destination IP
			Destination port
			Protocol (Telnet/SSH/ RawTCP)
			Inactivity timeout (0 for unlimited)
			Modem init string
		PPP	Modem init string
	freeKVM configuration	freeKVM connection Enable/Disable	
		Automatic IP detection	
		IP address	
		Client program	
		Socket/Screen number for VNC connection	
		Client program path	
	Serial Port Parameters (except remote port)	Baudrate	
		Data bit	
		Stop bit	
		Paritybit	
		Flow control	
		DTR option (except Dial-in modem / Dial-in terminal server)	
		Enable/Disable delimiter (RawTCP only)	
		Delimiter (RawTCP only)	
		Delimiter option (with / without delimiter) (RawTCP only)	
		Inter character timeout (ms) (RawTCP only)	
	Remote Port Parameters (remote port only)	Destination IP	
		Destination port	
		Protocol	
		OEM type	
		SMASH (Enable/Disable)	
		Allow unattended continuous connection	
		User name	
		Password	
		Reestablishment interval	
	Port logging (only provided in console server mode)	Port logging (Enable/Disable)	
		Logging direction (Server output / User input / Both with arrows / Both without arrows)	
		Port log storage location (Memory / CF card / NFS server)	
		Port log to SYSLOG server Enable/Disable	
		SYSLOG facility for port logging	
		Port log buffer size	
		Port log file name option (User port title / Specify below)	
		Port log file name	
		Time stamp to port log (Enable/Disable)	
		Show last 10 lines of a log upon connect (Enable /Disable)	
		Strip the ^M from SYSLOG (Port log SYSLOG server enable only)	
		Automatic backup on mounting	
	Port event handling (only provided on port logging enabled)	Monitoring interval (sec.)	
		Key word	
		Case sensitive	
		Email notification (Enable/Disable)	
		Title of email	
		Recipient's email address	

		SNMP trap notification (Enable/Disable)		
		Title of SNMP trap		
		Use global SNMP configuration		
		First / Second Trap receiver settings	IP Address	
			Community	
			User name	
			Security level	
			Engine ID	
			Version (v1, v2c, v3)	
	Authentication	None		
		Local		
		RADIUS server	First/Second authentication server	
			First/Second accounting server	
			Shared secret	
			Timeout (0-300 sec.)	
			Retries (1-50 times)	
		TACAS+ server	First/Second authentication server	
			First/Second accounting server	
			Shared secret	
			Authorization service	
		LDAP server	First/Second authentication server	
			LDAP search base	
			Domain name for active directory	
		Kerberos server	First/Second authentication server	
			Realm for first/second kerberos server	
		Custom PAM		
	User access control	**<<Everyone>> or individual user's or access list's access**	Port	
			Monitor	
			Power	
		Multiple session	Enable/Disable multiple session	
			Session display mode (Server output / User input / Both)	
			Display data direction arrows Enable/Disable	
	Alert configuration	**Console server**	Email alert for port login (Enable/Disable)	
			Title of email	
			Recipient's email address	
			Email alert for device connection	
			Title of email	
			Recipient's email address	
			Email alert for active detection	
			Title of email	
			Recipient's email address	
			Email alert for service processor	
			Title of email	
			Recipient's email address	
			Port login trap (Enable/Disable)	
			Device connection trap (Enable/Disable)	
			Active detection trap (Enable/Disable)	
			Service processor trap (Enable/Disable)	
			Use global SNMP configuration	
			First / Second Trap receiver settings	IP Address
				Community
				User name
				Security level
				Engine ID
				Version (v1, v2c, v3)
			Email alert for dial-in modem test	

		Dial-in modem (Dial-in modem test enabled)	Title of email	
			Recipient's email address	
			Dial-in modem test trap	
			Use global SNMP configuration	
			First / Second Trap receiver settings	IP Address
				Community
				User name
				Security level
				Engine ID
				Version (v1, v2c, v3)
	Power control configuration	Power controller		
		Outlet		
	Service processor configuration	Destination IP		
		Destination port		
		User name		
		Password		
		Sensor alert configration	Sensor type	
			Email alert	
			SNMP alert	

그림 4-1은 웹 기반 시리얼 포트 설정 화면을 보여줍니다.

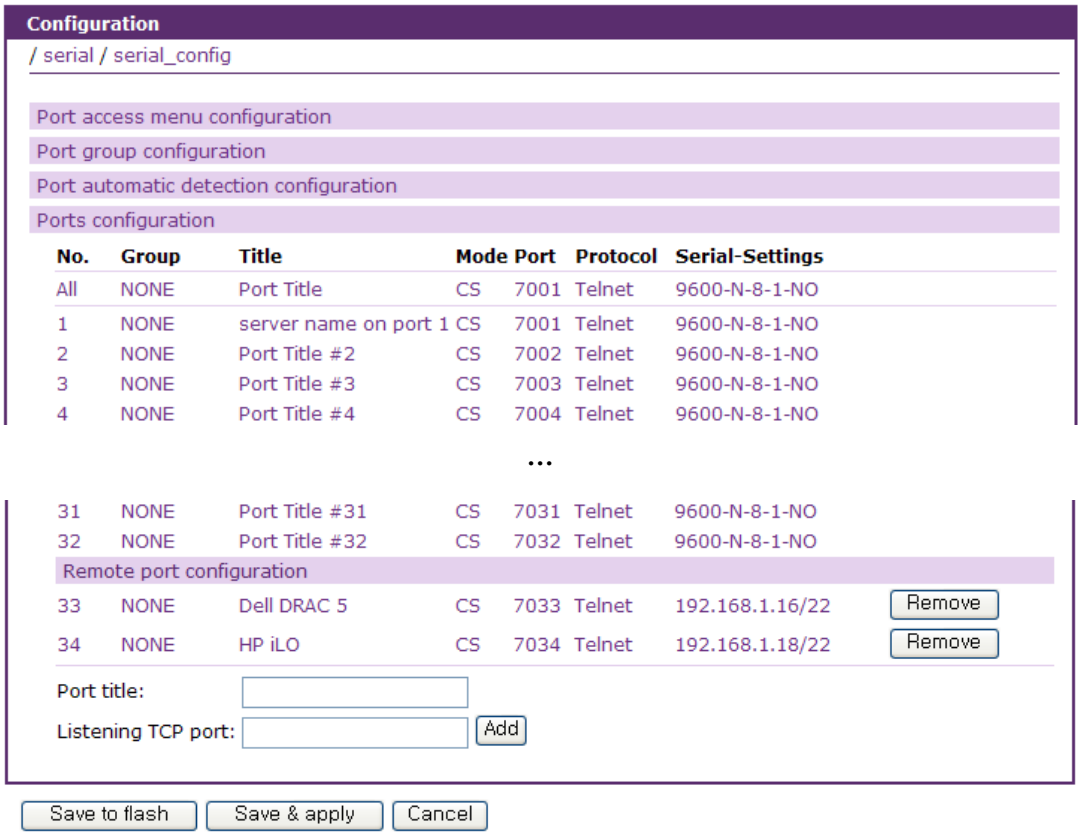


그림 4-1 시리얼 포트 설정 메인 화면

개별적으로 시리얼 포트 또는 원격 포트를 선택하고 설정하려면 해당 포트의 포트 번호, 타이틀,

모드, Dest/Assigned IP, Port, Protocol 또는 시리얼 설정을 클릭합니다. 클릭한 항목과 관련있는 설정 화면으로 연결되어 설정을 변경할 수 있게 됩니다. 시리얼 포트와 원격 포트를 한꺼번에 모두 설정하려면, 포트 번호에 **[All]**이라고 표시된 행의 항목을 선택하면 됩니다.

사용자는 원격 포트 설정에서 원격 포트 타이틀과 Listening TCP port를 입력하고 **[Add]** 버튼을 클릭하여 원격 포트를 추가할 수 있고, **[Remove]** 버튼을 클릭하여 원격 포트를 삭제할 수 있습니다.

사용자는 웹 인터페이스 상에서, 터미널 에뮬레이션 Java Applet을 이용하여 각 시리얼 포트 또는 원격 포트와 **Port access menu** 에 연결할 수 있습니다.

1. 사용자는 왼쪽 메뉴 바에 있는 **Serial port** > **Connection** 을 선택해야 합니다.
2. 연결하려는 포트의 포트 번호나 포트 타이틀을 클릭해야 합니다.
3. 사용자는 **Individual port connection**에 있는 터미널 Icon을 선택해야 합니다.
4. 사용자는 현재 **port access menu connection**에 제공된 시리얼 포트 링크를 사용할 수도 있습니다.

***참고**: 포트 연결에 대한 자세한 사항은 **4.7 Serial port 연결**을 참고하시기 바랍니다.*

4.2 Port access menu 설정

4.2.1 개요

VTS II는 **Port access menu**를 이용하여 Telnet/SSH 클라이언트 연결을 통해 지정된 가상 포트로 연결할 수 있습니다. **Port access menu**와 연결되면, VTS II는 **Port access menu** 를 통해 모든 시리얼 포트와 원격 포트로의 연결 경로를 보여줍니다. 이는 또한 포트 번호, 포트 타이틀 및 시리얼 포트 모드를 포함합니다. VTS II는 사용자가 메뉴의 동일한 포트 번호를 선택하여 콘솔 서버로 설정된 시리얼 포트에 접속하도록 허용합니다. 사용자는 R을 선택하여 원격 포트 리스트 화면으로 이동한 후 원격 포트 번호를 선택하여 원격 포트에 접속할 수 있습니다.

그림 4-2는 윈도우 Telnet 프로그램을 사용하여 **Port access menu**에 접속한 화면을 보여줍니다.

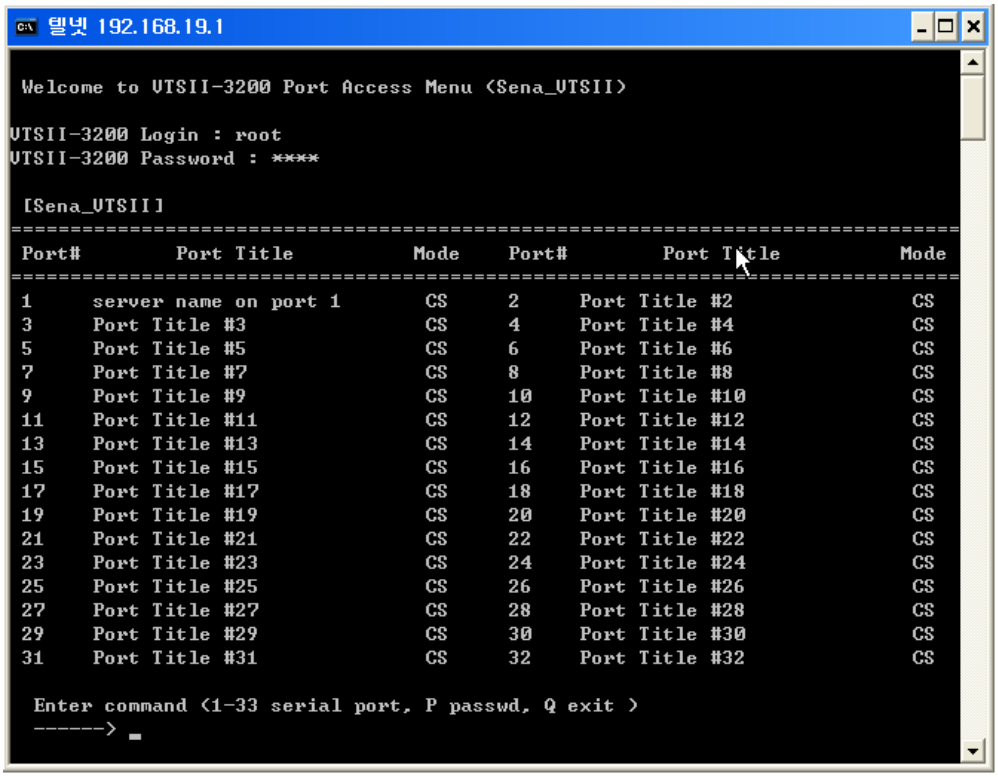


그림 4-2 Telnet을 이용하여 포트 액세스 메뉴에 접속하기

VTS II는 다음을 수행함으로써 사용자가 가상 포트에 연결되도록 합니다.

- VTS II의 IP 주소 및 **Port access menu** 로 지정된 TCP 포트 번호를 사용합니다.
- **Port access menu** 로 지정된 IP 주소 및 Telnet 또는 SSH의 TCP 포트 번호를 사용합니다.

예를 들어, 만일 VTS II의 IP 주소가 192.168.1.100이고, **Port access menu** 의 TCP 포트 번호가 7000인 경우, 사용자는 윈도우 명령 프롬프트에서 다음 명령을 입력할 수 있습니다.

```
telnet 192.168.1.100 7000 <ENTER>
```

Port access menu의 IP 주소가 192.168.1.132인 경우, 사용자는 윈도우 명령 프롬프트에서 다음을 입력하여 해당 포트 번호를 사용하지 않고도 포트에 연결할 수 있습니다.

```
telnet 192.168.1.132 <ENTER>
```

그림 4-3은 포트 액세스 메뉴 설정 화면을 보여줍니다.

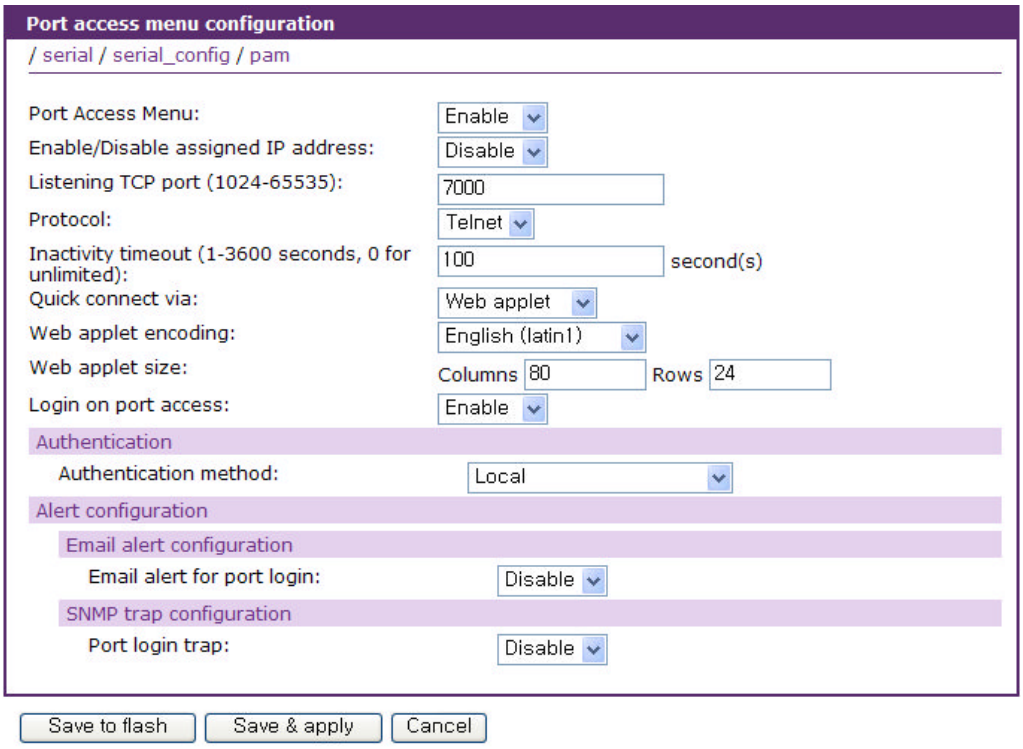


그림 4-3 포트 액세스 메뉴 설정

Login on port access를 Disable로 설정하면, Port access menu로 통해서 시리얼 포트로 연결할 때 시리얼 포트의 사용자 인증 절차 없이 접근 가능합니다.

Enable/Disable email alert를 Enable로 설정하면, 사용자가 Port access menu로 로그인 또는 로그아웃 할 때 설정된 주소로 설정된 제목의 이메일이 전송됩니다. **Enable/Disable port login trap**을 Enable로 설정하면, Trap receiver settings의 설정에 따라 SNMP trap을 전달합니다.

Qucick connect via 메뉴는 Web applet, Local client, User defined 중 하나를 선택할 수 있습니다. Web applet로 설정된 경우, JTA를 통해 Port access menu를 사용할 수 있습니다. 이때 **Web applet size**를 통해 JTA 윈도우의 크기를 지정합니다. Local client로 설정된 경우 Client 의 설정에 따라 해당 프로그램이 실행됩니다. User defined 로 설정하여 해당 경로에 있는 프로그램을 실행할 수도 있습니다.

***참고**: 포트 액세스 메뉴의 IP 주소를 할당하는 경우, 사용자는 다른 호스트 IP 주소와 충돌되지 않도록 주의하여야 합니다. 만일 충돌되는 경우, 포트 액세스 메뉴의 IP 주소가 Disable 상태가 됩니다. Assigned IP를 Disable 시키거나 Assigned IP를 0.0.0.0으로 하면 해당 시리얼 포트에 IP를 할당하지 않으며 해당 포트는 VTS II의 IP address 와 포트 번호를 통해서만 접속이 가능 합니다.*

4.2.2 Port access menu에 대한 인증

사용자가 VTS II의 **Port access menu**에 접속하기 위해서는 이중적인 인증 절차를 걸쳐야 합니다. **Port access menu**에 접속하려면 사용자는 우선 **Port access menu**에 대한 인증을 받아야 합니다. 다음에 **Port access menu**에서 시리얼 포트를 선택하면 해당되는 시리얼 포트 접속을 위한 인증을 받아야 합니다. 만일 Port access menu의 **Authentication method**가 **None**으로 설정된 경우, 모든 사용자는 **Port access menu** 접속하여 시리얼 포트/원격 포트를 사용할 수 있습니다. 시리얼 포트/원격 포트의 **Authentication method**가 **None**으로 설정된 경우에, 사용자는 인증 없이 시리얼 포트/원격포트에 접속할 수 있습니다.
만일 Port access menu의 **Authentication Method**가 Local로 설정되어 있거나 다른 방법(예. RADIUS, LDAP, KERBEROS 또는 TACACS+)이 지정되는 경우, 사용자는 다음 조건에 부합할 때만 **Port access menu**의 시리얼 포트에 접속할 수 있습니다.

- 사용자가 **Port access menu** 인증을 통과.
- 사용자가 **Port access menu** 의 시리얼 포트 인증을 통과.
- 사용자가 포트 사용자 목록에 등록됨.

사용자가 인증을 받은 경우, **Console server mode**로 설정되어 있는 시리얼 포트에만 접속할 수 있고, 다른 모드로 설정된 시리얼 포트에는 접속할 수 없습니다.
인증 방법에 대한 자세한 내용은 ***4.5.10 Authentication 설정***을 참조하시기 바랍니다.

4.2.3 Port access menu 프로토콜

Telnet/SSH를 사용하려면 **Port access menu** 프로토콜을 설정해야 합니다. **Port access menu**의 프로토콜이 각각의 시리얼 포트/원격 포트의 프로토콜과 일치하지 않을 수도 있습니다. 시리얼 포트/원격 포트의 프로토콜은 원격 호스트로부터 VTS II로의 연결 방법을 명시하는 것이므로, 사용자가 **Port access menu**를 통해 VTS II로 로그인 했다면 각각의 시리얼 포트의 프로토콜은 의미가 없습니다. **Port access menu**의 프로토콜이 각각의 시리얼 포트의 프로토콜 설정에 우선하게 되며, 이 경우 각 시리얼 포트/원격 포트의 설정은 적용되지 않습니다.

4.2.4 Port access menu options

Quick connect via option은 Serial port 연결 페이지를 통한 접속 시 사용할 Client 프로그램을 지정할 수 있게 합니다. **Quick connect via** option이 **Web applet**으로 설정되어 있다면, 웹 애플릿은 서버로부터 받은 데이터를 화면에 표시하기 위해 **Web applet encoding** option을 이용하여 설정된 문자모음으로 변환합니다. **Email alert for port login** option이 Enable로 설정되면 사용자가 Port access menu로 로그인 또는 로그아웃 할 때마다 VTS II는 이메일 경보 설정(**Email alert configuration**)에 따라 이메일을 전송합니다. **Port log in trap** option이 Enable로 설정되고, 트랩 수

신기 설정(Trap receiver settings)에서 IP 주소가 트랩 수신기로 바르게 설정되면, 사용자가 Port access menu로 로그인 또는 로그아웃 할 때마다 VTS II는 트랩 수신기 설정에 맞추어 트랩을 보냅니다. **Use global SNMP configuration**이 Enable로 설정되면 **SNMP Configuration**에서 설정된 트랩 수신기 설정이 SNMP 트랩의 목적지로 사용됩니다. 자세한 내용은 ***3.2 SNMP 설정***을 참조하시기 바랍니다.

4.2.5 Clustering시의 port access menu

Clustering Master / Slave(***5.2 Clustering Master / Slave 설정*** 참조)를 사용하는 경우 Master unit의 **Port access menu**를 통하여 Slave unit으로 접속하게 됩니다. **Port access menu**의 메인 메뉴에서 S를 입력하고 Slave unit 선택메뉴에서 1~48까지의 유닛 번호를 입력하여 원하는 Slave unit을 선택할 수 있습니다. Slave unit에 접속하면 해당 unit의 **Port access menu**가 나타나며, 여기서 원하는 Port를 선택하면 원하는 포트를 접근할 수 있습니다.

Clustering Peer-to-peer(***5.3 Clustering Peer-to-peer 설정*** 참조)를 사용하는 경우, **Port access menu**를 통하여 다른 Peer unit으로 접속할 수 있습니다. **Port access menu**의 메인 메뉴에서 R를 입력하고 Peer unit 선택메뉴에서 Peer 유닛 번호를 입력하면 원하는 Peer unit의 **Port access menu**로 연결되고, 원하는 포트를 선택해서 포트에 접근하게 됩니다.

```
 [SENA_VTSII]
================================================================================
Port#       Port Title         Mode    Port#       Port Title         Mode
================================================================================
 1   server name on port 1     CS      2   Port Title #2             CS
 3   Port Title #3             CS      4   Port Title #4             CS
 5   Port Title #5             CS      6   Port Title #6             CS
 7   Port Title #7             CS      8   Port Title #8             CS
 9   Port Title #9             CS     10   Port Title #10            CS
11   Port Title #11            CS     12   Port Title #12            CS
13   Port Title #13            CS     14   Port Title #14            CS
15   Port Title #15            CS     16   Port Title #16            CS
17   Port Title #17            CS     18   Port Title #18            CS
19   Port Title #19            CS     20   Port Title #20            CS
21   Port Title #21            CS     22   Port Title #22            CS
23   Port Title #23            CS     24   Port Title #24            CS
25   Port Title #25            CS     26   Port Title #26            CS
27   Port Title #27            CS     28   Port Title #28            CS
29   Port Title #29            CS     30   Port Title #30            CS
31   Port Title #31            CS     32   Port Title #32            CS

  Enter command (1-33 serial port, S slave unit, R peer unit, P passwd
                 <Enter> More, Q exit )
  ------> S

 [SENA_VTSII]
 ================================================================================
  Unit #        IP                  Unit #        IP
 ================================================================================
    1      192.168.19.2              2        ----------
    3      ----------                4        ----------
    5      ----------                6        ----------
    7      ----------                8        ----------
    9      ----------                10       ----------
```

```
  11      ----------                  12       ----------
  13      ----------                  14       ----------
  15      ----------                  16       ----------
  17      ----------                  18       ----------
  19      ----------                  20       ----------
  21      ----------                  22       ----------
  23      ----------                  24       ----------
  25      ----------                  26       ----------
  27      ----------                  28       ----------
  29     ----------                   30       ----------
  31      ----------                  32       ----------

 Enter command (1-48 slave unit, L serial port, R peer unit, P passwd,
                <Enter> More, Q exit )
 ------> R

[SENA_VTSII]
================================================================================
 Unit #         IP                  Unit #         IP
================================================================================
  1      [192.168.19.1]             2        192.168.19.3
  3      192.168.19.4

 Enter command (1-3 peer unit, L serial port, S slave unit, P passwd, Q exit)
 ------>
```

4.3 포트 그룹 설정

VTS II에서는 각 포트를 그룹으로 설정할 수 있습니다. 그룹으로 설정된 포트들은 한꺼번에 같은 명령어 전송이 가능합니다. 또한 한 포트로 연결해서 그룹내의 다른 포트로의 전환이 가능하며, 이때, **Login on earch port** 옵션이 Enable로 설정에 되면 사용자 인증과정을 거치게 됩니다. 그룹 내 포트들의 관리를 용이하게 하기위해, 포트 그룹은 모든 포트 설정을 적용할 대상을 선택하는데에도 사용됩니다. 모든 포트 설정에서 설정을 적용할 포트 그룹을 선택하고 저장하면 해당 포트 그룹에 속한 포트에 대해서만 설정을 적용합니다. (4.6 All Port 설정 참조) 그림 4-4 는 포트 그룹 관리를 위한 설정 화면을 보여줍니다. 포트 그룹내 포트들의 관리는 그림 4-5과 같은 설정 화면을 통해 관리하거나, 각 포트별 Port management 설정 화면에서도 가능합니다.(4.5.1 Port management 참조)

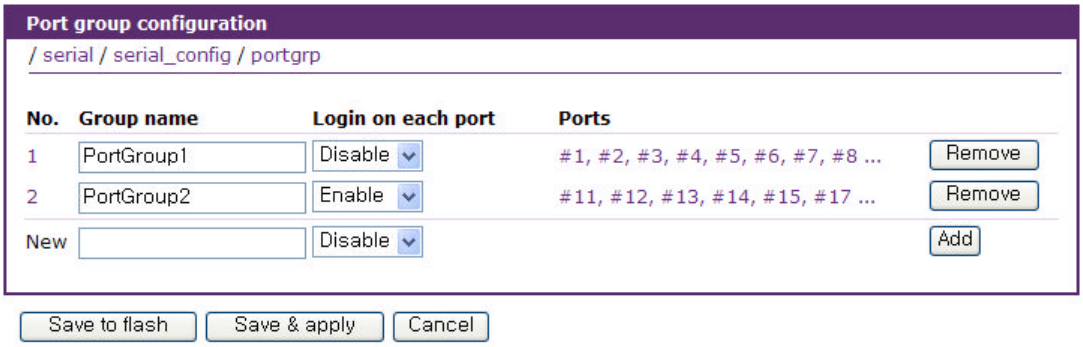


그림 4-4 포트 그룹 설정

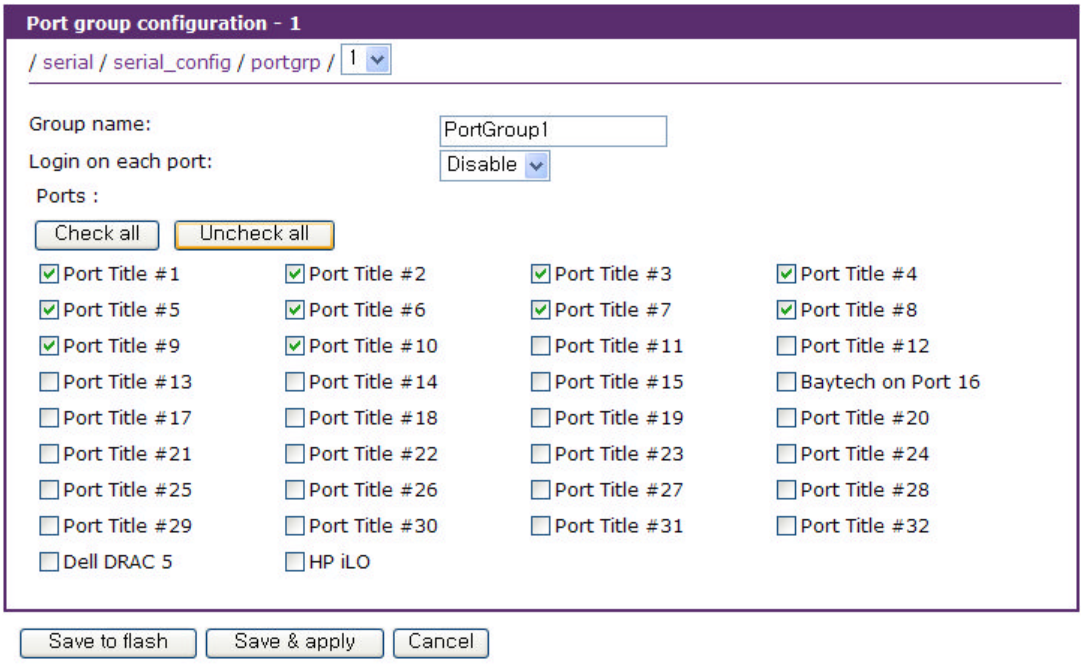


그림 4-5 포트 그룹 세부 설정

그룹내의 한 포트로 연결 후, port escape menu로 들어가면 port group 명령이 나타납니다.

```
Port Menu:

 b     send break
 l     show last 100 lines of log buffer
 a     send message to port user
 g     port group 'PortGroup1'

 x     close current connection to port
<Port Group 'PortGroup1'>
 c     send command to all ports
 s     switch to a port
 l     show last 100 lines of log buffer
 Select a port to connect
 ( [*]1 2 3 4 5 6 7 8 9 10  )
 -----> 2

 Entering server port, ..... type ^z for port menu.
```

Port group 명령어 'g'를 선택하면, **send command to all ports**, **switch to a port** 명령을 통해. 그룹내 모든 포트로 같은 명령어를 보내거나 다른 포트로 접속할 수 있습니다. 또, **show last 100 lines of log buffer**를 통해 다른 포트의 로그를 확인할 수 있습니다.

4.4 Port automatic detection configuration 설정

VTS II는 시리얼 포트에 연결된 장치의 시리얼 설정을 자동으로 검색할 수 있습니다. Port automatic detection 설정 화면을 통해 자동 검색시 시도되는 설정을 순서대로 정의합니다.

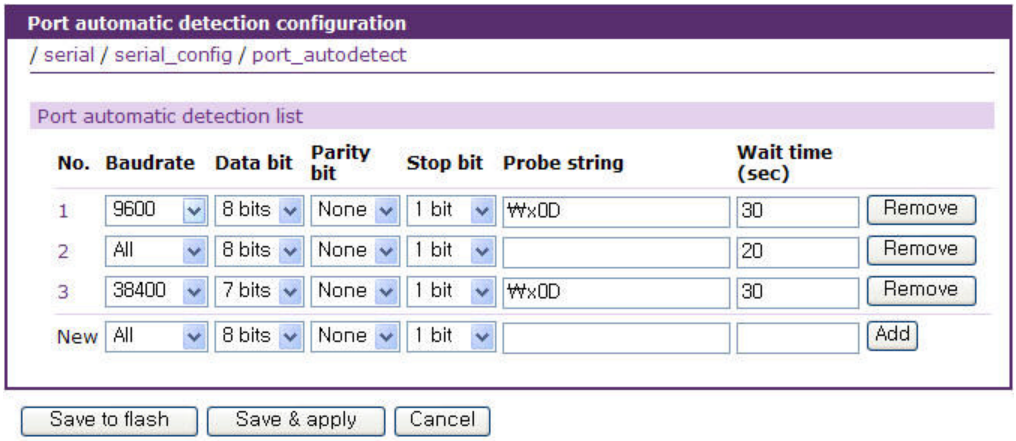


그림 4-6 Automatic detection list

그림 4-6은 9600-8-N-1, All-8-N-1, 38400-7-N-1의 순으로 probe string과 wait time을 달리하며 검색하도록 설정해놓은 룰입니다. Probe string이 없는 경우는 장치로부터 나오는 메시지를 wait time 동안 기다려서 적합한 시리얼 포트 설정을 찾아냅니다. Probe string이 있는 경우는 이를 보내고 나오는 응답을 wait time 동안 기다려서 적합한 설정을 찾아냅니다.

4.5 개별 포트 설정

VTS II의 시리얼 포트/원격 포트는 개별적으로 또는 모든 포트를 동시에 설정될 수 있는데, 개별 설정 및 모든 포트 설정에 대한 파라미터는 동일합니다. Basic configuration 페이지를 통해 간단히 기본적인 포트 설정을 하거나 보다 Advance configuration 페이지를 통해 상세한 설정을 할 수 있습니다. 그림 4-7은 Basic configuration 메뉴의 설정 화면을 보여줍니다. Basic configuaration 페이지에서는 포트 활성화 및 비활성화, Host mode 설정, Automatic Detection 등의 관련 설정을 입력된 정보를 바탕으로 자동으로 설정합니다.

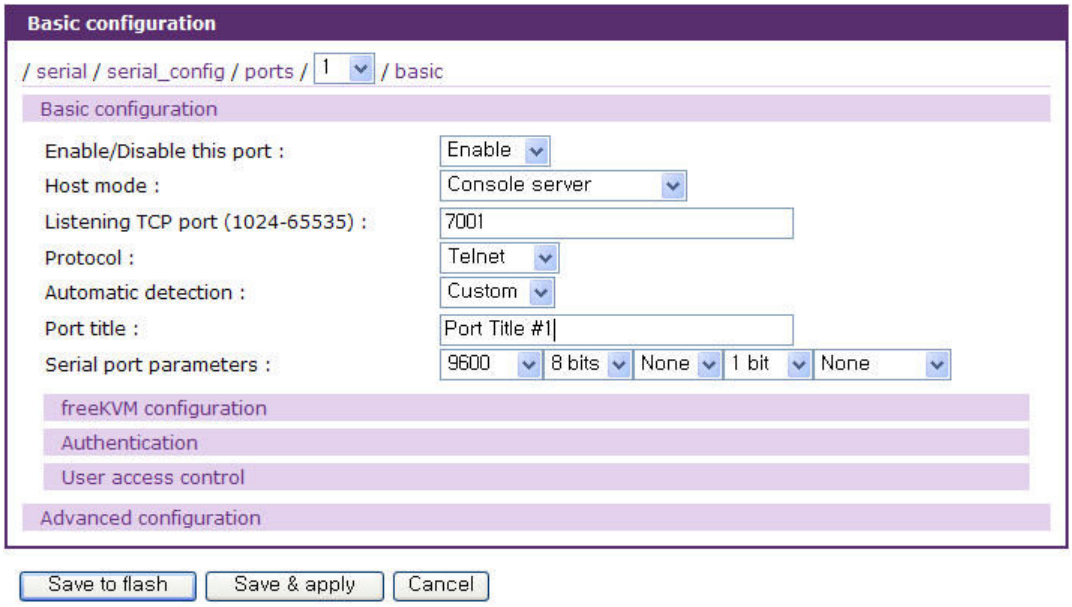


그림 4-7 Basic Configuration

Advanced configuration에서는 각각의 개별 포트 설정을 직접 입력할 수 있습니다. 개별 포트 설정은 다음과 같이 14개 그룹으로 분류됩니다.

1. Port management
2. Apply all port settings
3. Automatic detection
4. Port title
5. Host mode configuration
6. freeKVM configuration: *Only available if the host is set to Console Server Mode.*
7. Serial port parameters: *Only available for serial port*
8. Port logging: *Only available if the host is set to Console Server Mode.*
9. Port event handling: *Only available if the host is set to Console Server Mode and Port logging is enabled.*
10. Authentication
11. User access control: *Only available if the host is set to Console Server Mode.*
12. Alert configuration: *Only available if the host is set to Console Server Mode.*
13. Power control configuration : *Only available if a power controller is added.*
14. Service processor configuration: *Only available if the host is set to Console Server Mode and Service processor is IPMI or iLO.*

각각의 개별 포트 설정화면의 우측 상단에 있는 [--- Move to ---] 리스트 박스에서 이동을 원하는 포트를 선택하여 다른 포트의 설정화면으로 쉽게 이동할 수 있습니다.

4.5.1 Port management

각 시리얼 포트와 원격 포트는 Enable/Disable 될 수 있습니다. 만약 시리얼 포트/원격 포트가 Disable 상태가 되면 사용자는 해당 시리얼 포트로 접속할 수 없습니다. **Group** 설정을 통해 포트를 포트 그룹 설정에서 작성한 포트 그룹에 포함 시킬 수 있습니다. 그림 4-8는 Port Management 화면을 보여줍니다.

문제가 발생한 포트는 **[Reset this port]** 부분의 **[Reset]** 버튼을 눌러 재설정할 수 있고, **[Set this port as factory default]** 부분의 **[Set]** 버튼을 눌러 공장 출하시의 상태로 설정할 수 있습니다.

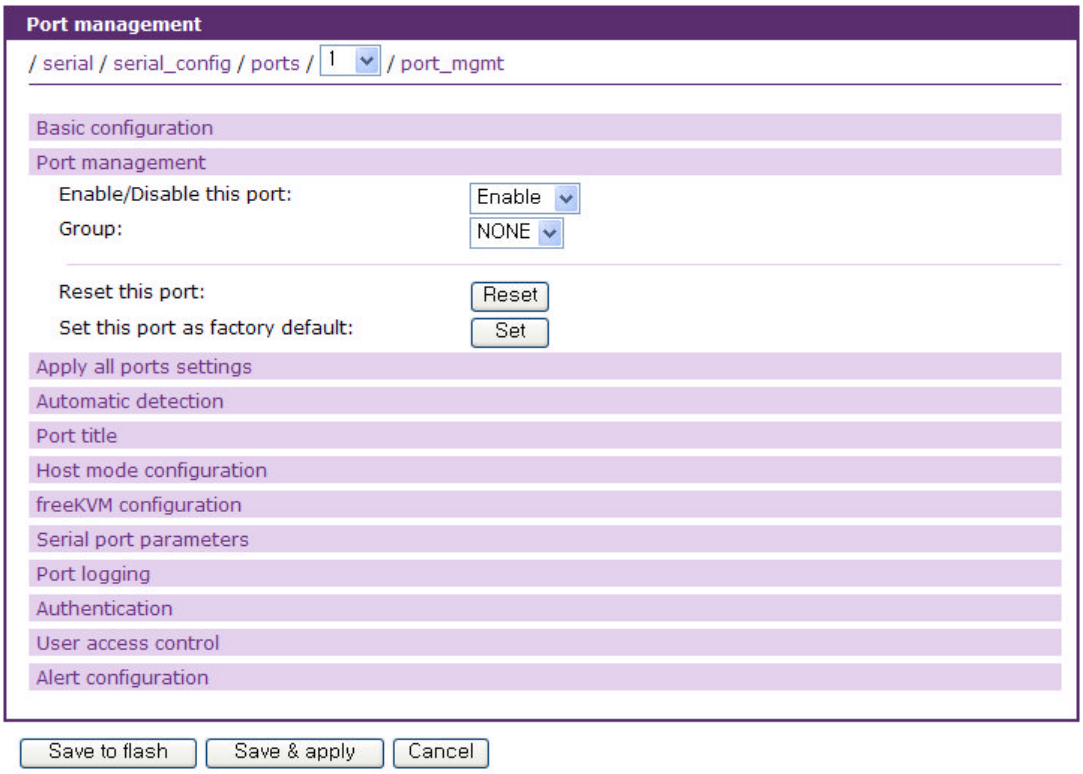


그림 4-8 Port Management

4.5.2 Apply all ports settinigs

사용자가 All ports settings를 수행하여 모든 포트의 설정을 한꺼번에 수행하다가, 변경해서는 안 되는 기존 포트 설정 값들을 All port settings 과정에서 수정되는 것을 막기 위해, VTS II는 개별 포트 설정에서 이를 허용할 지 말지 여부를 설정할 수 있게 합니다. **Apply all ports settings** 파라미터가 Enable로 설정되면 All port settings에서 설정을 변경하면 이 포트의 설정도 변경됩니다. Disable 설정된 경우, 기존의 포트 설정 값은 All ports setting을 수행하더라도 유지되게 됩니다.

그림 4-9는 Apply all ports settings 설정 화면을 보여줍니다.

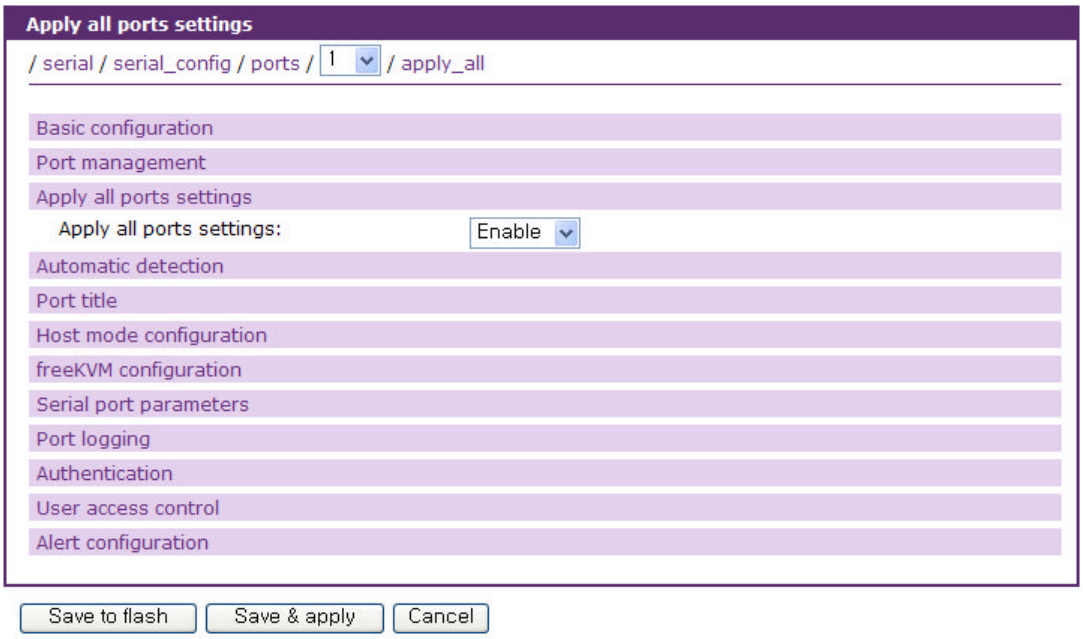


그림 4-9 Apply all ports settings 설정

4.5.3 Automatic detection

사용자는 각각의 포트에 연결된 장치에 대한 정보를 자동으로 검색할 지 여부를 설정합니다. 여기에는 장치의 시리얼 설정과 운영체제, 호스트 이름 정보, IP 주소, 콘솔 서버 종류 등이 포함될 수 있습니다. 자동으로 검색된 정보를 바탕으로 포트 타이틀과 콘솔 서버의 종류, freeKVM 및 시리얼 포트 설정을 변경할 수 있습니다.

그림 4-10은 Automatic detectioin 설정 화면을 보여줍니다.

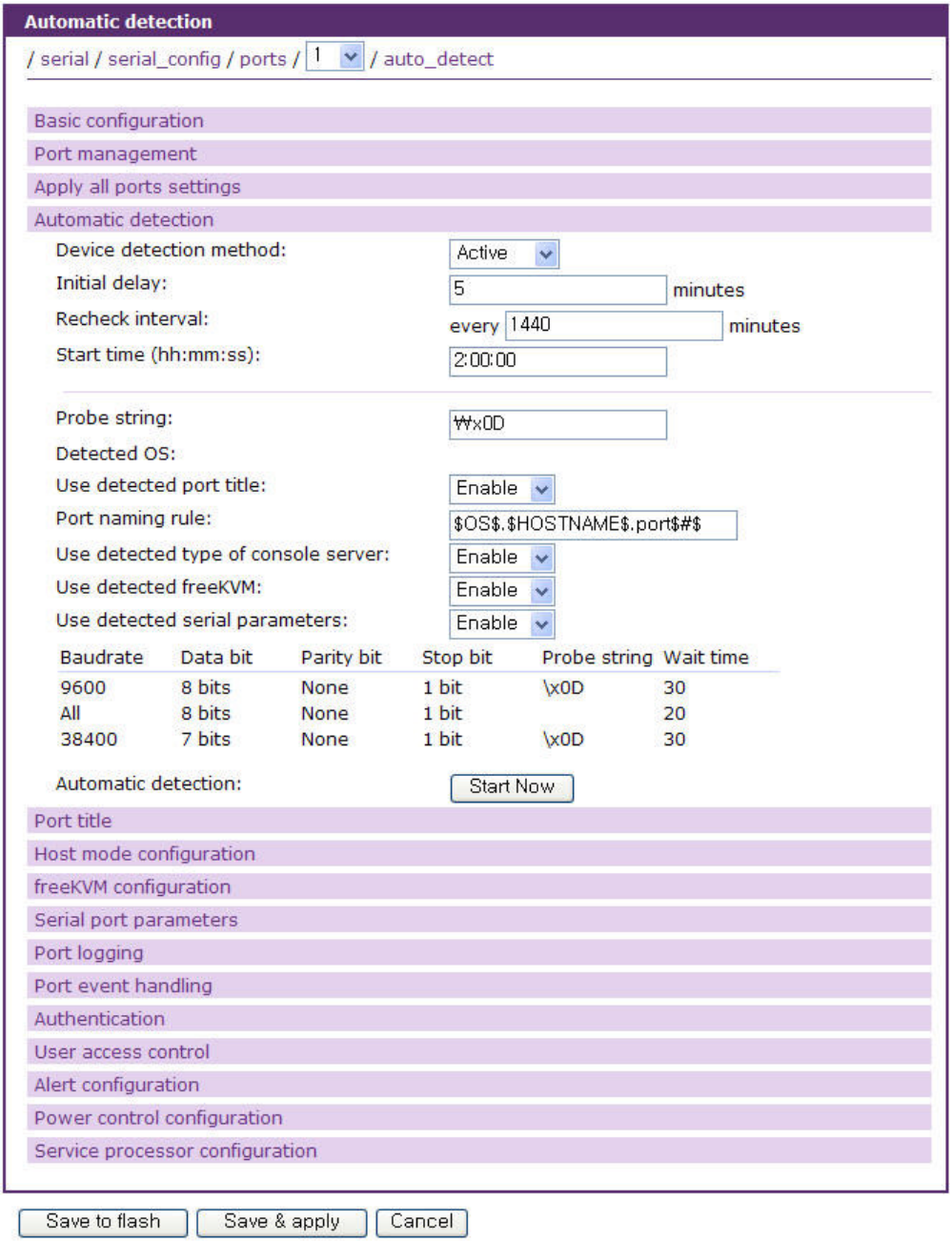


그림 4-10 Automatic detectioin 설정

Automatic detection에서 필요한 파라미터는 다음과 같습니다.

Device detection method

Initial delay

Recheck interval

Start time

Probe string

Use detected port title

Port naming rule

Use detected type of console server

Use detected freeKVM

Use detected serial parameters

Device detection method

시리얼 포트에 연결된 장치의 운영체제나 호스트 이름 등의 정보를 자동으로 수집할 지 여부와 수집 방법 를 설정합니다. **Host mode**가 **Console server** 모드이고 연결된 장치가 파워 컨트롤러가 아닐 때에만 **Off/Active/Passive** 중에서 선택 가능하고 그렇지 않으면 **Off**로 자동 설정됩니다. 원격 포트의 경우에는 항상 Off로 설정되고 변경될 수 없습니다. **Active**는 VTS II가 실제로 장치와 명령을 주고 받으면서 장치에서 받은 데이터를 바로 분석하여 장치의 정보를 구합니다. **Passive**는 포트 로그를 분석하여 장치의 정보를 구합니다. 따라서, **Passive**는 **Port logging**이 **Enable**로 설정되어야 선택 가능하게 됩니다. /etc/active_detect 또는 /etc/passive_detect script를 변경하여 장치에서 보내온 데이터에서 장치의 운영체제와 호스트 이름을 분리해 내는 방법을 수정할 수 있습니다. 운영체제는 /var/run/OSPortxx 파일에 호스트 이름은 /var/run/HostnamePortxx 파일에, 그 외 정보들은 /var/run/detectedPortxx 파일에 기록됩니다. 여기서, xx는 포트번호를 나타냅니다. 기본적으로 장치 정보 수집은 주기적으로 일어나며, 새로운 장비가 포트에 연결된 경우에도 정보 수집을 시행합니다. **Active**로 설정된 경우 VTS II가 장치정보를 분석한 결과를 **Alert 설정**에서 설정한 데로 Email이나 SNMP trap을 전송합니다. 자세한 내용은 ***4.5.11 Alert 설정***을 참조하시기 바랍니다.

Initial delay

Device detection method가 **Active** 혹은 **Passive**인 경우 입력 가능합니다. VTS II가 장치 정보를 수집하는 초기 지연 시간을 설정합니다.

Recheck interval

Device detection method이 **Active** 혹은 **Passive**인 경우 입력 가능합니다. VTS II가 장치 정보를 분석하는 주기를 설정합니다. 0인 경우 주기적으로 장치 검색을 수행하지 않습니다.

Start time

Device detection method가 **Active** 혹은 **Passive**인 경우 입력 가능합니다. VTS II가 장치 정보를 분석하는 시작 시간을 설정합니다. 시간을 입력하지 않으면 현재 시간을 시작 시간으로 동작합니다.

Probe string

Automatic detection이 **Enable**로 설정된 경우에만 입력 가능합니다. 장치 정보를 수집하기 위해 VTS II가 장치에게 보내는 명령을 설정합니다.

Use detected port title

자동으로 수집된 장치의 정보를 이 포트의 포트 타이틀로 사용할 것인지를 설정합니다. **Device detection method**가 **Active** 혹은 **Passive**로 설정된 경우에만 설정 가능합니다.

Port naming rule

Use detected port title이 **Enable**로 설정된 경우에만 입력할 수 있습니다. 자동으로 수집된 장치의 정보를 포트 타이틀로 구성하는 방법을 설정합니다. OS에는 장치의 운영체제 이름이 $HOSTNAME$에는 호스트 이름이 $#$에는 포트 번호가 들어가서 포트 타이틀을 구성하게 됩니다.

Use detected type of console server

자동으로 수집된 장치의 정보로 **type of console server** 설정을 변경할 지 설정합니다.

Use detected freeKVM

자동으로 수집된 장치의 정보로 **freeKVM**을 설정합니다.

Use detected serial parameters

4.4 Port automatic detection configuration 설정에서 정한 규칙을 바탕으로 자동으로 수집된 정보로 장치의 시리얼 포트 파라미터를 설정합니다.

4.5.4 Port Title

사용자는 각각의 포트에 연결된 장치에 대한 설명을 입력할 수 있습니다. 여기에는 장치의 유형, 협력 업체 또는 위치 정보 등이 포함될 수 있습니다. 포트 타이틀은 설정 프로세스에서 유용할 뿐만 아니라 **Serial port 연결** 및 **Port access menu**에서 포트에 대한 설명으로도 이용됩니다. 사용자가 직접 포트 타이틀을 입력하는 대신 자동 검색으로 찾아낸 장치에 대한 정보를 이용하여 포트 타이틀을 구성할 수도 있습니다. 자동 검색에 대한 자세한 내용은 ***4.5.3 Automatic detection*** 을 참조하시기 바랍니다.

그림 4-11은 포트 타이틀 설정 화면을 보여줍니다.

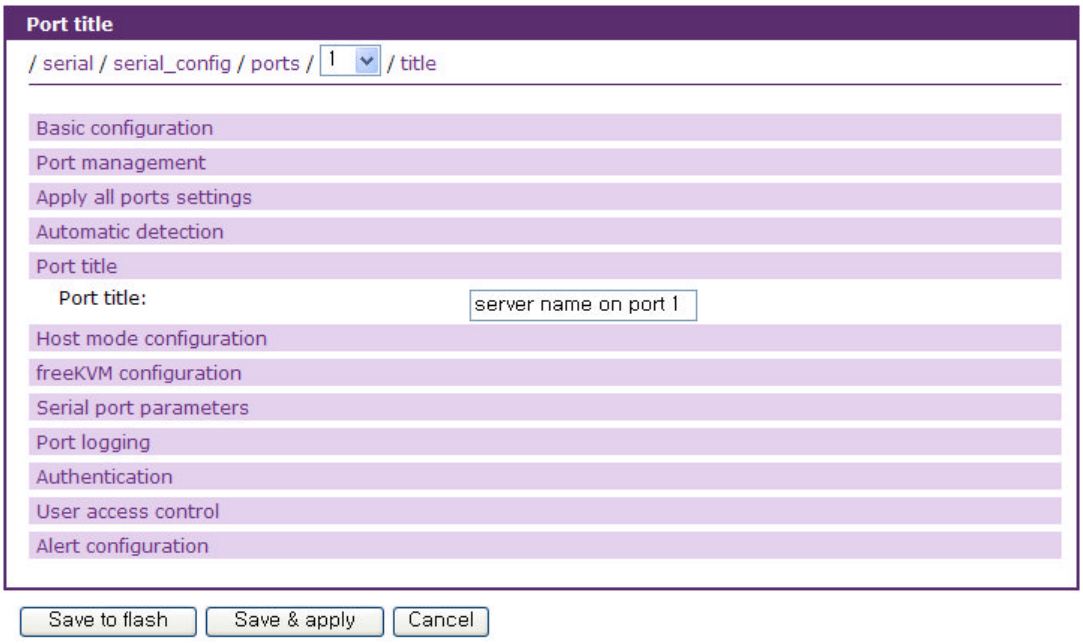


그림 4-11 포트 타이틀 설정

4.5.5 Host mode 설정

VTS II 작동 모드는 **Host mode**라고도 합니다. 다음과 같은 5개의 Host mode가 사용 가능합니다.

Console server mode
Terminal server mode
Dial-in modem mode
Dial-in terminal sever mode
PPP mode

Console Server Mode

이 모드에서는, Telnet 또는 SSH 클라이언트의 연결을 대기하고 있는 TCP 서버 소켓이 실행됩니다. Telnet/SSH 클라이언트가 VTS II에 접속하면, VTS II의 시리얼 포트/원격 포트에 연결된 장비의 콘솔 포트에 접속할 수 있습니다. 원격 포트의 경우에는 이 모드만 지원됩니다. 시리얼 포트가 콘솔 포트를 통해 장비에 연결하는 반면 원격 포트는 원격 포트 설정에서 지정된 원격 호스트로 지정된 프로토콜을 사용하여 접속합니다.

Terminal Server Mode

이 모드에서는, **Terminal server option**의 설정에 따라 VTS II의 시리얼 포트에 연결된 장치에서 원격 호스트로 Telnet 또는 SSH를 이용하여 접속하거나 VTS II의 쉘 프로그램을 실행하게 됩니다. 원격 포트에서는 지원되지 않습니다.

Dial-in Modem Mode

VTS II는 외장형 모뎀을 사용하여 망외(out-of-band) 접속 기능을 지원합니다. 시리얼 포트가 **Dial-in Modem Mode**로 설정된 경우, VTS II는 시리얼 포트가 외장형 모뎀과 연결된 것으로 간주하고, 원격 지로부터 전화 접속 연결을 기다립니다. 터미널 에뮬레이션 프로그램을 사용하여 모뎀에 접속하면 VTS II에 접속을 인증하기 위한 로그인 화면이 표시됩니다. 원격 포트에서는 지원되지 않습니다.

Dial-in Terminal Server Mode

Dial-in Terminal Server Mode는 터미널 서버 모드와 전화 접속 모뎀 모드의 혼합 모드입니다 사용자가 시리얼 포트를 **Dial-in Terminal Server Mode**로 설정하면, VTS II는 시리얼 포트가 외장형 모뎀과 연결된 것으로 간주하고, 전화 접속 연결을 기다립니다. 사용자가 터미널 에뮬레이션 프로그램을 사용해 VTS II에 전화 접속하는 경우, VTS II는 이 연결을 허용하고 이미 정의되어 있는 원격 호스트에 Telnet 또는 SSH로서 TCP 연결을 수행합니다. 원격 포트에서는 지원되지 않습니다.

PPP Mode

PPP mode의 자세한 설명은 ***3.11 PPP 설정***을 참조하시기 바랍니다.

그림 4-12 ~ 그림 4-16은 각 모드별 Host mode 설정 화면을 보여줍니다.

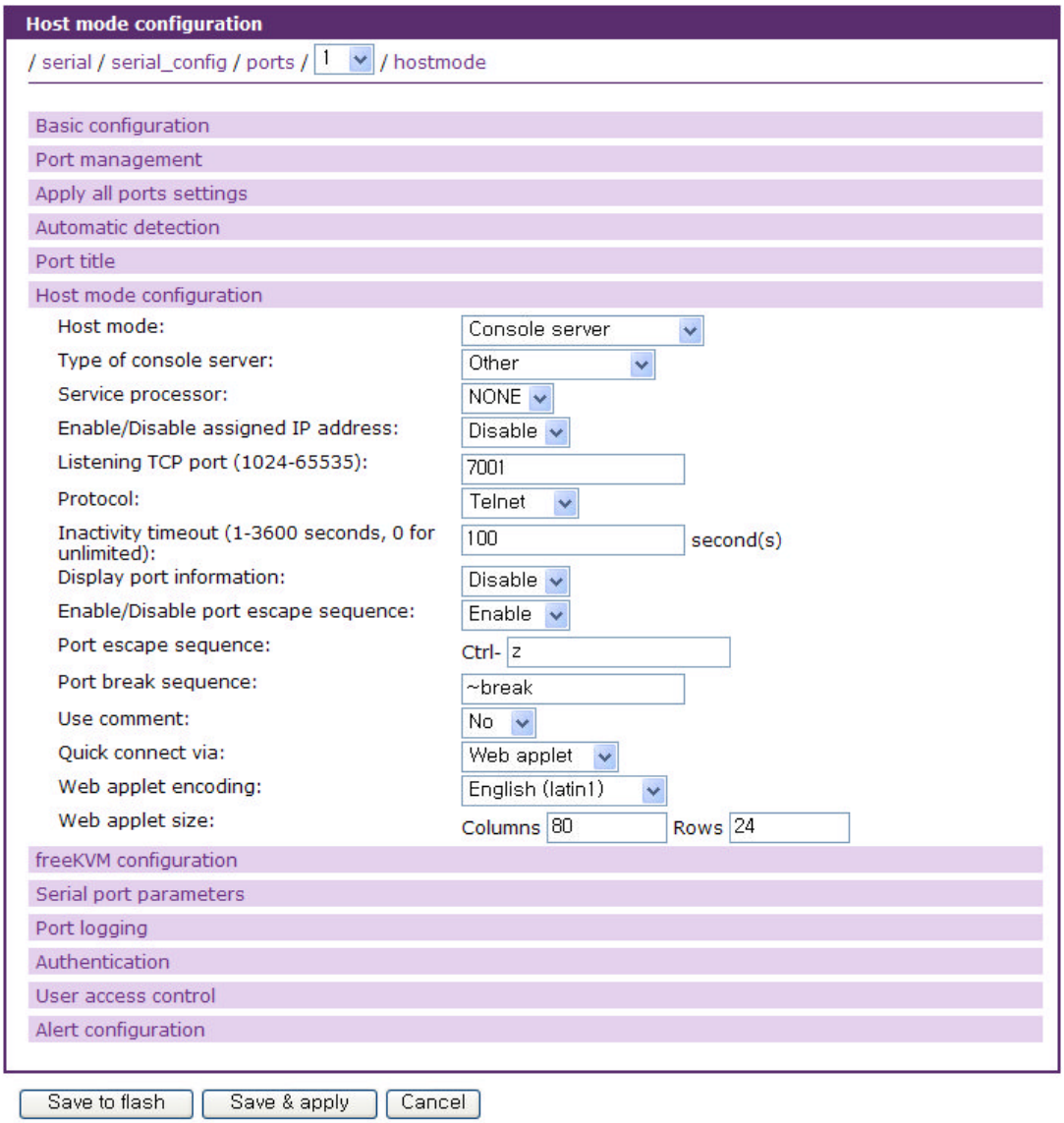


그림 4-12 Host mode 설정 - Console server mode

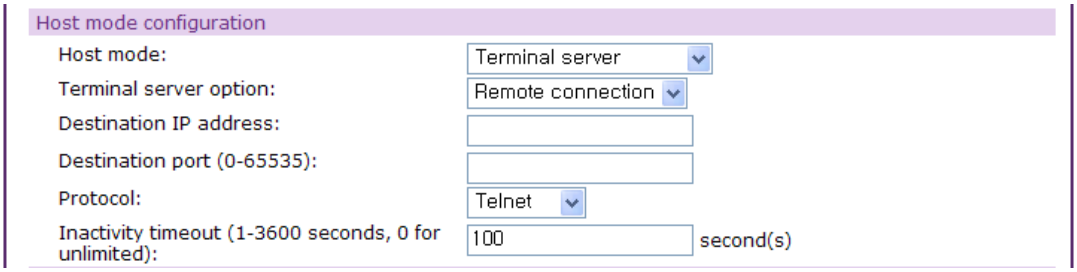


그림 4-13 Host mode 설정 - Terminal server mode

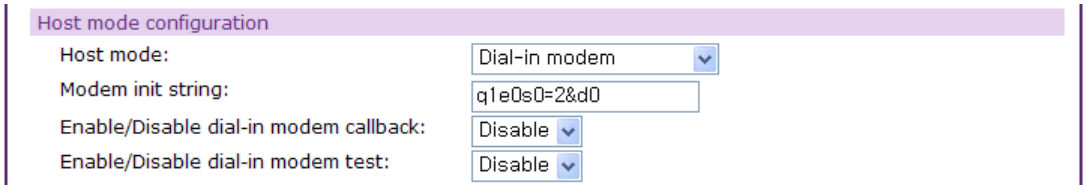


그림 4-14 Host mode 설정 - Dial-in modem mode

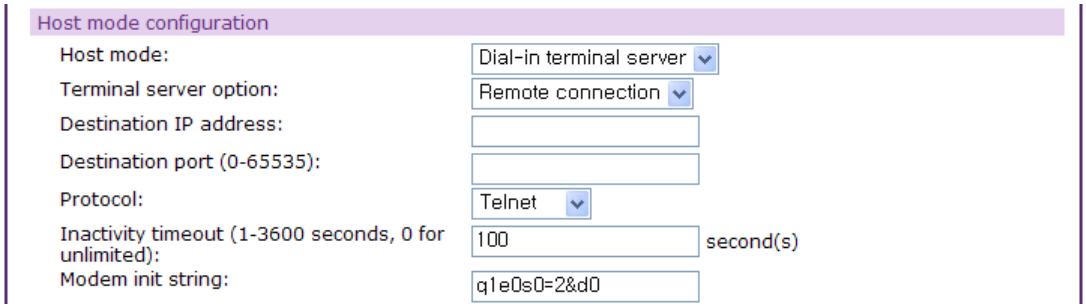


그림 4-15 Host mode 설정 - Dial-in terminal server mode

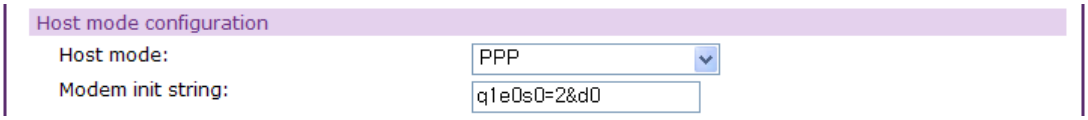


그림 4-16 Host mode 설정 – PPP mode

Console server mode 설정

Console server 모드의 경우, 사용자는 다음과 같이 매개 변수를 설정할 수 있습니다.

Type of console server

Service processor

Enable/Disable assigned IP

Assigned IP

Listening TCP port

Protocol

Inactivity timeout

Enable/Disable port escape sequence

Port escape sequence

Port break sequence

Use comment

Quick connect via

Client program path

Web applet encoding

Web applet size

Type of console server

시리얼 포트에 연결되어 있는 콘솔 서버의 타입이 MS SAC console인지 아닌지를 선택합니다.

Service processor

시리얼 포트에 연결되어 있는 콘솔 서버의 Service processor 종류를 선택합니다. Service processor의 종류에 따라 Service processor configuration 탭이 표시되며, 이 Service processor를 통해 원격 서버를 감시 / 제어할 수 있습니다.

Eanble/Disable assigned IP

Assigned IP를 사용할 지 여부를 결정하는데 사용합니다.

Assigned IP

사용자가 콘솔 서버의 시리얼 포트 또는 원격 포트에 IP 주소를 할당한 경우, 설정된 포트의 IP 주소를 통해 시리얼 포트 또는 원격 포트에 직접 접속할 수 있습니다. 사용자는 Telnet(23) 또는 SSH(22)의 표준 TCP 포트 번호가 있는 Telnet 또는 SSH 클라이언트 프로그램을 사용하여 포트에 접속할 수 있습니다.

포트의 IP 주소가 192.168.1.101로 할당된 경우, 사용자는 다음과 같이 포트에 연결할 수 있습니다.

```
telnet 192.168.1.101
```

할당된 IP 주소는 기존의 IP 주소와 충돌되지 않아야 합니다. 만일 충돌되는 경우, 시리얼 포트또는 원격 포트의 IP 주소는 Disable 상태가 됩니다. Port access menu에서와 같이 IP 주소를 사용하지 않으려면 Enable/Disable assigned IP를 Disable로 하거나 Assigned IP를 0.0.0.0으로 하면 됩니다.

Listening TCP port

사용자는 시리얼 포트 또는 원격 포트 접속을 위해 VTS II의 IP 주소 및 Listening TCP port number를 이용할 수 있습니다. 사용자는 Telnet/SSH 연결을 위한 해당 시리얼 포트의 TCP port number 및 VTS II의 IP 주소를 사용해야 합니다.

VTS II의 IP 주소가 192.168.1.100 이고, 해당되는 시리얼 포트의 TCP port number가 6001 인 경우, 사용자는 다음과 같이 해당 시리얼 포트에 연결할 수 있습니다.

```
telnet 192.168.1.100 6001
```

Protocol

Protocol로 **Telnet, SSH** 또는 **Raw TCP**를 선택합니다. 사용자가 Telnet 클라이언트 프로그램을 사용하는 경우 Telnet을 선택합니다. 사용자가 SSH 클라이언트 프로그램을 사용하는 경우 SSH를

선택합니다.

Inactivity timeout

Inactivity timeout 파라미터 설정의 목적은 TCP 연결 상태를 Closed 또는 Listen으로 유지하는데 있습니다. 지정된 Inactivity timeout 간격 동안 VTS II와 Telnet/SSH 클라이언트 사이에서 데이터 통신이 없는 경우, 기존에 연결된 세션은 자동으로 닫히게 됩니다. 사용자가 연결을 무한대로 유지하려는 경우, timeout 시간을 0으로 설정합니다. Inactivity timeout이 Enable 상태에 있는 경우라도, VTS II는 "keep alive"패킷을 주기적으로 전송하여 Telnet/SSH 클라이언트와 VTS II사이의 연결 상태를 지속적으로 검사합니다. Telnet/SSH 클라이언트가 패킷에 응답하지 않을 경우, 시스템은 연결 상태가 끊겨 있다고 간주하고, Inactivity 설정과 상관 없이 기존의 Telnet/SSH 연결을 닫습니다.

Enable/Disable port escape sequence

Port escape sequence를 사용할 지 여부를 결정하는데 사용합니다.

Port escape sequence

사용자가 시리얼 포트/원격 포트에 연결한 후, **Port escape sequence**를 입력하면 Port escape menu에 접근할 수 있습니다. Port escape menu에는 모든 사용자가 접근하는 **[show last 100 lines of log buffer]**, **[send message to port user]**, **[close current connection to port]**, Port 사용자를 위한 **[send break]** 그리고 Port와 Monitor 접근권한을 모두 가진 사용자의 **[disconnect a sniff session]** 메뉴 등이 있습니다. 시리얼 포트/원격 포트에 연결된 장치가 파워 컨트롤의 아웃렛에 연결되어 있고 로그인한 사용자가 Power 접근권한을 갖는다면, Port escape menu에는 **[power device on]**, **[power device off]**와 **[reboot device using power-switch]**등의 전원과 관련된 메뉴가 추가됩니다.

Port escape sequence로 설정된 문자를 포트로 전송하려면 Port escape sequence를 두번 입력하거나 port escape menu에서 Port escape sequence를 입력하면 됩니다.

Port break sequence

사용자는 포트에 연결 중 **port break sequence**로 설정된 값을 입력함으로써 해당 포트로 break 신호를 보낼 수 있습니다.

Use comment

Use comment를 Yes로 설정하면 포트 사용자가 포트로 연결할 때 주석을 입력할 수 있도록 합니다. 단 이 설정은 Protocol이 Telnet 또는 SSH일 경우만 적용됩니다. 입력된 주석은 시리얼 포트 연결 페이지의 Individual port connection 부분 중 Comments 항목에 표시됩니다. (자세한 내용은 ***4.7 Serial port 연결***을 참조하십시오.)

Quick connect via

Quick connect via로 VTS II 웹의 연결 페이지에서 구동 될 Client의 종류를 Web applet, Local client 또는 User defined로 선택합니다. 이 설정은 Protocol이 Telnet 또는 SSH인 경우에만 적용됩니다. 시리얼 포트 연결 페이지에서 사용자가 연결 아이콘을 선택할 경우, 사용자가 VTS II가 제공하는 웹기반 java applet을 사용하는 경우 Web applet을 선택합니다. 운영체제가 제공하는 Telnet 또는 SSH 클라이언트 프로그램을 자동으로 구동하는 경우 Local client를 선택합니다. Windows 운영체제의 경우 Protocol이 Telnet일 때 Local client를 선택하면 Hyper Terminal 프로그램이 실행됩니다. Client 프로그램의 위치를 지정하여 해당 프로그램을 실행하고자 하는 경우에는 User defined를 선택합니다.

Client program path

Quick connect via가 **user defined**로 설정된 경우, 실행될 프로그램을 정의합니다.

Web applet encoding

시리얼 포트와 연결된 장치나 서버로부터 받은 데이터를 웹 애플릿 화면에 적절하게 표현하기 위해 인코딩하는 방식을 설정하는데 사용합니다.

Web applet size

Quick connect via에서 Web applet 을 선택한 경우 JTA의 윈도우 사이즈를 지정할 수 있습니다.

Terminal server mode 설정

Terminal server mode의 경우, 사용자는 다음과 같은 파라미터를 설정할 수 있습니다.

Terminal server option
Terminal server shell program path
Destination IP
Destination port
Protocol
Inactivity timeout

Terminal server option

Remote connection으로 설정된 경우, VTS II의 시리얼 포트에 연결된 장치에서 Telnet , SSH 또는 TCP 프로토콜을 이용하여 원격 호스트로 접속합니다. Destination IP , Destination port등의 원격호스트 정보와 사용할 프로토콜, Inactivity timeout등을 설정해야 합니다. Shell program으로 설정된 경우, VTS II의 시리얼 포트로 접속하면 VTS II에서 **Terminal server shell program path**에 설정된 쉘 프로그램을 실행합니다.

Terminal server shell program path

Terminal server option이 **Shell program**으로 설정된 경우에 시리얼 포트로 접속이 이루어지면

VTS II가 실행할 쉘 프로그램을 지정합니다.

Destination IP 및 Destination port

Terminal server option이 **Remote connection**으로 설정된 경우, Destination IP 및 Destination port는 VTS II에 연결된 장치가 접속하고자 하는 원격지 호스트의 IP 주소 및 TCP port number를 의미합니다.

Protocol

Protocol은 Telnet, SSH 또는 Raw TCP가 될 수 있습니다. 사용자가 Telnet 또는 SSH 서버에 연결하려 하는 경우, Telnet 또는 SSH를 선택해야 합니다. **Terminal server option**이 **Remote connection**으로 설정된 경우에만 활성화됩니다.

Inactivity timeout

Inactivity timeout 시간 동안 VTS II와 Telnet/SSH 서버 사이에 데이터 통신이 없으면, 현재 Telnet 또는 SSH 세션이 종료되게 됩니다. 사용자가 연결을 무한대로 유지하려는 경우, 설정치를 0으로 합니다. **Terminal server option**이 **Remote connection**으로 설정된 경우에만 활성화됩니다.

Dial-in modem mode 설정

dial-in modem mode의 경우, 사용자는 다음과 같은 파라미터를 설정할 수 있습니다.

Modem init string.
Enable/Disable dial-in modem callback
Dial-in modem callback phone number
Dial-in modem callback login
Allow dial-in modem callback number change
Enable/Disable dial-in modem test
Dial-in modem test phone number
Dial-in modem test interval

Modem init string

모뎀 초기화 스트링은 시리얼 포트에 연결된 외장형 모뎀을 초기화하는데 사용됩니다. 사용자가 초기화 스트링을 지정하지 않은 경우, 기본 초기 명령이 사용됩니다. 기본으로 설정된 초기 명령 값은 'q1e0s0=2&d0'입니다. 모뎀 초기 스트링에 대한 자세한 내용은 모뎀 매뉴얼을 참조하십시오.

Enable/Disable dial-in modem callback

Dial-in modem callback이 활성화된 경우 전화 접속 연결이 되면 VTS II는 연결을 끊고 나서 **Dial-**

in modem callback phone number에 명시된 전화 번호로 연결하여 통신합니다.

Dial-in modem callback phone number

Dial-in modem callback이 활성화된 경우 VTS II가 연결할 전화번호를 명시합니다.

Dial-in modem callback login

Dial-in modem callback이 활성화된 경우, Dial-in modem callback login이 설정되면, 전화 접속 연결시 사용자 인증을 하고 인증 성공시 callback 과정이 진행됩니다.

Allow dial-in modem callback number change

Dial-in modem callback이 활성화된 경우, Allow dial-in modem callback number change이 설정되면, 전화 접속 연결시 **Dial-in modem callback phone number**를 변경할 것인지 묻고 callback 과정을 진행합니다.

Enable/Disable dial-in modem test

Dial-in modem test가 활성화된 경우, 모뎀이 정상 동작하는지 주기적으로 점검합니다. Dial-in modem test가 활성화되면 Alert 설정 화면에서 모뎀 테스트 결과를 이메일이나 SNMP trap을 통해 받을 수 있도록 설정할 수 있게 됩니다. 자세한 내용은 ***4.5.12 Alert 설정***을 참조하시기 바랍니다.

Dial-in modem test phone number

모뎀이 정상 동작하는지 점검하기 위해 VTS II가 연결할 전화번호를 명시합니다.

Dial-in modem test interval

모뎀이 정상 동작하는지를 점검할 주기를 시간단위로 지정합니다.

Dial-in terminal server mode 설정

Dial-in terminal server mode 의 경우, 사용자는 다음과 같은 파라미터를 설정할 수 있습니다.

Terminal server option: (**Terminal server mode** 섹션을 참조하십시오)
Destination IP: (**Terminal server mode** 섹션을 참조하십시오)
Destination TCP port: (**Terminal server mode** 섹션을 참조하십시오)
Protocol: (**Terminal server mode** 섹션을 참조하십시오)
Inactivity timeout: (**Terminal server mode** 섹션을 참조하십시오)
Modem init string: (**Dial-in modem mode** 섹션을 참조하십시오)

PPP mode 설정

PPP mode 의 경우, 사용자는 다음과 같은 파라미터를 설정할 수 있습니다.

Modem init string: (**Dial-in modem mode** 섹션을 참조하십시오)

4.5.6 freeKVM configuration

Console Server 모드에서 freeKVM 설정이 추가되면, 설정된 KVM 클라이언트 프로그램을 통해 VTS II의 시리얼 포트/원격 포트에 연결된 서버로 접속하여 서버의 화면을 키보드와 마우스로 조작할 수 있게 해 줍니다. Client program이 Web redirection으로 설정된 경우에는 Client program path에 지정된 URL로 연결됩니다.
VTS II의 포트에 연결된 원격 서버가 다수의 KVM 클라이언트 프로그램을 지원할 경우 사용자가 복수의 freeKVM 설정을 입력하도록 함으로써 사용자가 KVM 클라이언트 프로그램을 선택하여 사용할 수 있도록 합니다. (***4.7 Serial port 연결*** 참조)

그림 4-17은 freeKVM 설정 화면을 보여줍니다.

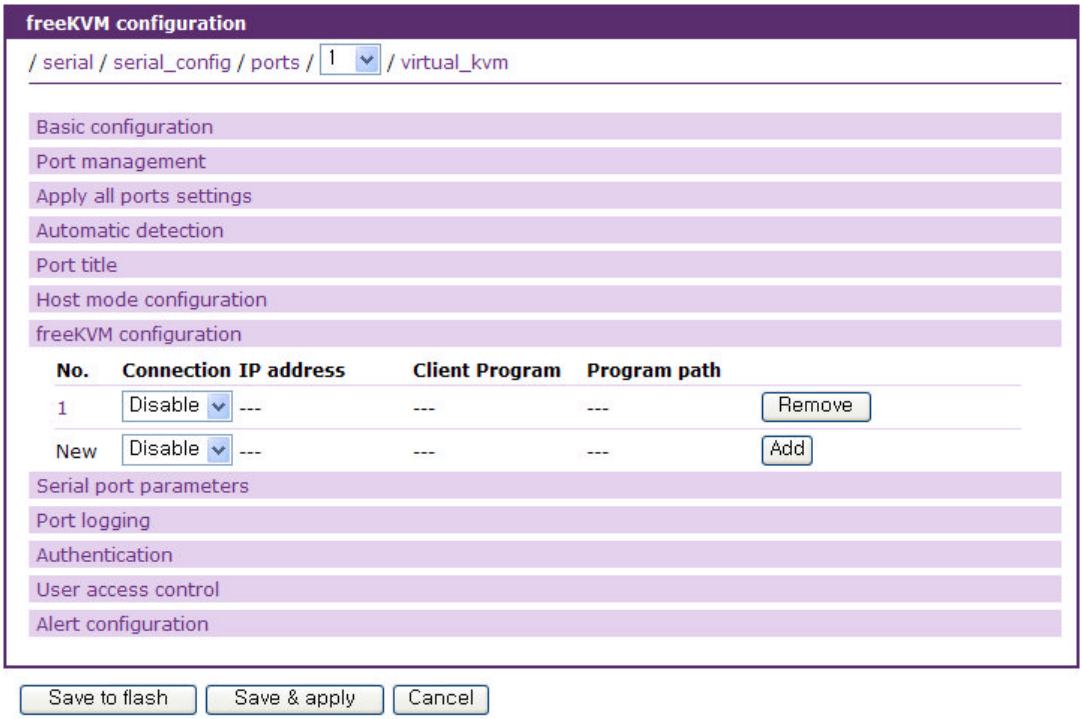


그림 4-17 freeKVM 설정

freeKVM 설정을 추가하려면 **[Add]** 버튼을 클릭하면 됩니다. 추가된 설정을 수정하려면 수정하려는 설정의 번호를 클릭하면 해당 freeKVM의 세부 내용을 수정하는 화면으로 이동합니다. 그림

4-18는 freeKVM 세부 설정 화면을 보여줍니다. **[Remove]** 버튼을 클릭하면 설정을 삭제할 수 있습니다.

freeKVM 연결을 위해 필요한 파라미터는 다음과 같습니다.

freeKVM connection

Automatic IP detection

IP address

Client program

Socket/Screen number for VNC connection

Client program path

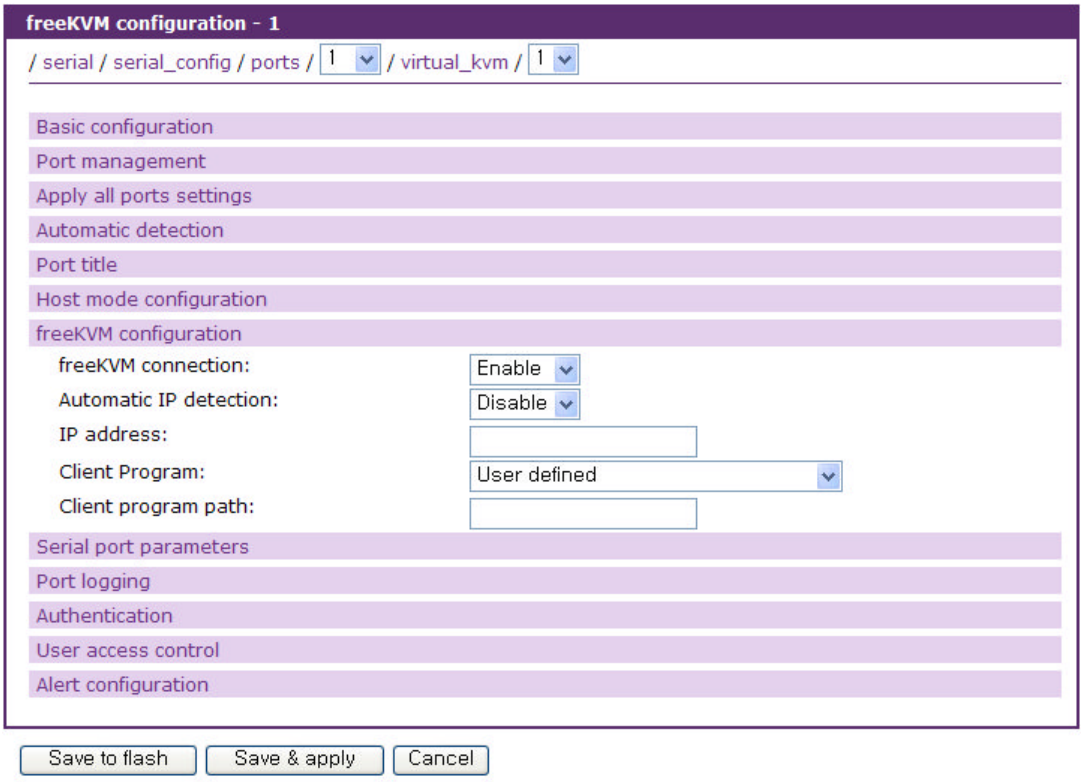


그림 4-18 freeKVM 세부 설정

free KVM connection

freeKVM 연결 기능을 사용할 것인지를 설정합니다.

Automatic IP detection

KVM 클라이언트 프로그램이 연결할 서버의 IP를 시리얼 콘솔로 접속하여 자동으로 검색할지 여부를 설정합니다. **Host mode configuration**의 **Type of console server**가 **MS SAC console**로 설정된 경우에만 이 기능을 사용할 수 있습니다.

IP address

KVM 클라이언트 프로그램이 연결할 서버의 IP를 설정합니다.

Client program

Client program path를 쉽게 지정할 수 있도록 검증된 클라이언트 프로그램 리스트를 제공합니다. Windows remote desktop standard connection, Windows remote desktop console connection, VNC, Radmin, Xmanager, Web redirection 중에서 선택하면 해당 클라이언트 프로그램이 **Client program path**에 자동으로 표시됩니다. User defined를 선택하면 **Client program path**를 사용자가 직접 입력해야 합니다.

Socket/Screen number for VNC connection

Client program이 VNC로 설정되었을 경우 VNC 연결을 위한 **Client program path**를 쉽게 설정할 수 있도록 합니다. Screen 번호 또는 TCP port 번호만 입력하면 VNC 연결을 위한 Client program path가 자동으로 설정됩니다.

Client program path

시리얼 포트나 원격포트에 연결된 서버로 KVM 세션을 연결할 수 있는 클라이언트 프로그램을 지정합니다. Client program에서 Web redirection을 선택하면 KVM을 지원하는 URL을 지정할 수 있습니다. IP는 클라이언트 프로그램이 접속할 서버의 IP 주소를 의미합니다.

4.5.7 Serial port parameters / Remote port parameters

시리얼 포트의 경우 장비를 VTS II의 시리얼 포트와 연결하려면, VTS II의 시리얼 포트 파라미터를 연결된 장비의 콘솔 포트에 맞게 설정해 주어야 합니다.

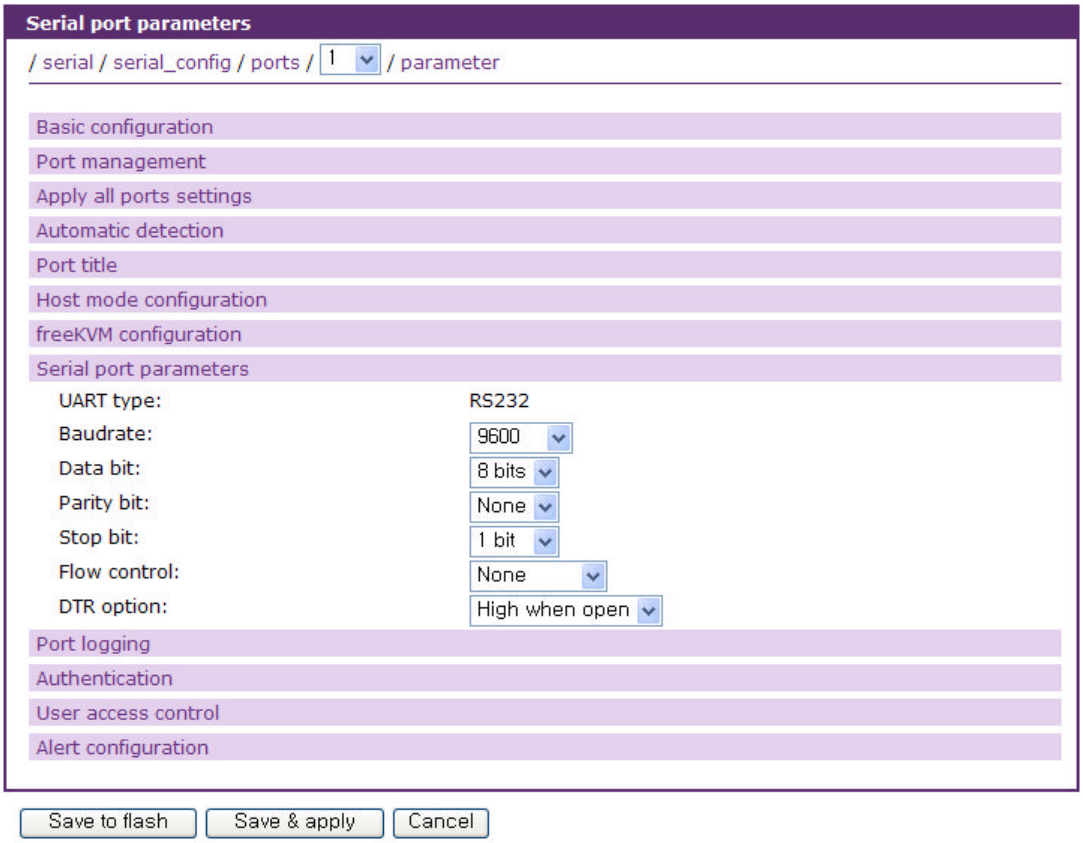


그림 4-19 Serial port parameters 설정

시리얼 통신에서 필요한 파라미터는 다음과 같습니다.

Baudrate

Data bit

Stop bit

Parity bit

Flow control

DTR option

Enable/Disable delimiter **(only for RawTCP protocol)**

Delimiter **(only for RawTCP protocol)**

Delimiter option **(only for RawTCP protocol)**

Inter character time-out **(only for RawTCP protocol)**

Baudrate

VTS II에서 지원하는 baud rate는 다음과 같습니다.

75, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200 및 230400

공장 출하시의 기본값은 9600입니다.

Data bit

Data bits는 7 bits와 8bits 중에서 하나를 선택할 수 있습니다. 공장 출하시의 기본값은 8 bits입니다.

Stop bits

Stop bits는 1 bit와 2 bits 중에서 선택할 수 있습니다. 공장 출하시의 기본값은 1 bit입니다.

Parity bit

Parity는 **None, Even** 또는 **Odd** 중에서 선택할 수 있습니다. 공장 출하시의 기본값은 None입니다.

Flow control

흐름 제어 값은 None, 소프트웨어(XON/XOFF) 또는 하드웨어(RTS/CTS) 중에서 선택할 수 있습니다. 공장 출하시의 기본값은 None입니다.

DTR option

시리얼 포트의 DTR 출력 동작은 **Always HIGH, Always LOW** 또는 **High when open**으로 설정할 수 있습니다. DTR 동작이 **High when open**으로 설정된 경우, TCP 연결이 이루어진 상태에서는 DTR 핀의 상태가 High로 유지됩니다. Host mode가 Dial-in modem mode 또는 Dial-in terminal server mode로 설정된 경우, DTR 동작 설정이 지원되지 않습니다.

Enable/Disable delimiter

프로토콜이 RawTCP인 경우, 시리얼 포트로부터 들어오는 데이터를 클라이언트에게 보낼 패킷으로 나누는 방법을 설정합니다. 이 설정이 Enable되어 있으면 시리얼 포트에서 받은 데이터를 **Delimiter**가 발견될 때마다 패킷으로 분리하여 클라이언트에 전송합니다. Disable로 설정되면 **Inter character time-out** 시간 동안 시리얼 포트로부터 데이터가 들어오지 않으면 패킷을 클아이언트로 전송합니다.

Delimiter

Enable/Disable delimiter가 Enable로 설정된 경우, 데이터를 분리하는데 사용할 분리자를 지정합니다.

Delimiter option

Enable/Disable delimiter가 Enable로 설정된 경우, 분리자로 분리된 패킷을 전송할 때 분리자도 함께 전송할 지 여부를 설정합니다.

Inter character time-out

Enable/Disable delimiter가 Disable로 설정된 경우, 시리얼 포트로부터 전송된 데이터를 분리하는데 사용되는 문자간 시간간격을 설정합니다. 이 시간이 지나도록 데이터가 추가로 들어오지 않으

면 클라이어트로 데이터를 전송합니다.

원격 포트의 경우, 클라이언트의 연결 요청시 접속할 원격 호스트의 정보와 접속에 이용할 프로토콜을 설정해야 합니다.

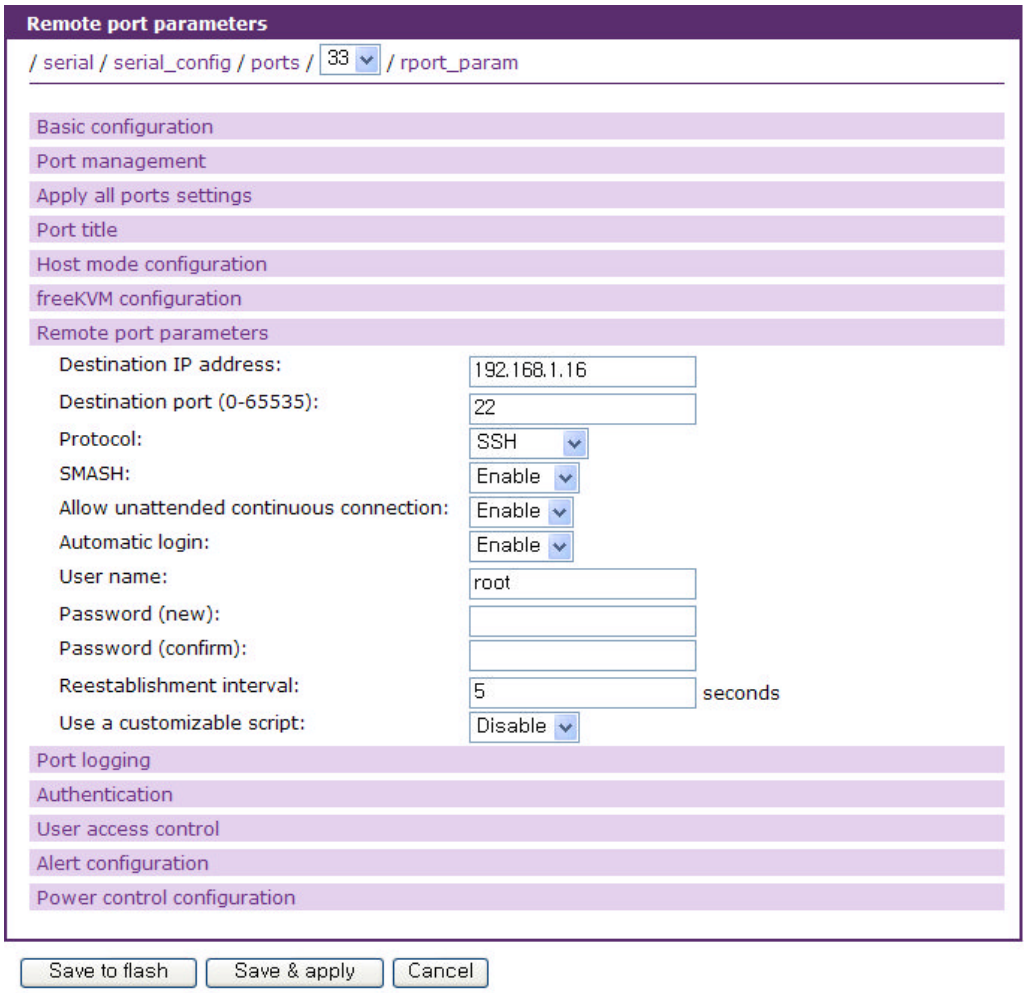


그림 4-20 Remote port parameters 설정

원격 포트에서 필요한 파라미터는 다음과 같습니다.

Destination IP

Destination port

Protocol

OEM type

SMASH

Allow unattended continuous connection

Automatic login

User name

Password

Reestablishment interval

Use a customizable script

Destination IP

접속할 원격 호스트의 IP 주소를 설정합니다.

Destination port

원격 호스트에 접속하는데 사용할 TCP port number를 설정합니다.

Protocol

원격 호스트에 접속하는데 사용되는 프로토콜을 설정합니다. Telnet, SSH, RawTCP, RMCP+(SOL) 중 하나의 값을 가질수 있습니다. RMCP+(SOL)이 선택되면 Destination IP와 Destination Port가 Service processor configuration에서 Destination IP와 Destination Port로 사용됩니다.(***4.5.14 Service processor configuration*** 참조) 그리고, Serial Port Connection 페이지에 SOL을 이용해 IPMI를 제어할 수 있는 컨솔로 연결가능한 아이콘이 표시됩니다.

OEM type

Protocol이 RMCP+(SOL)로 선택된 경우 IPMI가 제공되는 형식을 지정합니다. None과 Intel IPMI 2.0 BMC 중에서 선택할 수 있습니다.

SMASH

Host mode configuration 에서 Service processor를 iLO 나 DRAC을 선택하였을 경우 SMASH를 사용 여부를 지정합니다.

Allow unattended continuous connection

원격 포트에 접속하지 않아도 원격 호스트로의 연결을 계속유지할 지 여부를 설정합니다. Disable로 설정된 경우에는 사용자가 원격 포트로 접속할 때 VTS II는 원격 호스트로 연결을 시도합니다. Enable로 설정된 경우에는 VTS II는 원격 호스트로의 연결을 계속 유지합니다.

Automatic login

사용자가 Remote port에 연결했을 때 Remote port가 원격 호스트에 자동으로 login 할 것이지에 대한 여부를 설정합니다. 이는 Allow unattended continuous connection 이 설정되면 자동으로 설정됩니다.

User name

Allow unattended continuous connection이 Enable로 설정된 경우, VTS II가 원격 호스트로 연결을 유지하기 위해 접속할 때 사용하는 사용자 이름을 설정합니다.

Password

Allow unattended continuous connection이 Enable로 설정된 경우, VTS II가 원격 호스트로 연결을 유지하기 위해 접속할 때 사용하는 사용자의 패스워드를 설정합니다.

Reestablishment interval

Allow unattended continuous connection이 Enable로 설정된 경우, VTS II가 원격 호스트로 연결이 끊어졌을 때 다시 접속하는 간격을 설정합니다.

Use a customizable script

Allow unattended continuous connection이 Enable로 설정된 경우, **Automatic login** 자동으로 인증을 수행하는 방법을 설정합니다. Enable로 설정하면, 사용자 편집이 가능한 perl script(/etc/rportcon)를 실행하여 대상 장비에 연결합니다. Disable로 설정하면 /etc/autologin/portxx의 파일이나 기본 설정 파일인 /etc/autologin.def을 참조하여 장비의 사용자 인증을 처리합니다.

4.5.8 Port Logging

Console Server 모드에서 Port Logging이 Enable 되면, VTS II의 시리얼 포트 또는 원격 포트로 전송되는 데이터를 메모리, ATA/IDE fixed disk card, USB 메모리, NFS 서버 또는 Samba 서버로 저장할 수 있습니다. 동시에 SYSLOG 서버에 저장할 지를 지정할 수 있습니다.

또한, 사용자는 port event handling 설정에서 포트로 들어 오는 메시지의 특정 키워드를 선택하여 Email / SNMP trap 을 통해 관리자에게 전달할 수 있습니다. 사용자는 이 기능을 통해 연결된 장치로부터 받는 데이터를 감시할 수 있습니다. 자세한 내용은 섹션 ***4.5.9 Port event handling 설정*** 을 참조하십시오.

시리얼 포트 또는 원격 포트의 Host mode가 Console server mode로 설정된 경우에만 Port Logging 기능이 유효합니다. 시리얼 포트가 Terminal server 또는 Dial-in modem mode로 설정된 경우 Port Logging 기능을 사용할 수 없습니다.

Port Logging에 대한 설정 파라미터는 다음과 같습니다.

Port logging
Logging direction
Port log storage location
Port log to SYSLOG server
SYSLOG facility for port logging
Port log buffer size

Port log file name option

Port log file name

Time stamp to port log

Show last 10 lines of a log upon connect

Strip the ^M from SYSLOG

Automatic backup on mounting

Port log view

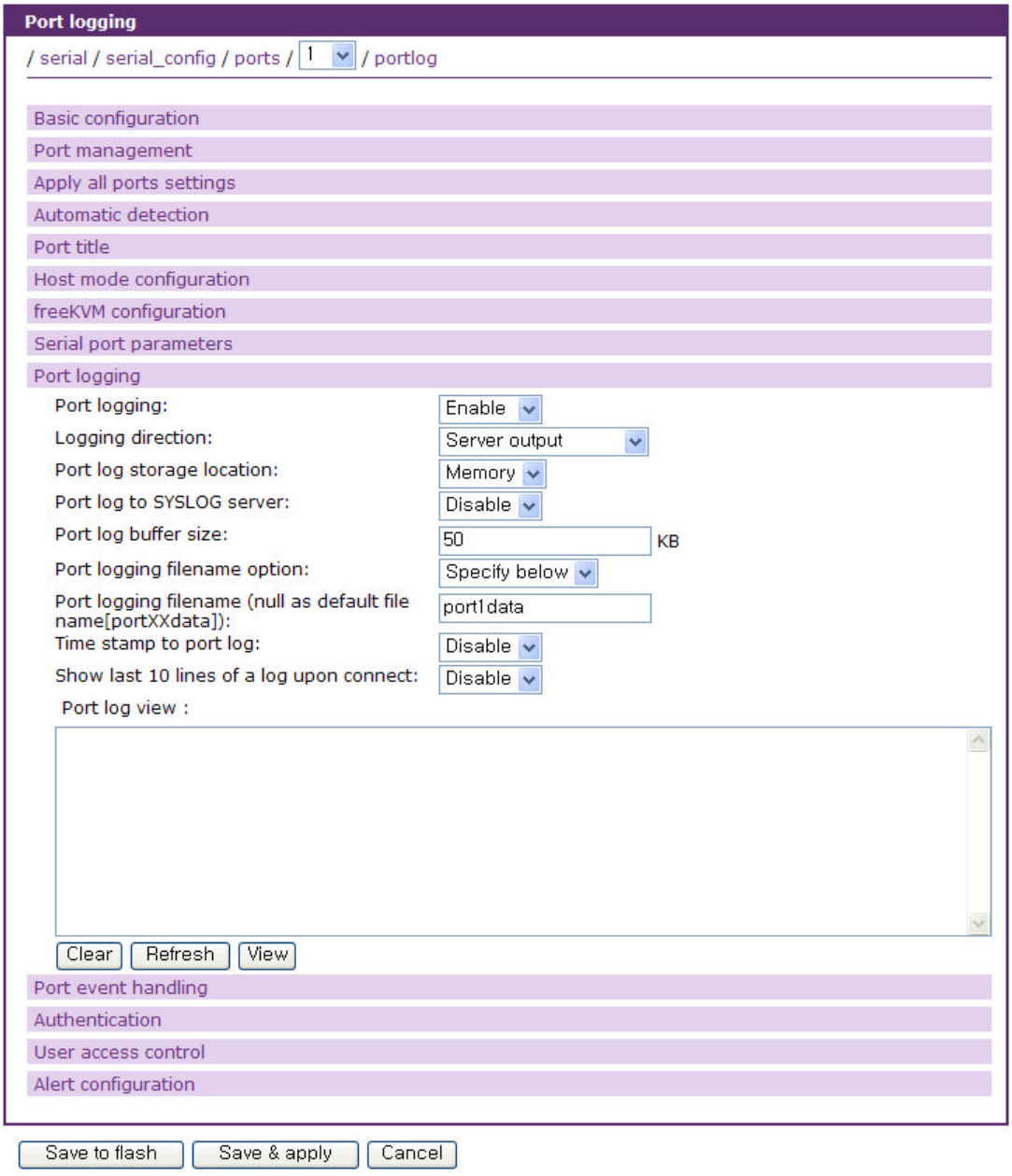


그림 4-21 포트 로깅 설정

Port logging

Port logging 기능을 사용할 것인지를 설정합니다. 공장 출하 시의 기본값은 Disable입니다.

Logging direction

사용자가 시리얼 포트로 전달하는 내용을 기록(User input), 시리얼 포트로부터의 데이터를 기록(Server output), 양방향 데이터를 기록하면서 방향표시 화살표를 사용할 것(Both with arrows)인지 사용하지 않을 것(Both without arrows)인지를 결정합니다. 공장 출하 시의 기본값은 Server output 입니다.

Port log storage location

포트 로그 데이터는 VTS II의 내부 메모리, ATA/IDE fixed disk card, USB 메모리, NFS 서버 또는 Samba 서버에 저장할 수 있습니다. 포트 로그가 메모리에 저장되는 경우, VTS II가 꺼질 때 포트 로그 데이터는 삭제됩니다. 시리얼 포트 로그 데이터를 보존하려면, 저장 위치를 ATA/IDE fixed disk card, USB 메모리, NFS 서버 또는 Samba 서버로 설정하거나 SYSLOG server로 저장을 설정해야 합니다. 사용자는 저장 위치에 상응하는 저장 매체를 미리 설정해야 합니다. 저장 위치가 적절하게 설정되지 않았다면, 사용자는 저장위치를 선택할 수 없게 됩니다.

Port log to SYSLOG server

이 파라미터가 Enable로 설정되면 포트 로그 데이터는 지정된 저장 위치와 동시에 SYSLOG 서버에도 저장할 수 있습니다.

SYSLOG facility for port logging

Port log to SYSLOG server이 Enable일 경우에만 설정 가능합니다. 로그를 SYSLOG 서버에 저장할 때 저장할 facility를 지정합니다. 포트 로그가 실제 SYSLOG 서버로 저장되려면 SYSLOG-NG 설정에서 SYSLOG-NG 규칙 중에 여기서 지정한 facility를 포함한 규칙이 하나 이상 있어야 합니다. 이런한 규칙에 따라 지정한 Destination으로 포트 로그를 저장하게 됩니다. 자세한 내용은 ***8.3 SYSLOG-NG 설정***을 참조하시기 바랍니다.

Port log buffer size

이 파라미터는 logging되는 포트 로그 데이터의 최대 크기를 정의합니다. Log 데이터를 저장하기 위해 내부 메모리를 사용하는 경우, 포트 버퍼의 전체 크기는 3200 Kbytes를 초과하지 않아야 합니다. 공장 출하 시 기본값은 50Kbytes입니다.

로그 데이터를 저장하기 위해 ATA/IDE fixed disk card나 USB 메모리를 사용하는 경우, 최대 포트 버퍼 크기는 카드의 용량에 따라 달라집니다.

로그 데이터를 저장하기 위해 NFS 서버나 Samba 서버를 사용하는 경우, 최대 Port buffer size는 서버의 환경에 따르게 되며, 사용자는 NFS 서버나 Samba 서버를 적절하게 운영하여 Port logging 시스템이 작동할 수 있도록 해야 합니다.

Port log filename option

Use port title로 설정되면 포트 타이틀이 포트 로그 파일 이름으로 사용됩니다. **Specify below**로 설정되면 **Port logging filename**에 입력된 파일 이름이 로그 파일 이름으로 사용됩니다.

Port log filename

Port logging filename option이 **Specify below**로 설정되면 **Port log filename**에 입력된 파일 이름이 로그 파일 이름으로 사용됩니다. 로그 파일 이름이 입력되어 있지 않을 경우에는 기본 설정 값인 portXXdata 라는 이름이 사용 됩니다. 여기서 XX은 해당 시리얼 포트의 번호를 표시합니다.

Time stamp to port log

이 파라미터 값이 설정되면 기록되는 포트 로그는 행마다 Time stamp가 포함되게 됩니다. 기본 값은 Disable 입니다.

Show last 10 lines of a log upon connect

이 파라미터가 **Enable**로 설정되면, 사용자가 포트로 연결할 때 로그의 마지막 10행이 표시됩니다. 기본값은 **Disable**입니다.

Strip the ^M from SYSLOG

Port log to SYSLOG server가 **Enable**로 설정되고 이 파라미터가 **Enable**로 설정되면, 포트 로그 데이터 중에서 SYSLOG 서버에서 ^M으로 표시되는 0x0D 데이터가 스페이스로 대체되어 포트 로그 데이터에 0x0D 데이터가 포함되지 않은 상태로 SYSLOG 서버에 저장됩니다.

Automatic backup on mounting

Port log storage location이 CF card, USB 메모리, NFS 서버 또는 Samba 서버로 설정된 경우에만 설정할 수 있습니다. 이 설정이 Enable되면 해당 저장 공간이 다시 마운트될 경우 로그를 저장하는 백업 파일을 만듭니다.

Port log view

Port log view 화면에는 현재 포트 로그가 표시됩니다. **[Clear]** 버튼은 현재 로그를 삭제합니다. **[Refresh]** 버튼은 로그를 다시 불러오기 위해 사용됩니다. **[View]** 버튼은 로그를 확인하고 로그를 처리하는 작업을 수행하는 View port log 화면을 생성합니다. View port log에 대한 자세한 내용은 그림 4-39 View port log을 참조하시기 바랍니다.

4.5.9 Port event handling 설정

Port logging 이 Enable이 되면 포트로 들어 오는 메시지를 검사해서 이미 설정된 키워드가 발견되면 Email 또는 SNMP trap 을 통해 관리자에게 전달하게 할 수 있습니다. Port event handling은

포트 로깅 데이터 중 원하는 키워드를 지정하여 해당 키워드가 발견되면 원하는 Reaction을 수행하게 됩니다. Reaction에 대한 설정은 각 키워드 별로 설정할 수 있으면 Email과 SNMP trap의 두 가지 Reaction을 동시에 혹은 개별적으로 실행이 가능합니다.
키워드를 등록하려면 검색하려는 키워드를 입력하고 **[Add]** 버튼을 누르면 됩니다. 그림 4-22은 포트 이벤트 핸들링 – 키워드 등록 화면을 보여줍니다. 키워드를 등록한 후나 등록된 키워드의 행 번호를 선택하여 키워드를 설정하는 화면으로 이동한 후 키워드를 설정합니다. 그림 4-23은 포트 이벤트 핸들링 – 키워드 설정 화면을 보여줍니다.

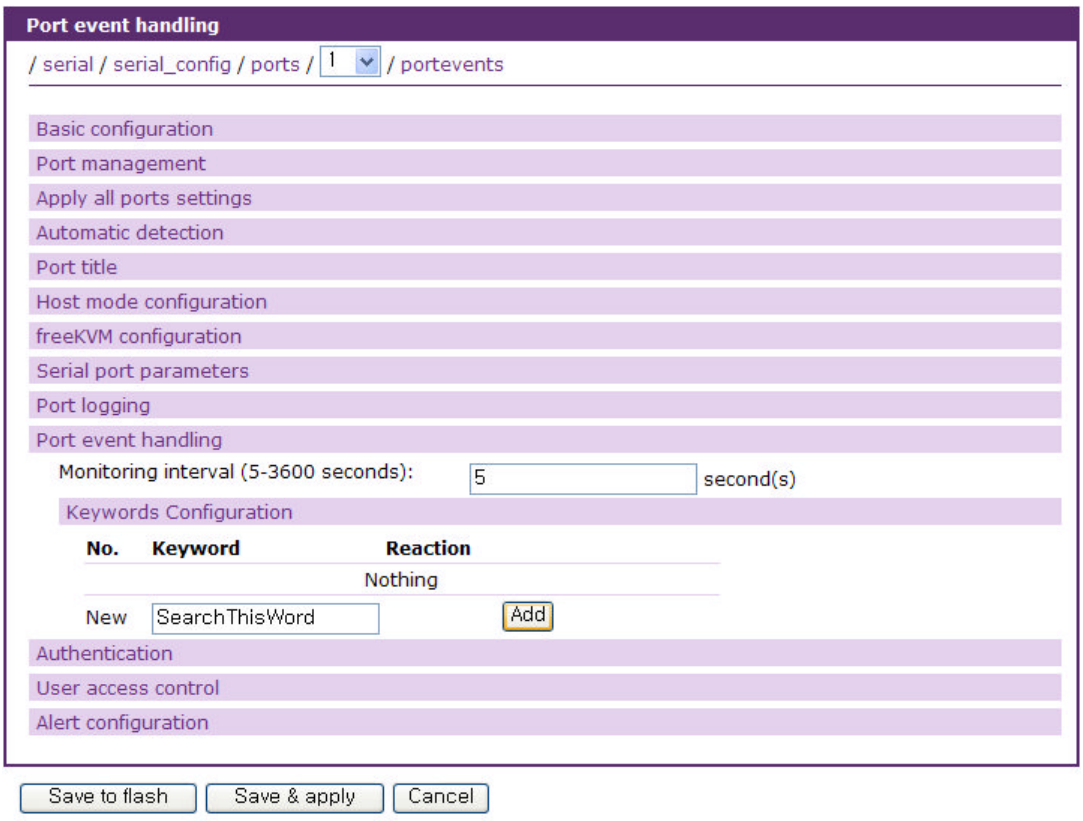


그림 4-22 포트 이벤트 핸들링 – 키워드 등록

Port event handling을 위한 파라미터 및 키워드 별 파라미터는 다음과 같습니다.

Monitoring interval

Key word

Case sensitive

Email notification

Title of email

Recipient's email address

SNMP trap notification

Title of SNMP trap

Use global SNMP configuration

First/Second SNMP trap receiver settings

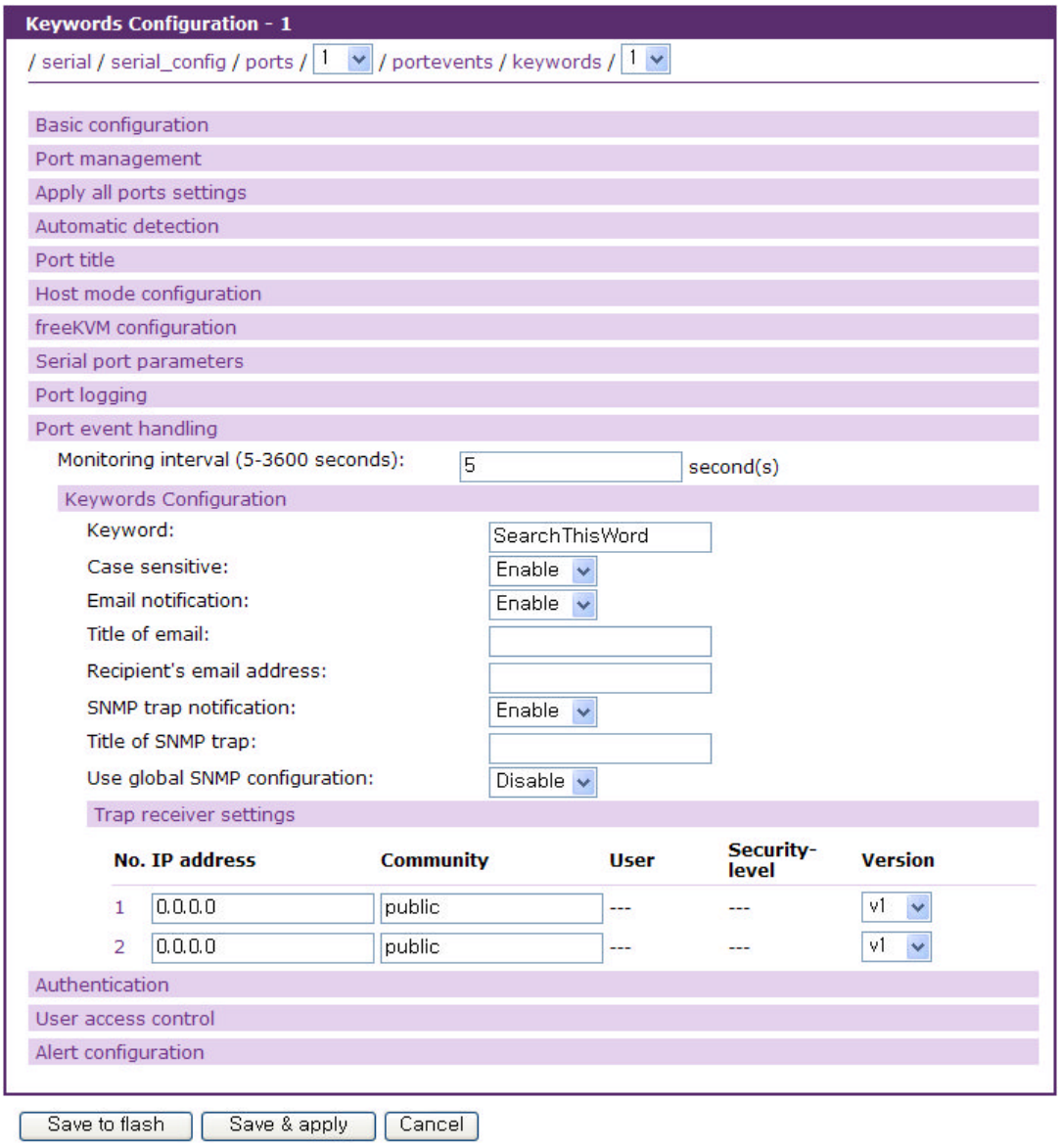


그림 4-23 포트 이벤트 핸들링 – 키워드 설정

Monitoring interval

Port logging이 설정되고 Port event handling이 설정되면 해당 포트로부터 Keyword를 검사해서 적절한 Reaction을 하게 됩니다. 이 때, Monitoring interval 값에 따라 버퍼링되어 있는 Port log에서 Keyword를 찾는 주기가 결정 됩니다. 이 값을 작게 설정 해주면 빠른 시간에 Keyword를 찾을 수 있으나 시스템 리소스를 많이 사용하게 되므로 전체 시스템의 성능이 저하됩니다. 그러므로 사용 목적상 적절한 값 중 최대값을 설정하는 것이 가장 좋습니다.

Case sensitive

이 파라미터가 **Disable**로 설정되면 Keyword 검사할 때 대소문자를 구별하지 않습니다.

Email notification 설정

Email notification을 수행하고자 할 경우 Email notification을 Enable로 하고 수신자의 주소와 메일의 제목을 설정합니다.

SNMP trap notification 설정

SNMP trap notification이 Enable인 경우, 키워드가 발견되면 SNMP trap이 설정된 IP로 전달됩니다. SNMP trap 설정에 필요한 각 항목들의 대한 설명은 ***3.2 SNMP 설정***을 참고하십시오.

Use global SNMP configuration

이 파라미터가 **Enable**로 설정되면, 네트워크 설정 항목 중 SNMP 설정에서 명시된 트랩 수신기 설정이 트랩 수신기로 사용됩니다.

키워드가 Port event handling 설정에 추가되면, VTS II는 이 키워드가 발생하는지 감시합니다. 키워드가 발생하고 사용자가 경고 발생을 해제할 때까지 시리얼 포트 연결 페이지의 포트 타이틀 좌측에 경고 아이콘이 표시됩니다. 시리얼 포트 연결페이지나 시리얼 포트 연결 후 포트 이스케이프 메뉴에서 경보 발생을 해제할 수 있습니다. 그림 4-24은 포트 타이틀이 server name on port1인 1번 포트에 경고 아이콘이 표시된 상황을 보여줍니다.

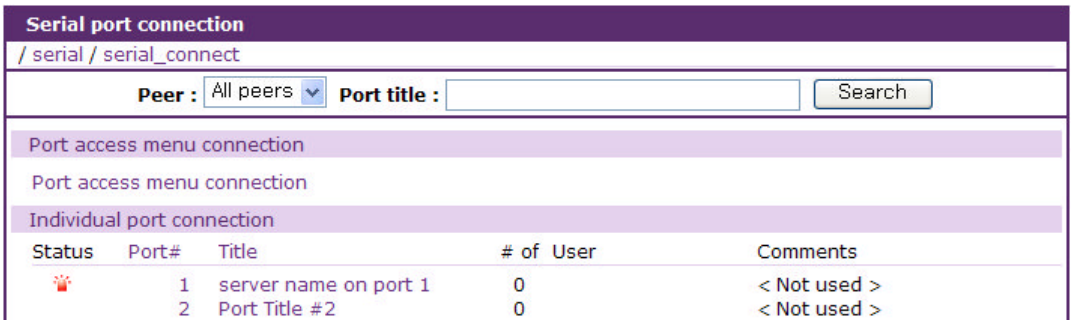


그림 4-24 경고 아이콘을 포함한 시리얼 포트 연결 페이지

4.5.10 Authentication 설정

인증(Authentication)은 일반적으로 사용자 이름 및 비밀 번호를 기초로 하여 개별적으로 사용자를 식별하는 과정입니다. VTS II는 시리얼 포트에 접속하는 사용자를 인증하기 위한 방법으로 **None**, **Local, RADIUS, TACACS+, Kerberos** 및 **LDAP** 와 같은 여러 인증 옵션을 지원합니다.

인증을 **None** 으로 설정하면, 인증 과정 없이 사용자가 포트에 접속할 수 있으며, **Local**로 설정된

경우, VTS II는 사용자를 인증하기 위해 VTS II 자신의 사용자 목록을 사용합니다. **Custom PAM** 옵션을 선택하여 Linux-PAM (Pluggable Authentication Modules for Linux)을 지원할 수 도 있습니다. 그 외의 경우는, 외부 인증 서버를 이용하는 경우로서, VTS II는 외부 인증 서버(예. RADIUS, Kerberos, TACACS+ 및 LDAP 서버) 에 사용자 인증을 요청할 것입니다. 그림 4-25은 외부 인증 서버를 사용할 때의 사용자 인증 프로세스를 개념적으로 보여줍니다.

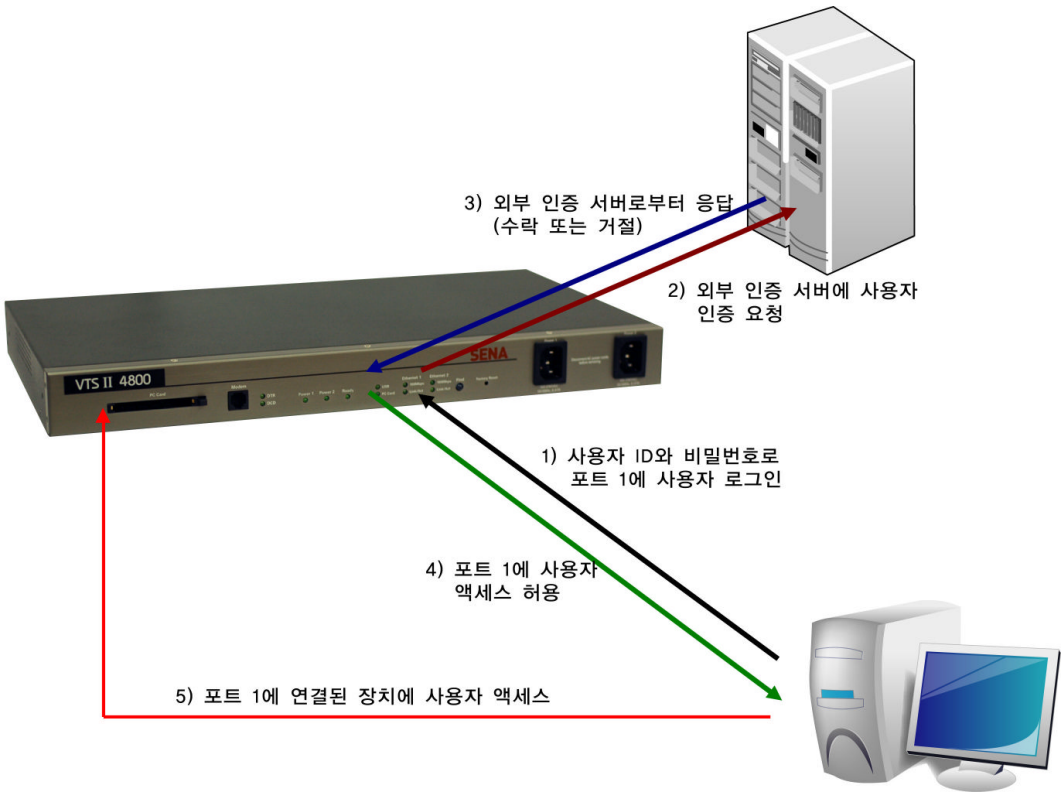


그림 4-25 외부 서버에 의한 사용자 인증 개념

사용자는 또한 인증 방법을 조합하여 선택할 수 있습니다. 이 경우에는, 처음의 방법으로 VTS II가 인증을 시도하다가 실패한 경우, 두 번째 방법으로 인증을 시도합니다. 예를 들어, RADIUS 인증은 Local 인증과 결합될 수 있습니다. 사용자가 **RADIUS server - Local** 인증 방법을 선택하는 경우, VTS II는 RADIUS를 우선 사용하여 외부 RADIUS 서버에 인증을 요청하고, 실패한 경우에는 VTS II 자신의 사용자 목록을 통해 인증을 시도합니다.

RADIUS down - Local 인증 방법의 경우에는, 외부 RADIUS 서버에 인증을 요청하고, RADIUS 서버가 다운되었을 때만 VTS II는 자신의 사용자 목록을 통해 인증을 시도합니다.

주의 :

Custom PAM은 Linux-PAM을 지원합니다. 이를 사용하려면 `/ets/pam.d/custom` 파일을 생성해야합니다.

다음은 VTS II가 각 시리얼 포트에 제공한 모든 인증 옵션입니다.

None

Local

RADIUS server

RADIUS server - Local

Local - RADIUS server

RADIUS down - Local

TACACS+ server

TACACS+ server - Local

Local - TACACS+ server

TACACS+ down - Local

LDAP server

LDAP server - Local

Local - LDAP server

LDAP down - Local

Kerberos server

Kerberos server - Local

Local - Kerberos server

Custom PAM

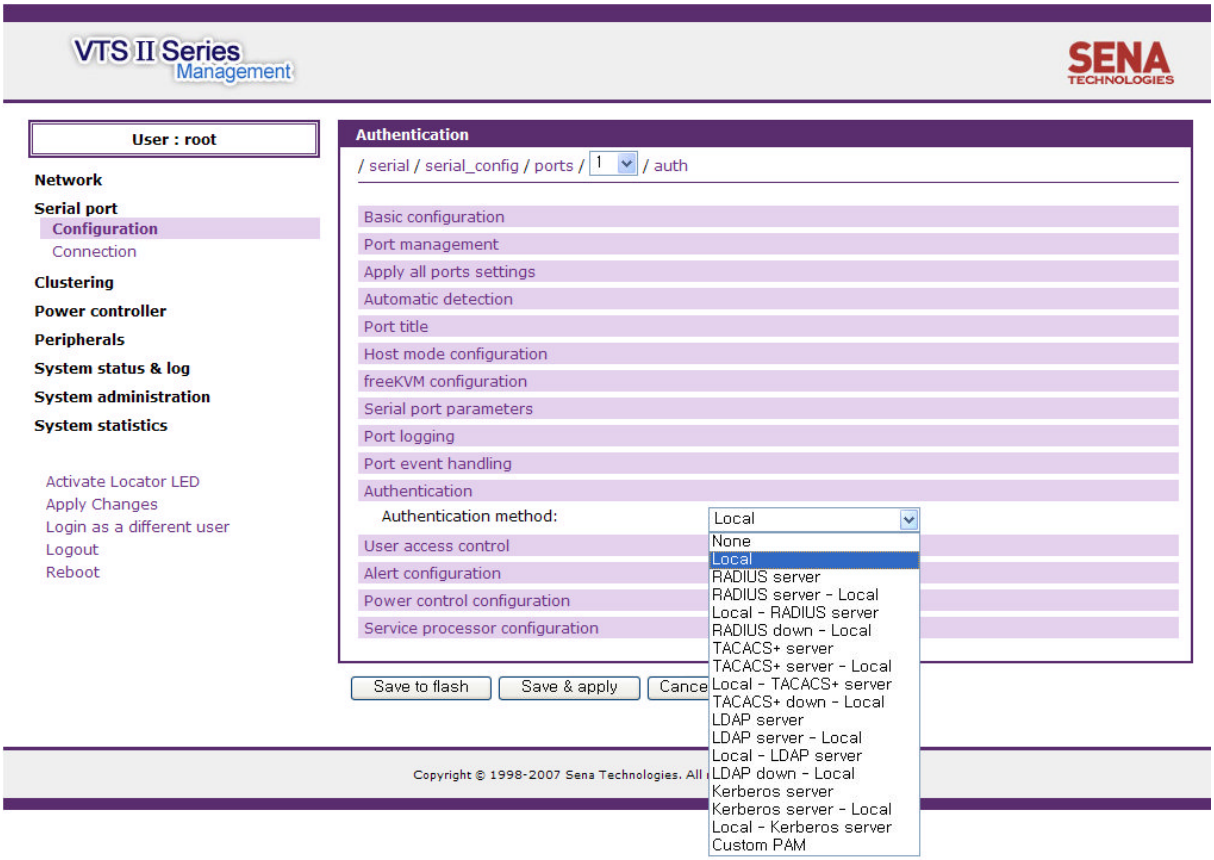


그림 4-26 시리얼 포트에 대한 인증 옵션

각 인증 서버별 필요한 설정 파라미터는 다음과 같습니다.

RADIUS server

- **First/Second authentication server**
- **First/Second accounting server**
- **Shared secret**
- **Timeout**
- **Retries**

TACAS+ server

- **First/Second authentication server**
- **First/Second accounting server**
- **Shared secret**
- **Authrization service**

LDAP server

- **First/Second authentication server**
- **LDAP search base**
- **Domain name for active directory**

Kerberos server

- **First/Second authentication server**

Realm for first/second kerberos server

그림 4-27은 RADIUS 서버 – local에 대한 인증 설정 화면을 보여줍니다.

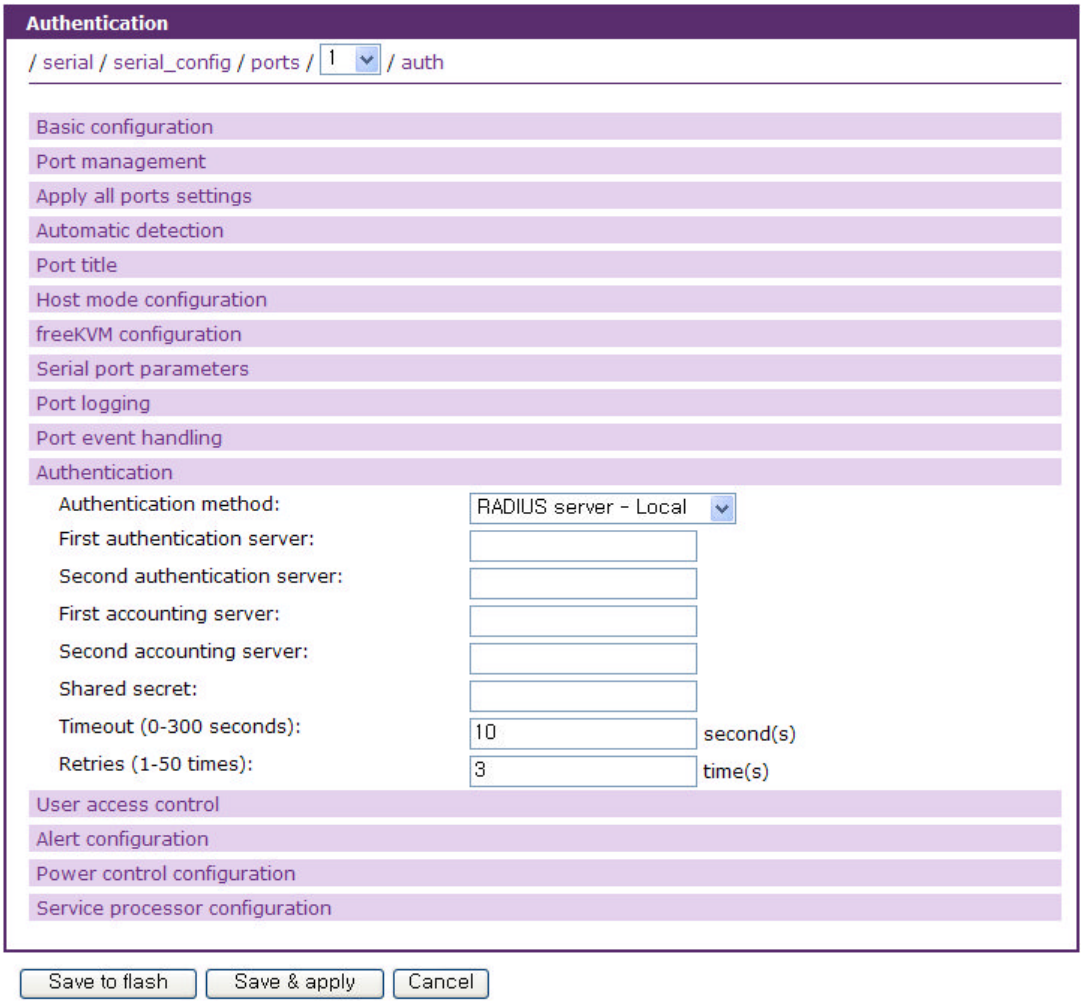


그림 4-27 RADIUS 서버 – local에 대한 인증 설정

4.5.11 User access control 설정

VTS II 시리얼 포트/원격 포트의 연결시 접근권한 또는 파워 컨트롤러 아웃렛을 제어하려는 사용자의 접근권한을 설정합니다. Multiple session 부분에서는 Multiple session을 어떻게 운용할 것인지를 설정합니다.

Port 접근권한과 **Monitor** 접근권한은 시리얼 포트/원격 포트로의 연결시 접근권한을 결정합니다. **Power** 접근권한은 파워 컨트롤러 아웃렛에 연결된 시리얼 포트의 전원을 제어하는 것을 제한하거나 허용하는데 사용됩니다. 포트가 파워 컨트롤러 아웃렛에 연결되지 않은 경우 Power 접근권한은 사용되지 않습니다.

<<Everyone>>의 접근권한은 User access control에서 개별적으로 명시되는 사용자를 제외한 모든 사용자의 접근 권한을 명시합니다. <<Everyone>>의 접근권한과 다른 접근권한을 가진 사용자는 User access control 설정의 사용자 리스트 또는 액세스 리스트에 별도로 등록해야 합니다.

사용자 접근권한의 관점에서 사용자는 세 가지 그룹으로 나뉠 수 있습니다. Port / Monitor 접근권한 모두를 가진 사용자, Port 접근권한만 가진 사용자, Monitor 접근권한만 가진 사용자입니다.
Port 접근권한을 가진 사용자 그룹은 포트에 연결하여 읽기/쓰기 기능을 다 이용할 수 있습니다. Monitor 접근권한만 가진 사용자 그룹은 읽기 기능만 가집니다. Port / Monitor 접근권한 모두를 가진 사용자 그룹은 Port 접근권한을 가진 사용자 그룹이 갖는 읽기/쓰기 기능뿐만 아니라 포트에 연결된 다른 사용자의 연결을 끊을 수도 있습니다.

사용자가 Authentication 설정에 따라 VTS II나 인증 서버의 인증을 거쳐야 하는 것은 물론이고, User access control 설정에 따라 접근권한이 부여되어야만 시리얼 포트에 연결이 가능합니다. Authentication 설정에 관한 자세한 내용은 ***4.5.10 Authentication 설정***을 참조하시기 바랍니다.

User access control

접근권한 형태는 Port, Monitor, Power의 세 종류가 있습니다. Port 접근권한은 메인 세션으로 포트에 연결할 수 있는지 여부를 명시합니다. Monitor 접근권한은 Sniff session으로 포트에 접근할 수 있는지 여부를 나타냅니다. Power 접근권한은 포트의 전원 취급할 수 있는지를 표시합니다.
<<Everyone>>의 접근권한은 별도로 등록되지 않은 일반 사용자의 접근권한에 적용됩니다. 만약 <<Everyone>>의 접근권한과 다른 접근권한을 가진 사용자가 있다면 접근권한을 별도로 명시하여 등록해야 합니다. 같은 접근권한을 갖는 사용자들을 하나의 액세스 리스트로 만들어 액세스 리스트의 접근권한을 명시하여 등록할 수도 있습니다. 액세스 리스트에 자세한 내용은 ***9.2 액세스 리스트***를 참조하시기 바랍니다.
관리자가 특정 포트로의 접근을 제한하고 싶은 사용자가 있다면, 관리자는 <<Everyone>>의 접근권한을 체크한 상태로 등록하고 제한하려는 사용자의 접근권한을 체크하지 않은 상태로 사용자를 등록하면 됩니다. 관리자가 특정 사용자만에게만 시리얼 포트로의 접근을 허용하려 한다면 <<Everyone>>의 접근권한을 체크하지 않은 상태로 설정하고, 특정사용자의 접근권한을 체크한 상태로 사용자를 등록하면 됩니다.

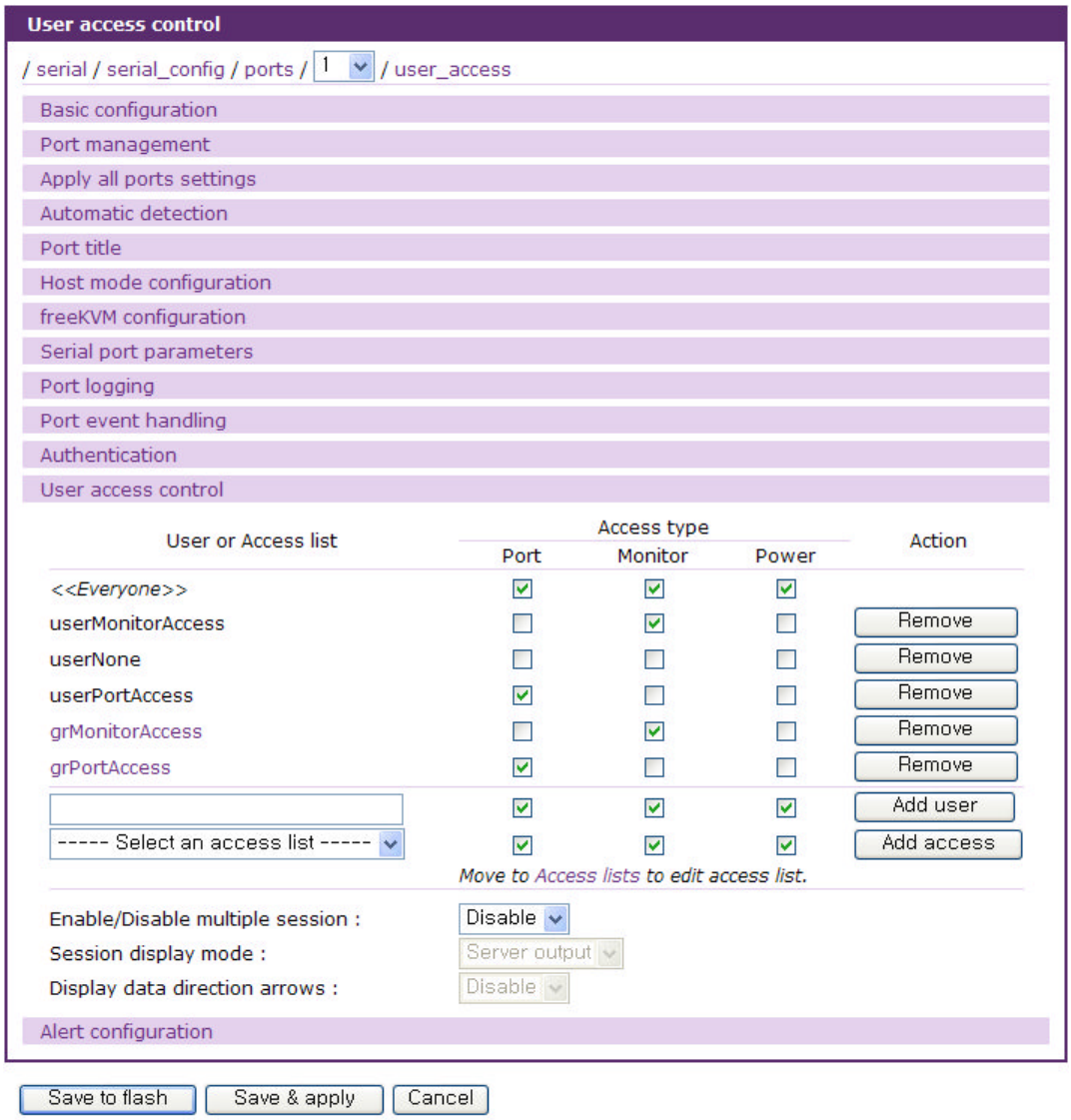


그림 4-28 시리얼 포트에 대한 액세스 제어 설정

Multiple session

Multiple session을 통해 여러 명의 사용자가 하나의 시리얼 포트/원격 포트에 접속할 수 있습니다. Port 또는 Monitor 접근권한을 가진 사용자는 다른 사용자가 이미 포트에 접속되어 있더라도 시리얼 포트/원격 포트에 접속할 수 있습니다. 동시에 접속할 수 있는 Multiple session user의 개수는 16개로 한정되어 있으며 또한 시스템의 리소스에 의해 제한될 수 있습니다.

사용자의 Multiple session을 인정하려면 **Enable/Disable multiple mode**를 **Enable**로 설정해야 합니다. **Session display mode**는 **User input**, **Server output**와 **Both**로 설정할 수 있습니다. **User input** 모드로 설정된 경우, Multiple session 사용자는 시리얼 포트/원격 포트로 전달되는 메시지만을 관찰할 수 있습니다. **Server output** 모드로 설정된 경우에는 시리얼 포트/원격 포트로부터의 메시지만을 관찰할 수 있습니다. **Both**모드로 설정된 경우, 모든 전송되는 데이터를 관찰할 수 있습니다.

Display data direction arrows는 나가고 들어가는 데이터의 방향을 표시하는 화살표를 데이터와

함께 표시할 지 여부를 설정합니다.

기존에 이미 사용자가 포트에 연결되어 있을 때, Multiple session 사용자가 다음에 연결하는 경우, 그림 4-29와 같은 화면이 나타나게 됩니다. 이 때 Port escape sequence를 입력하면 Port escape menu가 나타납니다. Port / Monitor 접근권한을 모두 갖고 있는 사용자는 Port / Monitor 접근권한만 가진 일반 사용자보다 높은 권한을 보유하게 되며, **[disconnect a sniff session]** 메뉴를 이용하여 현재 접속되어 있는 다른 Session 사용자를 종료할 권한도 보유하고 있습니다.
사용자는 **[send messages to port user]**를 통해 원하는 사용자에게 메시지를 전달할 수도 있습니다. **[show last 100 lines of log buffer]**를 선택하여 로그를 확인할 수도 있고, **[close current connection to port]**를 통해 현재의 연결을 종료할 수도 있습니다. 포트 이벤트 핸들링에 등록된 키워드가 발생하면 메뉴에 경보가 표시되고 **[clear alert]** 메뉴를 선택하여 경보를 해제할 수 있습니다.

```
 Welcome to VTSII-3200 Console Server (Sena_VTSII)
 PORT – server name on port 1

VTSII-3200 Login : admin
VTSII-3200 Password : *****

 Entering server port, ..... type ^z for port menu.

>> 'root' initiated a new r/w session
```

port escape sequence를 입력한 후

```
Port menu:

<<<< Alert detected ! >>>>
b     send break

l     show last 100 lines of log buffer
d     disconnect a sniff session
a     send message to port user
c     clear alert

x     close current connection to port
```

그림 4-29 Sniff user 인터페이스 화면

4.5.12 Alert 설정

Host mode가 Console server mode인 경우, 포트 로그인이나 포트 연결 이벤트가 발생할 때 이메일 에이전트는 이메일 경보 설정에 따라 이메일을 전송하고, SNMP 에이전트는 SNMP trap 설정에 따라 SNMP trap을 관리자에게 전달합니다.
Automatic detection설정에서 **Device detection method**가 **Active**로 설정된 경우 설정에 따라

VTS II가 주기적으로 분석한 장치 정보를 이메일이나 SNMP trap을 전송할 수 있습니다.
Host mode 설정에서 **Service processor**가 IPMI로 선택되고 **Service processor configuration**에 설정된 Sensor 경보가 발생하면 설정에 따라 이메일이나 SNMP trap을 전송할 수 있습니다.
원격 포트의 경우에는 포트 로그인과 Service processor Alert만 지원됩니다.

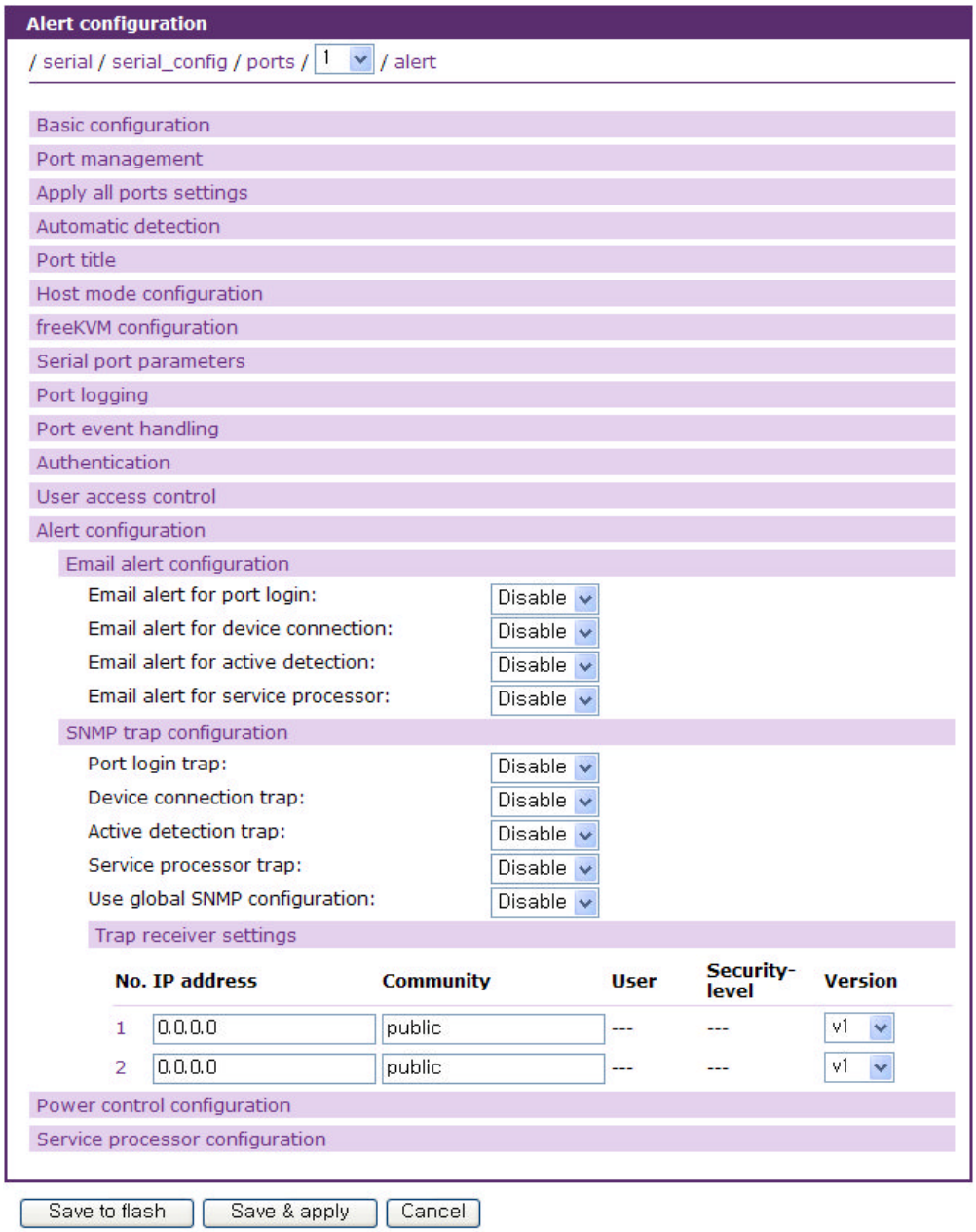


그림 4-30 Console server mode의 Alert 설정

Alert 설정에 대한 설정 파라미터는 다음과 같습니다.

Email alert for port login

Email alert for device connection

Email alert for active detection

Email alert for service processor
Title of email
Recipient's email address
Port login trap
Device connection trap
Active detection trap
Service processor trap
Use global SNMP configuration
Trap receiver settings

Email alert for port login
사용자가 시리얼 포트 또는 원격 포트로 로그인 또는 로그아웃 할 때 이메일을 전송할지 여부를 설정 합니다.

Email alert for device connection
시리얼 포트가 장비로 연결되거나 연결이 끊길 때 이메일을 전송할지 여부를 설정합니다.

Email alert for active detection
Automatic detection 설정에서 **Device detection method**가 **Active**로 설정된 경우, 주기적으로 분석된 장치정보를 이메일로 전송할 지 여부를 설정합니다.

Email alert for service processor
Host mode 설정에서 Service processor가 IPMI로 설정되고 Service processor configuration에 설정된 Sensor 경보가 발생할 때 이메일을 전송할지 여부를 설정합니다.

Title of email
전송되는 이메일의 제목을 설정합니다.

Recipient's email address
전송되는 이메일을 받을 주소를 설정합니다.

Port login trap
사용자가 시리얼 포트 또는 원격 포트로 로그인 또는 로그아웃 할 때 SNMP trap을 발생시킬지 여부를 설정 합니다.

Device connection trap
시리얼 포트가 장비로 연결되거나 연결이 끊길 때 SNMP trap을 발생시킬지 여부를 설정합니다.

Active detection trap

Automatic detection 설정에서 **Device detection method**가 **Active**로 설정된 경우, 주기적으로 분석된 장치정보에 관한 SNMP trap을 발생시킬지 여부를 설정합니다.

Service processor trap

Host mode 설정에서 Service processor가 IPMI로 설정되고 Service processor configuration에 설정된 Sensor 경보가 발생할 때 SNMP trap을 발생시킬지 여부를 설정합니다.

Use global SNMP configuration

이 파라미터가 **Enable**로 설정되면, 네트워크 설정 항목 중 SNMP 설정에서 명시된 트랩 수신기 설정이 트랩 수신기로 사용됩니다.

Trap receiver settings

SNMP trap 설정에 필요한 각 항목들에 대한 설명은 ***3.2 SNMP 설정***을 참고하십시오.

Host mode가 Dial-in modem mode이고 Dial-in modem test가 설정되었을 경우, Dial-in modem test에 대한 이벤트가 발생할 때, 이메일 에이전트는 이메일 경보 설정에 따라 이메일을 전송하고, SNMP 에이전트는 SNMP trap 설정에 따라 SNMP trap을 관리자에게 전달합니다.

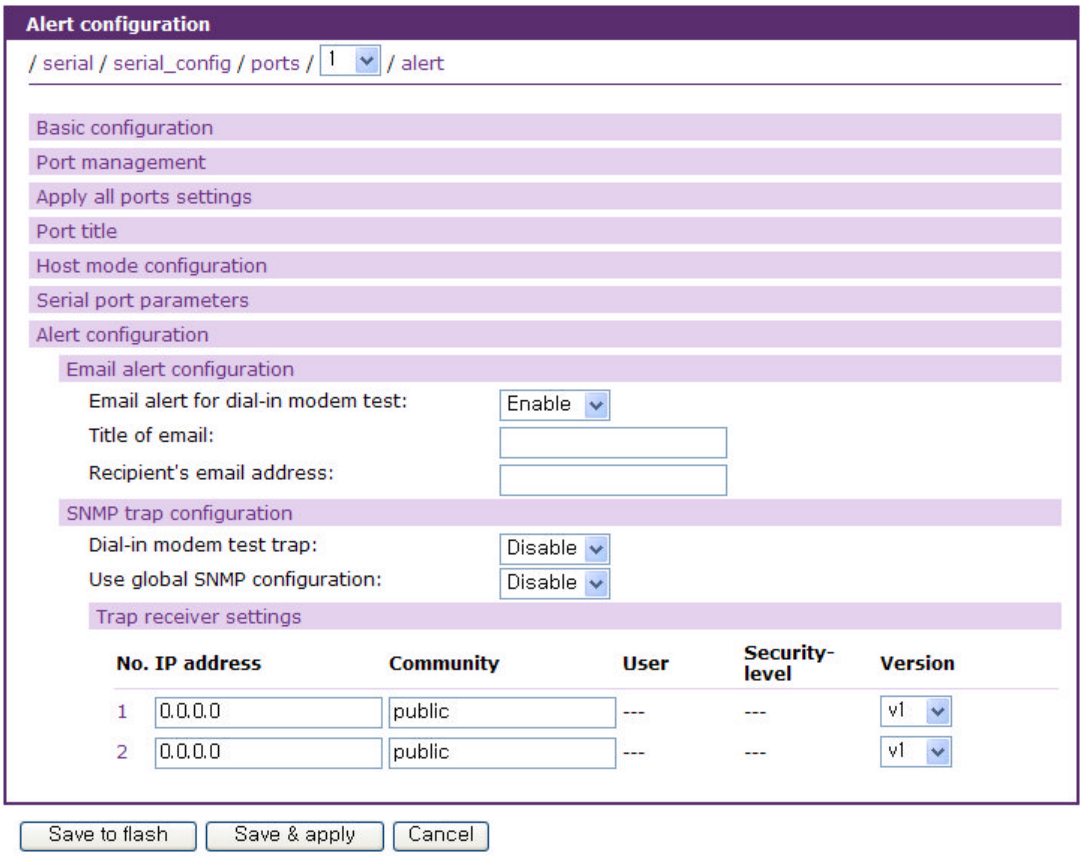


그림 4-31 Dial-in modem mode의 Alert 설정

Alert 설정에 대한 설정 파라미터는 다음과 같습니다.

Email alert for dial-in modem test

Title of email

Recipient's email address

Dial-in modem test trap

Use global SNMP configuration

Trap receiver settings

Email alert for dial-in modem test

Dial-in modem test에 대한 이벤트가 발생할 때 이메일을 전송할지 여부를 설정 합니다.

Dial-in modem test trap

Dial-in modem test에 대한 이벤트가 발생할 때 SNMP trap을 발생시킬지 여부를 설정 합니다.

4.5.13 Power control 설정

파워 컨트롤러가 VTS II에 연결되어 있다면, 시리얼 포트가 그 파워 컨트롤러의 어느 아웃렛에 연결되어 있는지를 설정합니다. 이 설정을 이용하여 시리얼 포트에 연결된 장치의 전원을 관리합니다.

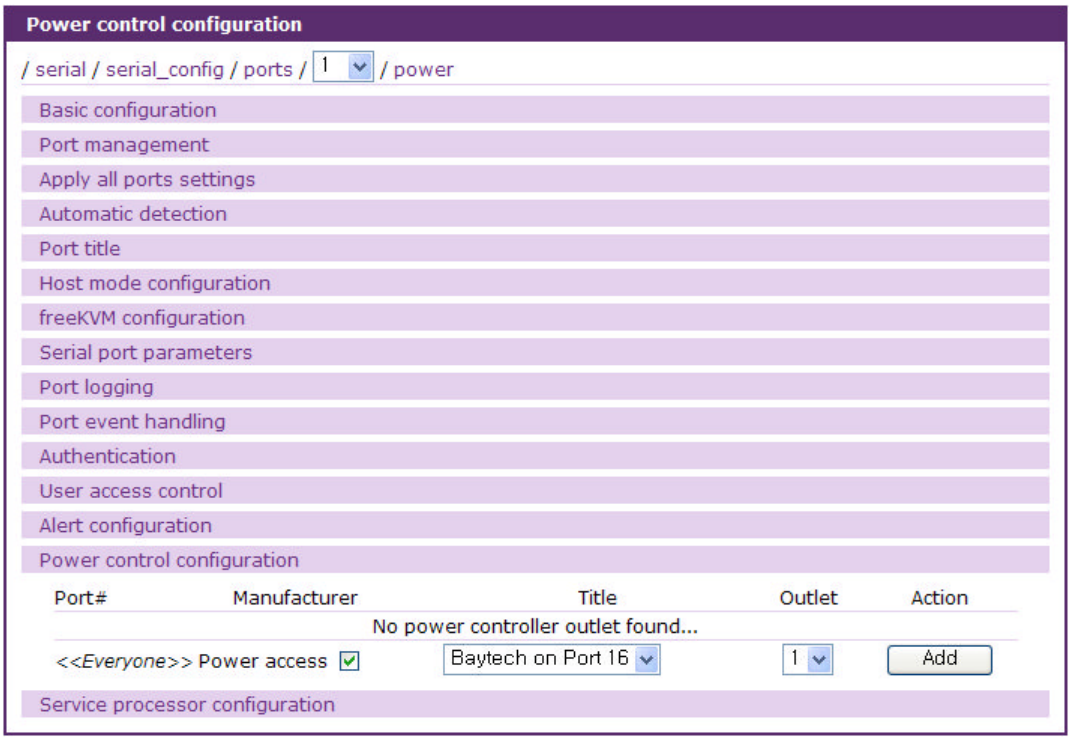


그림 4-32 Power control 설정

4.5.14 Service processor configuration

Host mode 설정에서 Host mode가 Console server mode로 설정되고 Service processor가 IPMI 또는 iLO로 설정되면, 원격 호스트를 IPMI나 iLO를 통해 감시 제어하기 위해 필요한 파라미터를 설정합니다. 그림 4-33는 Service processor configuration 화면을 보여줍니다.

Service processor configuration에 대한 설정 파라미터는 다음과 같습니다.

Destination IP

Destination port

User name

Password

Sensor alert configuration

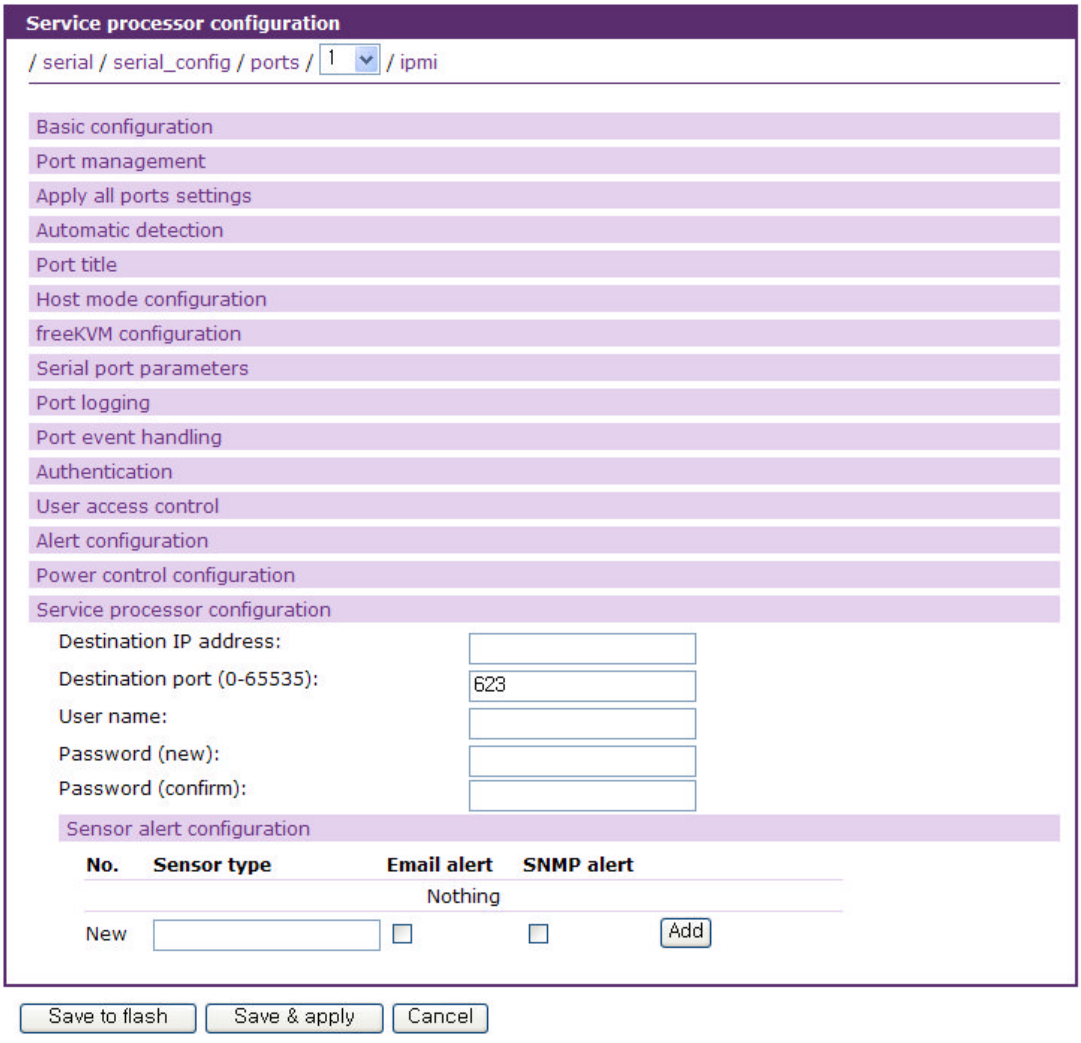


그림 4-33 Service processor configuration

Destination IP

원격 서버를 감시 / 제어하는 BMC(Baseboard Management Controller)의 IP 주소를 설정합니다. Service processor가 IPMI이고, 원격 포트의 Remote port parameters 설정에서 Protocol을 RMCP+(SOL)로 선택한 경우 Remote port paramters에서 설정한 Destination IP가 표시되고 읽기 전용 파라미터가 되어 변경할 수 없습니다.

Destination port

원격 서버를 감시 / 제어하는 BMC(Baseboard Management Controller)의 TCP port 번호를 설정합니다. Service processor가 IPMI이고, 원격 포트의 Remote port parameters 설정에서 Protocol을 RMCP+(SOL)로 선택한 경우 Remote port paramters에서 설정한 Destination port가 표시되고 읽기 전용 파라미터가 되어 변경할 수 없습니다.

User name

원격 서버를 감시 / 제어하는 BMC(Baseboard Management Controller)로 접속하는데 필요한 사용자 이름을 입력합니다.

User password

원격 서버를 감시 / 제어하는 BMC(Baseboard Management Controller)로 접속하는데 필요한 사용자의 패스워드를 입력합니다.

Sensor alert configuration

Service processor가 IPMI 일 경우 원격 서버의 경보를 발생시킬 Sensor의 종료와 이메일이나 SNMP trap 같은 경보의 종류를 설정합니다. 경보를 발생시킬 Sensor를 등록하더라도 실제로 경보를 발생시키려면 Alert 설정에서 Email alert for service processor 나 Service processor trap을 Enable로 설정해야 합니다.

4.6 All Port 설정

모든 시리얼 포트가 유사하거나 동일하게 수정되는 경우, 이 기능을 이용하게 됩니다. **All port configuration** 상태에서 설정한 값은 개별 포트의 **Apply all port setting** 옵션이 **Disable**로 설정되어 있지 않은 모든 시리얼 포트에 적용됩니다.

All port configuration 파라미터는 아래의 그룹으로 나뉘어 질 수 있습니다:

1. Port management
2. Automatic detection
3. Port title
4. Host mode configuration

5. freeKVM configuration: *Only valid and visible if host mode set to Console Server Mode*.
6. Serial port parameters: *Invalid for remote port*
7. Port logging*: Only valid and visible if host mode set to Console Server Mode*.
8. Port event handling: *Only available if the host is set to Console Server Mode and Port logging is enabled.*
9. Authentication
10. User access control: *Only available if the host is set to Console Server Mode.*
11. Alert configuration: *Only available if the host is set to Console Server Mode.*
12. Service processor configuration: *Only available if the host is set to Console Server Mode and Service processor is IPMI or iLO.*

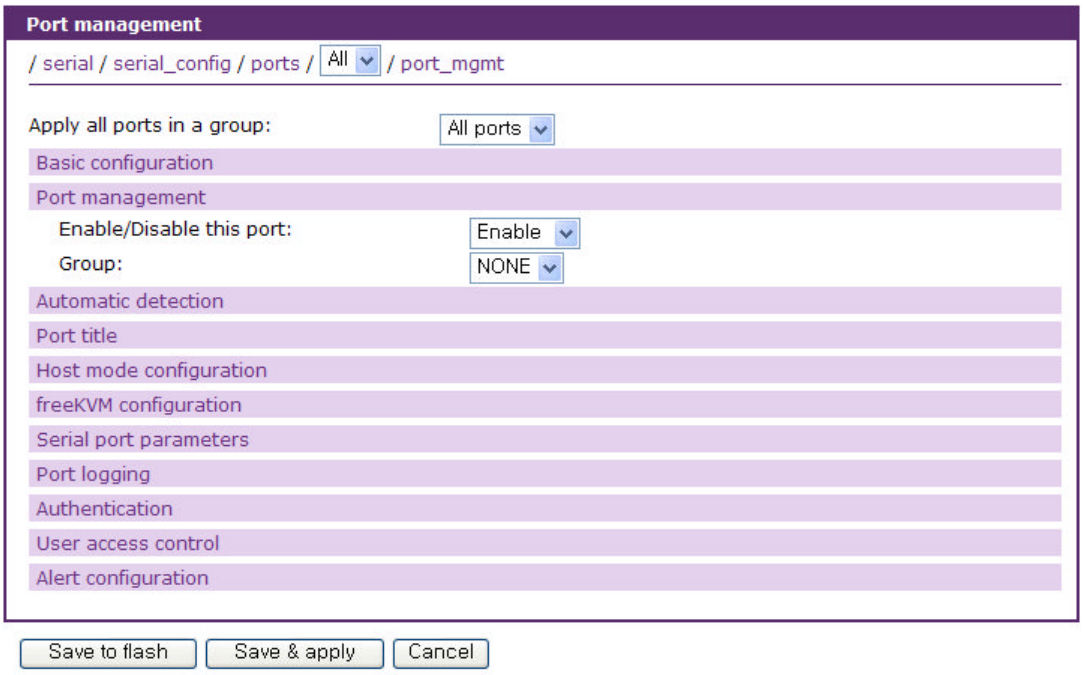


그림 4-34 모든 포트 설정

Apply all ports in a group

해당 그룹에 해당하는 포트들에게 설정을 적용합니다.

Enable/disable this port

이 파라미터는 포트의 기능 사용여부를 설정합니다.

Port title

이 파라미터가 특정 단어로 설정된 경우, 각 시리얼 포트 또는 원격 포트에 대한 포트 타이틀은 그 단어 및 포트 번호의 조합으로 설정됩니다. 예를 들어, 포트 타이틀이 "my server"로 설정되는 경우, 포트 #1의 포트 타이틀은 "my server1"로 설정되고 포트 #2의 포트 타이틀은 "my server2"로 자동으로 설정됩니다. 원격 포트 #1은 "my server33"(시리얼 포트 수 + 1 예는 VTS II 3200의 경우)으로 설정됩니다.

Host mode configuration

Host mode가 Consol server mode로 설정되는 경우, 허용된 각 시리얼의 할당 IP 주소는 다음과 같은 방식으로 자동으로 할당됩니다.

(IP address assigned + serial port number - 1) for serial port and

(IP address assigned + remote port number – 1 + serial port count) for remote port

예를 들어, 할당된 IP 주소가 모든 포트 설정에서 192.168.1.1로 할당되는 경우, 포트 1의 IP 주소는 192.168.1.1이 되며 포트 2의 IP 주소는 192.168.1.2이 됩니다. VTSII3200인 경우, 원격 포트1의 IP 주소는 192.168.1.33이 됩니다. 이와 유사하게, Listening TCP port number는 또한 다음의 방정식으로 설정됩니다.

(listening TCP port number + serial port number - 1) for serial port and

(listening TCP port number + remote port number – 1 + serial port count) for remote port

Host mode가 Terminal server 모드로 설정되는 경우, 각 시리얼 포트의 Destination IP 주소는 Console server 의 경우와 같은 방식으로 할당됩니다. 그러나, Destination TCP port number는 serial port number와 상관없이 동일 합니다. 예를 들어, Destination IP 주소 및 TCP port number가 192.168.1.1:8001로 설정되는 경우, 포트 1의 Destination IP 주소와 TCP port number는 192.168.1.1:8001가 되며 포트 2의 Destination IP 주소와 TCP port number는 192.168.1.2:8001가 됩니다.

freeKVM configuration, Serial port parameters, Port logging, Port event handling, Authentication, User access control, Alert configuration, Service processor configuration

위 그룹의 파라미터의 경우, All Port 설정에서 설정된 값은 모든 시리얼 포트 또는 원격 포트에서 동일하게 설정됩니다. 다만, Serial port parameters 설정의 경우에는 원격 포트에 영향을 미치지 않습니다.

4.7 Serial port 연결

VTS II의 웹 설정 인터페이스는 사용자로 하여금 사용자 자신의 Telnet 또는 SSH 클라이언트 프로그램을 사용하지 않고도 시리얼 포트에 접속할 수 있도록 하는 웹 기반 **Serial port connection** 기능을 제공합니다. 사용자가 좌측 메뉴 바에서 시리얼 포트 연결 메뉴 항목(**Serial port** > **Connection**)을 선택하는 경우, 그림 4-35과 같은 화면이 나타납니다.

이 페이지에서는 **port access menu**, **시리얼 포트, 원격 포트**, 클러스터링 슬레이브 장치 및 클러스터링 Peer-to-peer의 다른 Peer 장치의 사용 가능한 모든 **시리얼 포트**에 대한 연결 기능을 제공합니다.

표시해야 할 포트 수가 웹 서버 설정(***3.8 웹 서버 설정*** 참조)에서 지정된 한 페이지에 표시되는 시리얼 포트 수를 초과할 경우 전체 포트를 그 숫자만큼 나누어서 한 페이지에 표시하고, 다른 페이지로 쉽게 이동할 수 있도록 우측 상단에 [--- Movt to ---] 리스트 박스를 제공합니다.
Status 칼럼에는 전원이 꺼져 있거나 전원 상태를 알 수 없는 경우 또는 Port event handling 설정에서 입력한 키워드가 발견되어 경보가 발견된 경우에 해당 아이콘이 표시됩니다. 파원 관련 아이콘을 클릭하면 Serial port power control 페이지로 연결되어 시리얼 포트의 파워를 제어할 수 있습니다. 포트 이벤트 발생 경보 아이콘을 클릭하면 View port log 페이지가 열려 로그를 확인할 수도 있고 경보를 해제할 수도 있습니다.
Port # 칼럼명을 클릭하여 포트 번호 순서로 정렬할 수 있습니다. 처음에는 오름차순으로 정렬하고 한 번 더 클릭하면 내림차순으로 정렬합니다. [--- Movt to ---] 리스트 박스에는 이동할 페이지의 첫 번째 포트의 포트 번호가 함께 표시됩니다. 원격 포트는 실제 시리얼 포트 수보다 큰 값이 표시되고, 클러스터링 슬레이브 장치의 경우에는 포트 번호 앞에 슬레이브 장치 번호가 붙습니다. 클러스터링 Peer-to-peer의 Peer 장치의 경우 Peer 장치 번호가 표시되고, Peer 장치의 클러스터링 슬레이브 장치일 경우 Peer 장치 번호 다음에 클러스터링 슬레이브 장치 번호가 표시됩니다.
Title 칼럼명을 클리하면 포트 타이틀 순서로 정렬합니다. 처음에는 오름차순으로 정렬하고 한 더 클릭하면 내림차순으로 정렬합니다. [--- Movt to ---] 리스트 박스에는 이동할 페이지의 첫 번째 포트의 포트 타이틀이 함께 표시됩니다.
또한, Peer 번호나 포트 타이틀 같은 검색조건을 선택하거나 입력하고 **[Search]** 버튼을 클릭하면 시리얼 포트 연결페이지에 표시되는 포트를 제한할 수 있습니다.

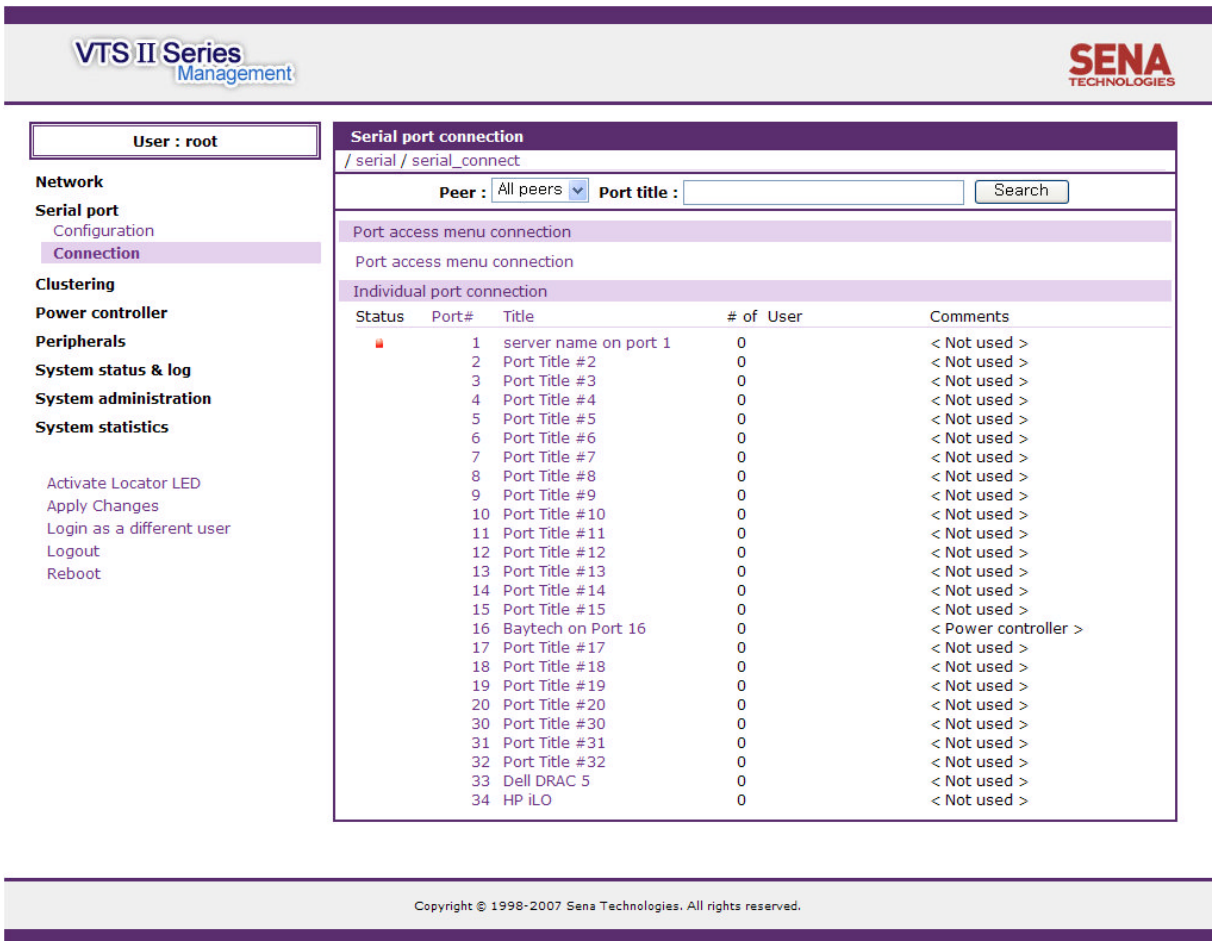


그림 4-35 시리얼 포트 연결 페이지

사용자는 제어하려는 포트의 포트번호나 타이틀을 클릭하여 조작 가능한 작업들을 리스트할 수 있습니다. 작업리스트에서 원하는 작업을 선택하여 포트를 제어할 수 있습니다. 그림 4-36는 포트 번호나 타이틀을 클릭하여 나타난 작업리스트를 보여줍니다. 포트의 작업리스트가 표시된 상태에서 포트 번호나 타이틀을 클릭하면 작업리스트가 사라집니다. 이 상태에서 다른 포트 번호나 타이틀을 선택하면 이전 포트의 작업리스트는 사라지고 새로 선택한 포트의 작업리스트가 표시됩니다.

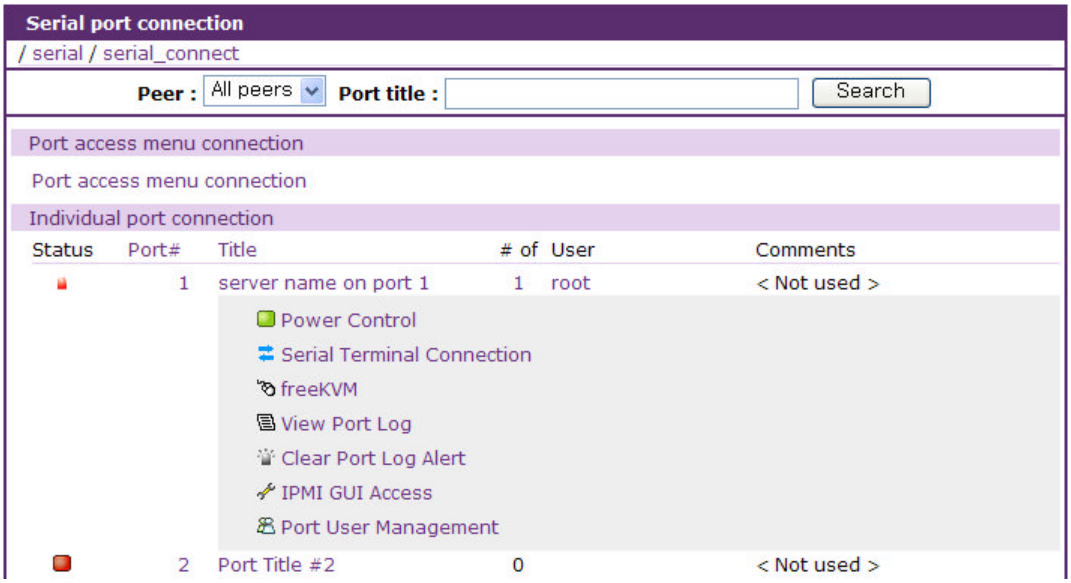


그림 4-36 포트 작업리스트

사용자는 자신들이 접속하려는 포트의 작업리스트에 있는 터미널 모양의 Serial Terminal Connection 아이콘을 클릭함으로써 포트에 접속할 수 있습니다. 사용자가 해당 포트의 터미널 아이콘을 클릭하면 터미널 에뮬레이션 팝업 창이 나타나 사용자에게 시리얼 포트 접속에 대한 권한을 부여합니다.

***참고**: 해당 포트의 프로토콜이 Telnet 또는 SSH로 설정 되어 있을 경우에는 팝업되는 터미널 에뮬레이션 창의 종류는 **4.5.5 Host mode 설정**에서 기술된 바와 같이 Quick connect via 메뉴의 설정값에 따라 달라집니다.*

Java Telnet Applet은 포트에 접속하기 위한 텍스트 기반의 사용자 인터페이스를 제공합니다. Java Telnet Applet은 Telnet 또는 SSH 연결만을 지원하며, 포트의 Host mode가 Raw TCP 연결 모드로 설정된 경우는 웹을 통해 포트에 접속할 수 없습니다. 연결할 포트를 클릭하면, Java Telnet Applet 창이 나타나게 되고, 사용자는 그 포트에 접속하기 위해 필요한 자신의 사용자 ID 및 비밀 번호를 입력하라는 요청을 받게 됩니다. 인증을 받은 경우, 사용자는 현재 시리얼 포트, 원격 포트 또는 클러스터링 슬레이브 장치/클러스터링 Peer 장치의 포트에 접속할 수 있습니다. Java Telnet Applet 창의 타이틀 바는 Telnet 또는 SSH의 연결 상태, 포트 번호와 포트 타이틀과 같은 정보를 보여줍니다. 창 아래의 버튼들은 Local echo ON/OFF, 연결, 종료 또는 브레이크 전달 등의 기능을 제공하고 있습니다.

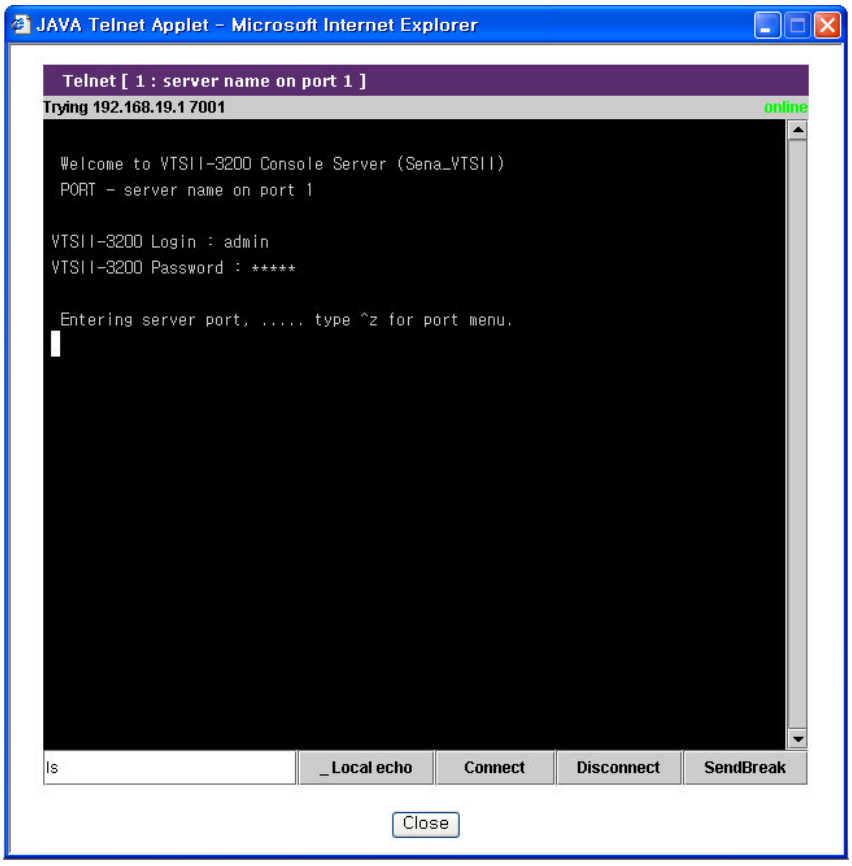


그림 4-37 JTA Telnet 윈도우

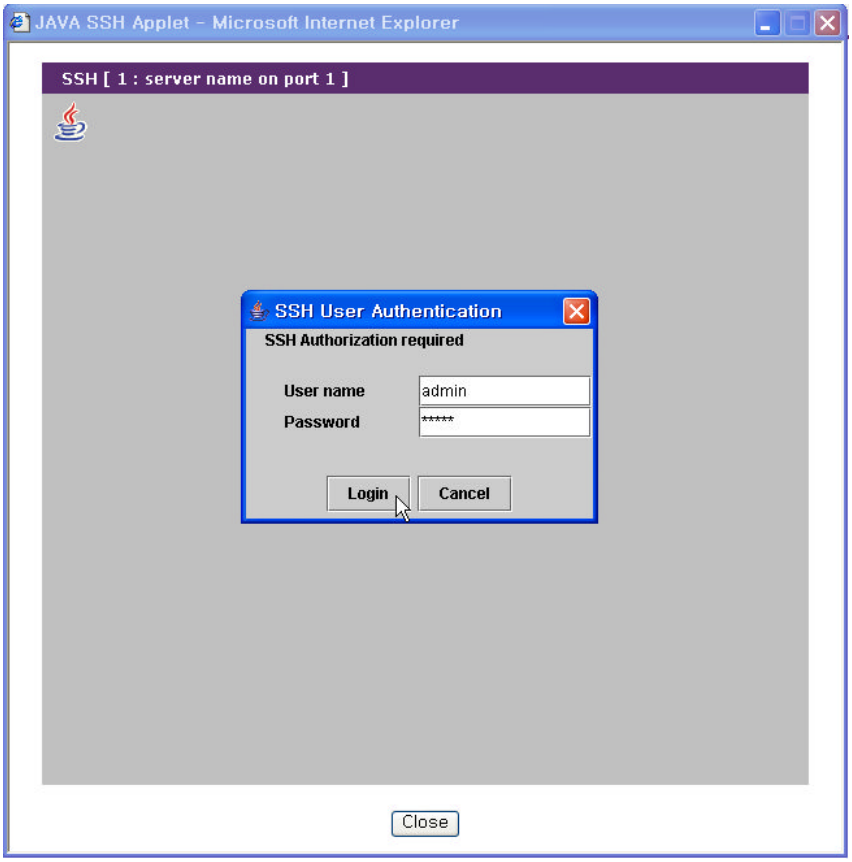


그림 4-38 JTA SSH 윈도우

VTS II가 SSH 버전 1을 지원할 지 여부는 시큐리티 프로파일의 SSH V1 항목에서 설정합니다. (***9.7 Security Profile*** 참조). Java Telnet Applet을 이용하여 SSH로 연결할 때 사용되는 SSH 버전은 웹 서버 설정의 Web applet option 항목에서 설정합니다. (***3.8 웹 서버 설정*** 참조).

참고*: SSH 공개 키로 등록된 사용자는 Java Telnet Applet 이 SSH 공개 키 인증을 제공하지 않기 때문에 Java Telnet Applet을 이용하여 웹을 통해 포트에 접속할 수 없습니다.*

시리얼 포트/원격 포트의 전원 제어에 대한 연결 기능을 제공합니다. 작업리스트에 있는 On/Off 상태를 표시하는 Power Control 아이콘을 클릭하면, 사용자는 시리얼 포트/원격 포트의 전원제어(**Serial port power control**)하는 페이지로 이동할 수 있고 그 페이지에서 포트에 연결된 장치의 전원을 관리할 수 있습니다. VTS II에 추가된 파워 컨트롤러를 관리할 수 있는 파워 컨트롤러 관리(**Power controller management**) 페이지로의 연결 기능을 제공합니다. 포트가 파워컨트롤러에 연결되어 있고 파워컨트롤러로 설정되어 있으면, 작업리스트에 Power Controller Management 아이콘이 표시되는데 이 아이콘을 클릭하면, 파워 컨트롤러 관리 페이지로 이동하여 파워 컨트롤러를 제어할 수 있습니다. 자세한 내용은 ***6.3.4 파워 컨트롤러 유닛 관리 – 시리얼 포트 연결***을 참조하시기 바랍니다.

포트에 연결된 서버가 KVM 연결을 지원하고 freeKVM 설정이 되어 있는 포트의 경우 작업리스트에 freeKVM 연결 아이콘이 표시됩니다. 사용자가 freeKVM 연결 아이콘을 클릭하면 KVM 클라이언트 프로그램을 실행하여 서버를 제어 관리할 수 있습니다. 복수의 freeKVM이 설정되어 있으면 복수의 freeKVM 설정 중에서 클라이언트가 지원하는 KVM 클라이언트 프로그램을 선택할 수 있도록 KVM 리스트가 표시되고 이 화면에서 선택한 KVM 클라이언트 프로그램을 실행합니다.

View Port Log 아이콘을 선택하면 그림 4-39와 같은 View port log 화면이 나타납니다. **[Clear]** 버튼을 클리하여 현재 로그를 삭제할 수 있습니다. **[Refresh]** 버튼을 클릭하여 최신 로그를 표시할 수 있고, **[Close]** 버튼을 클릭하여 View port log 화면을 닫을 수 있습니다. 로그내에 Port event handling 설정에서 등록한 키워드가 발견되면 화면 상단에 경고가 표시되고 **[Clear alert]** 버튼이 표시됩니다. 이 버튼을 클릭하면 경보를 해제할 수 있습니다.
작업리스트에 있는 Clear Port Log Alert 아이콘도 로그내 키워드가 발견될 때 표시되는데, 이 아이콘도 경보를 해제하기 위해 사용됩니다.

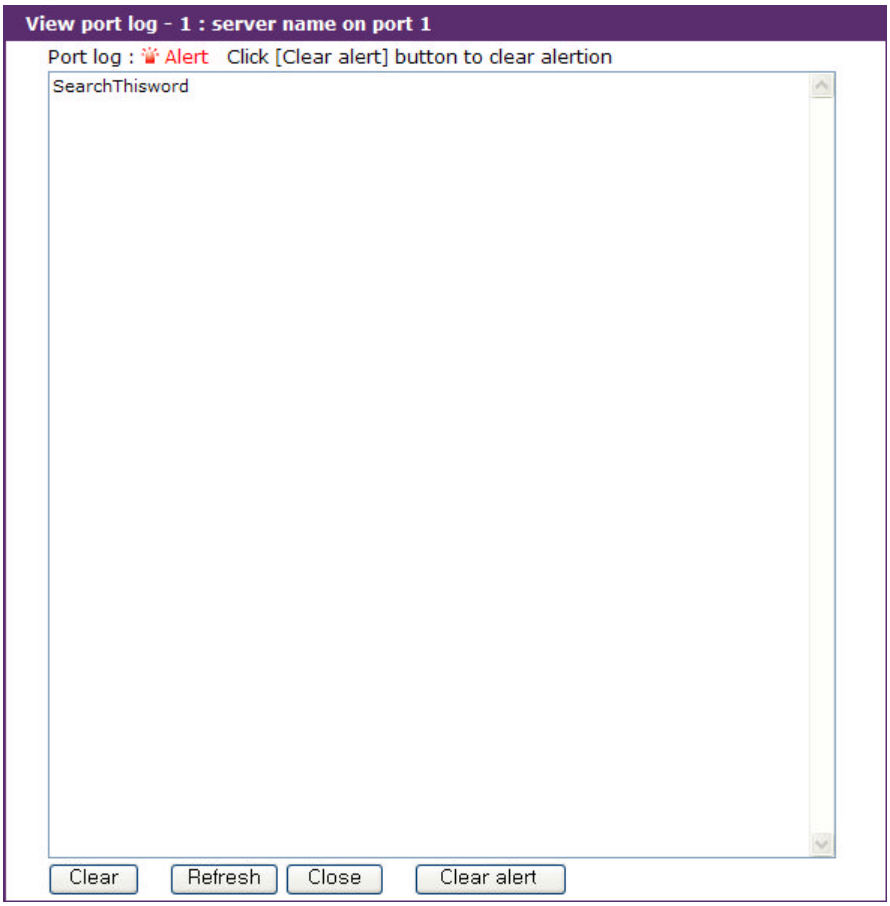


그림 4-39 View port log

Host mode 설정에서 Service processor의 종류에 따라 IPMI GUI Access, iLO GUI Access, DRAC GUI Access 의 아이콘이 표시됩니다.

Service processor를 IPMI로 설정했을 경우 IPMI GUI Access 아이콘이 표시됩니다. 이 아이콘을 클릭하면 IPMI를 통해 원격 호스트를 감시 / 제어하는 웹인터페이스로 연결됩니다. 그림 4-40은 IPMI GUI Access 화면을 보여줍니다. 상단의 리스트 박스에서 원하는 작업을 선택하여 세부 항목별로 원격 호스트를 감시 / 제어할 수 있습니다.

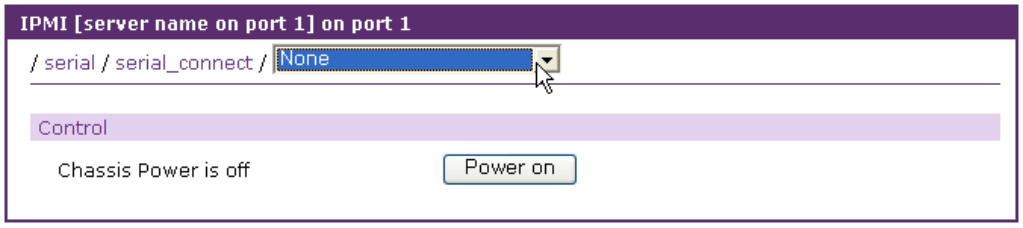


그림 4-40 IPMI GUI Access

원격 포트에서 Host mode 설정에서 Service processor를 IPMI로 설정하고 Remote port parameters 설정에서 Protocol을 RMCP+(SOL)로 선택하면, IPMI GUI Access 화면에 **[Connect to system]** 버튼과 **[De-activate SOL on another session]** 버튼이 나타납니다. 그림 4-41은 이렇게 설정된

상태에서 원격 포트의 IPMI GUI Access 화면을 표시합니다. **[Connect to system]** 버튼을 클릭하면 원격 포트에서 지정한 원격 호스트의 BMC로 연결하여 SOL을 통해 직접 원격 호스틀 감시 / 제어할 수 있습니다. **[De-activate SOL on another session]** 버튼을 클릭하면 현재 접속되어 있는 SOL 연결을 끊어 새로운 SOL 연결을 가능하도록 합니다. 이 경우 Serial port 연결 페이지의 원격 포트 작업리스트에 나타나는 Serial Terminal Connection 아이콘을 클릭하여 SOL 연결을 시도할 수도 있습니다.

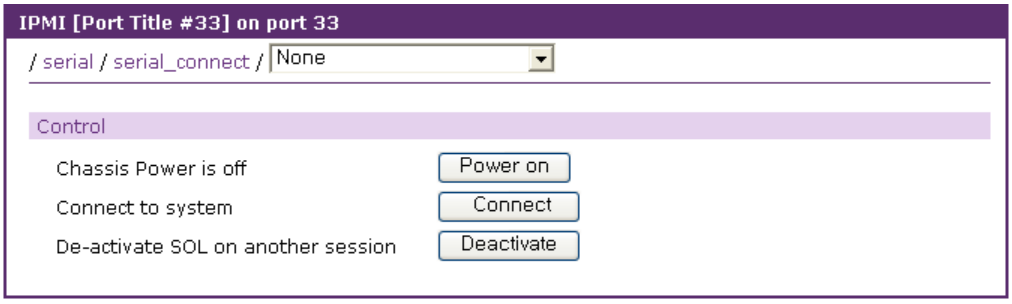


그림 4-41 원격 포트의 IPMI GUI Access

Service processor를 iLO로 설정했을 경우 iLO GUI Access 아이콘이 표시됩니다. 이 아이콘을 클릭하면 iLO를 통해 원격 호스트를 감시 / 제어하는 웹인터페이스로 연결됩니다.

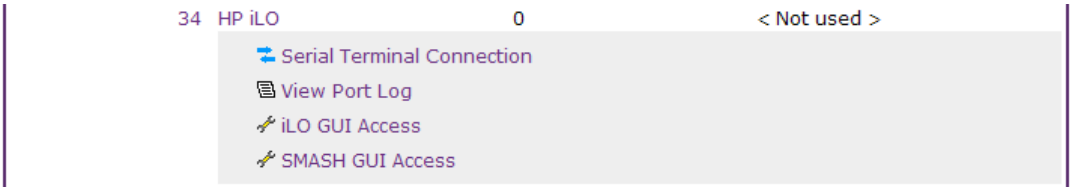


그림 4-42 iLO GUI Access

iLO GUI Access 화면은 System summary, Control, Access settings, IP settings, System Health information, SNMP, iLO event log 등으로 구성되어 있습니다. **System summary** 탭에서는 BIOS information, System information, Processor information, Memory device등의 정보를 표시합니다. **Control** 탭에서는 원격 호스트에 접속하거나, 파워를 컨트롤 할 수 있습니다. **Access settings** 탭에서는 SSH, Telnet, Web, Terminal, Virtual media 등의 포트를 지정하거나 Access 가능 여부를 설정할 수 있습니다. **IP settings** 탭을 통해서는 원격 호스트의 IP address를 변경할 수 있습니다. **System health information** 탭에서는 원격 호스트의 Fan, Temperature, VRM, Power supply 등의 정보를 볼수 있습니다. **SNMP** 탭에서는 iLO의 SNMP에 대한 정보를 설정할 수 있습니다. **iLO Event log** 탭을 통해 iLO의 event log를 볼 수 있습니다.

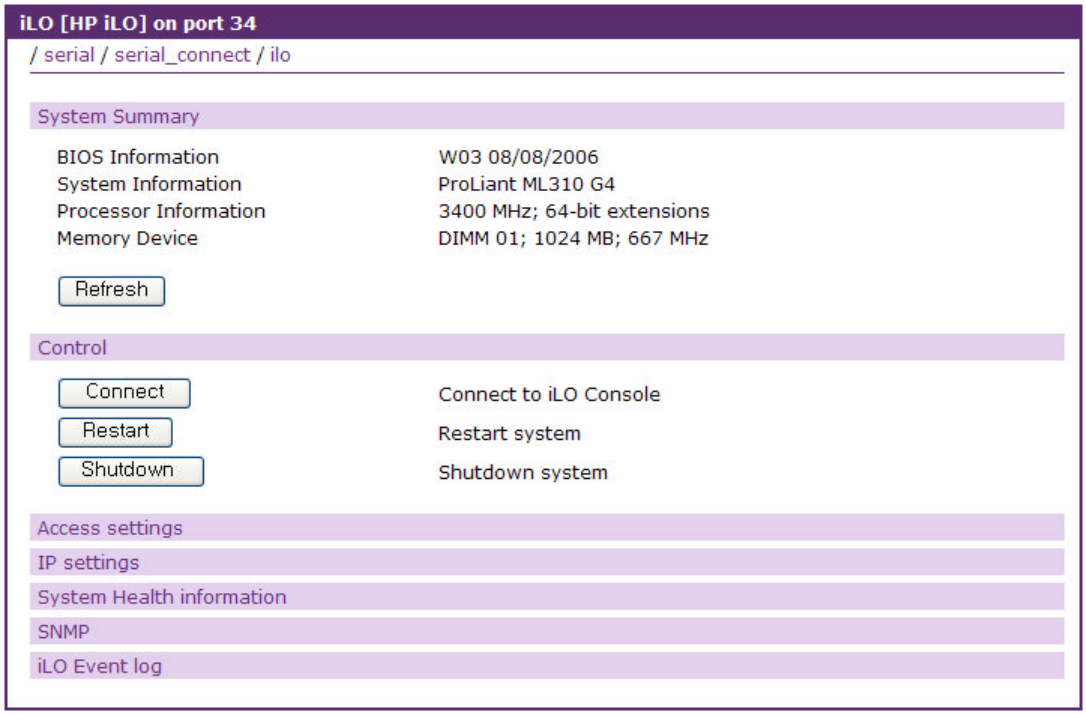


그림 4-43 원격 포트의 iLO GUI Access

Service processor를 DRAC으로 설정했을 경우 DRAC GUI Access 아이콘이 표시됩니다. 이 아이콘을 클릭하면 DRAC을 통해 원격 호스트를 감시 / 제어하는 웹인터페이스로 연결됩니다.

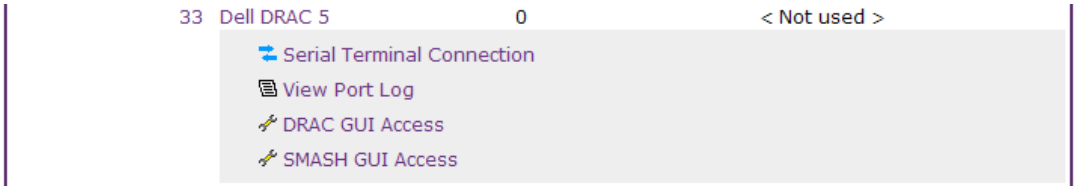


그림 4-44 DRAC GUI Access

DRAC GUI Access 화면은 System summary, Control, Access settings, IP settings, System Health information, SNMP, iLO event log 등으로 구성되어 있습니다. **System summary** 탭에서는 System Model, System BIOS Version, BMC Firmware Version, Service TAG, Host name, OS name등의 정보를 표시합니다. **Control** 탭에서는 원격 호스트에 접속하거나, 파워를 컨트롤 할 수 있습니다. **Access settings** 탭에서는 SSH, Telnet, Web, Console 등의 포트를 지정하거나 Access 가능 여부를 설정할 수 있습니다. **IP settings** 탭을 통해서는 원격 호스트의 IP address를 변경할 수 있습니다. **DRAC Event log** 탭을 통해 DRAC의 event log를 볼 수 있습니다.

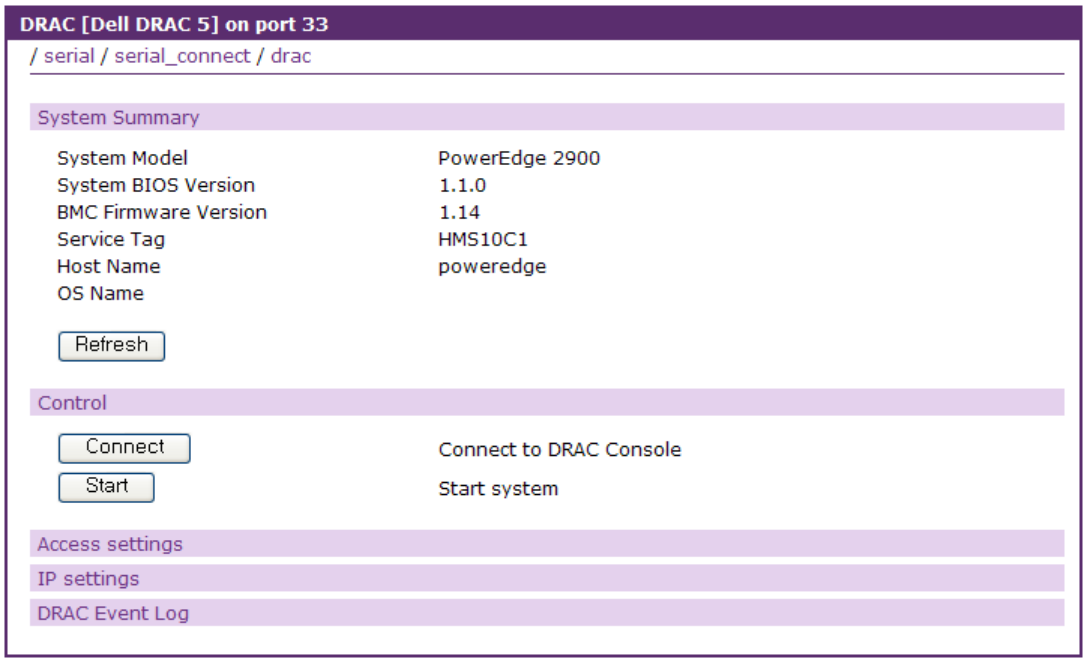


그림 4-45 원격 포트의 DRAC GUI Access

SMASH를 지원하는 Service processor(iLO/DRAC) 에 대해서는 Remote port parameter 설정에서 SMASH의 사용 여부를 설정할 수 있습니다. SMASH GUI Access 화면에서는 현재의 Target에 대해 수행할 수 있는 명령들을 버튼을 표시합니다. 해당 버튼을 클릭함으로써 현재의 Target에 해당 명령을 수행하도록 합니다. 만약 Property 중 변경 가능하다면 Property의 값은 에디트박스로 표시되어 변경할 수 있습니다. 값을 변경하고 변경할 property들을 선택한 후 하단의 Set 버튼을 누르면 해당 property의 값이 변경됩니다.

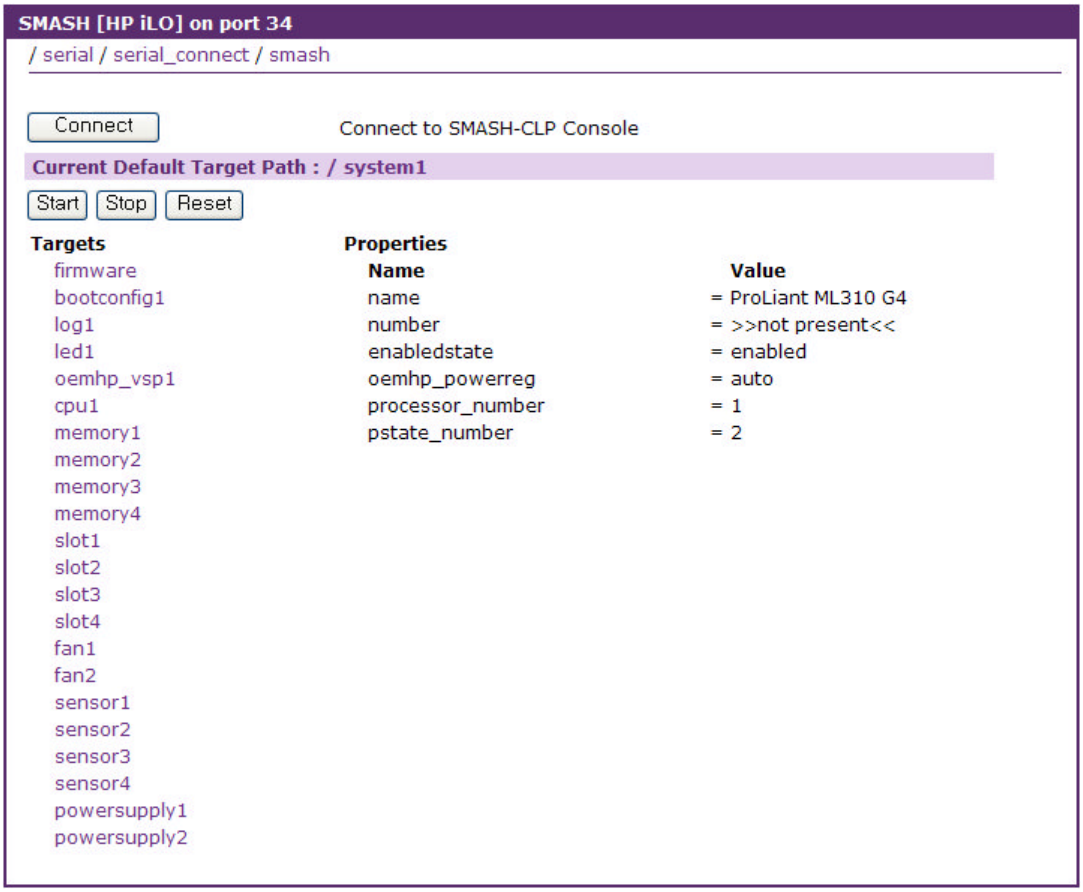


그림 4-46 원격 포트의 SMASH GUI Access

또한, 시리얼 연결 페이지에는 현재 포트의 접속 상황에 대한 정보도 표시합니다. 접속한 사용자의 수(# 항목), 포트 사용자 아이디(User 항목) 및 포트 사용자가 입력한 주석(Comments 항목)을 포트별로 표시합니다.

시리얼 포트 연결 페이지에 표시되는 메인 세션 사용자 외에 현재 연결 중인 사용자들의 리스트를 확인할 수도 있고, 사용자의 연결을 강제로 종료할 수도 있습니다. 해당 시리얼 포트의 [# of User] 항목을 클릭하거나 작업리스트에 있는 Port User Management 아이콘을 클릭하면 그림 4-47 로그인 중인 시리얼 포트 사용자 리스트 화면이 나타 납니다.

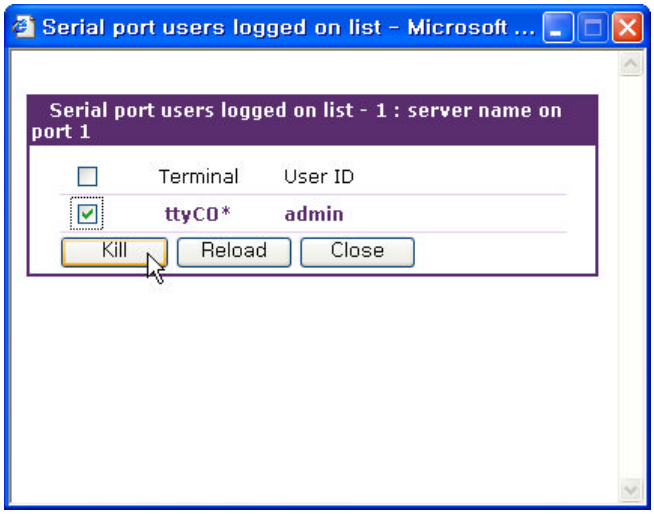


그림 4-47 로그인 중인 시리얼 포트 사용자 리스트

이 화면의 사용자 리스트 중에서 연결 종료하려는 사용자들을 체크한 후 **[Kill]** 버튼을 누르면 해당 사용자들의 연결을 강제로 종료할 수 있습니다.

VTS II는 웹 인터페이스에 로그인하지 않고 직접 시리얼 포트, 원격 포트 또는 슬레이브 장치의 시리얼 포트에 접근하는 웹 페이지를 제공합니다. 웹브라우저의 주소창에 다음과 같이 입력하면 시리얼 포트에 직접 연결하는 JTA 애플릿을 포함한 페이지로 이동합니다

.

`http://<IP>/connect.asp?p=<port number>`

또는

`http://<IP>/connect.asp?t=<port title>`

여기서 <IP>는 VTS II의 IP 주소 또는 도메인 이름을 의미합니다. <port number>는 시리얼 포트 번호, <port title>은 시리얼 포트의 이름입니다. 사용자는 <port number>의 포트 번호를 가진 포트로 또는 포트 이름에 <port title>을 포함한 포트로 연결할 수 있습니다. <port number>는 다음의 형식을 가집니다.

`[R{peer_number}][S{slave_unit_number}][P]port_number`

예) 1. 시리얼 포트 #1 : `1 or P1`

2. 클러스터링 슬레이브 장치 #1의 시리얼 포트 #2 : S1P2
3. 클러스터링 Peer-to-peer 장치 #2 시리얼 포트 #3 : R2P3
4. 클러스터링 Peer-to-peer 장치 #2의 클러스터링 슬레이브 장치 #3의 시리얼 포트 #4 : R2S3P4

그림 4-48와 그림 4-49은 <port number>와 <port title>을 사용하여 직접 시리얼 포트로 연결하는 예를 보여줍니다.

User 항목을 다음과 같이 입력하여 사용자는 SSH 원격 시리얼 콘솔을 통하여 시리얼 포트, 원격 포트 또는 슬레이브 장치의 시리얼 포트에 연결할 수 있습니다.

<user>:p=<port number>

또는

<user>:t=<port title>

또는

<user>:<tcp port number>

여기서 <port number>는 포트 번호, <port title>은 포트의 이름입니다. 사용자는 <port number>의 포트 번호를 가진 포트로 또는 포트 이름이 <port title>과 일치하는 포트로 연결할 수 있습니다. Port number로 시리얼 포트에 직접 연결에서의 <port number>와 같은 형식을 갖습니다. <tcp port number>는 포트의 TCP 포트 번호입니다. TCP 포트 번호가 <tcp port number>인 시리얼 포트로 연결할 수 있습니다.

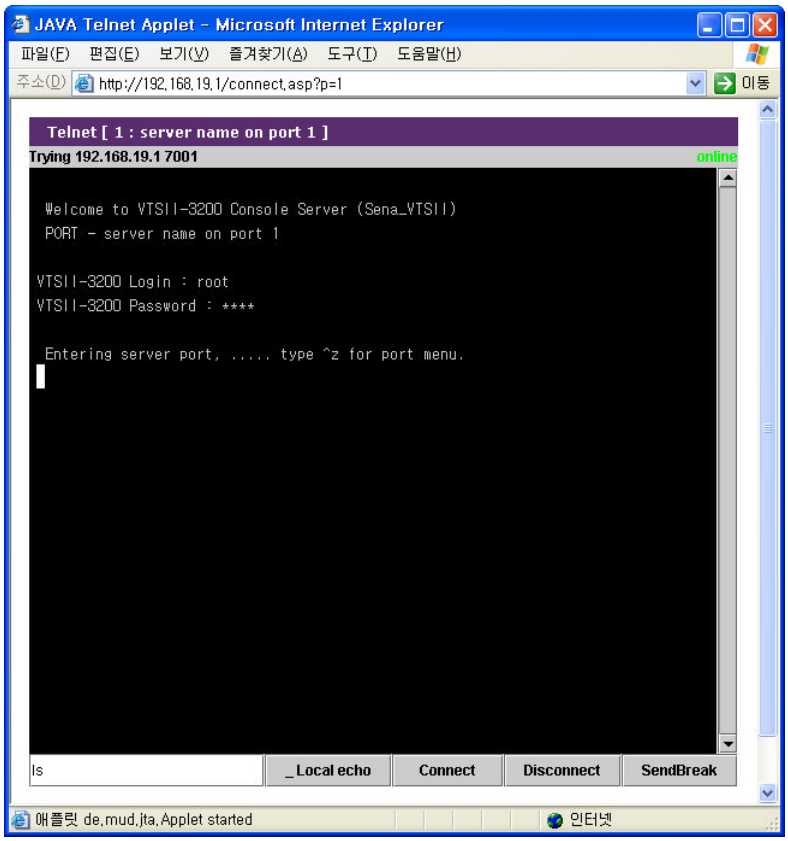


그림 4-48 Port number로 시리얼 포트에 직접 연결

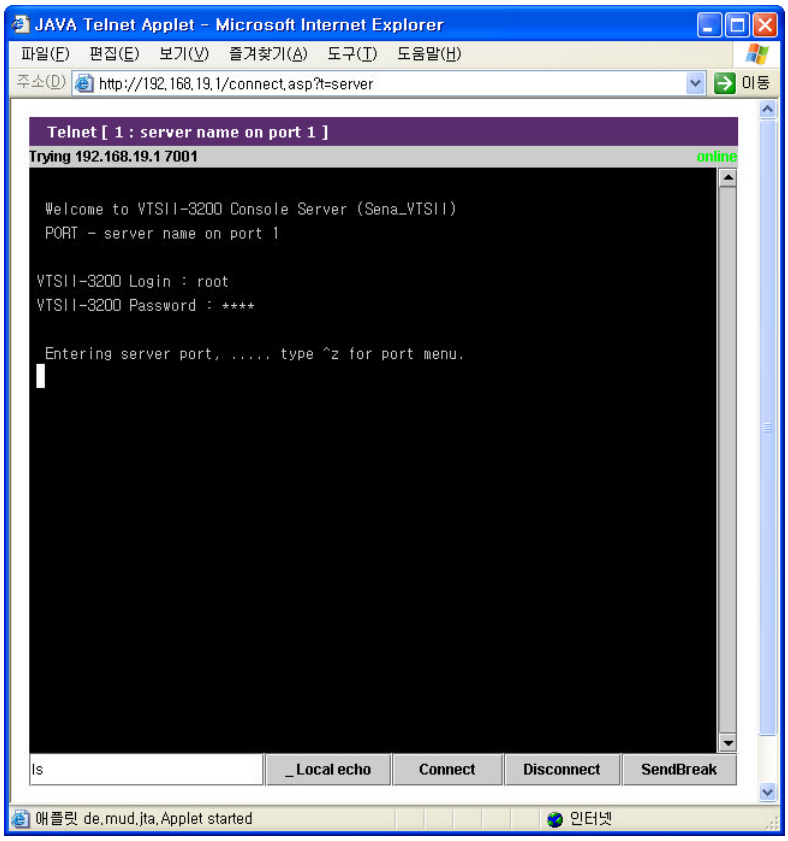


그림 4-49 Port title로 시리얼 포트에 직접 연결

그림 4-50과 그림 4-51은 리눅스에서 <port number>과 <port title>을 이용하여 SSH 원격 시리얼 콘솔을 통하여 포트에 연결하는 예입니다. 그림 4-52은 리눅스에서 <tcp port number>를 이용하여 SSH 원격 시리얼 콘솔을 통하여 포트에 연결하는 예입니다.

```
[root@loclahost ~] ssh root:p=1@192.168.19.1
root:p=1@192.168.19.1's password:

    Entering server port, ..... type ^z for port menu.
```

그림 4-50 SSH 원격 시리얼 콘솔을 통한 포트 연결 - port number

```
[root@loclahost ~] ssh 'root:t=server name on port 1@192.168.19.1'
root:t=server name on port 1@192.168.19.1's password:

    Entering server port, ..... type ^z for port menu.
```

그림 4-51 SSH 원격 시리얼 콘솔을 통한 포트 연결 - port title

```
[root@loclahost ~] ssh root:7001@192.168.19.1
root:7001@192.168.19.1's password:

    Entering server port, ..... type ^z for port menu.
```

그림 4-52 SSH 원격 시리얼 콘솔을 통한 포트 연결 – tcp port number

5: Clustering 설정

5.1 개요

VTS II는 Clustering 기능을 사용하여 하나의 VTS II를 통해, 다른 여러 VTS II들의 시리얼 포트들도 접속할 수 있습니다. VTS II의 Clustering 방법에는 Clustering Master/Slave 방법과 Clustering Peer-to-peer 방법이 있습니다.

Clustering Master/Slave 사용자는 하나의 마스터 VTS II를 통해 최대 1,632개까지의 시리얼 포트(*=(48 시리얼 포트 + 48 원격 포트) * 16 개의 슬레이브 장치 + 마스터 장치의 48 시리얼 포트 + 마스터 장치의 48 원격 포트*)를 접속할 수 있습니다.
슬레이브 장치의 시리얼 포트로 접근하기 위해 VTS II는 NAT(Network Address Translation)에 기반한 방법론을 사용합니다. 커널 기반의 간단한 IP forwarding 방식을 사용하여, VTS II는 효율적이고 유연하고 빠르면서 안전한 접근 방법을 제공합니다. 만약, 사용자가 현재 환경을 반영하는 IP forwarding 규칙을 수동으로 설정한다면, VTS II는 다른 터미널 서버들도 또한 관리할 수 있게 됩니다.
마스터 VTS II의 TCP port로 전송되는 데이터는 슬레이브 VTS II의 (IP 주소: TCP 포트)에 전달됩니다. 따라서, 사용자가 마스터 VTS II에서 IP forwarding 규칙만 설정해 주면, 마스터 VTS II를 통해 슬레이브 VTS II들에게 접속할 수 있게 됩니다. 슬레이브 VTS II에는 추가적인 설정이 필요 없습니다.

사용자가 마스터 VTS II를 경유하여 슬레이브 VTS II의 시리얼 포트에 접속을 시도한다고 생각해 봅시다. 다음은 현재 사용자의 응용 환경입니다.

- 사용자 컴퓨터의 IP 주소: 192.168.0.100
- 마스터 VTS II의 IP 주소: 192.168.0.2
- 슬레이브 VTS II의 IP 주소: 192.168.0.3.
- 마스터 VTS II의 TCP 포트 7201을 슬레이브 VTS II의 시리얼 포트 1 (TCP 포트, 7001)를 위해 따로 지정합니다.

그림 5-1은 이러한 조건 하의 VTS II Clustering 기능에 대한 작동 개념을 보여줍니다.

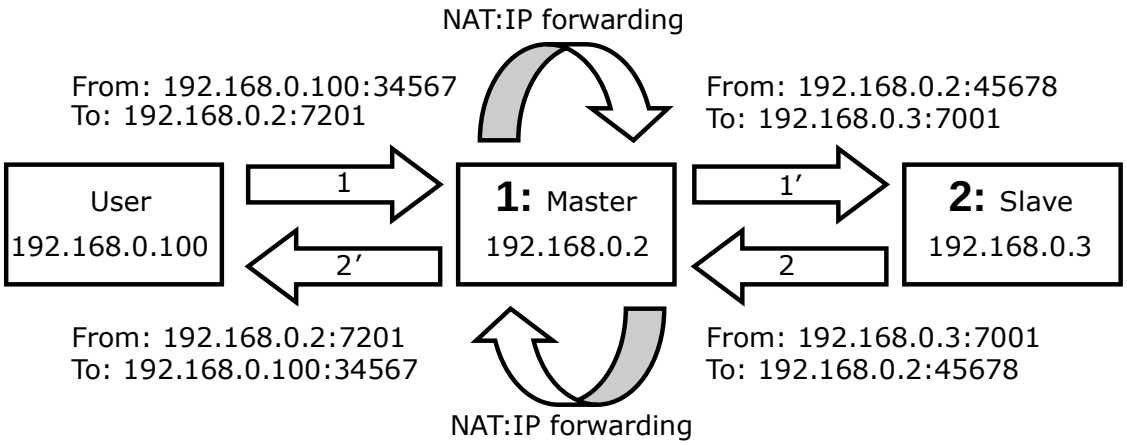


그림 5-1 Clustering Master / Slave 작동 개념

그림 5-2는 초고속 인터넷 환경에서, 마스터 VTS II를 통해 슬레이브 VTS II에 연결하는 응용도를 나타냅니다.

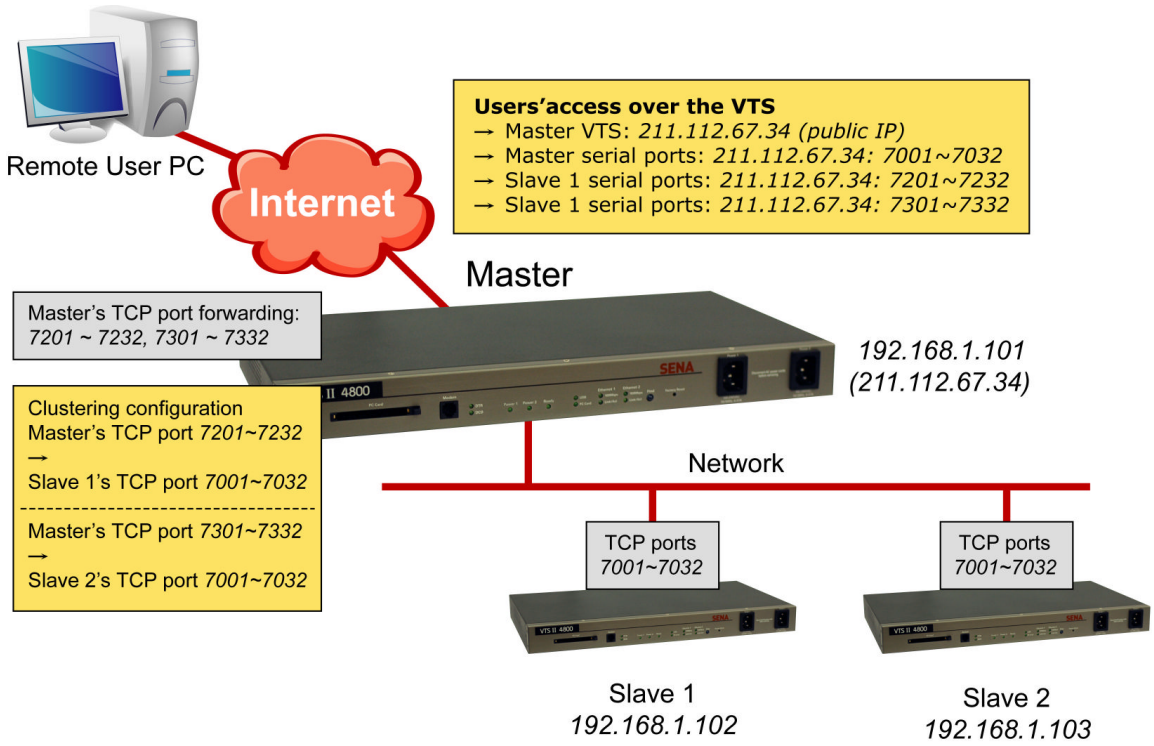


그림 5-2 Clustering Master / Slave 예제

Clustering Master / Slave는 마스터 장치를 통해서 슬레이브 장치에 접근할 수 있습니다. Clustering

Peer-to-peer는 Clustering내의 어느 Peer를 통해서도 다른 Peer로 접근할 수 있습니다. 즉, Clusterng 내의 한 Peer는 IP forwarding 방식을 이용하여 다른 Peer로 접근할 수 있도록 해준다는 점에서 Clustering Master / Slave 방식의 마스터 장치의 역할을 할뿐만 아니라, 다른 Peer들을 통해 사용자가 접근할 수 있다는 점에서 슬레이브 장치의 역할을 동시에 할 수 있습니다. Clustering Peer-to-peer 내의 모든 Peer들이 마스터 장치 역할과 슬레이브 장치 역할을 동시에 하기 때문에, Clustering Master / Slave에서 마스터 장치의 네트워크 연결이 끊어지면 슬레이브 장치로 접근이 차단되는 것과는 달리 Clustering Peer-to-peer에서는 한 Peer의 연결이 차단되더라도 다른 Peer를 통해 클러스터링내의 다른 Peer들로 접속이 가능합니다. Clustering Peer-to-peer의 한 Peer가 Clustering Master / Slave의 마스터 장치라면, 사용자들은 그 Peer의 포트뿐만 아니라 그 Peer의 슬레이브 장치의 포트에도 접근할 수 있습니다. 다른 Peer의 슬레이브 장치에 접근할 경우에는 다른 Peer의 슬레이브 장치로 직접 데이터를 주고 받지 않고, 다른 Peer에게 데이터를 보내면 다른 Peer가 자신의 슬레이브 장치에게 데이터를 보내고 역순으로 데이터를 받습니다. 이런 한 특징을 이용하면 Clustering Master / Slave가 갖는 포트수 제한을 극복할 수도 있고, Clustering을 유연하게 구성할 수도 있습니다.

Clustering Peer-to-peer에서는 모든 Peer들이 같은 IP forwarding table을 갖게 되며 한 Peer가 참여하거나 탈퇴할 때 이 값들을 자동으로 갱신합니다. 어느 Peer의 설정이 변경되면 사용자가 변경내용을 알리기 위한 조치를 하지 않더라도 모든 Peer들이 갱신된 내용을 자동으로 반영합니다.

그림 5-3은 Clustering Peer-to-peer 동작원리를 보여줍니다.

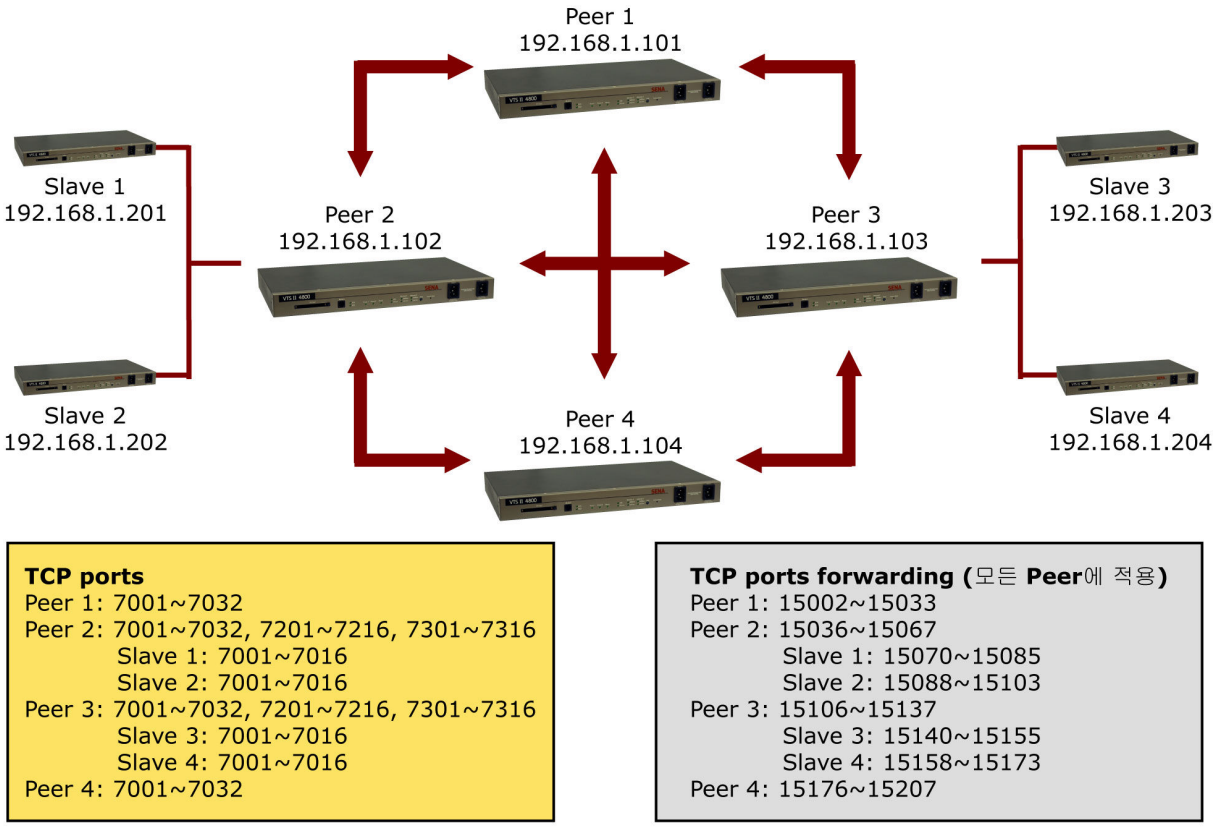


그림 5-3 Clustering Peer-to-peer 동작원리

5.2 Clustering Master / Slave 설정

Clustering 기능을 적용하기 위해서는 **Authentication mode**와 **Update master on changes**를 제외한 모든 설정을 마스터 장치에서 하면 됩니다. **Authentication mode**는 사용자가 마스터 장치를 통해 슬레이브 장치의 포트로 연결할 때 그리고 그 포트의 Authentication mode가 **Local**로 설정되어 있을 때, 사용자 인증을 마스터 장치에서 할지 슬레이브 장치에서 할지를 결정합니다. **Update master on changes**는 슬레이브 장치의 설정이 변경되어 적용될 경우 슬레이브 장치의 변경 사항을 마스트 장치의 슬레이브 정보에 자동 갱신할 지 여부를 설정합니다. VTS II의 **Clustering mode**가 **Master**로 설정되면 **Authentication mode**와 **Update master on changes** 항목은 비활성화 됩니다.

사용자가 한 VTS II를 마스터로 설정하기 원하는 경우, **Clustering 설정** 화면에서 설정해야 하는데, 장치를 미스터로 설정하면 마스터 설정에 관련된 설정 화면이 나타납니다. 그림 5-4는 Clustering Master / Slave 설정 화면을 보여줍니다. 사용자가 Clustering mode를 마스터로 설정하고 저장하면, 그림 5-5와 같은 마스터 장치를 위한 Clustering Master / Slave 설정 화면이 표시됩니다. Clustering mode가 Slave 일경우 Clustering master unit filtering을 통해 Master가 될 수 있는 유닛의 IP adress를 설정할 수 있습니다.

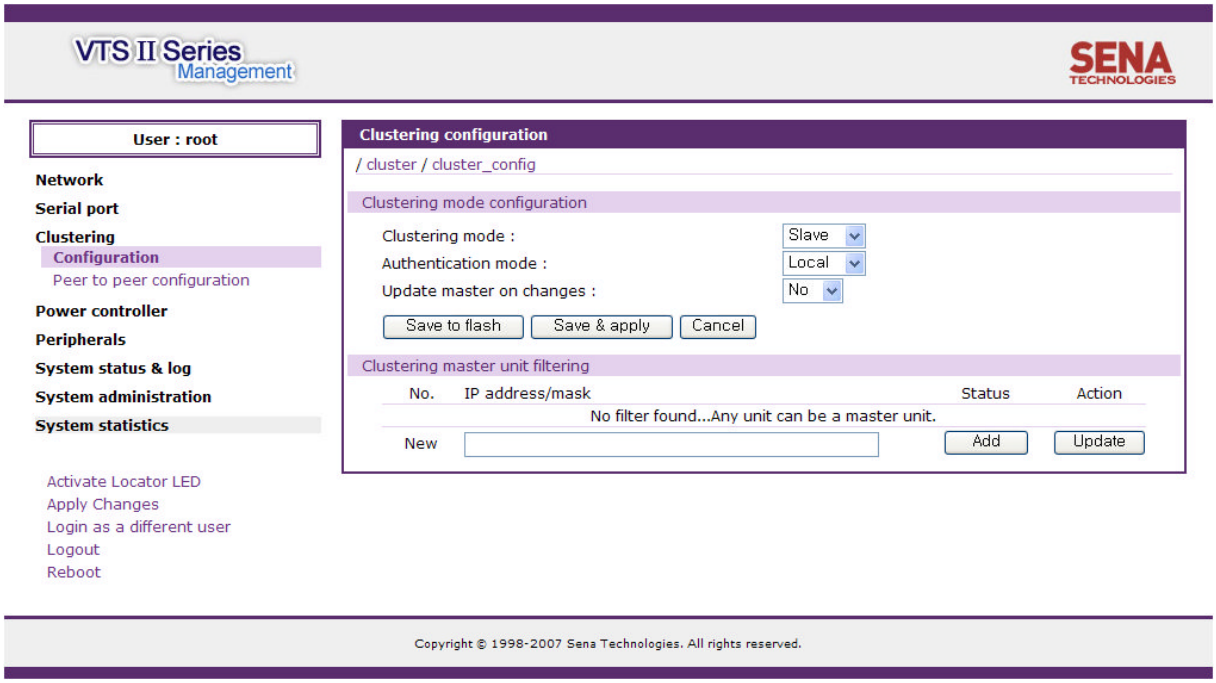


그림 5-4 Clustering Master / Slave 설정

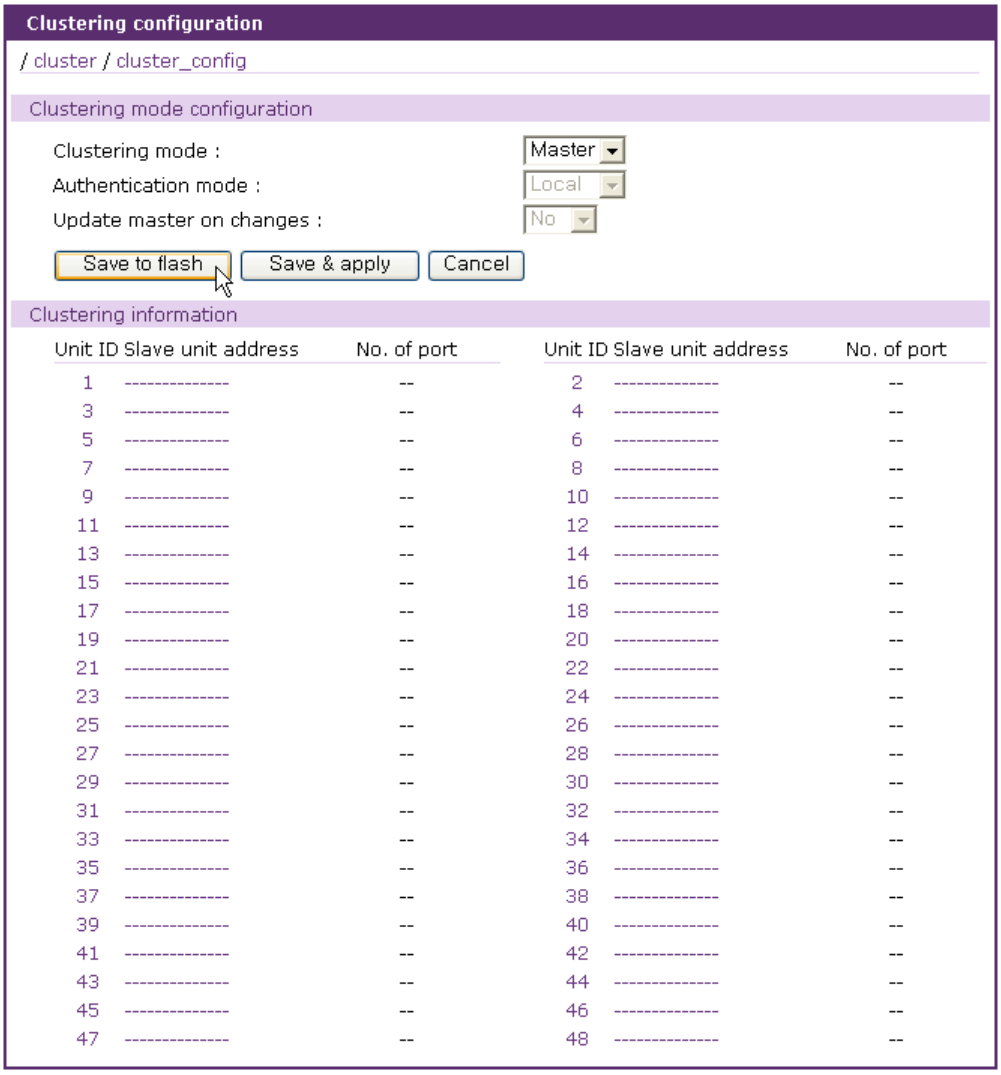


그림 5-5 Clustering Master / Slave 설정 – Master로 설정 후

슬레이브 장치를 추가하려면, 사용자는 슬레이브 장치 ID 또는 주소를 클릭하여 그림 5-6과 같은 Slave Unit 설정화면으로 이동하여 추가적인 설정을 할 수 있습니다. 이 화면에서 슬레이브 장치를 Enable로 선택하면, 지정된 슬레이브 장치에 대한 추가적인 설정을 할 수 있는 그림 5-8과 같은 화면으로 바뀝니다.

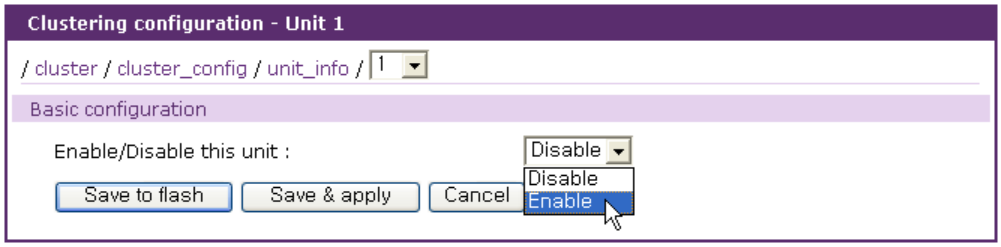


그림 5-6 Clustering Master / Slave 설정 – Slave Unit 설정

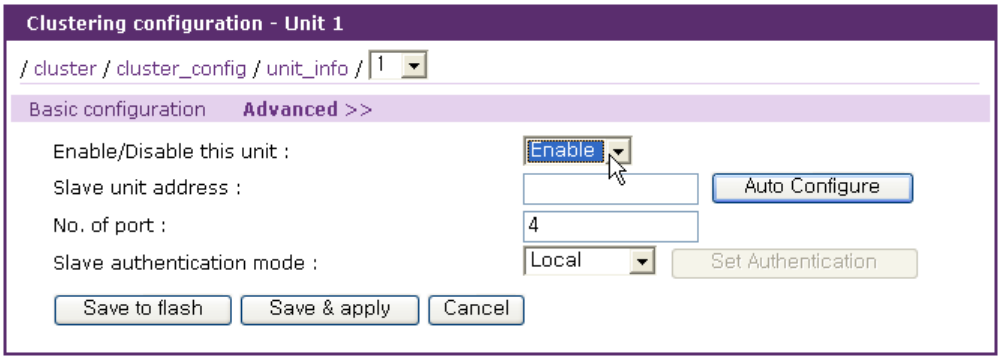


그림 5-7 Clustering Master / Slave 설정 – Enable 선택 후 Slave Unit 설정

사용자는 슬레이브 장치의 설정을 구성하기 위해 IP forwarding 테이블을 수동으로 구성할 수도 있고, 슬레이브 장치에 요청하여 설정을 Import하여 자동으로 구성할 수도 있습니다. 수동으로 슬레이브 장치의 정보를 구성하려면 **Advanced >>** 링크를 클릭하여 그림 5-8과 같은 슬레이브 장치 IP forwarding 테이블화면에서 설정하면 됩니다.

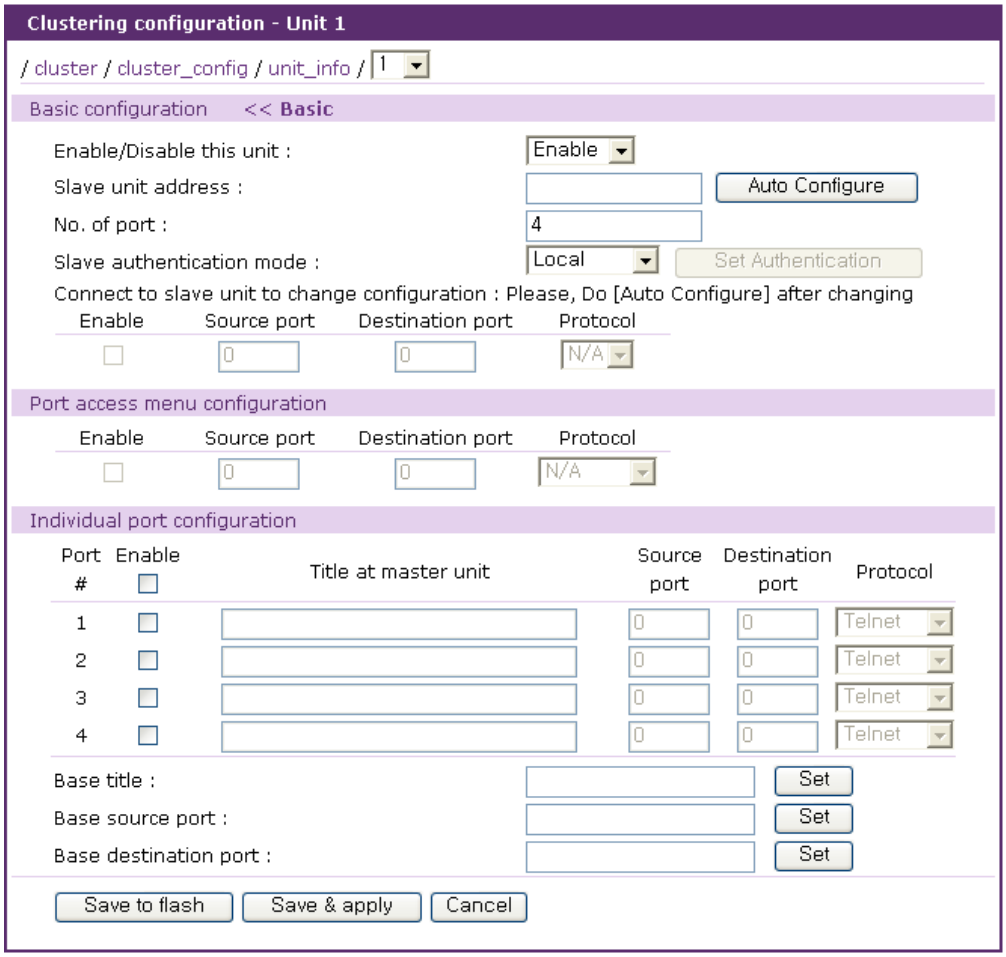


그림 5-8 Clustering Master / Slave 설정 – 슬레이브 장치 IP forwarding 테이블

슬레이브 장치 IP forwarding 테이블화면에는 **Port access menu**, 웹인터페이스를 위한 웹서비스 포트 및 시리얼 포트/원격 포트에 접속하기 위한 IP forwarding 테이블이 제공됩니다. Source port는 마스터 장치의 TCP 포트 번호이며, Destination Port는 Source port로 전송되는 데이터가 전달될 슬레이브 장치의 TCP 포트 번호입니다. 수동으로 슬레이브 장치의 정보를 설정할 경우 **Port access menu**와 웹서비스 포트는 설정할 수 없습니다.

IP forwarding 테이블을 자동으로 설정하려면 슬레이브 장치의 IP 주소 또는 도메인 이름을 입력한 다음 **[Auto Configure]** 버튼을 클릭합니다. 마스터 장치는 슬레이브 장치의 포트 정보를 자동으로 Import하고 그에 대한 마스터의 소스 포트 정보를 자동으로 설정합니다. 그림 5-9는 자동 설정이 성공했을 때 메시지를 나타내고 그림 5-10는 자동 설정 실행 후 결과를 보여줍니다. 자동 설정 프로세스가 실패한 경우, 오류 메시지가 나타납니다. 가장 일반적인 오류는 부정확한 IP 주소 입력 또는 네트워크 문제(예. 네트워크 설정이 끊긴 경우)입니다. 그림 5-11은 자동 설정이 실패했을 경우 나타나는 메시지를 보여줍니다.

마스터는 슬레이브 장치의 설정을 자동 설정으로 가져 오면 그 장치에서 Console server 모드로 설정된 포트만 자동으로 찾아서 해당되는 정보를 Import 하게 됩니다. 사용자는 Base title을 설정하여 슬레이브 장치의 포트 타이틀을 일괄적으로 설정할 수 있습니다. 하나의 Base port 번호를 설정하여 그에 따라서 Source port 번호 또는 Destination port 번호를 설정하도록 지정할 수도 있습니다. 웹 인터페이스는 슬레이브 장치를 설정하는 웹 인터페이스로 연결되는 링크를 제공합니다. **Connect to slave unit to change configuration** 부분의 **Protocol**을 설정함으로써, 슬레이브 장치를 설정하는 웹 인터페이스로 연결할 때 사용할 프로토콜을 선택할 수 있습니다.

참고: *Source port 번호는 마스터 장치 포트의 기존 설정과 충돌되도록 설정하지 말아야 합니다. 충돌되는 경우, Clustering 기능이 비활성 상태가 됩니다.*

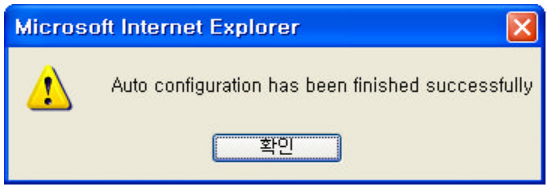


그림 5-9 Clustering Master / Slave 설정 – 자동 설정 성공 메시지

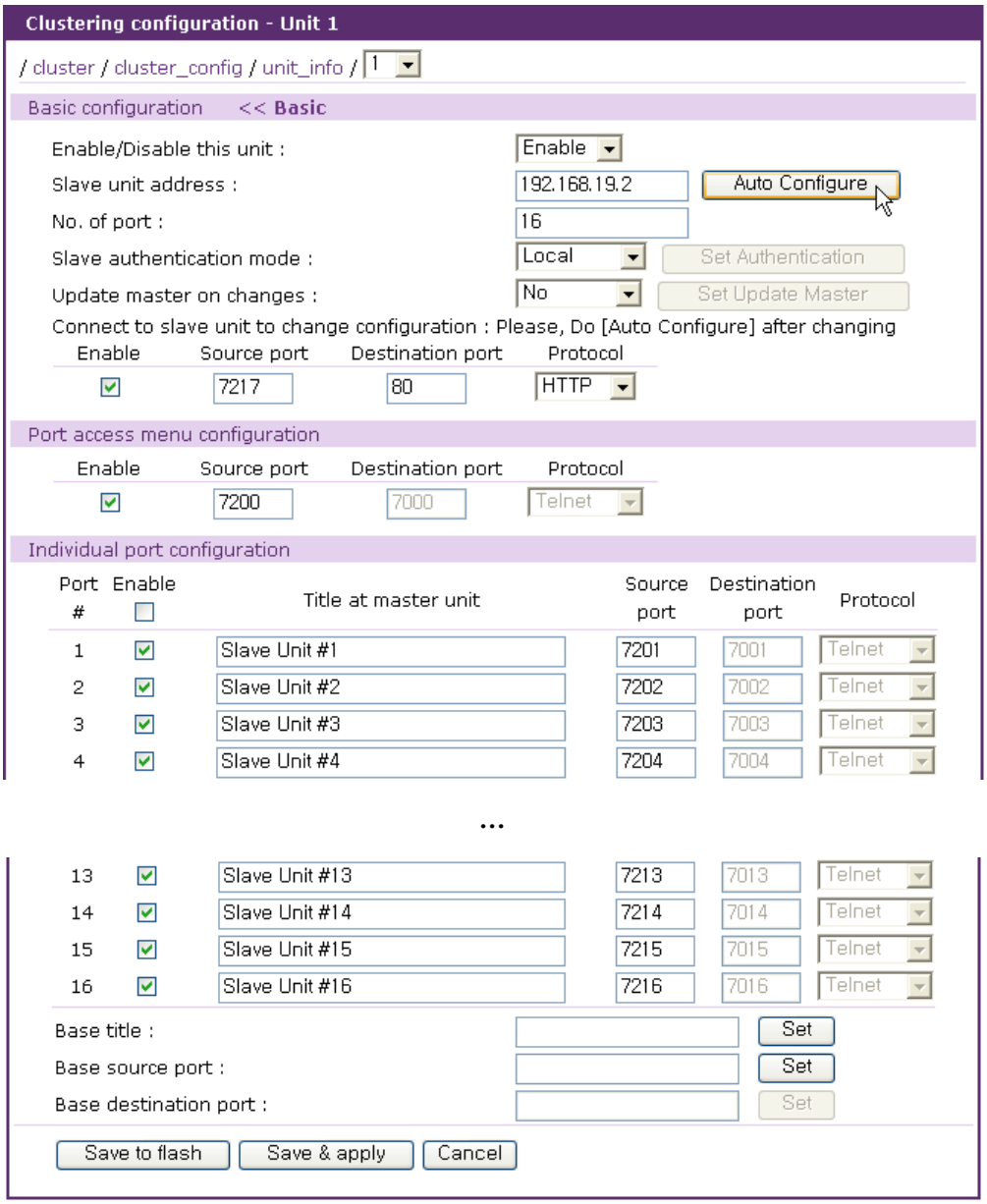


그림 5-10 Clustering Master / Slave 설정 – 자동 설정 후

그림 5-11 Clustering Master / Slave 설정 – 자동 설정 오류 메시지

자동 설정 프로세스가 성공하면 슬레이브 장치의 포트 정보가 정확하게 설정되었는지 확인하십시오. 그런 다음 슬레이브 장치에 대한 Clustering 설정을 완료하기 위해 **[Save & apply]** 버튼을 클릭하여 설정을 저장하고 적용하십시오. 그림 5-12는 Clustering 설정을 저장하고 적용한 결과를 보여줍니다.

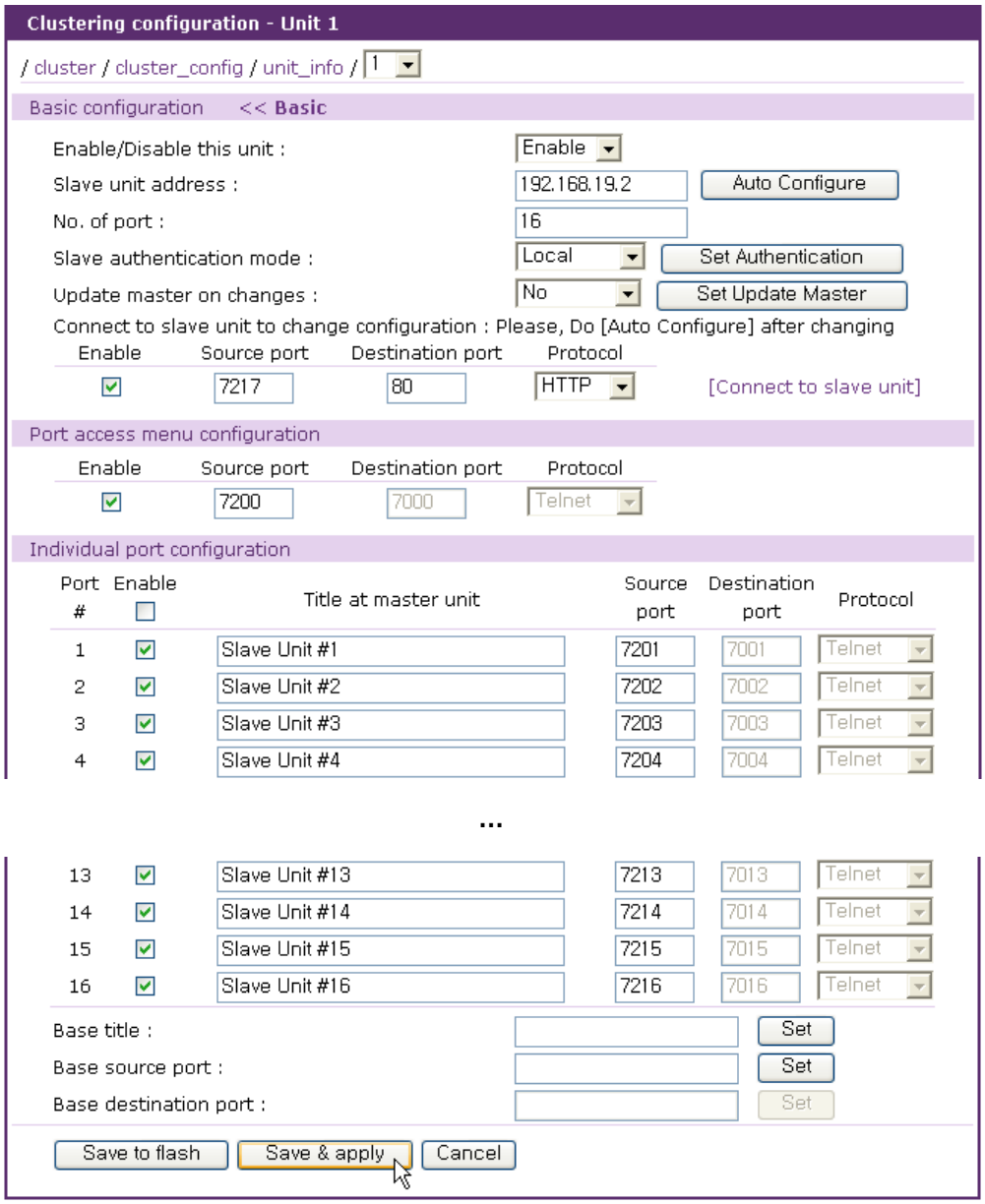


그림 5-12 Clustering Master / Slave 설정 – 자동 설정 Save & apply 후

Slave authentication mode를 선택하고 **[Set Authentication]** 버튼을 클릭함으로써, 사용자는 슬레이브 장치의 clustering authentication mode를 변경할 수 있습니다. **Update master on changes**를 선택하고 **[Set Update Master]** 버튼을 클릭하면 슬레이브 장치의 **Update master on changes**를 변경할 수 있습니다. **[Connect to slave unit]** 라는 링크를 클릭하면 사용자는 슬레이브 장치의 설정을 변경할 수 있는 슬레이브 장치의 웹 인터페이스로 이동할 수 있습니다. 슬레이브 장치의 설정을 변경한 후 사용자는 **[Auto Configure]** 버튼을 클릭하여 슬레이브 장치의 변경된 설정을 마스터 장치의 Clustering 설정에 반영해야 합니다. 그러나, **Update master on changes**가 **Yes**로 설정되어 있으면 슬레이브 장치의 설정을 변경하고 적용하면 마스터 장치에 자동으로 반영됩니다.

5.3 Clustering Peer-to-peer 설정

웹 인터페이스의 **Clustering > Peer to peer configuration**을 메뉴를 선택하면 그림 5-13와 같은 **Peer to peer mode configuration** 화면이 나타납니다.

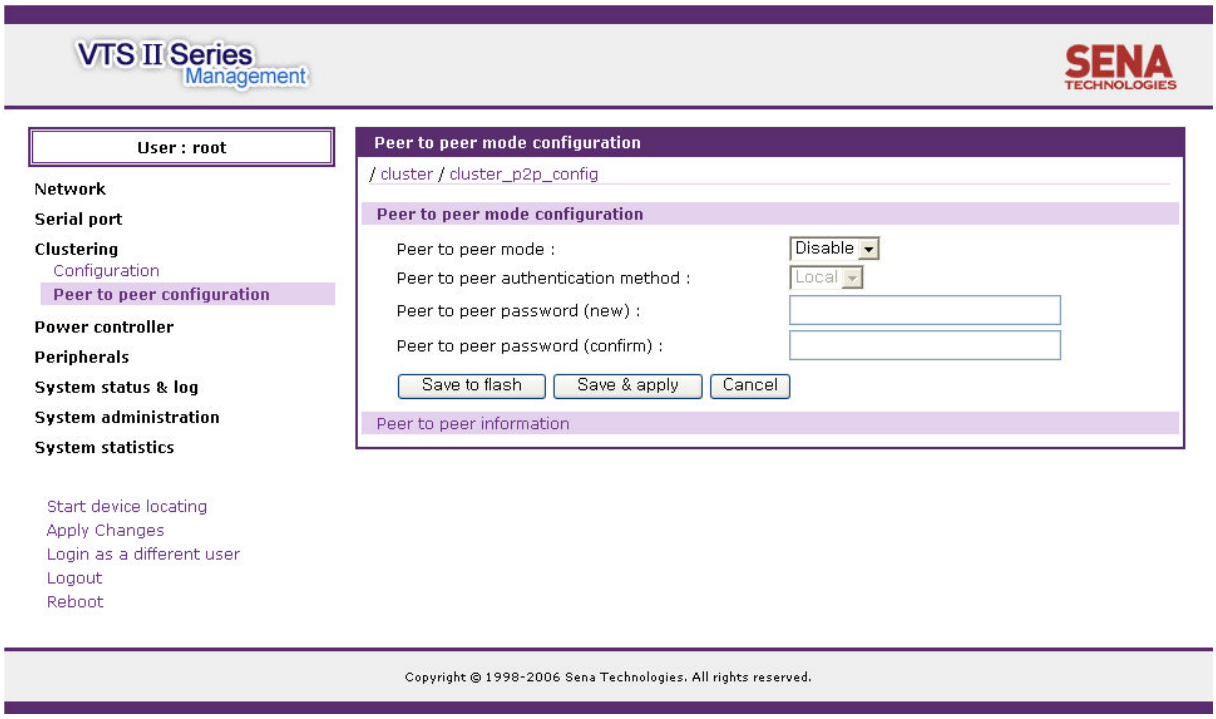


그림 5-13 Clustering Peer topeer mode configuration으로 이동

Peer to peer mode 파라미터는 이 장치가 Peer to peer mode를 사용할 지 여부를 결정합니다. Peer to peer mode가 Enable로 선택된 경우 다음 파라미터들을 설정할 수 있습니다. **Peer to peer authentication method**는 다른 Peer에서 이 장치의 Authentication이 Local로 설정된 포터로 연결하려고 할 때, 어디서 인증을 할 것인지를 결정합니다. **Local**로 설정된 경우에는 이 장치의 로컬 인증 절차를 따릅니다. Peer로 설정된 경우에는 다른 Peer에서 인증 절차를 따르게 됩니다. **Peer to peer password**는 모든 Peer들이 최신 정보로 갱신하기 위해 데이터를 주고 받을 때 클러스터링의 Peer로써의 자격이 있는지 여부를 판단하는데 사용됩니다. 패스워드가 다른 Peer가 Peer 정보를 요청하거나 갱신하려고 하면 클러스터링내의 Peer들은 이 작업을 무시합니다.

Peer to peer information 링크를 선택하면 그림 5-14과 같은 Clustering peer to peer information 화면이 나타납니다.

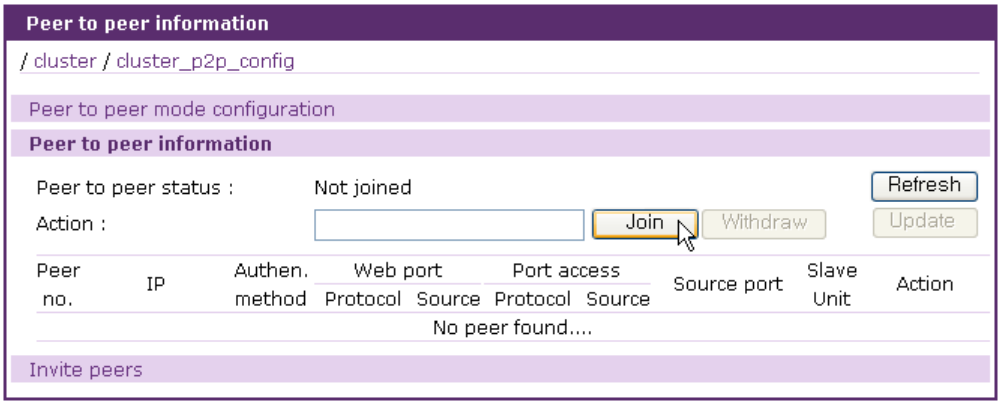


그림 5-14 Clustering peer to peer information

Peer to peer status는 Clustering peer to peer의 현재 상태를 표시합니다. 표시 가능한 상태는 다음과 같습니다.

- Not ready : Peer to peer mode가 Enable되지 않았거나 적용되지 않은 상태
- Not joined : 아직 Join하지 않은 상태
- Joining : Join을 시도하는 상태
- Joined : Join 작업이 완료된 상태
- Changing peers : Peer to peer 그룹내의 Peer들의 정보를 갱신하고 있는 상태
- Withdrawing : Peer to peer 그룹의 탈퇴가 진행 중인 상태
- Withdrawn : Peer to peer 그룹을 탈퇴한 상태

사용자는 **[Refresh]** 버튼을 클릭하여 현재 페이지를 최신 정보로 갱신할 수 있습니다. 참가하려는 Peer to peer 그룹에 속한 Peer의 주소를 입력하고 **[Join]** 버튼을 클릭하면 Peer to peer 그룹에 참여할 수 있습니다. 이 때 Peer의 주소에 입력할 Peer의 Peer to peer mode가 Enable로 설정되지 않았거나 적용되지 않은 상태이거나, Peer to peer 그룹의 Peer들과 패스워드가 일치하지 않으면 Peer로 참가할 수 없습니다. 입력한 주소를 가진 Peer가 Peer to peer 그룹에 참가할 준비는 되어 있으나 아직 Peer to peer 그룹에 참가하지 않은 상태면 참가하려는 Peer와 함께 새로운 Peer to peer 그룹을 형성합니다. 그림 5-15는 다른 Peer to peer 그룹으로 Join하려는 화면입니다.

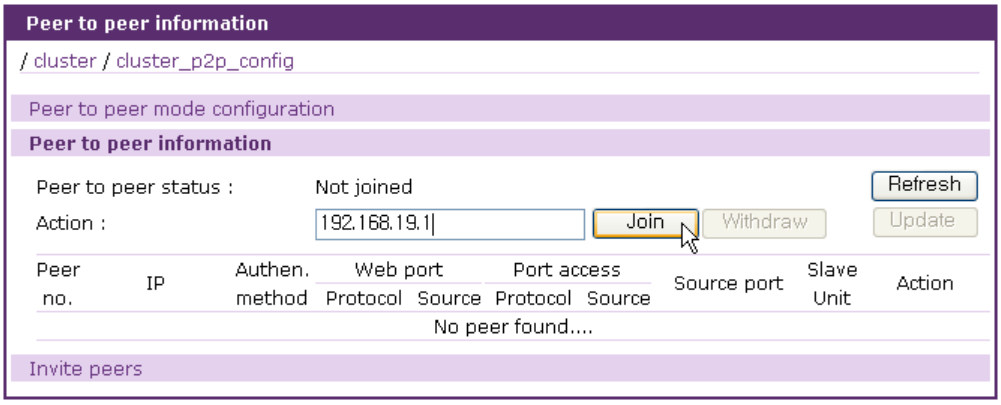


그림 5-15 Clustering Peer-to-peer - Join

그림 5-16는 Join 완료 후 Join하려던 Peer의 Peer to peer information 화면입니다.

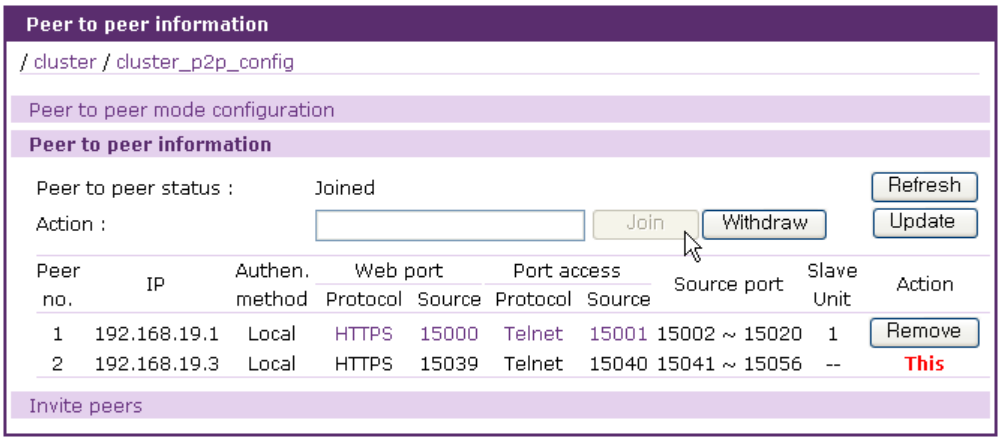


그림 5-16 Clustering Peer-to-peer – Join 완료 후 화면

그림 5-17은 Join 대상인 Peer의 화면입니다.

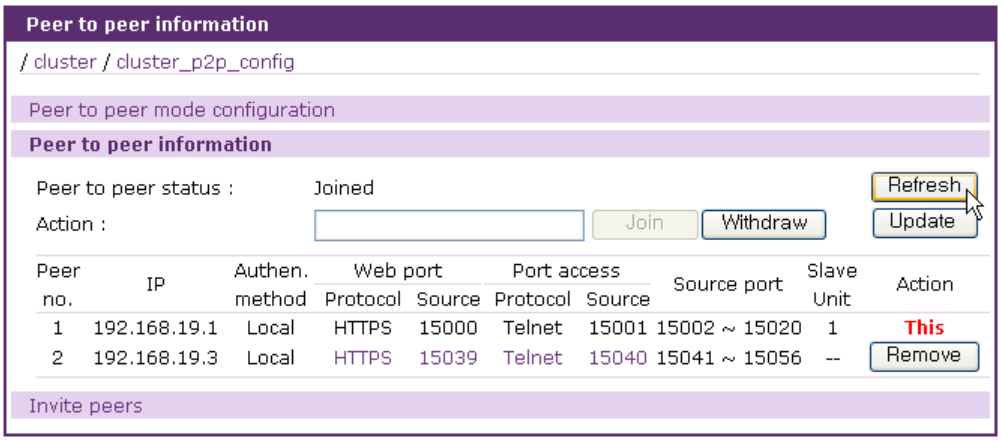


그림 5-17 Clustering Peer-to-peer – Join 완료 후 Join 대상 peer의 화면

Peer to peer 그룹에 속한 Peer들의 리스트에는 Peer 번호, Peer 주소, Peer to peer authentication method, 웹 인터페이스 정보와 링크, Port access menu 정보와 링크, 시리얼포트와 원격포트의 Source Port 범위 및 Slave 장치 개수등이 표시됩니다. 웹 인터페이스 링크를 클릭하면 해당 Peer의 웹 인터페이스로 이동하여 해당 Peer의 설정을 변경할 수 있습니다. Port access menu 링크를 클릭하여 해당 Peer의 Port access menu로 접속할 수 있습니다.

Join이 Peer to peer 그룹에 참여하기 위한 수단이라면, 다른 호스트들을 이 호스트가 속한 Peer to peer 그룹으로 참여하도록 요청하는 수단이 Invite입니다. Peer to peer information 화면에서 **Invite peers** 링크를 선택한 후 참여를 요청할 Peer들의 주소를 입력한 후 **[Invite]** 버튼을 클릭합니다. Invite를 이용하여 한 번에 최대 10개의 호스트에게 Join을 요청할 수 있으므로 사용자는 Peer to peer 그룹을 쉽게 구성할 수 있습니다. 그림 5-18은 다른 호스트를 Invite하는 화면을 보여줍니다.

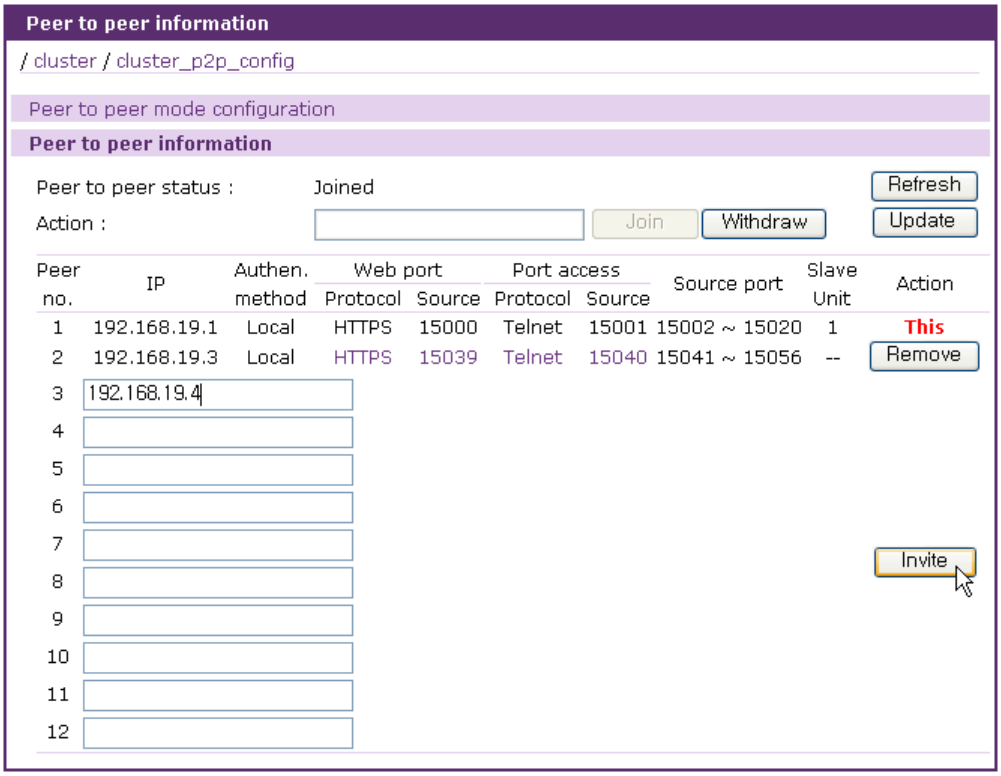


그림 5-18 Clustering Peer-to-peer – Invite

그림 5-19은 Invite 완료 후 화면을 보여줍니다.

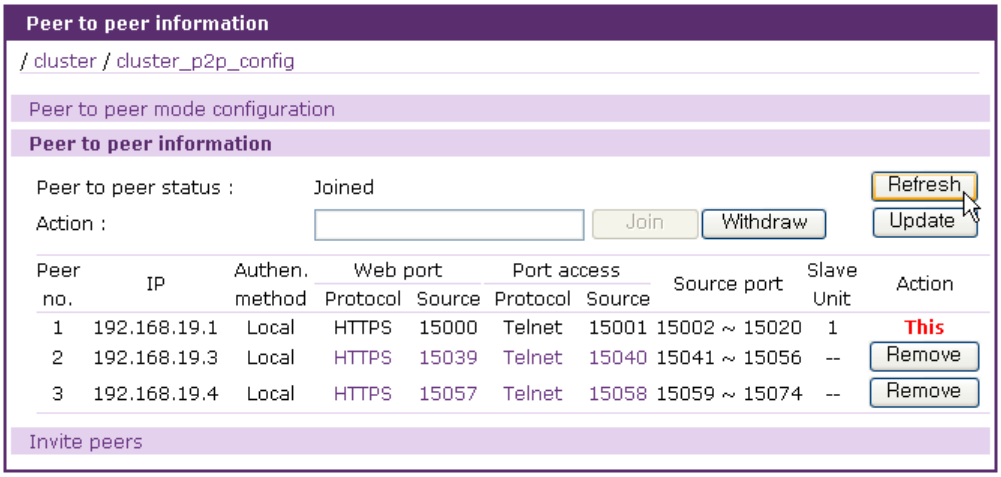


그림 5-19 Clustering Peer-to-peer – Invite 완료 후

Peer to peer 그룹에 참가한 Peer가 그룹을 탈퇴하려면 **[Withdraw]** 버튼을 클릭하면 됩니다. **[Remove]** 버튼은 Peer 리스트에서 Peer를 제거하기 위해 사용됩니다. **[Update]** 버튼을 클릭하면 Peer 리스트의 Peer들 중에서 응답이 없었던 Peer들의 정보를 요청하여 갱신합니다.

5.4 Clustering 연결

모든 시리얼 포트/원격 포트, Clustering Master / Slave의 Slave 장치의 포트, Clustering Peer-to-peer에서 Peer의 포트는 Serial port 연결페이지에 표시됩니다.

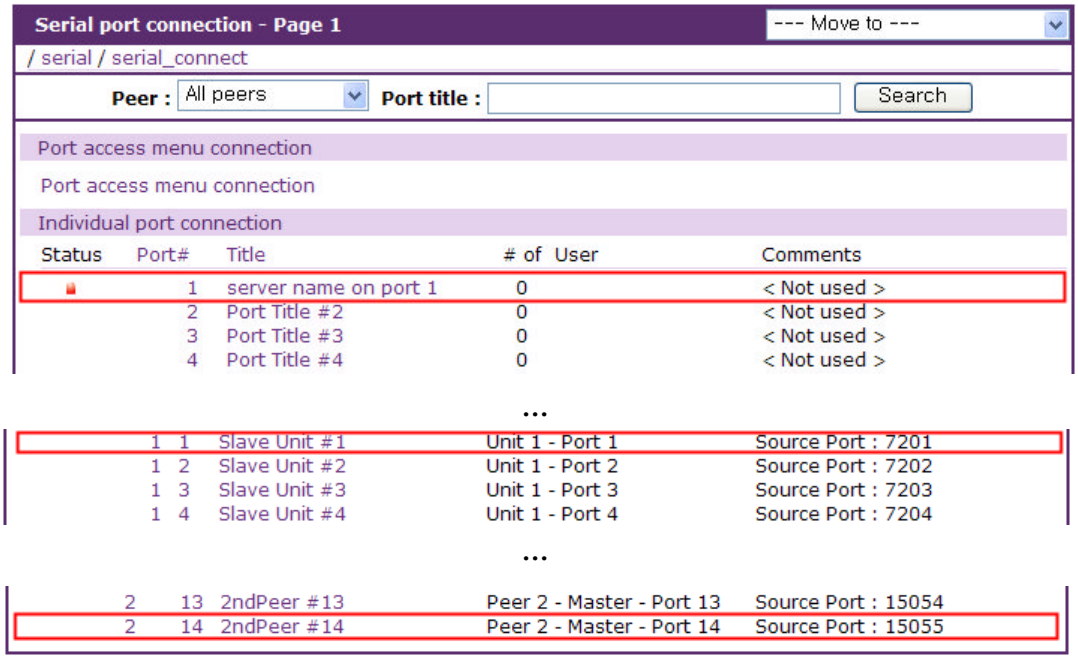
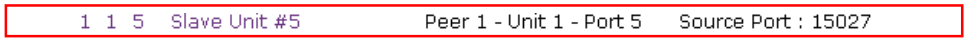


그림 5-20 Serial port 연결페이지 – Clustering Master / Slave 와 Clustering Peer –to-peer

그림 5-20는 Clustering Master / Slave의 Slave 장치와 Clustering Peer-to-peer의 Peer 정보를 포함한 장치의 Serial port 연결페이지를 보여줍니다. 포트 번호는 Peer 번호, Slave 장치의 유닛 번호와 Port 번호로 구성됩니다. 그림 5-20에서 첫 번째 사각형의 포트 번호는 해당 포트가 이 장치의 시리얼 포트/원격 포트임을 표시합니다. (예: 이 장치의 1번 포트). 두 번째 사각형의 포트 번호는 해당 포트가 Clustering Slave 장치의 시리얼 포트/원격 포트임을 나타냅니다. (예: Slave 1번 장치의 1번 포트). 세 번째 사각형의 포트 번호처럼 Peer 번호와 Port 번호만 있고 Slave 장치의 유닛 번호가 없는 경우에는 이 포트가 다른 Peer의 마스터 장치의 시리얼 포트/원격 포트임을 보여줍니다. (예: Peer 2번 장치의 마스트 장치의 14번 포트).



위와 같은 형식의 포트 번호는 다른 Peer의 슬레이브 장치의 포트임을 표시합니다. (예: Peer 1번 장치의 Slave 1번 장치의 5번 포트)

Serial port 연결페이지를 통한 클러스터링 포트의 연결, 웹 인터페이스를 통한 클러스터링 포트의 직접 연결, SSH 원격 시리얼 콘솔을 통한 클러스터링 포트의 연결등은 ***4.7 Serial port 연결***을 참조하시기 바랍니다. Port access menu로 통해 Clustering이 설정된 장치로 접근하는 방법은 ***4.2.5 Clustering 시의 port access menu***를 참조하시기 바랍니다.

6: Power Controller

6.1 개요

SENA PM 시리즈, Baytech RPC 시리즈, Servertech 시리즈 같은 파워 컨트롤러를 VTS II에 추가하고 설정하고 제어할 수 있습니다. 사용자가 VTS II에 파워 컨트롤러를 추가하고 VTS II의 시리얼 포트에 연결된 장치를 파워 컨트롤러의 아웃렛에 꽂고 난 후 파워 컨트롤러 설정(**power controller configuration**) 화면이나 시리얼 포트 설정의 **power control configuration** 화면에서 그것을 설정할 수 있습니다. power control configuration에 대한 자세한 내용은 ***4.5.13 Power control 설정*** 부분을 참조하십시오. 사용자는 파워 컨트롤러 관리 (**power controller management**) 화면이나 시리얼 포트 연결 화면에서 이동할 수 있는 **serial port power control** 화면에서 제어할 수 있습니다.
VTS II의 파워 컨트롤러 기능의 특징은 사용자가 VTS II 시리얼 포트에 연결된 장치의 전원 관리를 용이하게 하는 것입니다. 사용자는 장치를 켜고 꺼고 재부팅할 수 있을 뿐만 아니라 파워 컨트롤러의 상태를 감시할 수도 있습니다. 설정 또는 감시 항목은 파워 컨트롤러의 종류에 따라 달라집니다.

지원되는 파워 컨트롤러는 다음과 같습니다.

- SENA PM 시리즈
- Baytech RPC 시리즈
- Servertech 시리즈

6.2 파워 컨트롤러 설정

사용자는 파워 컨트롤러를 VTS II에 추가 / 제거하고, 파워 컨트롤러의 아웃렛 수, 이름과 경보 기능을 설정하고 아웃렛을 특정 장치나 VTS II 시리얼 포트에 연결된 서버로 연결합니다. 사용자는 또한 시리얼 포트 설정의 power control configuration 화면에서도 파워 컨트롤러의 아웃렛을 VTS II 시리얼 포트와 연결되었다는 설정할 수 있습니다.

6.2.1 power controller 추가 / 제거

메뉴바에서 **Power controller > Configuration** 메뉴항목을 선택하면 파워 컨트롤러 설정(**power controller configuration**)화면이 표시됩니다. (그림 6-1 파워 컨트롤러 설정 참조). **Add power controller** 부분에서 파워 컨트롤러가 연결되어 있는 포트와 파워 컨트롤러 제조사를 선택하고 SENA PM의 경우에는 병렬연결된 유닛의 총수를 선택한 후 **[Add controller]** 버튼을 클릭하면

파워 컨트롤러가 추가됩니다. 파워 컨트롤러가 추가되면 파워 컨트롤러 유닛 설정 화면이 표시되고 사용자는 여기서 추가된 파워 컨트롤러의 정보를 설정할 수 있습니다.
사용자는 **Power controllers** 부분에 있는 **[Remove]** 버튼을 클릭하여 파워 컨트롤러를 제가할 수 있습니다.

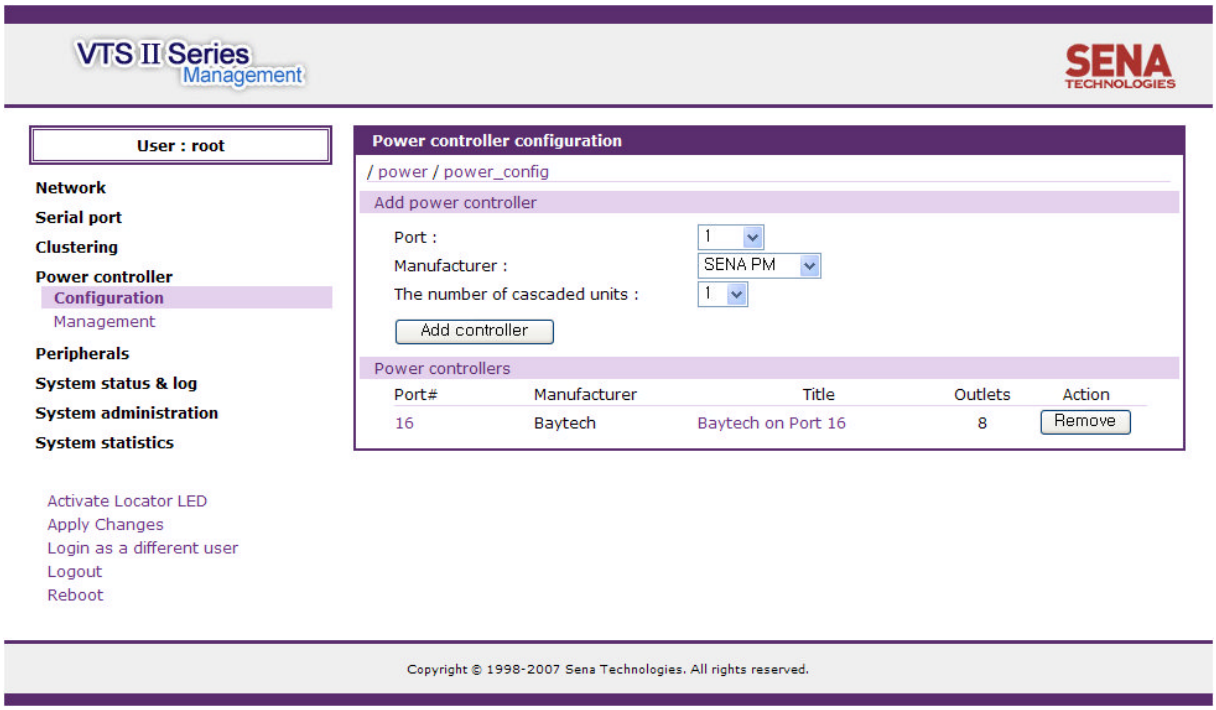


그림 6-1 파워 컨트롤러 설정

VTS II는 SNMP를 지원하는 Power controller를 지원합니다. 사용자는 기존의 원격 포트를 이용하거나 새로운 원격 포트를 생성하여 Power controller를 설정할 수 있습니다. 이때 사용자는 그림 6-2과 같이 Power controller에 접속하기 위한 정보(Power controller의 IP address, SNMP 포트, GET/SET Community, SNMP 버전)를 설정합니다. 새로운 원격 포트를 생성하는 경우, 원격 포트의 TCP port를 의미하는 **Listening TCP port** 설정하여야 합니다.

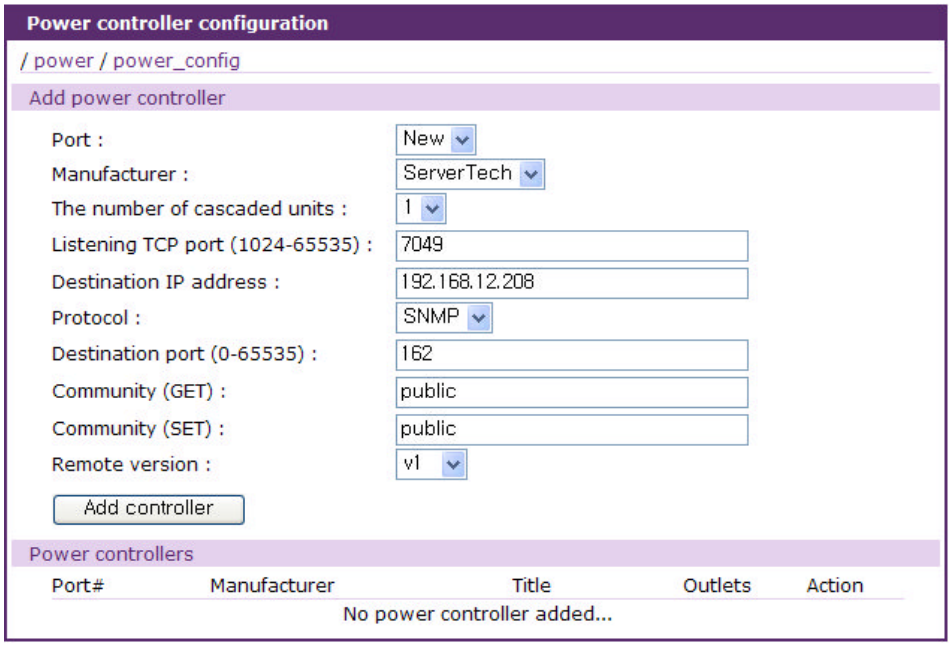


그림 6-2 Remote 파워 콘트롤러 설정

6.2.2 파워 컨트롤러 유닛 설정 – Power controller 탭

파워 컨트롤러가 추가되거나 파워 컨트롤러 설정 화면(그림 6-1 파워 컨트롤러 설정 참조)에서 Power controllers 부분의 파워 컨트롤러 리스트에 있는 파워 컨트롤러가 선택되면, 파워 컨트롤러 설정의 Power controller 탭(그림 6-3 파워 컨트롤러 유닛 설정 – power controller 탭 참조) 화면이 표시됩니다.

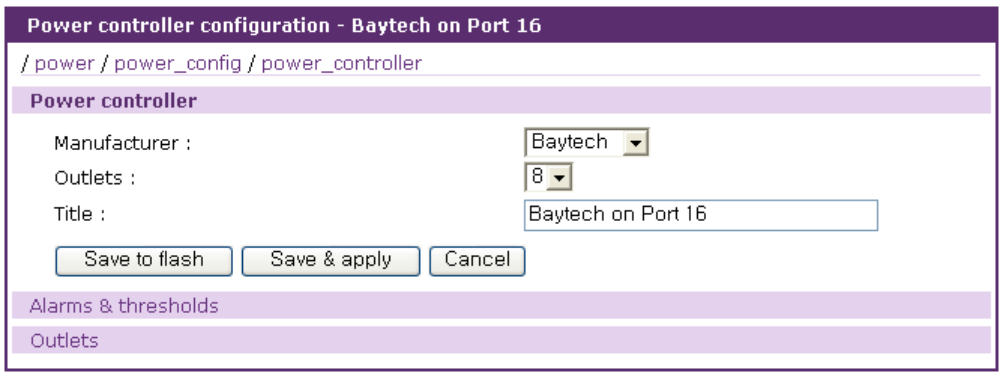


그림 6-3 파워 컨트롤러 유닛 설정 – power controller 탭

사용자는 여기서 파워 컨트롤러의 제조사, 아웃렛 수와 이름을 설정할 수 있습니다. 두개 이상의 파워 컨트롤러가 추가 되었다면, 사용자는 이 파워 컨트롤러 이름으로 각각의 파워 컨트롤러를 구별할 수 있게 되고, 파워 컨트롤러를 설정하거나 관리할 때 쉽게 원하는 파워 컨트롤러에 접근할 수 있게 됩니다.

6.2.3 파워 컨트롤러 유닛 설정 – Alarms & thresholds 탭

파워 컨트롤러 설정 화면(그림 6-1 파워 컨트롤러 설정 참조)에서 Power controllers 부분의 파워 컨트롤러 리스트에서 파워 컨트롤러를 선택한 후 파워 컨트롤러 유닛 설정 화면에서 **Alarms & thresholds** 탭을 선택하면 파워 컨트롤러의 경보기능 설정 화면 (그림 6-4 파워 컨트롤러 유닛 설정 – alarms & thresholds 탭 참조)이 표시됩니다. 여기서 설정하는 항목들은 파워 컨트롤러의 종류에 따라 달라질 수 있습니다.

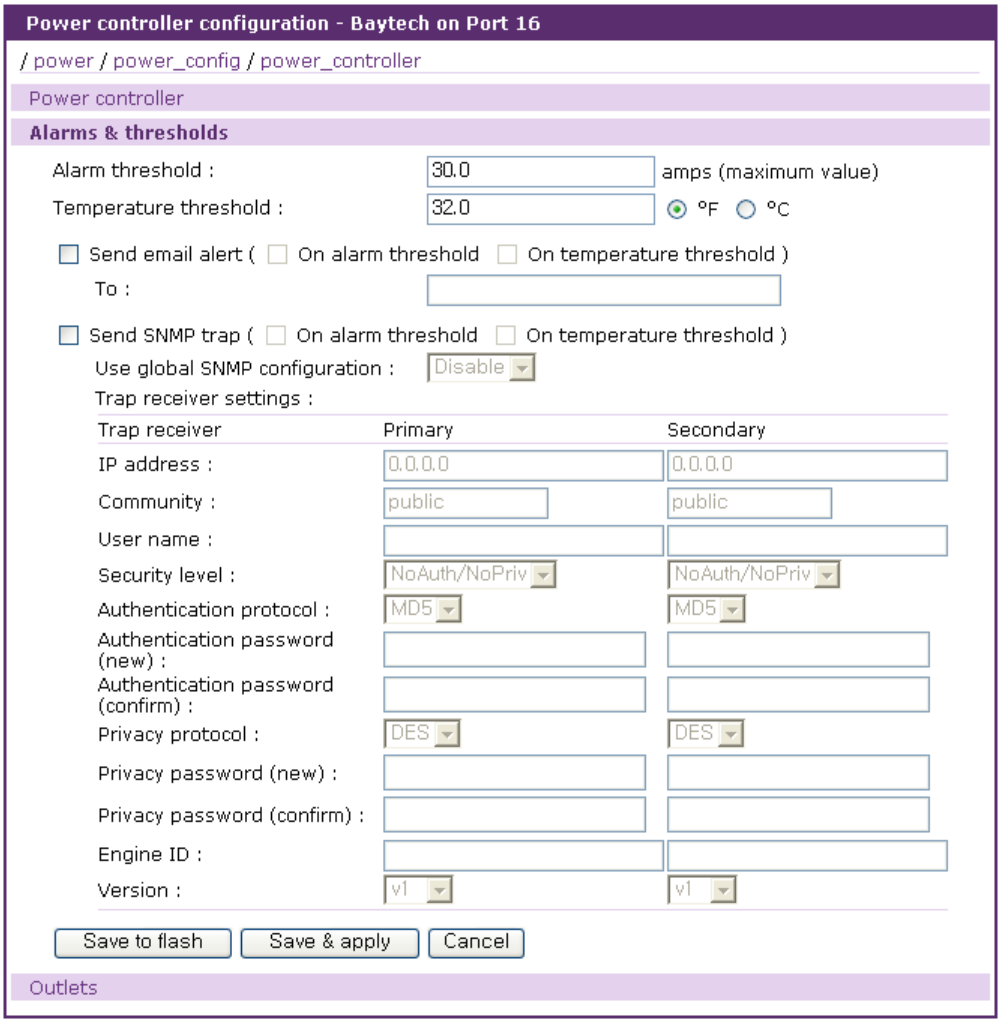


그림 6-4 파워 컨트롤러 유닛 설정 – alarms & thresholds 탭

파워 컨트롤러 경보 기능 설정을 위한 파라미터는 다음과 같습니다:

Alarm threshold

Temperature threshold

Send email alert

Send SNMP trap

Alarm threshold

이 파라미터의 값을 초과하는 전류가 파워 컨트롤러에서 감지될 때 경보를 발생합니다. 이 경보값에 도달하게 되면 Send email alert와 Send SNMP trap 부분에 설정된 정보에 따라 이메일 경보나 SNMP 트랩이 전달됩니다.

Temperature threshold

파워 컨트롤러 내부의 온도가 이 파라미터의 값을 초과할 때 경보가 발생합니다. 이 경보값에 도달하게 되면 Send email alert와 Send SNMP trap 부분에 설정된 정보에 따라 이메일 경보나 SNMP 트랩이 전달됩니다.

Send email alert

Send email alert : 경보 발생시 이메일을 보낼지 여부를 설정합니다.

On alarm threshold : 파워 컨트롤러의 전류가 alarm threshold 값에 도달했을 때 이메일을 전송할 지 여부를 설정합니다.

On temperature threshold : 파워 컨트롤러 내부 온도가 temperature threshold 값에 도달했을 때 이메일을 전송할 지 여부를 설정합니다.

To : 이메일을 받을 주소를 설정합니다.

Send SNMP trap

Send SNMP trap : 경보 발생시 SNMP 트랩을 발생시킬지 여부를 설정합니다.

On alarm threshold : 파워 컨트롤러의 전류가 alarm threshold 값에 도달했을 때 SNMP 트랩을 발생시킬 지 여부를 설정합니다.

On temperature threshold : 파워 컨트롤러 내부 온도가 temperature threshold 값에 도달했을 때 SNMP 트랩을 발생시킬 지 여부를 설정합니다.

Use global SNMP configuration : 네트워크 설정의 SNMP 설정에서 명시된 트랩수신기를 사용할 지 여부를 설정합니다.

Trap receiver settings : SNMP 트랩 설정에 필요한 각 항목들에 대한 설명은 ***3.2 SNMP 설정***을 참고하십시오.

6.2.4 파워 컨트롤러 유닛 설정 – Outlets 탭

파워 컨트롤러 설정 화면(그림 6-1 파워 컨트롤러 설정 참조)에서 Power controllers 부분의 파워 컨트롤러 리스트에서 파워 컨트롤러를 선택한 후 파워 컨트롤러 유닛 설정 화면에서 Outlets 탭을 선택하면 파워 컨트롤러의 아웃렛 설정 화면 (그림 6-5 파워 컨트롤러 유닛 설정 - outlets 탭 참조)이 표시됩니다.

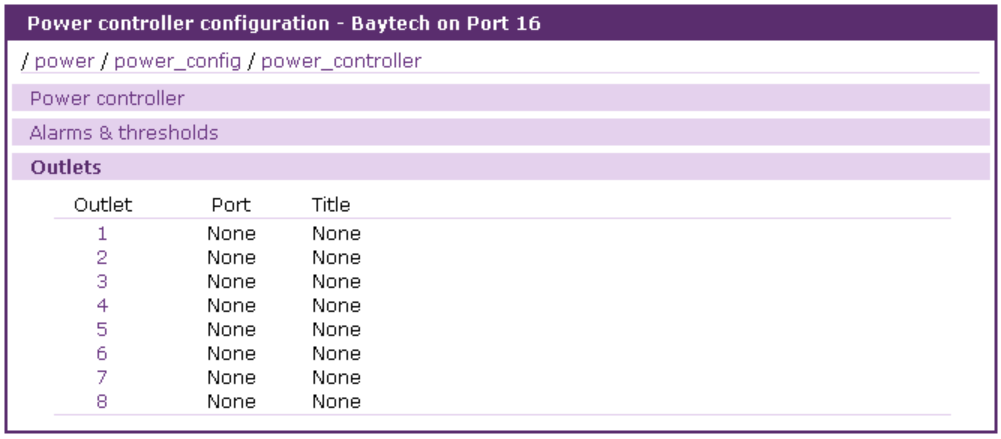


그림 6-5 파워 컨트롤러 유닛 설정 - outlets 탭

사용자는 아웃렛 번호를 클릭하여 아웃렛 설정 부분을 펼칠 수도 있고, 펼쳐진 아웃렛의 번호를 클릭하여 아웃렛 설정 부분을 다시 접을 수도 있습니다. 그림 6-6는 펼쳐진 아웃렛 설정 부분을 표시합니다.

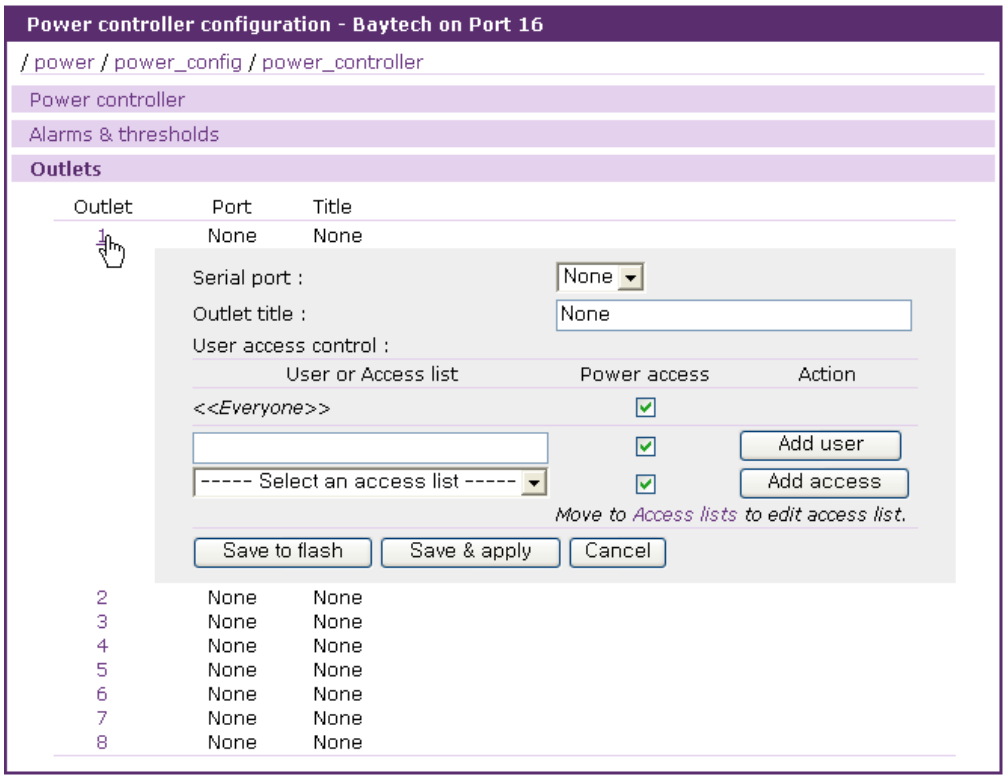


그림 6-6 파워 컨트롤러 유닛 설정 - 아웃렛 설정

아웃렛 설정을 위한 파라미터는 다음과 같습니다:

Serial port

Outlet title

User access control

Serial port

VTS II의 시리얼 포트에 연결된 장비에 전원을 제공하는 파워 컨트롤러의 아웃렛을 표시합니다. None은 이 아웃렛이 VTS II 시리얼 포트에 연결된 장비가 아닌 다른 장비에 연결되었다는 것을 의미합니다. VTS II의 시리얼 포트 번호가 설정되었다면, **Outlet title**은 시리얼 포트 설정의 포트 타이틀 값으로 설정되고, Power 사용자 접근권한(**User access control**)은 시리얼 포트 설정의 사용자 접근권한 설정(User access control 설정)으로 대치 되고 이 설정들은 편집할 수 없게 됩니다. (그림 6-7 파워 컨트롤러 유닛 설정 – 시리얼 포트에 연결된 아웃렛 설정 참조)

Outlet title

이 파라미터는 아웃렛을 묘사하는 이름입니다. 사용자가 아웃렛을 설정하거나 관리할 때, 이 항목은 사용자들이 아웃렛을 구분할 수 있도록 합니다. **Serial port** 항목이 시리얼 포트 번호로 설정되면 이 항목은 편집 불가능하게 되고, 시리얼 포트의 타이틀로 설정되고 시리얼 포트 설정의 Port title 설정화면으로 이동할 수 있는 연결이 제공됩니다. (그림 6-7 파워 컨트롤러 유닛 설정 – 시리얼 포트에 연결된 아웃렛 설정 참조)

User access control

사용자가 이 아웃렛에 접근권한이 있는지 여부를 설정합니다. 사용자가 Power 접근권한을 가지면 사용자는 시리얼 포트 연결 화면(***6.3.4 파워 컨트롤러 유닛 관리 – 시리얼 포트 연결*** 참조)에서 전원 상태를 감시할 수 있고, 파워 컨트롤러 유닛 관리 화면(***6.3.3 파워 컨트롤러 유닛 관리 – Outlets 탭*** 참조) 또는 시리얼 포트 연결 화면의 작업리스트의 Power Control 아이콘에서 연결되는 serial port power control 화면(***6.3.5 파원 컨트롤러 유닛 관리 – Serial port power control*** 참조)에서 파워 컨트롤러 아웃렛을 제어할 수 있습니다.

<<Everyone>> 접근권한이 체크되면, User access control 부분의 사용자 리스트나 Access list에 등록된 사용자를 제외한 모든 사용자는 Power 접근권한을 갖게 되고, 반대의 경우에는 접근권한을 갖지 않게 됩니다.

Serial port 항목이 시리얼 포트 번호로 설정되면 이 항목은 편집이 불가능하게 되고, 시리얼 포트 설정의 User access control 설정의 Power 접근권한의 설정으로 대체됩니다. 시리얼 포트 설정의 User access control 설정으로 이동할 수 있는 링크가 제공됩니다. (그림 6-7 파워 컨트롤러 유닛 설정 – 시리얼 포트에 연결된 아웃렛 설정 참조)

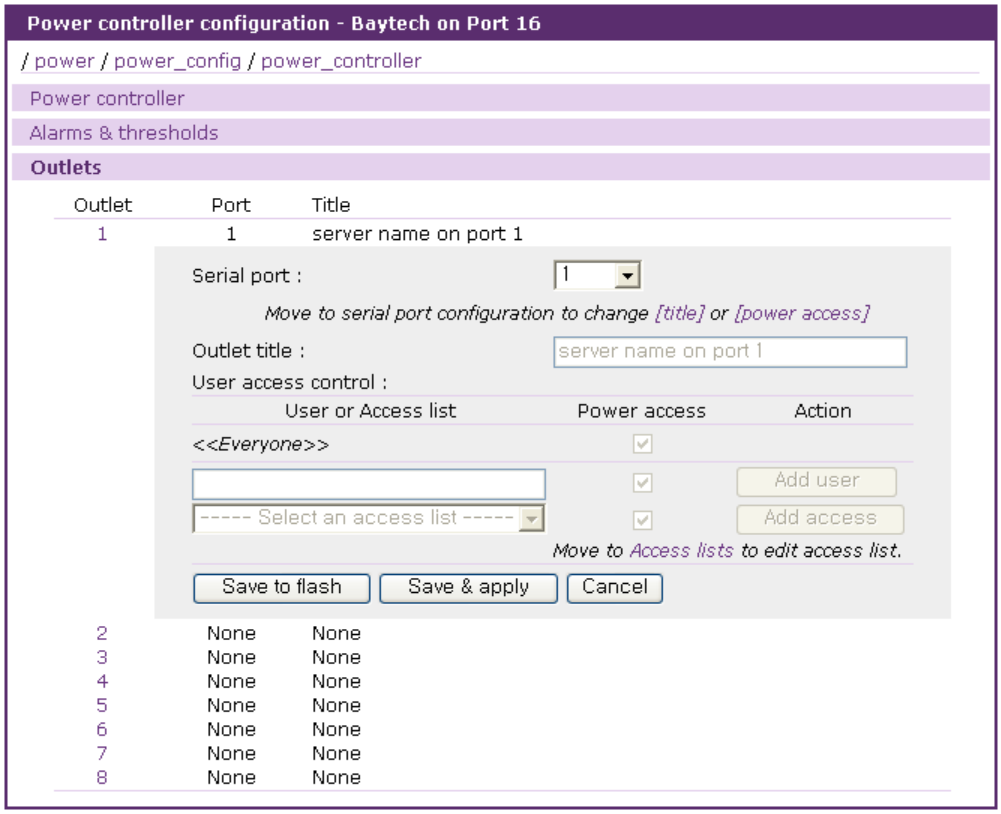


그림 6-7 파워 컨트롤러 유닛 설정 – 시리얼 포트에 연결된 아웃렛 설정

6.2.5 시리얼 포트 설정의 power control 설정 편집

Power control configuration 화면은 serial port 설정의 하나입니다. 파워 컨트롤러가 VTS II에 추가되면, 각 포트의 시리얼 포트 설정에는 Power control configuration 탭이 추가됩니다. (***4.5.13 Power control 설정*** 참조).

이 화면은 VTS II의 시리얼 포트에 연결된 장비를 파워 컨트롤러의 아웃렛과 연결할 수 있도록 도와줍니다. 반면 아웃렛 설정 화면은 파워 컨트롤러 아웃렛을 장비와 연결할 수 있도록 설정합니다. (***6.2.4 파워 컨트롤러 유닛 설정 – Outlets 탭*** 참조).

6.3 파워 컨트롤러 관리

사용자는 파워 컨트롤러와 아웃렛을 파워 컨트롤러 관리 화면, Serial port 연결 화면과 Serial port 연결 화면에서 연동되는 Serial port power control 화면에서 감시 / 관리합니다.

6.3.1 파워 컨트롤러 관리 – 파워 컨트롤러 리스트

메뉴바에서 **Power controller > Management** 메뉴항목을 선택하면, 파워 컨트롤러 관리 화면(그림 6-8 파워 컨트롤러 관리 – 파워 컨트롤러 리스트 참조)에 VTS II에 추가된 파워 컨트롤러 리스트

가 표시됩니다. 파워 컨트롤러가 연결된 VTS II의 시리얼 포트 번호, 제조사, 이름, 아웃렛 개수 등과 같은 파워 컨트롤러의 정보가 나타나고, 파워 컨트롤러의 상태도 표시됩니다. 파워 컨트롤러의 상태가 Connected 이면, 파워 컨트롤러의 시리얼 포트 번호나 이름을 선택하여 파워 컨트롤러 유닛의 관리 화면으로 이동할 수 있습니다.

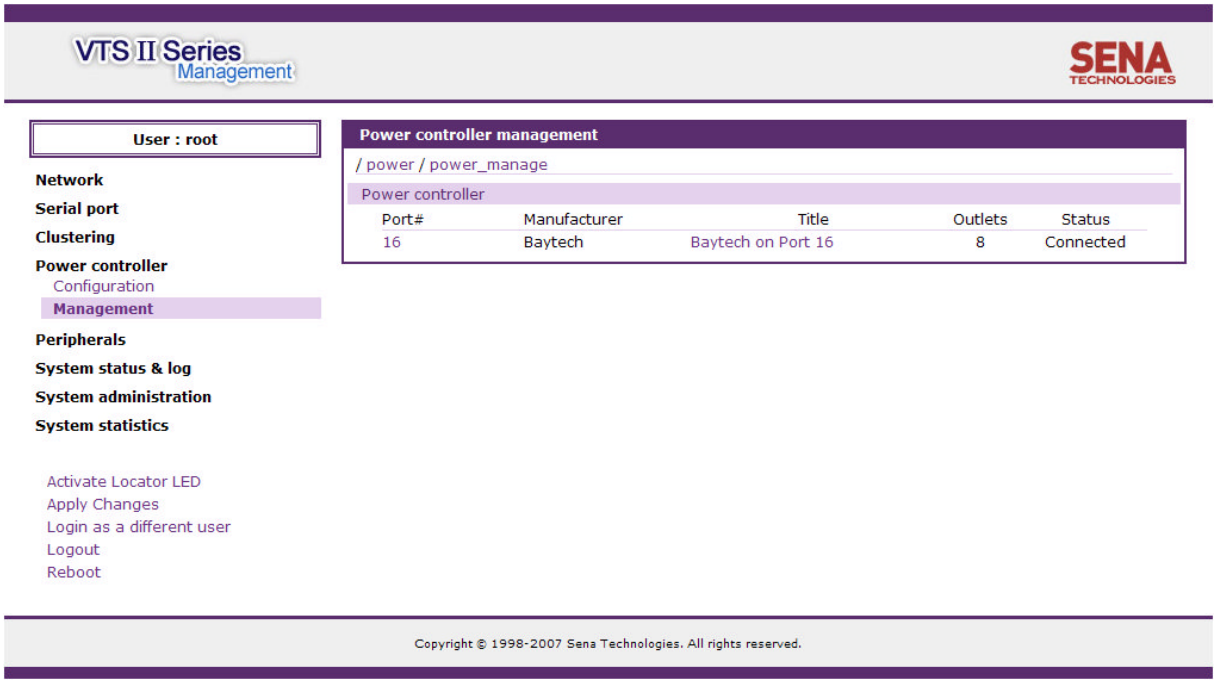


그림 6-8 파워 컨트롤러 관리 – 파워 컨트롤러 리스트

6.3.2 파워 컨트롤러 유닛 관리 – Power controller 탭

파워 컨트롤러 관리 화면(그림 6-8 파워 컨트롤러 관리 – 파워 컨트롤러 리스트 참조)의 파워 컨트롤러 리스트에서 파워 컨트롤러를 선택하여 파워 컨트롤러 관리의 파워 컨트롤러 탭화면 (그림 6-9 파워 컨트롤러 유닛 관리 – power controller 탭 참조)을 열 수 있습니다. 이 화면은 Serial port 연결 화면의 작업리스트에 있는 Power Controller Management 아이콘을 클릭하여 접근할 수도 있습니다.

파워 컨트롤러의 정보와 상태가 표시됩니다. **[Clear]** 버튼을 클릭하여 **Max current detected**등과 같은 값을 재설정 할 수 있습니다. 파워 컨트롤러 종류에 따라 표시되는 항목이 달라질 수 있습니다.

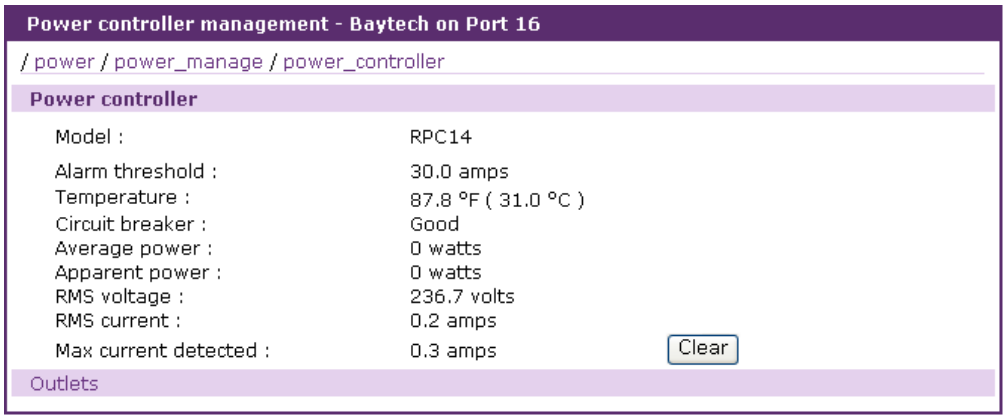


그림 6-9 파워 컨트롤러 유닛 관리 – power controller 탭

6.3.3 파워 컨트롤러 유닛 관리 – Outlets 탭

파워 컨트롤러 관리 (그림 6-8 파워 컨트롤러 관리 – 파워 컨트롤러 리스트 참조) 화면의 파워 컨트롤러 리스트에서 파워 컨트롤러를 선택하면 열리는 파워 컨트롤러 유닛 관리 화면에서 Outlets 탭을 선택하면 파워 컨트롤러 유닛 관리의 Outlets 탭 화면(그림 6-10 파워 컨트롤러 유닛 관리 – outlets 탭 참조)에 접근할 수 있습니다.

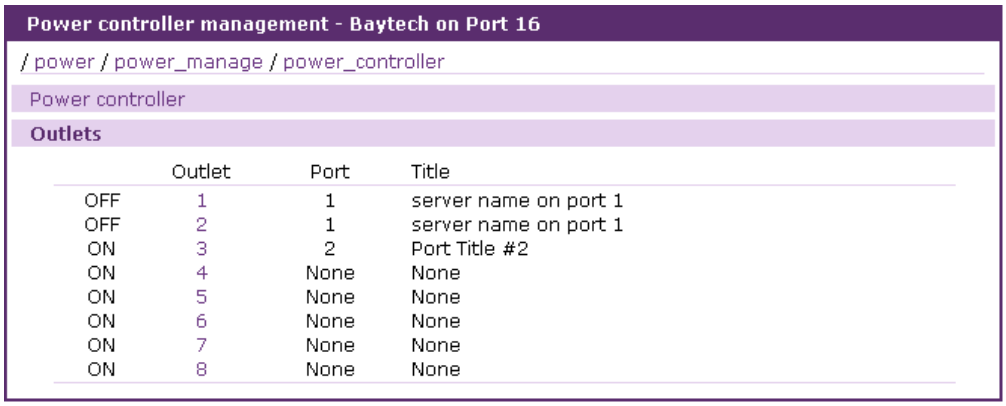


그림 6-10 파워 컨트롤러 유닛 관리 – outlets 탭

이 화면에는 아웃렛이 연결되어 있는 시리얼 포트 번호, 아웃렛 이름등과 같은 파워 컨트롤러 아웃렛 정보와 아웃렛의 상태가 표시됩니다. 아웃렛에 연결된 장비의 전원을 관리할 수 있는 아웃렛 관리 부분도 제공됩니다. 사용자는 이 부분에서 장비를 켜고 꺼거나 재부팅할 수 있습니다. 아웃렛의 번호를 클릭하여 해당 아웃렛의 아웃렛 관리 부분을 펼치거나 접을 수 있습니다. 그림 6-11은 아웃렛 관리 부분이 펼쳐진 화면입니다.

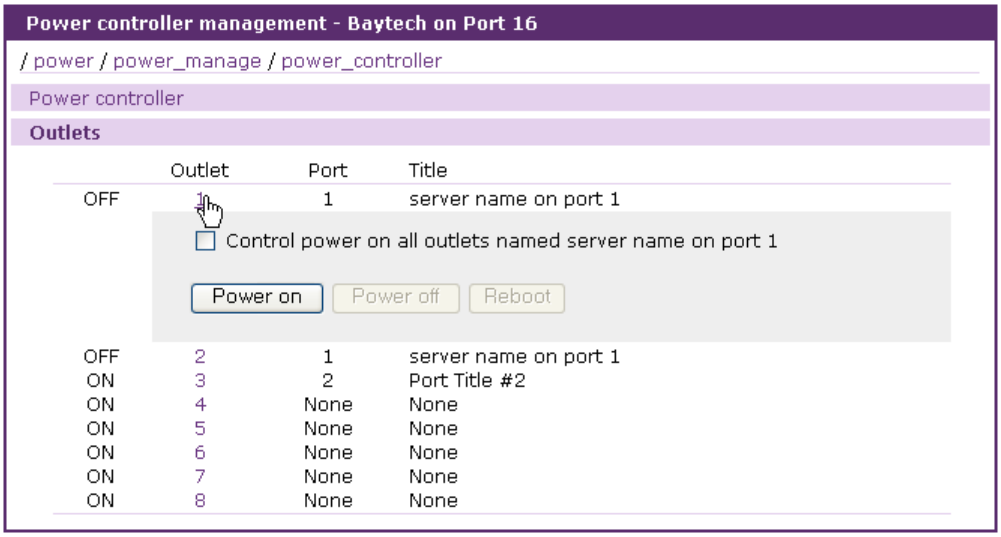


그림 6-11 파워 컨트롤러 유닛 관리 – 아웃렛 관리

시리얼 포트 장비에 두개 이상의 아웃렛이 연결된 경우, **[Control power on all outlets named …]** 체크박스를 체크하고 **[Power on]** 버튼을 클릭하면 아웃렛이 연결된 시리얼 포트의 장비에 전원을 공급하는 모든 아웃렛을 한꺼번에 켤 수 있습니다. 또, 이러한 경우, 전원을 꺼거나 재부팅할 경우 모든 아웃렛의 전원이 꺼지거나 재부팅됩니다.

6.3.4 파워 컨트롤러 유닛 관리 – 시리얼 포트 연결

메뉴바에서 **Serial port - Connection** 메뉴 항목을 선택해서 나오는 시리얼 포트 연결 화면 (그림 4-35 시리얼 포트 연결 페이지와 그림 4-36 포트 작업리스트 참조)에서도 파워 컨트롤러의 현재 상태를 확인할 수 있습니다. 파워 컨트롤러 유닛 관리 화면이 아웃렛의 관점에서 파워 컨트롤러의 상태를 표시한다면, 시리얼 포트 연결 화면에서는 VTS II 시리얼 포트 장비의 전원 상태를 표시합니다.

파워 컨트롤러의 상태를 표시할 뿐만 아니라, 사용자들이 시리얼 포트의 전원을 감시하고 제어할 수 있는 Serial port power control 화면으로 이동할 수 있는 링크도 제공합니다. 포트 작업리스트의 Power Control 아이콘이 켜짐(녹색 아이콘) 또는 꺼짐(적색 아이콘) 상태일 경우에만 Power Control 아이콘을 클릭하여 사용자는 Serial port power control화면으로 이동할 수 있습니다. (그림 6-13 파워 컨트롤러 유닛 관리 – Serial port power control 참조). Power Control 아이콘이 전이(황색 아이콘) 상태일 경우에는 연결될 수 없습니다.

파워 컨트롤러가 연결된 시리얼 포트는 작업리스트에 파워 컨트롤러 유닛 관리 화면으로 이동할 수 있는 Power Controller Management 아이콘이 표시됩니다.

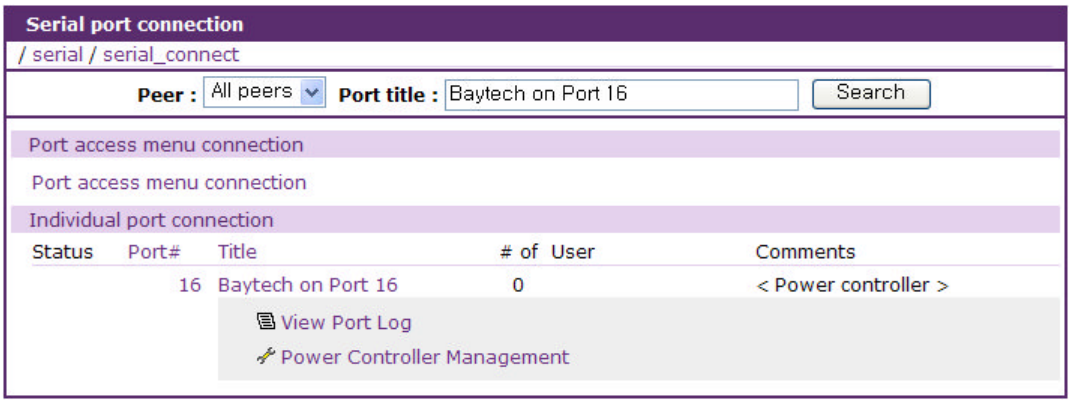


그림 6-12 시리얼 포트 연결 화면 - 파워컨트롤러가 연결된 포트의 작업리스트

6.3.5 파원 컨트롤러 유닛 관리 – Serial port power control

Serial port 연결 화면의 작업리스트에서 켜짐 / 꺼짐 상태 표시의 Power Control 아이콘을 클릭하면 Serial port power control 화면(그림 6-13 파워 컨트롤러 유닛 관리 – Serial port power control 참조)으로 이동합니다. 파워 컨트롤러 아웃렛 관리 화면이 파워 컨트롤러의 아웃렛을 제어하는 반면, 이 화면은 시리얼 포트에 연결된 장비의 전원을 제어하는데 사용됩니다.

그림 6-13 파워 컨트롤러 유닛 관리 – Serial port power control

이 화면에서 시리얼 포트 장비가 연결된 아웃렛의 정보와 함께 장비의 전원 상태를 확인할 수 있습니다. 이 화면에서 장비의 전원 켜고 껴거나 재부팅할 수 있습니다. 시리얼 포트 장비에 여러 아웃렛이 연결된 경우 동시에 모든 아웃렛이 동작됩니다.

7: 주변 장치 설정

7.1 PC 카드 설정

VTS II는 기능의 유연성 및 확장성을 위해 PC 카드 슬롯을 제공하고 있습니다. 다음 4가지 유형의 PC 카드가 지원됩니다.

- LAN 카드
- 무선 LAN 카드
- 모뎀 카드
- ATA/IDE fixed disk card

사용자는 LAN 또는 무선 LAN 카드를 이용하여 또 다른 네트워크 연결을 통해 VTS II에 접속할 수 있으며, ATA/IDE fixed disk card를 이용해 시스템 및 시리얼 포트 로그 데이터를 저장할 수 있습니다. 모뎀 카드를 사용함으로써 외장형 모뎀에 연결하는 시리얼 포트 없이 VTS II에 망외(out-of-band) 접속을 할 수도 있습니다.

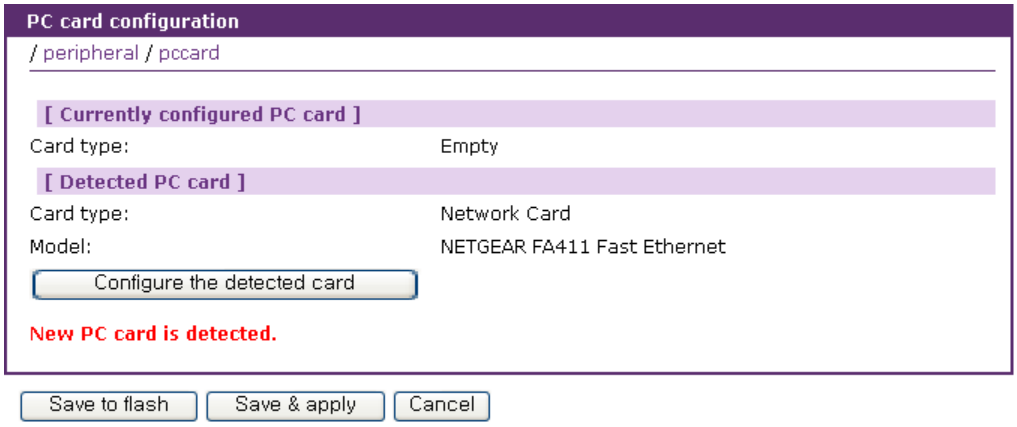


그림 7-1 초기 PC 카드 설정 메뉴 화면

PC 카드 슬롯을 사용하기 위해 사용자는 다음의 단계를 수행해야 합니다.

단계 1. PC 카드를 PC 카드 슬롯에 삽입합니다.

단계 2. PC 카드 설정 메뉴의 **[Configure the detected card]** 버튼을 선택합니다.

단계 3. VTS II는 카드를 검색하기 위해 플러그 앤 플레이(plug & play) 기능을 사용할 것이며, 설정 메뉴 화면에 나타날 것입니다. 사용자는 현재 카드를 동작시키기 위한 파라미터를 설정할 수 있습니다.

단계 4. **[Save to flash]** 버튼을 선택하여 설정을 저장합니다.

단계 5. 메뉴의 **[Apply changes]**를 선택하여 새로운 설정을 적용시킵니다.

VTS II가 지원하는 PC 카드 목록을 보려면 ***부록 B: VTS II가 지원하는 PC 카드*** 부분을 참조하십시오.

PC 카드를 정지 또는 제거하기 위해 사용자는 다음과 같은 단계를 수행해야 합니다.

단계 1. **[Stop Card service]**를 선택합니다.

단계 2. **[Save to flash]**을 선택하여 변경 사항을 저장합니다.

단계 3. 메뉴의 **[Apply changes]**를 선택하여 변경 사항을 적용합니다.

단계 4. PC 카드 슬롯으로부터 PC 카드를 제거합니다.

참고: 위 지침에 따르지 않고 슬롯으로부터 PC 카드를 제거하는 경우 시스템 고장의 원인이 될 수도 있습니다.

7.1.1 LAN 카드 설정

LAN 카드를 PC 카드 슬롯에 설치하면 VTS II는 3개의 IP 주소를 보유하게 됩니다. 이때, IP 주소는 반드시 유효한 것을 지정해야 합니다.

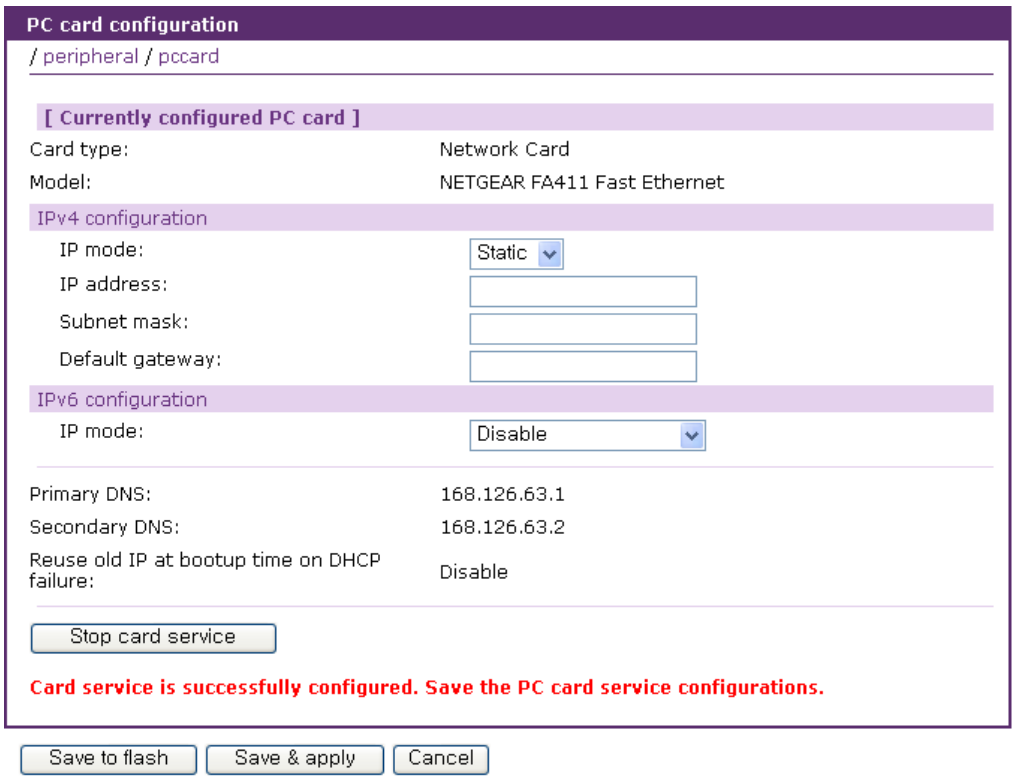


그림 7-2 PC LAN 카드 설정

카드가 인식된 후, 사용자의 네트워크 환경에 맞게 추가적인 네트워크 파라미터들을 설정하여야 올바르게 동작하게 됩니다. 네트워크 파라미터의 설정은 ***3.1 IP 설정***에 자세히 설명되어 있습니다. VTS II가 지원하는 PC 카드 목록을 보려면 ***부록 B: VTS II가 지원하는 PC 카드*** 를 참조하십시오.

7.1.2 무선 LAN 카드 설정

무선 LAN 카드를 PC 카드 슬롯에 설치하면 VTS II는 3개의 IP 주소를 보유하게 됩니다. 이때, IP 주소는 반드시 유효한 것을 지정해야 합니다.

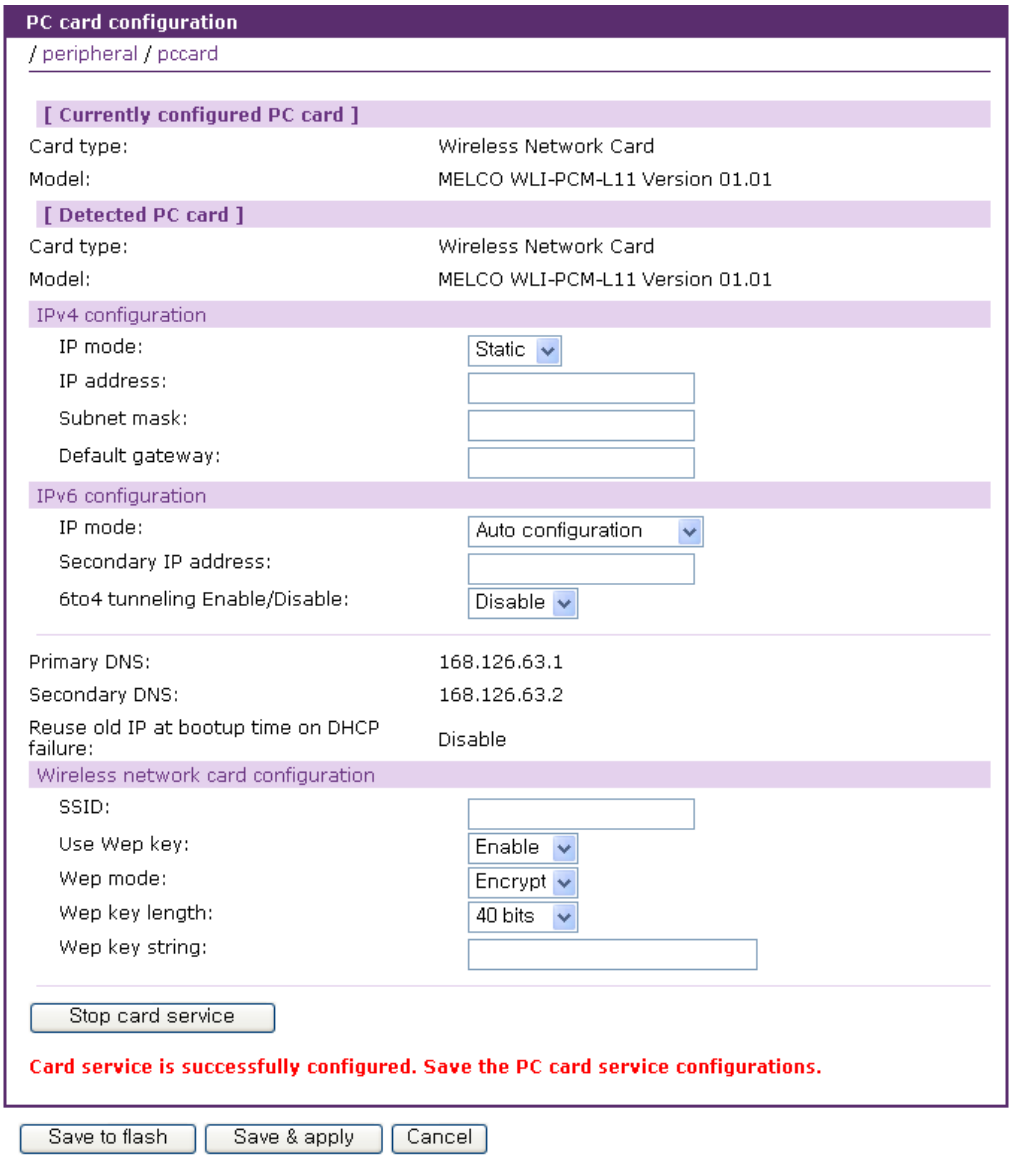


그림 7-3 PC 무선 LAN 카드 설정

카드가 인식된 후, 사용자의 네트워크 환경에 맞게 추가적인 네트워크 파라미터들을 설정하여야 올바르게 동작하게 됩니다. 네트워크 파라미터의 설정은 ***3.1 IP 설정***에 자세히 설명되어 있습니다.

VTS II는 무선 LAN 설정을 위해 SSID(Service Set Identifier)와 WEP(Wired Equivalent Privacy) 키 기능을 지원합니다. 사용자는 AP (Access Point)를 지정하기 위해 SSID를 설정할 수 있으며 또한, encypted 또는 shared로 WEP 모드를 설정할 수 있습니다. WEP 키 길이는 반드시 40 또는 128

bit 여야 합니다. 40-bit WEP 키이면, 사용자는 분리자 콜론(:)이 없는 5개의 16진수 코드 세트를 입력해야 합니다. 128-bit WEP 키이면, 분리자 콜론(:)이 없는 13개의 16진수 코드 세트를 입력하도록 합니다.

예를 들어, 128-bit WEP 키 옵션을 사용하기 위해 사용자는 다음과 같이 13개의 16진수 코드 세트를 반드시 입력해야 합니다.

000F25E4C2000F25E4C2000F24

VTS II가 지원하는 PC 카드 목록을 보려면 ***부록 B: VTS II가 지원하는 PC 카드***를 참조하십시오.

7.1.3 Serial modem 카드 설정

모뎀 카드를 사용함으로써 외장형 모뎀에 연결하는 시리얼 포트 없이 사용자가 온라인에 접근 가능합니다. 대부분의 56 Kbps 전화선 모뎀 및 다양한 모뎀 카드가 지원됩니다. VTS II가 지원하는 PC 카드 목록을 보려면 ***부록 B: VTS II가 지원하는 PC 카드***를 참조하십시오.

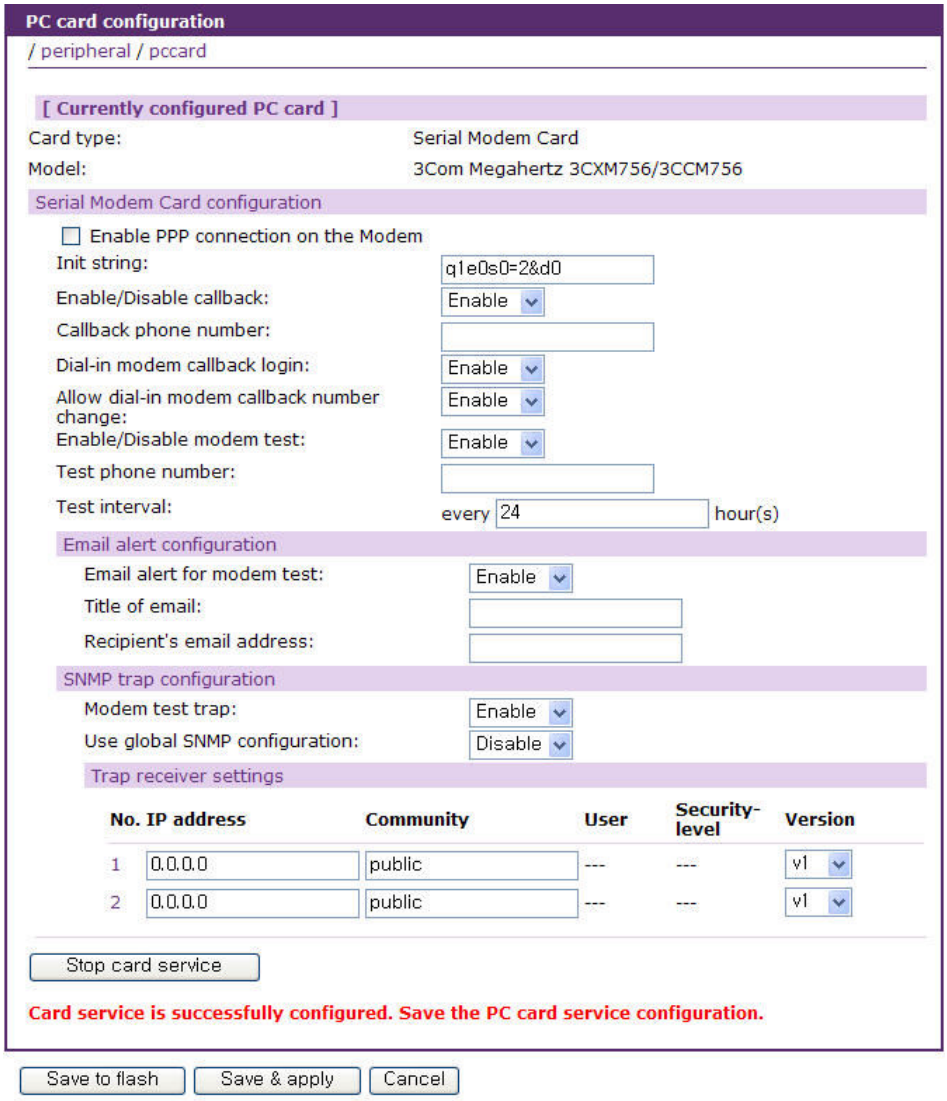


그림 7-4 PC 시리얼 모뎀 카드 설정

기본 모뎀 초기화 스트링 값은 “q1e0s0=2&d0”입니다. 이는 모뎀이 무음 모드(quiet mode)(‘q1’), 에코 오프 모드(echo off mode)(‘e0’), 자동 응답 모드 방식 2(Auto Answer mode equaling two)(“s0=2”) 그리고 DTR line 무시(‘&d0’)의 설정을 의미합니다. 해당 명령 세트에 대한 자세한 정보는 모뎀 매뉴얼을 참조하십시오.

Callback 항목, Modem test 항목과 Alert 설정은 ***4.5.5 Host mode 설정***과 ***4.5.12 Alert 설정***의 Dial-in modem mode 부분을 참조하십시오.

7.1.4 ATA/IDE fixed disk 카드 설정

사용자는 시스템 및 시리얼 포트 로그를 저장하기 위해 PC ATA/IDE fixed disk card를 사용하는데 필요한 전체 데이터 크기를 반드시 설정해야 합니다. VTS II는 전체 저장 크기 및 디스크에서 사용 가능한 디스크 공간을 자동으로 설정합니다.
사용자는 Delete 버튼을 눌러 카드의 모든 파일을 삭제할 수 있습니다.
사용자는 Format 버튼을 눌러 카드를 포맷할 수 있습니다. VTS II는 디스크 카드의 **EXT2** 및 **VFAT** 파일 시스템을 지원합니다.
사용자는 VTS II의 시스템 설정을 export 및 import 함으로써, VTS II 설정 파일을 저장 또는 복구할 수 있습니다.

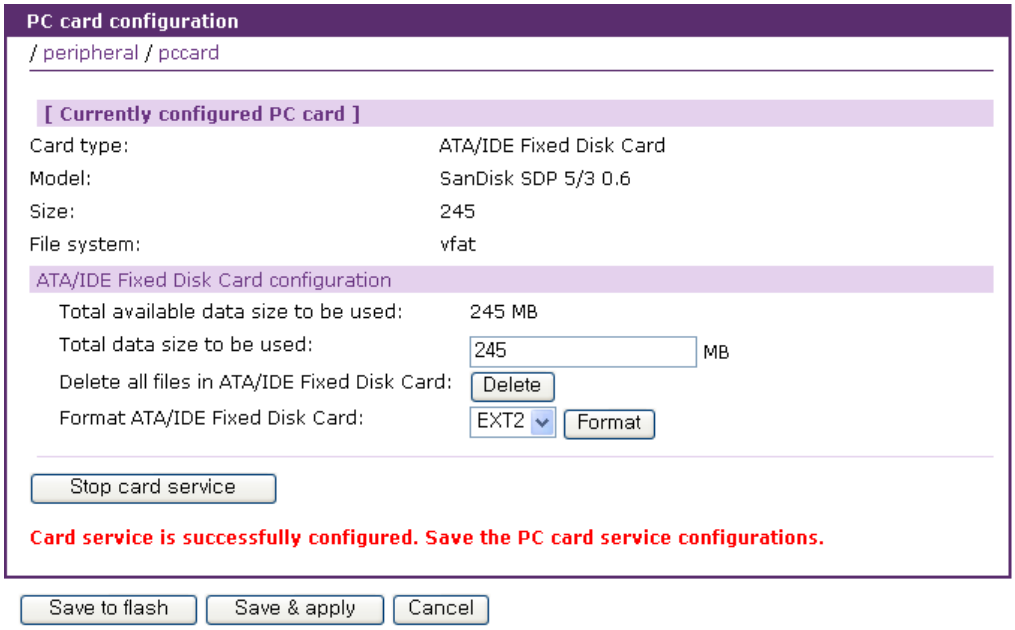


그림 7-5 PC ATA/IDE fixed disk card 설정

7.2 Modem 설정

내장 모뎀을 사용함으로써 외장형 모뎀에 연결하는 시리얼 포트 없이 사용자가 온라인에 접근 가능합니다.

Enable PPP connection on the Modem 은 모뎀을 PPP mode로 사용할 것임의 의미합니다.

기본 모뎀 초기화 스트링 값은 'q1e0s0=2&d0'입니다. 이는 모뎀이 무음 모드(quiet mode)('q1'), 에코 오프 모드(echo off mode)('e0'), 자동 응답 모드 방식 2(Auto Answer mode equaling two)("s0=2") 그리고 DTR line 무시('&d0')의 설정을 의미합니다.

Callback 항목, Modem test 항목과 Alert 설정은 ***4.5.5 Host mode 설정***과 ***4.5.12 Alert 설정***의 Dial-in modem mode 부분을 참조하십시오.

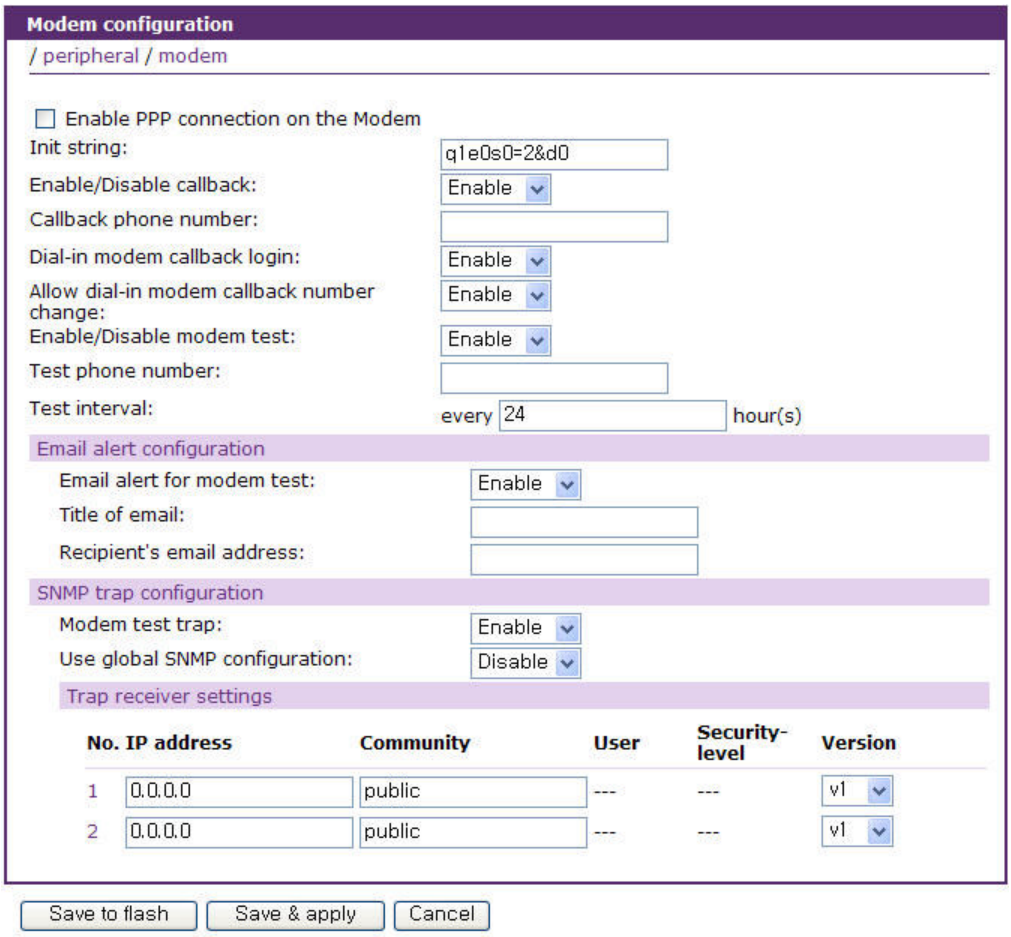


그림 7-6 모뎀 설정

7.3 USB 설정

VTS II는 기능의 유연성 및 확장성을 위해 USB 슬롯을 제공하고 있습니다. 현재 USB 저장 장치가 지원됩니다. 사용자는 USB 저장 장치를 이용해 시스템 및 시리얼 포트 로그 데이터를 저장할 수 있습니다.

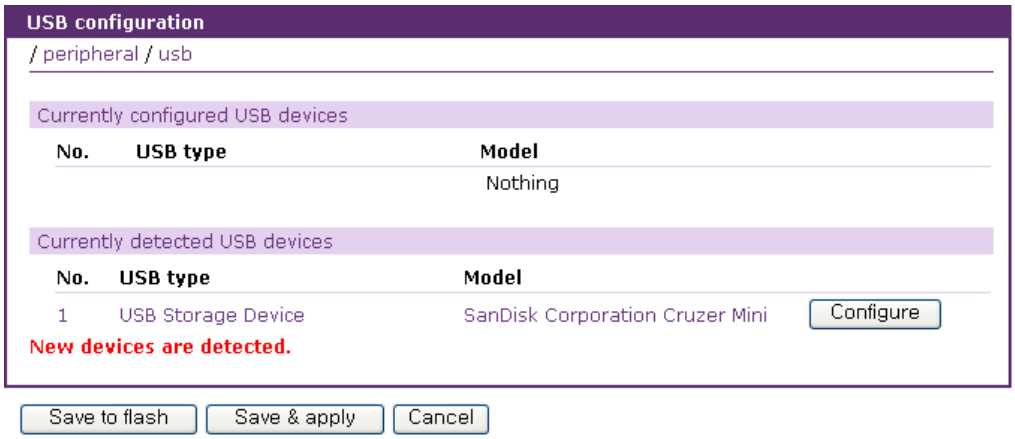


그림 7-7 초기 USB 설정 메뉴 화면

USB 장비를 사용하기 위해 사용자는 다음의 단계를 수행해야 합니다.

단계 1. USB 장비를 USB 슬롯에 삽입합니다.

단계 2. USB 설정 메뉴의 **Currently detected USB devices** 목록에서 **[Configure]** 버튼을 선택합니다.

단계 3. VTS II는 검색된 장비를 **Currently configured USB devices** 목록에 넣을 것이며, 이 목록에서 해당 장비를 선택하면, 설정 메뉴 화면이 나타날 것입니다. 사용자는 현재 장비를 동작시키기 위한 파라미터를 설정할 수 있습니다.

단계 4. **[Save to flash]** 버튼을 선택하여 설정을 저장합니다.

단계 5. 메뉴의 **[Apply changes]**를 선택하여 새로운 설정을 적용시킵니다.

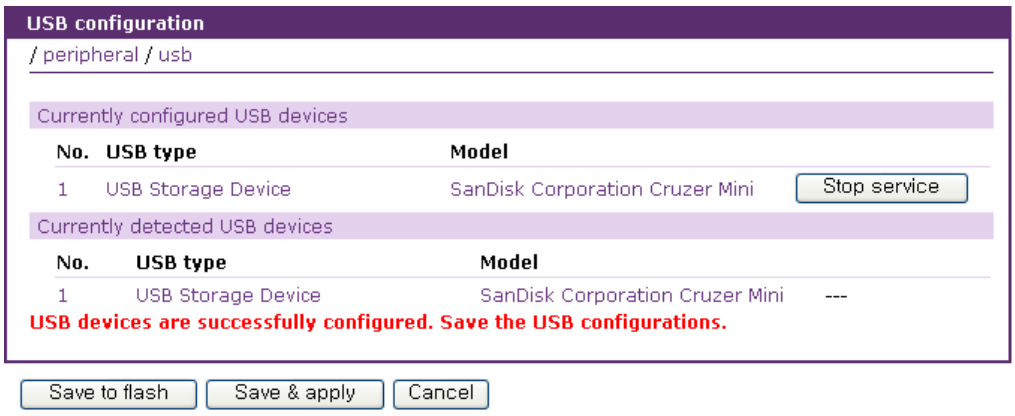


그림 7-8 설정된 USB 장비 화면

PC 카드를 정지 또는 제거하기 위해 사용자는 다음과 같은 단계를 수행해야 합니다.

단계 1. **[Stop service]**를 선택합니다.

단계 2. **[Save to flash]**을 선택하여 변경 사항을 저장합니다.

단계 3. 메뉴의 **[Apply changes]**를 선택하여 변경 사항을 적용합니다.

단계 4. USB 슬롯으로부터 USB 장비를 제거합니다.

참고: 위 지침에 따르지 않고 슬롯으로부터 USB 장비를 제거하는 경우 시스템 고장의 원인이 될 수도 있습니다.

7.3.1 USB 저장 장치 설정

사용자는 시스템 및 시리얼 포트 로그를 저장하기 위해 USB 저장 장치를 사용하는데 필요한 전체 데이터 크기를 반드시 설정해야 합니다. VTS II는 전체 저장 크기 및 디스크에서 사용 가능한 디스크 공간을 자동으로 설정합니다.

사용자는 Delete 버튼을 눌러 카드의 모든 파일을 삭제할 수 있습니다.

사용자는 Format 버튼을 눌러 카드를 포맷할 수 있습니다. VTS II는 디스크 카드의 **FAT** 파일 시스템을 지원합니다.

사용자는 VTS II의 시스템 설정을 export 및 import 함으로써, VTS II 설정 파일을 저장 또는 복구할 수 있습니다.

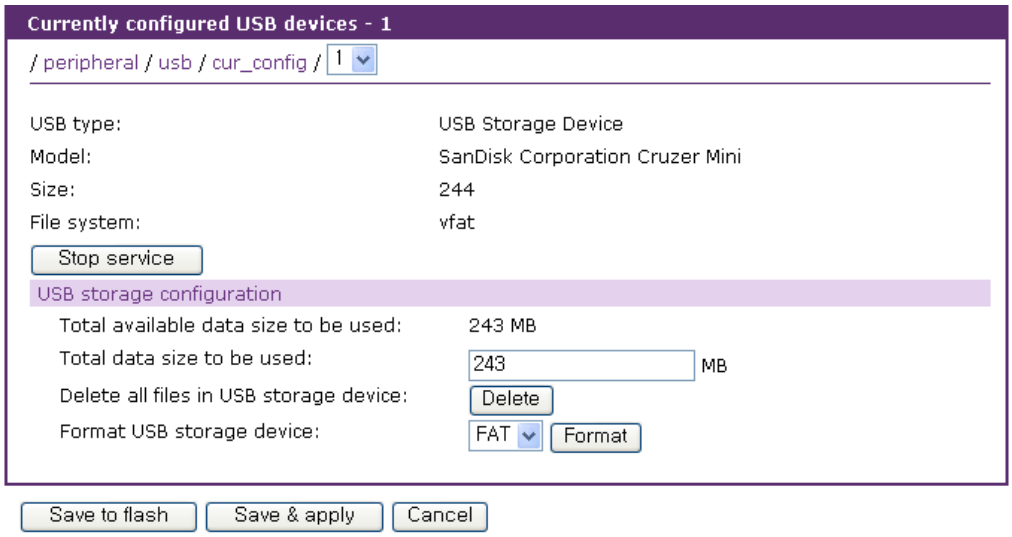


그림 7-9 USB 저장 장치 설정 화면

7.3.2 USB 무선 LAN 설정

무선 LAN 장치를 USB 슬롯에 설치하면 VTS II는 PC LAN 카드와 같이 하나의 IP 주소를 추가로 보유하게 됩니다. USB 무선 LAN 설정 화면은 그림 7-10과 같습니다. 무선 LAN 설정은 7.1.2 **무선 LAN 카드 설정**을 참조하십시오.

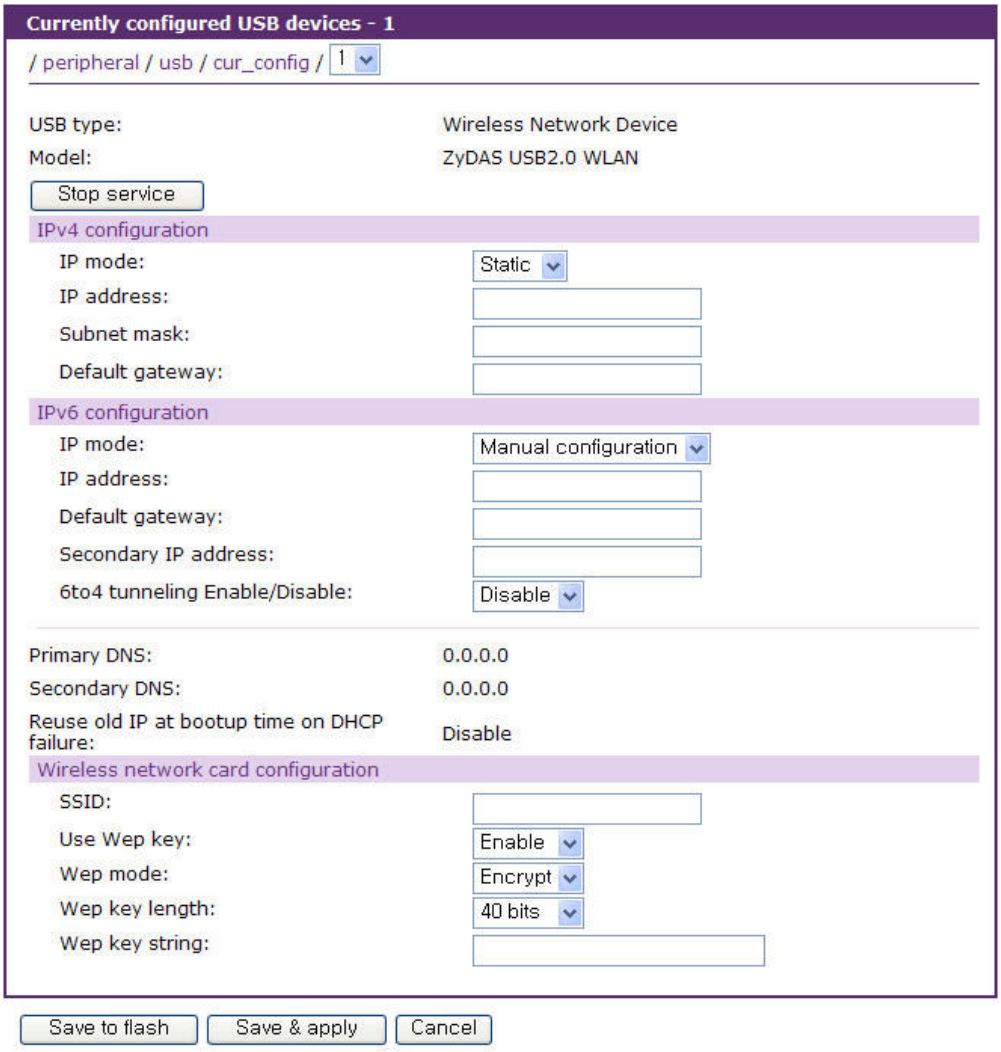


그림 7-10 USB 무선 LAN 설정

VTS II가 지원하는 USB 무선 LAN 목록을 보려면 부록 C: **VTS II가 지원하는 USB 장치**를 참조하십시오.

8: 시스템 상태 및 로그

VTS II는 상태 디스플레이 화면(Status Display Screen)을 통해 시스템 상태와 로그 데이터를 보여주며 관리를 위해 사용됩니다. 시스템 상태 데이터는 모델 이름, 시리얼 번호, 펌웨어 버전, 바이오스 버전 및 VTS II의 네트워크 설정 등이 있습니다. 또한 VTS II는 System logging 기능을 통해 지정된 수취인에게 Email로 로그 데이터를 자동으로 전달하게 설정될 수 있습니다.

8.1 시스템 상태

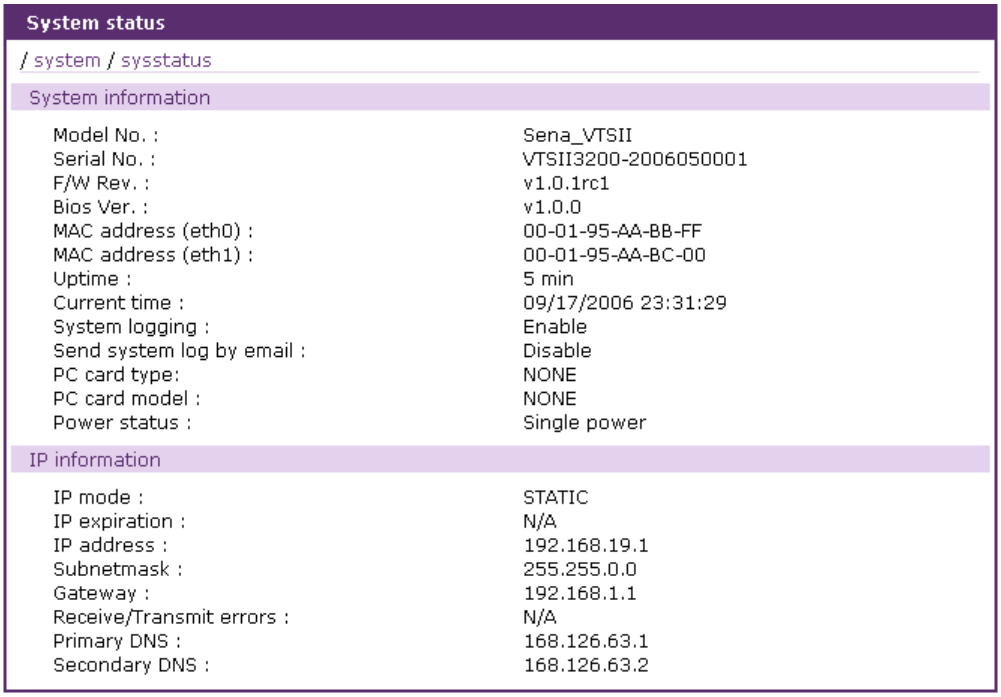


그림 8-1 시스템 상태 디스플레이

8.2 시스템 로그 설정

VTS II는 System logging 기능과 시스템 로그 상태 표시 기능을 제공합니다. 사용자는 SYSLOG-NG 설정에서 System logging 사용시 필요한 정보로써 시스템 로그를 저장하는 위치 및 시스템 로그 버퍼 크기를 선택할 수 있습니다.

System log storage location

시스템 로그는 **VTS II 내부 메모리**, PC 카드 슬롯에 삽입된 **ATA/IDE fixed disk card**, USB 슬롯의 **USB 저장 장치**, **NFS 서버의 설치 지점** 또는 **Samaba 서버의 설치 지점**에 저장될 수 있습니다. 시스템 로그 데이터를 저장하는데 내부 메모리를 사용하는 경우, 로그 데이터는 VTS II가 꺼질 때

삭제됩니다. 시스템 로그 데이터를 보존하려면, 저장 위치를 ATA/IDE fixed disk card, USB 메모리, NFS 서버 또는 Samba 서버로 설정하거나 System log to SYSLOG server를 Enable로 설정해야 합니다. 이를 수행하기 위해 사용자는 먼저 각각의 매체를 사용하기 위한 파라미터들을 설정해야 합니다. 매체가 적절히 설정되지 않은 경우, 사용자는 해당되는 매체를 저장 장소로 설정할 수 없습니다.

System log to SYSLOG server

시스템 로그 데이터는 지정된 저장 위치와 동시에 SYSLOG 서버에도 저장할 수 있습니다.

System log buffer size

이 파라미터는 로깅될 수 있는 시스템 로그 데이터의 최대량을 정의합니다. 데이터를 저장하기 위해 내부 메모리를 사용하는 경우, 시스템 로그 전체 크기는 300 Kbytes를 초과할 수 없습니다.
로그 데이터를 저장하기 위해 ATA/IDE fixed disk card나 USB 저장 장치를 사용하는 경우, 최대 버퍼 크기는 장치의 용량에 따라 달라집니다.
로그 데이터를 저장하기 위해 NFS 서버, Samba 서버를 사용하는 경우, 최대 버퍼 크기는 무한대입니다. 사용자는 NFS 서버, Samba 서버를 설정하여 시스템 로그 기능이 적절히 작동할 수 있도록 해야 합니다.

System log filename

이 파라미터는 Logging되는 파일의 이름을 정의합니다. 디폴트 설정은 **messages**입니다.

Automatic backup on mounting

System log storage location이 CF card, USB, NFS server, Samba server로 설정된 경우에만 설정할 수 있습니다. 이 설정이 Enable되면 해당 저장 공간이 다시 마운트될 경우 로그를 저장하는 백업 파일을 만듭니다.

Send system log by Email

VTS II는 발송되지 않은 로그 메시지 개수가 미리 지정한 수치에 이르면 로그 데이터를 자동으로 보내도록 설정할 수 있습니다. 사용자는 Email을 전송하기 위한 파라미터를 반드시 설정해야 합니다. 이 파라미터에는 Email을 전송하는데 필요한 로그 개수, 수취인 Email 주소 등이 포함될 수 있습니다.

그림 8-2는 설정 및 시스템 로그 보기 화면을 보여줍니다.

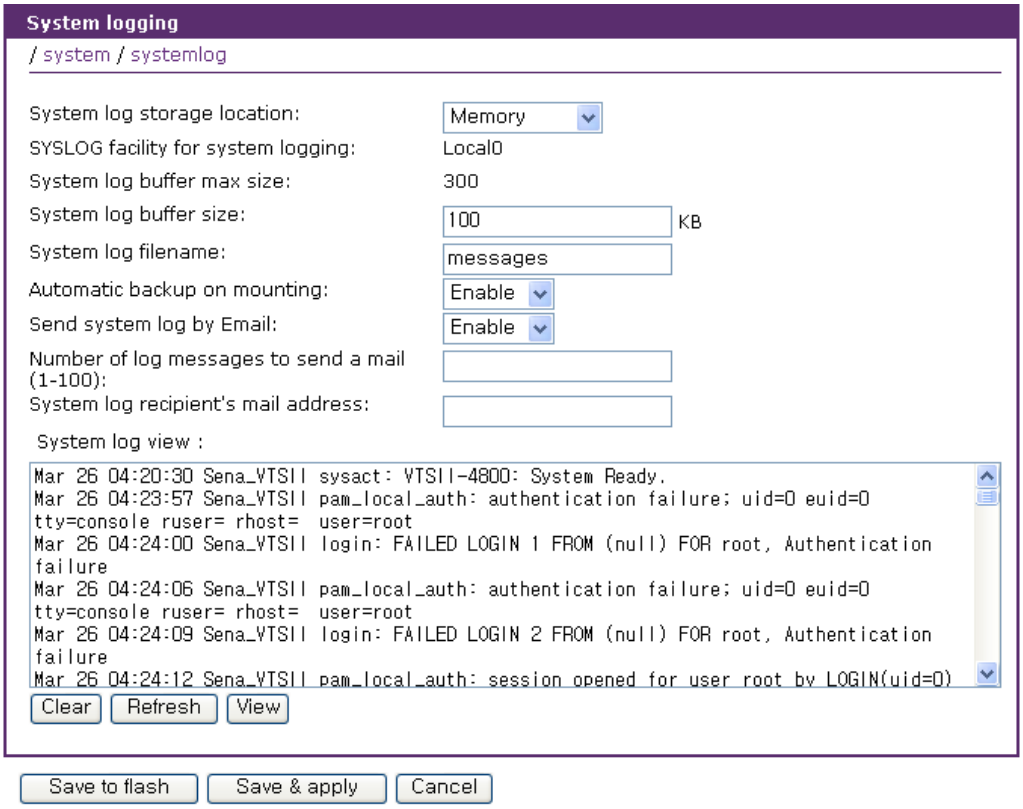


그림 8-2 시스템 로그 설정 및 보기

8.3 SYSLOG-NG 설정

VTS II는 시스템에서 발생하는 각종 로그를 기록할 수 있는 방법을 제공합니다. SYSLOG-NG는 기존의 syslogd의 단점을 보완한 프로그램으로 다양하게 설정할 수 있어, 원하는 형태로 설정해 운영할 수 있습니다. 해당 로그에 대한 무결성과 암호화를 추가했으며, 로그 필터링으로 원하는 로그를 잡아낼 수도 있습니다.

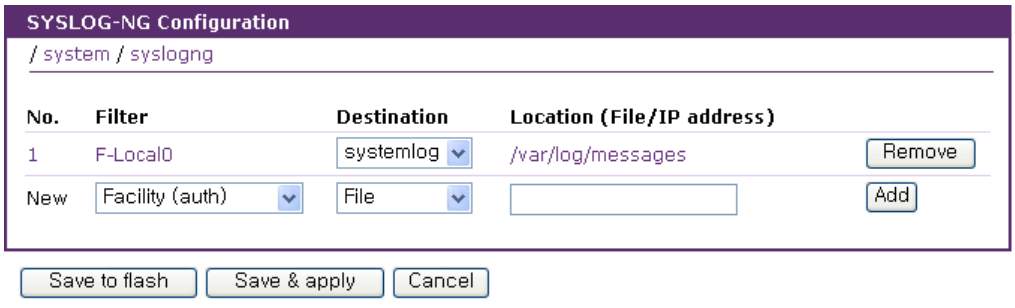


그림 8-3 SYSLOG-NG 초기 설정 화면

Filter, Destination과 Location을 입력하고 **[Add]** 버튼을 클릭하면 새로운 SYSLOG-NG 규칙이 추가됩니다. 삭제하려는 SYSLOG-NG 규칙에 있는 **[Remove]**을 클릭함으로써 사용되지 않는 SYSLOG-NG 규칙을 삭제할 수 있습니다. SYSLOG-NG 규칙의 Filter 항목을 선택하면 SYSLOG-NG 규칙을 편집할 수 있습니다. (그림 8-4 SYSLOG-NG 세부 설정 화면 참조)

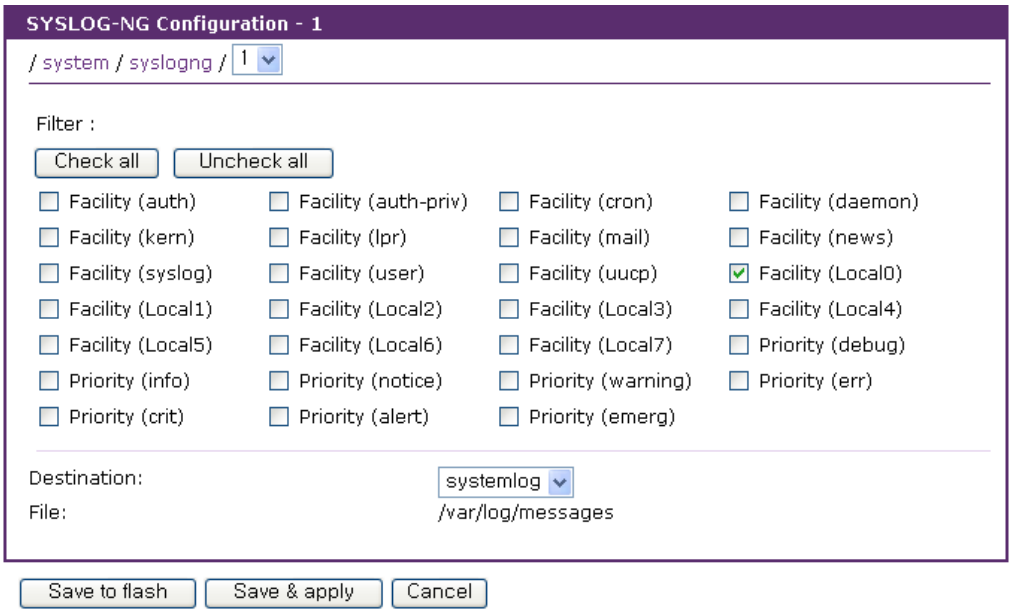


그림 8-4 SYSLOG-NG 세부 설정 화면

Filter에서는 로그 기록을 필터링하게 됩니다. 체크된 Filter들만 로그가 기록됩니다. Port Logging에서 **Port log to SYSLOG server**를 Enable로 설정하면 **SYSLOG facility for port logging**이 활성화됩니다. 선택된 facility를 필터링하는 SYSLOG-NG 규칙이 존재해야 Port Logging 설정에서 의도한데로 Port Logging이 SYSLOG server로 기록됩니다. **Destination**은 File, UDP, TCP, systemlog등의 항목을 가집니다. File을 사용하면 해당 파일을 생성해 로그를 기록하게 됩니다. UDP 나 TCP를 선택하게 되면 설정한 IP 주소로 해당 로그를 보내게 됩니다. systemlog는 ***8.2 시스템 로그 설정***에 의해 설정한 내용에 따라 로그를 기록하게 됩니다.

8.4 Users logged on list

사용자는 시스템의 현재 및 과거의 사용자 활동을 관찰할 수 있습니다.

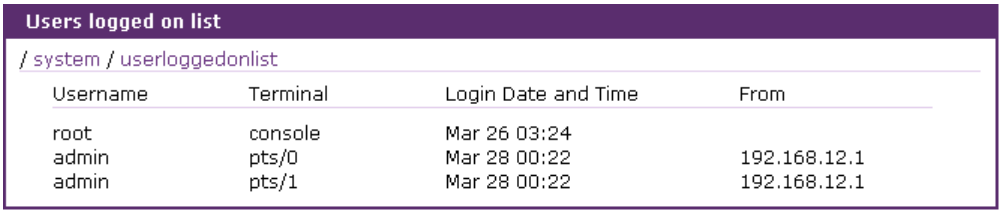


그림 8-5 사용자 로그온 목록

Users logged on list는 시스템에 로그인 한 사용자를 위해 다음의 정보를 보여줍니다.

User name(사용자 이름)

Terminal type for the session (세션에 대한 터미널 유형)

Time connected (연결된 시간)

IP address of the remote host (원격 호스트의 IP 주소)

참고: 웹을 통해 접속하는 사용자는 목록에 나타나지 않습니다. HTTP/HTTPS 프로토콜을 통한 접속은 연결이 유지되지 않습니다.

9: 시스템 관리

VTS II는 3개의 사용자 프로파일 유형을 이용하여 다른 기능에 대한 접속 가능성을 관리합니다. 사용자 유형의 세가지 레벨은 **System admin**, **Port admin** 및 **User** 로 나눌 수 있습니다.

System admin 그룹은 VTS II 설정을 읽고 쓸 수 있는 접속 권한을 갖습니다. **System admin** 은 어떠한 제한 없이 VTS II를 사용할 수 있을 뿐만 아니라 VTS II 설정을 검토 또는 편집할 수 있습니다.
Port admin 그룹은 시리얼 포트/원격 포트와 파워 컨트롤러의 아웃렛 설정 값을 읽고 쓸 수 있는 접속 권한을 갖으며, 나머지 VTS II 설정 값들은 읽을 수 있는 권한만 갖습니다. 또한, 포트에 대한 접속 권한을 갖습니다.
User 그룹은 VTS II 설정을 수정할 수 있는 권한이 없습니다. **User** 는 VTS II 시리얼 포트/원격 포트에 접속 또는 port access menu 에 접속하기 위해 웹 인터페이스의 Serial port 연결 화면에 접속할 수 있습니다. 파워 컨트롤러를 관리하기 위해 웹 인터페이스의 파워 컨트롤러 관리(Power controller management) 화면에도 접속할 수 있습니다.

VTS II는 사용자 인증 방법으로 Local 인증 방법 외에 인증 서버를 이용한 방법을 지원합니다. RADIUS, TACAS+, LDAP등과 같은 원격 인증 방법을 설정하면, VTS II는 원격 인증 서버에 사용자명과 패스워드를 보내서 서버의 응답을 확인합니다. 사용자는 원격 인증이 실패하면 Local 인증을 시도하는 또는 그 반대로 동작하는 연동 인증 방법을 사용할 수 있습니다.

사용자는 VTS II의 장치 이름, 날짜와 시간, 현재 사용자의 패스워드를 설정하며, 설정을 저장하거나 저장된 설정을 다시 불러 올 수 있습니다. 또한 사용자는 웹 인터페이스, 원격 콘솔 및 시리얼 콘솔을 사용하여 VTS II 펌웨어를 업그레이드할 수도 있습니다.

9.1 사용자 관리

VTS II는 4개의 사용자 그룹으로 사용자들을 관리합니다. VTS II의 설정 및 시리얼 포트/원격 포트 접속 권한은 사용자 그룹에 따라 다릅니다.

- **User: 일반 포트 사용자 그룹**
  - 이 그룹에 포함되는 모든 사용자는 시리얼 포트에 접속할 수 있습니다.
  - 이 그룹에 속한 Power 접근권한을 가진 모든 사용자는 이 시리얼 포트가 연결된 아웃렛의 전원을 관리하기 위한 화면에 접속할 수 있습니다.
  - 이 그룹의 사용자는 **port access menu** 에 접속할 수 있습니다.
  - 이 그룹의 사용자는 웹 인터페이스의 **Serial port 연결** 메뉴와 파워 컨트롤러 관리 메뉴를

사용할 수 있습니다.

- 이 그룹의 사용자는 VTS II 설정 메뉴 또는 CLI 에 접속할 수 없습니다.

참고:

시리얼 포트에 연결된 장비와 전원을 사용자들을 그룹으로 관리할 수 있게 하기 위해 [User access control] 기능이 제공됩니다.

- **Port admin: Serial port 관리자 그룹**
  - **Port admin** 그룹은 **User** 그룹보다 높은 권한을 가집니다.
  - **Port admin** 그룹은 웹 인터페이스 또는 시스템 콘솔 접속을 통해 VTS II 설정 메뉴에 접속할 수 있습니다. 이 그룹은 Serial Port, Clustering 및 파워 컨트롤러 아웃렛과 관련된 설정 파라미터만을 변경할 수 있습니다. 그 외의 VTS II 시스템의 설정 파라미터들을 변경하는 권한을 이 그룹의 사용자들에게 제공되지 않습니다 (예. 네트워크 설정, PC 카드 및 시스템 관리).
  - 이 그룹에 포함된 사용자는 CLI 에 접속할 수 없습니다.

- **System admin : 시스템 관리자 그룹**
  - **System admin** 그룹은 **Port admin** 그룹보다 높은 권한을 가집니다.
  - **System admin** 그룹은 웹 인터페이스 또는 시스템 콘솔을 통해 설정 메뉴에 접속하여 시스템의 모든 파라미터들을 수정할 수 있습니다.
  - **System admin** 그룹은 CLI 에 접속할 수 있으며, CLI 에서 제공되는 각종 shell program들을 수행할 수 있습니다. 이 그룹은 CLI 를 통해 VTS II 설정 및 port access menu 에 접속할 수 있습니다.

- **root: 시스템 슈퍼 관리자**
  - **root** 는 시리얼 포트에 연결된 시스템 관리자 그룹보다 높은 권한을 가집니다.
  - **root** 는 Linux CLI 에 아무 제한 없이 접속할 수 있습니다. CLI 를 통해 사용자 관리, 파일을 삭제, 수정 및 shell program 수행 등 모든 기능을 제한 없이 사용합니다.
  - **root** 는 단 한 명이며, 사용자 이름은 변경할 수 없습니다.

공장 출하시의 기본 사용자 이름 및 비밀 번호는 다음과 같습니다.

시스템 슈퍼 관리자

Login: root **Password**: root

시스템 관리자

Login: admin **Password**: admin

표 9-1에 VTS II에서 관리되는 사용자 그룹 및 해당되는 사용자 그룹의 권한을 요약해 놓았습니다.

표 9-1사용자 그룹 및 권한

그룹	root	System admin	Port admin	User
기본 사용자 이름	Root	admin	-	-
설정 기본 인터페이스	CLI	텍스트 메뉴	-	-
인터페이스 프로그램	CLI 텍스트 메뉴 port access menu	CLI 텍스트 메뉴 port access menu	텍스트 메뉴 port access menu	port access menu
SSH 공개 키 업로드	O	O	X	X
CLI 접속	O	O	X	X
VTS II 설정 텍스트 메뉴 접속	O	O	△**	X
port access menu 접속	O	O	O	O
웹 GUI 접속	O	O	△**	△***
시스템 파라미터 변경	O	O	△**	X
사용자 파라미터 변경	O	O	X	X
사용자 편집/삭제	O	O	X	X

참고:

*1) ***

Port admin 그룹은 Serial port / Clustering 및 파워 컨트롤러 아웃렛 기능과 관련된 설정만 수정할 수 있습니다. 그 외의 설정은 오직 읽을 권한만 있습니다.

*2) ****

User 그룹은 웹 설정 화면에서 오직 Serial port / Clustering 연결 및 파워 컨트롤로 관리 화면에만 접속할 수 있습니다.

그림 9-1은 User 그룹을 관리하기 위한 웹 인터페이스의 화면입니다.

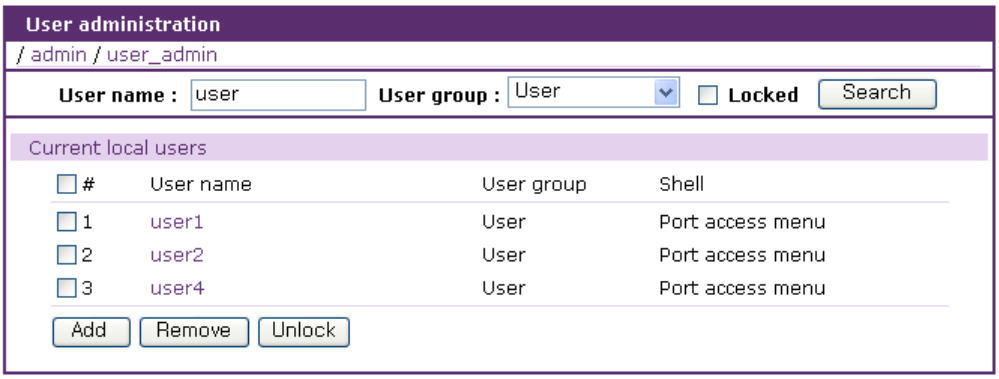


그림 9-1. 사용자 관리

사용자 이름, 사용자 그룹 또는 두 항목 모두를 입력하여 조건을 만족하는 사용자만을 검색할 수 있습니다. 사용자 이름이 입력되지 않으면 모든 사용자를 검색합니다. 사용자 이름이 입력되면 입력된 값으로 시작하는 사용자가 검색됩니다. 사용자 그룹이 선택되면 그 그룹에 속한 사용자만 검색되고, [All group] 일 경우 모든 그룹의 사용자가 검색됩니다. 또 Locked를 선택하고 검색을

하면 사용이 중단된 사용자가 검색됩니다.

사용자를 추가 하려면, **[Add]** 버튼을 클릭하여 사용자 추가 화면을 연 후, 사용자 이름, 그룹 및 비밀 번호를 입력한 다음 **[Add]** 버튼을 선택합니다. 그림 9-2는 **사용자 추가** 화면을 보여줍니다. 새로운 사용자 계정을 생성하기 위해 다음 파라미터들을 적절히 설정하여야 합니다.

사용자 이름 (User Name)

사용자 그룹 (User Group): User, Port admin, System admin 중 하나

사용자 비밀 번호 (User Password)

shell 프로그램(Shell program): CLI, Configuration menu, Port access menu 중 하나

SSH 공개 키 인증(SSH public key authentication): Enabled 또는 Disabled 중 하나

SSH 버전(SSH version): v1 또는 v2 중 하나

SSH 공개 키 파일(SSH public key file)

기본적으로는, SSH를 통해 VTS II로부터 인증을 받을 때, 사용자 이름 및 비밀 번호를 이용한 인증을 받는 것이 기본이나, 사용자에 따른 SSH 공개 키를 VTS II에 업로드하면, SSH 클라이언트 프로그램 및 공개 키 파일을 사용함으로써, 자동으로 VTS II로부터 인증을 받을 수 있습니다.

참고:

사용자 추가 또는 변경시 사용자 이름 및 password는 최소한 3자 이상이어야 합니다. 3자가 되지 않을 경우에는 오류가 발생하게 됩니다.

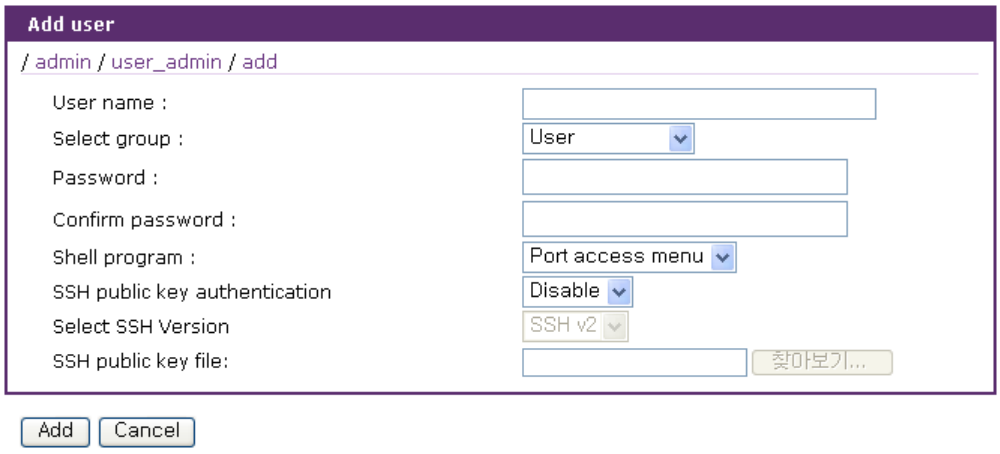


그림 9-2. 사용자 추가하기

사용자를 제거하려면 다음을 수행하십시오.

- 사용자 관리 화면에서 사용자들을 체크합니다.
- **[Remove]** 버튼을 클릭합니다.

사용자 계정의 파라미터를 변경하려면, 사용자 관리화면에서 사용자 이름을 선택하여 사용자 편집 화면을 연 후, 사용자 추가의 방법으로 사용자 계정의 파라미터를 편집합니다.

9.2 액세스 리스트

개별 포트의 User access contorl 설정을 용이하게 하기 위해 액세스 리스트 기능을 지원합니다. 액세스 리스트를 만든 후 액세스 리스트에 사용자를 추가하고 개별 포트 설정의 User access control 설정에서 액세스 리스트를 추가하여 해당 액세스 리스트에 포함된 모든 사용자의 접근권한을 일괄적으로 지정할 수 있습니다.

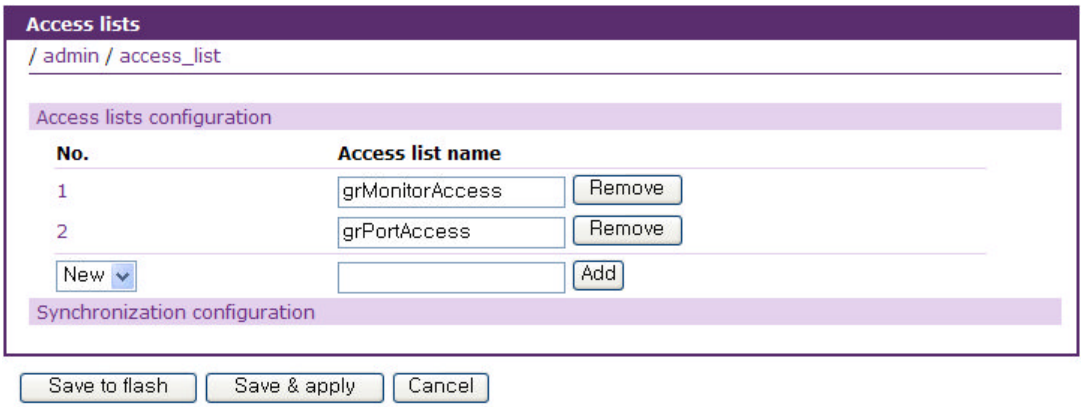


그림 9-3. 액세스 리스트 - 액세스 리스트 관리

그림 9-3은 액세스 리스트를 관리하는 화면을 보여줍니다. 등록된 액세스 리스트들이 나열됩니다. 액세스 리스트 등록을 하려면 다음의 절차를 따르십시오.

1. 액세스 리스트 번호를 **[New]**로 선택
2. 액세스 리스트 이름 입력
3. **[Add]** 버튼을 클릭

이미 등록된 액세스 리스트를 복사하여 새로운 액세스 리스트를 만들수도 있습니다. 복사 대상 액세스 리스트의 사용자 정보도 복사됩니다. 액세스 리스트를 복사하려면 다음의 절차를 따르십시오.

1. 액세스 리스트 번호를 복사 대상 액세스 리스트 번호로 선택
   (**[Add]** 버튼이 **[Copy]** 버튼으로 바뀜)
2. 새로 만들어질 액세스 리스트 이름 입력
3. **[Copy]** 버튼 클릭

[Remove] 버튼을 클릭하여 액세스 리스트를 제거할 수도 있고, 액세스 리스트의 이름을 직접 수정하여 변경할 수도 있습니다. 액세스 리스트를 제거하거나 이름을 바꾸어도 개별 포트의 User access control에서 사용된 액세스 리스트를 자동으로 제거하거나 이름을 바꾸지 않기 때문에 개별포트가 존재하지 않는 액세스 리스트를 참조할 수 있으므로 주의하시기 바랍니다.

액세스 리스트 이름을 선택하면 액세스 리스트 사용자 관리화면으로 이동할 수 있습니다.

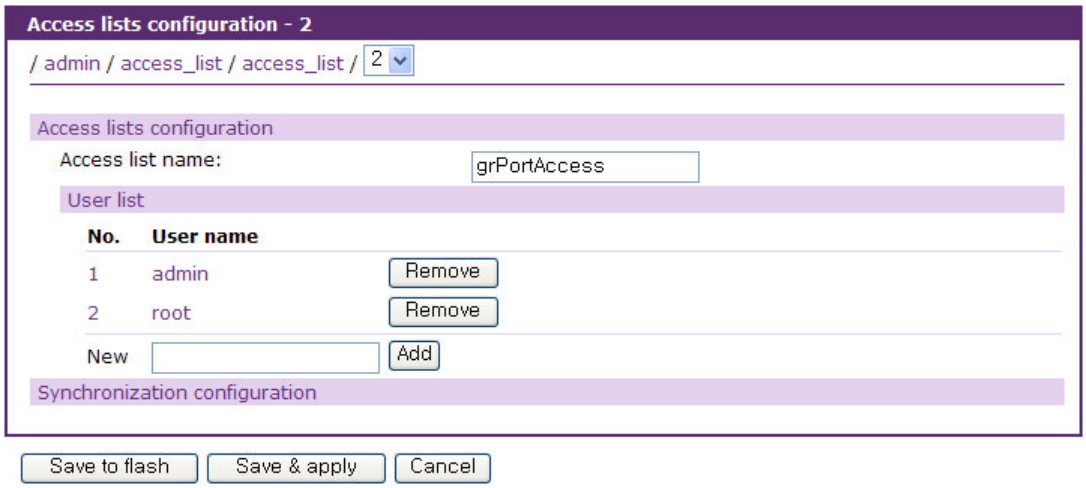


그림 9-4. 액세스 리스트 – 사용자 관리

그림 9-4는 액세스 리스트의 사용자를 관리하는 화면을 보여줍니다. 액세스 리스트에 등록된 사용자를 나열합니다. 사용자 이름을 입력하고 **[Add]** 버튼을 클릭하여 사용자를 등록할 수 있고, **[Remove]** 버튼을 클릭하여 사용자를 액세스 리스트에서 삭제할 수도 있습니다.
[Access list name] 리스트 박스에서 [--- Access lists ---] 항목을 선택하여 액세스 리스트 관리하면으로 이동할 수 있고, 다른 액세스 리스트를 선택하여 액세스 리스트 사용자 관리화면으로 이동할 수도 있습니다.

참고:
Access list name중 ***web_admin****과* ***web_padmin****은 remote authentication시 local에 사용자 이름이 없는 경우 사용자의 권한을 부여하기 위해 사용되는 그룹입니다. web_admin에 포함되어 있는 사용자가 remote authentication을 통해 접속하는 경우 System admin 권한을, web_padmin에 포함되어 있는 사용자는 Port admin권한을 갖게 됩니다.*

Synchronization configuration

VTS II는 clustering 혹은 peer to peer로 여러유닛을 관리하는 경우 access list를 공통으로 관리할 수 있도록 동기화 메뉴를 제공합니다. 대상 VTS II 장비들을 동기화가 가능하도록 그림 9-5와 그림 9-6과 같이 설정을 합니다.

우선, Access list를 받을 장비들을 그림 9-5와 같이 Slave로 설정합니다.

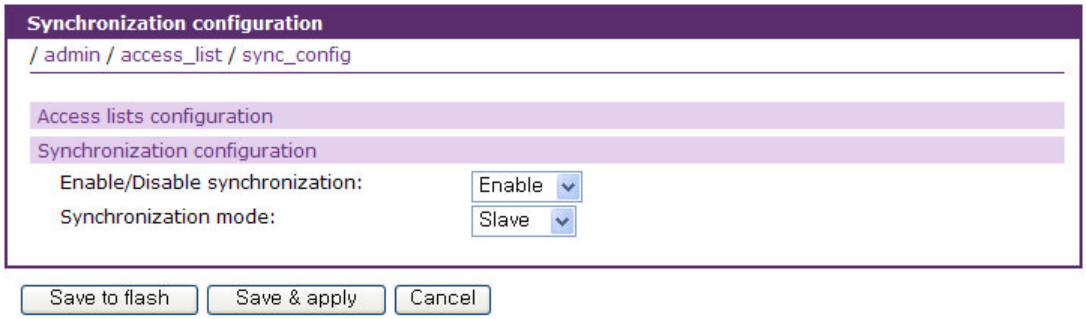


그림 9-5 access list synchronization - slave

설정을 관리할 VTS II 장치를 선택하여 그림 9-6과 같이 **Synchronization mode**를 **master**로 설정하고, 대상 장비들의 리스트를 구성후 **Synchronize** 버튼을 누르면 Master 장비의 access list 설정이 Slave 장비들로 전달 변경이 됩니다.

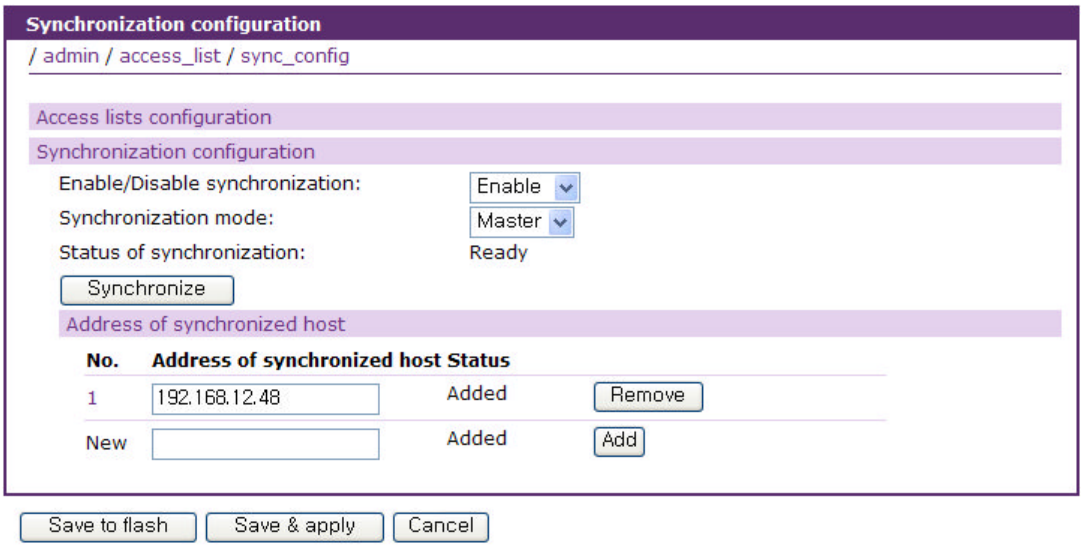


그림 9-6 access list synchronization - master

9.3 패스워드 변경

그림 9-7은 패스워드 변경 화면을 보여줍니다. 현재 사용자의 패스워드를 변경하려면, 현재 패스워드를 입력하고, 새 패스워드를 입력한 후 새 패스워드를 확인하기 위해 한번 더 새 패스워드를 입력해야 합니다.

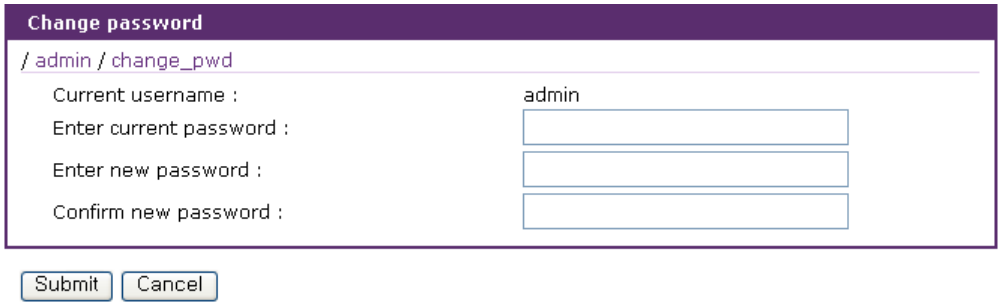


그림 9-7. 패스워드 변경

Port access menu에만 접근할 수 있는 사용자도 Port access menu 화면에서 패스워드를 변경할 수 있습니다. Port access menu에 연결하면 아래와 같은 화면이 표시됩니다. 명령 입력란에 P를 입력한 후 새 패스워드를 입력하고 확인하기 위해 한번 더 입력하면 패스워드가 바뀝니다.

```
[Sena_VTSII]
================================================================================
 Port#       Port Title         Mode    Port#       Port Title         Mode
================================================================================
 1    Port Title #1             CS    2    Port Title #2             CS
 3    Port Title #3             CS    4    Port Title #4             CS
 5    Port Title #5             CS    6    Port Title #6             CS
 7    Port Title #7             CS    8    Port Title #8             CS
 9    Port Title #9             CS    10   Port Title #10            CS
 11   Port Title #11            CS    12   Port Title #12            CS
 13   Port Title #13            CS    14   Port Title #14            CS
 15   Port Title #15            CS    16   Port Title #16            CS
 17   Port Title #17            CS    18   Port Title #18            CS
 19   Port Title #19            CS    20   Port Title #20            CS
 21   Port Title #21            CS    22   Port Title #22            CS
 23   Port Title #23            CS    24   Port Title #24            CS
 25   Port Title #25            CS    26   Port Title #26            CS
 27   Port Title #27            CS    28   Port Title #28            CS
 29   Port Title #29            CS    30   Port Title #30            CS
 31   Port Title #31            CS    32   Port Title #32            CS

  Enter command (1-48 serial port, P passwd, Q exit )
  ------> P
 Enter new password : *****
 Retype new password : *****
 ..
 Save Done.
 Password was changed.
```

9.4 장치 이름(Device name) 설정

VTS II의 관리를 위해 자체적으로 장비 이름을 설정할 수 있습니다. 그림 9-8는 장치 이름 설정 화면입니다. 사용자가 Device name을 변경하게 되면 VTS II의 Hostname이 변경됩니다.

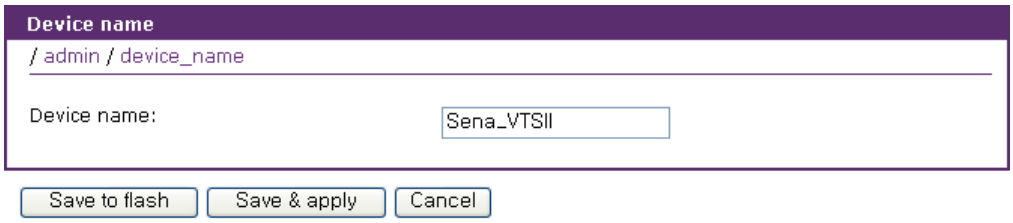


그림 9-8. 장치 이름 설정

Device name 변경하면 CLI 상의 프롬프트 또한 아래와 같이 해당되는 Hostname으로 변경이 됩니다.

```
[root@Sena_VTSII ~]#
```

VTS II의 Device name 설정이 공백 문자는 허용이 되지 않으며 사용자가 Device name 을 빈 문자로 지정하게 되면 VTS II의 Hostname 은 VTS II의 IP 주소로 자동으로 지정이 됩니다. 또한 Device name은 VTS II Manager와 같은 관리 프로그램에서 장비 식별을 위해 사용됩니다.

9.5 날짜 및 시간 설정

VTS II는 현재의 날짜 및 시간 정보를 가지고 있습니다. VTS II의 시계 및 달력 설정은 내부 배터리 전원에 의해 백업됩니다. 사용자는 그림 9-9에 나타난 바와 같이 현재 날짜 및 시간을 변경할 수 있습니다.

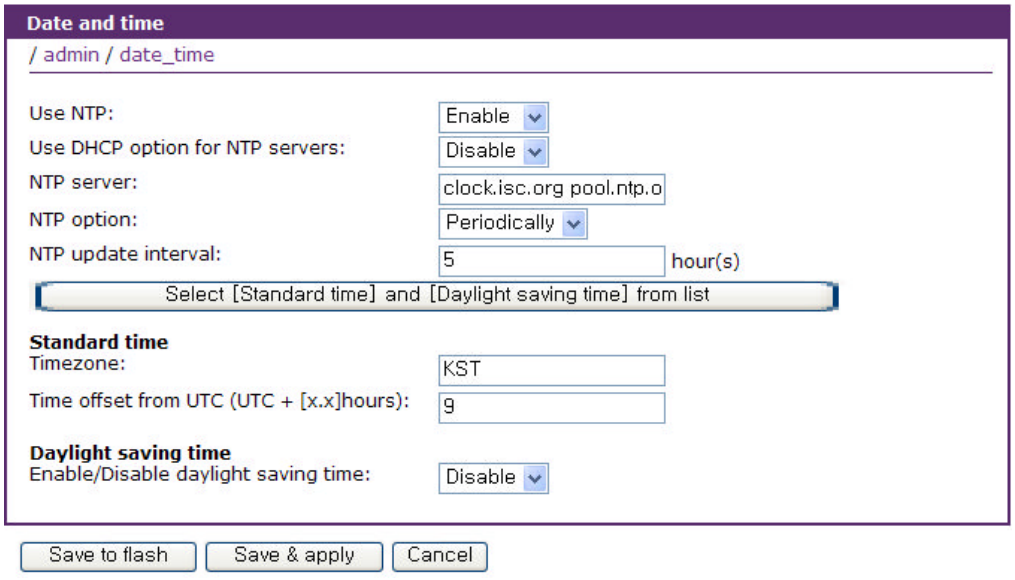


그림 9-9. 날짜 및 시간 설정

날짜 및 시간 설정을 설정하기 위한 방법은 2가지가 있습니다. 첫번째 방법은, NTP 서버를 사용하는 것입니다. NTP 기능이 활성 상태가 되면, NTP option에 따라 설정이 적용될 때나 VTS II가 재부팅될 때마다 혹은 주기적으로 NTP 서버로부터 날짜 및 시간 정보를 얻을 수 있습니다. NTP 서버가 0.0.0.0 으로 설정되면, VTS II는 기본 NTP 서버를 사용합니다. 이런 경우에, VTS II는 인터넷과 연결되어 있어야 합니다. **Use DHCP option for NTP servers** 를 설정하게 되면 DHCP 서버에서 받은 NTP server 정보를 받아서 사용합니다. 사용자는 또한 현재 위치에 따라서 협정 세계 표준시(UTC)로부터 오프셋 시간을 설정해야 합니다. 한국의 경우는, 동경과 같은 +9 시간으로 설정해 주셔야 합니다.
두번째 방법은, NTP를 사용하지 않고 수동으로 날짜 및 시간을 설정하는 것입니다. 이 경우, 날짜 및 시간 정보는 내부 배터리 백업에 의해 유지됩니다.

시스템 날짜와 시간을 정확하게 설정하려면 사용자의 위치에 따른 timezone과 UTC로부터의 오프셋 값을 설정해야 합니다. 사용자가 daylight saving time을 이용한다면, daylight saving timezone, UTC로부터의 오프셋, 시작일시, 종료일시 등과 같은 속성을 설정해야 합니다. VTS II는 이런 파라미터를 이용하여 정확한 시스템 날짜와 시간을 계산합니다. **Select [Standard time] and [Daylight saving time] from list** 버튼을 누르면 이 설정을 리스트에서 선택하여 쉽게 설정할 수 있도록 도와주는 화면이 표시됩니다.

9.6 설정 관리

사용자는 현재의 설정을 CF card, NFS server, user space 또는 local machine등과 같은 저장 위치에 파일로 저장할 수 있고, 저장된 설정 파일을 이용해서 현재 설정값으로 불러 올 수도 있습니다. 또한 웹서버 인증서나 SSH 인증서를 Upload 할 수 있습니다. 그림 9-10은 설정 관리 화면을 보여줍니다.

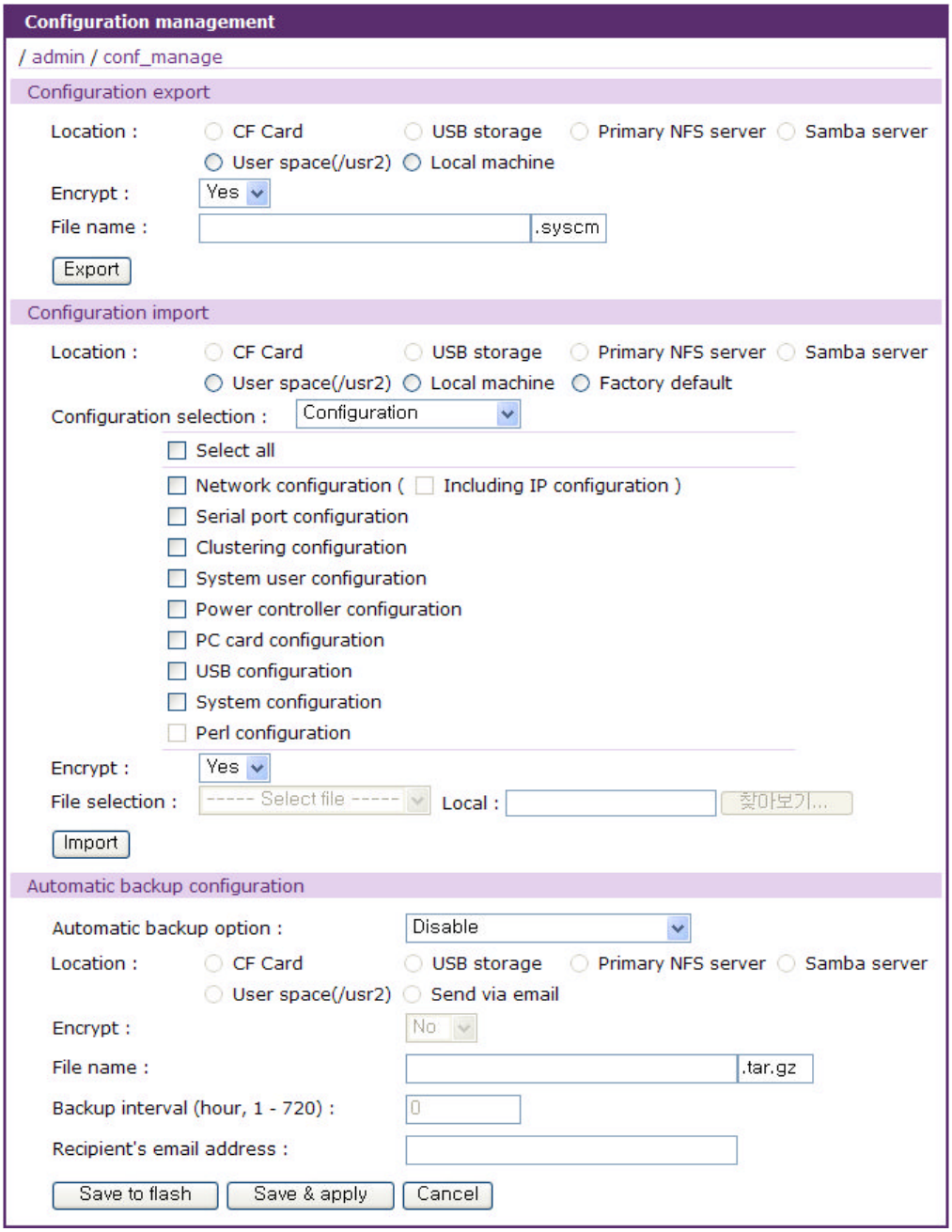


그림 9-10. 설정 관리

VTS II를 공장 출하 상태의 설정 상태로 되돌리기 위해서는 **Configuration import** 탭의 **Location** 파라미터를 **Factory default**로 선택하여 설정을 불러오거나, VTS II의 후면 패널의 Reset Button 을 누르면 됩니다.

VTS II가 자동으로 설정을 저장하는 기능을 지원합니다. **Automatic backup configuration**을 설정하고 적용하면 VTS II는 지정된 시간에 지정된 방법으로 설정을 자동으로 저장합니다.

설정 저장하기, 설정 불러오기 및 자동 설정 저장을 정상적으로 수행하기 위해서는 다음 파라미터들을 적절히 설정하여야 합니다. **Configuration import** 탭에서 Configuration selection 메뉴는

Configuration, Webserver certificate, CA certificate 의 항목을 가집니다. 설정을 불러오기 위해서는 Configuration을 사용하고, Webserver certificate를 선택하여 웹서버 인증서를 업로드할 수 있습니다. CA certificate를 선택하여 SSH 접속시의 인증서를 업로드 할 수 있습니다.

설정 저장하기

Location : 설정 파일을 저장할 위치

Encrypt : 설정 파일 암호화 여부

File name : 설정 파일 이름

설정 불러오기

Location : 설정 파일을 불러올 위치. Factory default 선택하면 공장 출하시 설정으로 복원

Configuration selection : 불러올 설정의 종류

Encrypt : 불러올 설정 파일의 암호화 여부

File selection : Location이 CF card, NFS server 또는 User space 인 경우 해당 위치에 존재하는 Encrypt 옵션을 만족하는 파일이 열거

Local : Location이 Local machine일 경우 Local machine에 저장된 설정 파일을 찾는 화면 표시

자동 설정 저장

Automatic backup option : 자동 설정 저장 방법을 지정

Disable – 자동 설정 저장 하지 않음.

Periodically – 주기적으로 설정 저장. Backup interval 설정 필요.

10 minutes after last change – 설정 변경 후 10분 경과시 설정 저장.

Location : 설정 파일을 저장할 위치

Encrypt : 설정 파일 암호화 여부

File name : 설정 파일 이름

Backup interval : Automatic backup option이 Periodically 일 경우 자동 설정 저장 주기

Recipient's email address : Location이 Send via email일 경우 메일 수신자의 주소

현재 설정을 저장하려면 다음의 절차를 따르십시오.

1. 설정 파일을 저장할 위치를 선택
2. 암호화 옵션을 선택
3. 파일이름을 입력
4. **[Export]** 버튼을 클릭

저장된 설정을 불러오려면 다음의 절차를 따르십시오.

1. 불러올 위치를 선택
2. 불러올 설정 유형을 선택
3. 암호화 옵션을 선택

4. 위치가 Local machine도 Factory default도 아닐 경우파일 선택 리스트 박스에서 암호화 옵션을 만족하는 해당 위치의 설정 파일을 선택
5. 위치가 Local machine일 경우 찾아보기 버튼 클릭하여 암호화 옵션을 만족하는 파일 선택
6. **[Import]** 버튼을 클릭

9.7 Security Profile

VTS II를 운영하는 보안 정책을 설정합니다. VTS II 서비스에 관련된 보안, 네트워크 보안, 개별 포트의 연결에 대한 보안등의 시스템 보안 및 패스워드 관리를 통한 보안등에 관한 정책을 결정합니다.

시큐리티 프로파일은 다음과 같이 2개 그룹으로 분류됩니다.

1. System security
2. Password security

9.7.1 System security

VTS II 서비스, 네트워크, 개별 포트의 연결과 관련한 시스템 보안에 관한 정책을 결정합니다. 그림 9-11은 시스템 시큐리티 프로파일 설정 화면입니다.

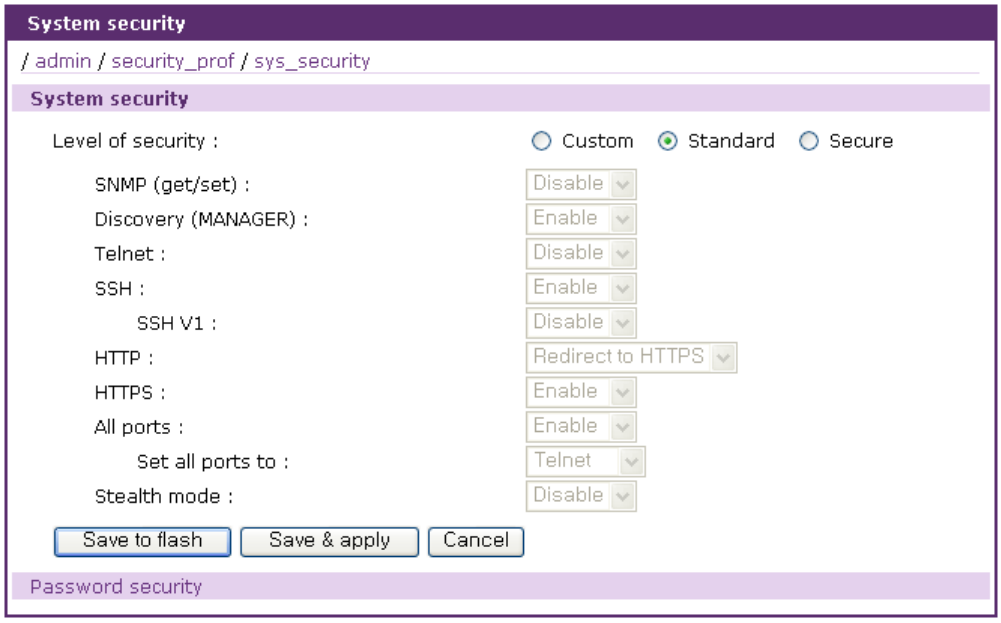


그림 9-11. Security profile – System security

설정 가능한 파라미터는 다음과 같습니다.

Level of security

SNMP (get/set)

Discovery(MANAGER)

Telnet

SSH

SSH V1

HTTP

HTTPS

All ports

Set all ports to

Stealth mode

Level of security

보안 수준을 설정합니다. Custom으로 설정되면 각각의 보안 항목을 사용자가 지정할 수 있습니다. Standard 또는 Secure로 설정되면 해당 보안 수준에 해당하는 값으로 자동 설정 됩니다. Factory default로 재설정하면 보안 수준은 Standard로 설정됩니다. 보안 수준별 보안 항목의 값은 다음과 같습니다.

Security Item	Custom	Standard	Secure
SNMP (get/set)	Configurable	Disable	Disable
Discovery (MANAGER)	Configurable	Enable	Disable
Telnet	Configurable	Disable	Disable
SSH	Configurable	Enable	Enable
SSH V1	Configurable	Disable	Disable
HTTP	Configurable	Redirect to HTTPS	Disable
HTTPS	Configurable	Enable	Enable
All ports	Configurable	Any	Any
Set all ports to	Configurable	Any	SSH
Stealth mode	Configurable	Disable	Enable

SNMP (get/set)

SNMP 프로토콜을 통해 VTS II의 상태를 변경하거나 조회하는 서비스를 제공할 지 여부를 설정합니다.

Discovery(MANAGER)

VTS II Manager에서 네트워크에 연결되어 있는 VTS II를 찾기 위한 요구에 대해 응답할 것인지 여부를 설정합니다.

Telnet

Telnet console을 통해 VTS II에 접근하는 것을 허용할 지 여부를 결정합니다. 다음의 IP 필터링 규칙을 추가하거나 변경하여 지원합니다.

상태	Interface	Option	IP address/Mask	Protocol	Port	Chain rule

Disable	all	Normal	anywhere	Telnet	23	DROP
Enable	all	Normal	anywhere	Telnet	23	ACCEPT

IP 필터링 규칙에 대한 자세한 내용은 ***3.5 IP 필터링***을 참조하시기 바랍니다.

SSH

SSH console을 통해 VTS II에 접근하는 것을 허용할 지 여부를 결정합니다. 다음의 IP 필터링 규칙을 추가하거나 변경하여 지원합니다.

상태	Interface	Option	IP address/Mask	Protocol	Port	Chain rule
Disable	all	Normal	anywhere	SSH	22	DROP
Enable	all	Normal	anywhere	SSH	22	ACCEPT

IP 필터링 규칙에 대한 자세한 내용은 ***3.5 IP 필터링***을 참조하시기 바랍니다.

SSH V1

SSH 버전1 프로토콜을 지원할 지 여부를 설정합니다. Disable로 설정할 경우 SSH 버전2만 지원됩니다.

HTTP

HTTP 프로토콜을 통한 웹 서비스를 제공할 지 여부를 설정합니다. 다음의 IP 필터링 규칙을 추가하거나 변경하여 지원합니다.

상태	Interface	Option	IP address/Mask	Protocol	Port	Chain rule
Disable	All	Normal	anywhere	HTTP	HTTP Port	DROP
Enable or Redirect to HTTPS	All	Normal	anywhere	HTTP	HTTP Port	ACCEPT

IP 필터링 규칙에 대한 자세한 내용은 ***3.5 IP 필터링***을 참조하시기 바랍니다. Redirect to HTTPS로 설정되면 HTTP를 통한 웹 인터페이스 연결은 HTTPS로 연결하도록 유도합니다.

HTTPS

HTTPS 프로토콜을 통한 웹 서비스를 제공할 지 여부를 설정합니다. 다음의 IP 필터링 규칙을 추가하거나 변경하여 지원합니다.

상태	Interface	Option	IP address/Mask	Protocol	Port	Chain rule
Disable	all	Normal	anywhere	HTTPS	HTTPS Port	DROP
Enable	all	Normal	anywhere	HTTPS	HTTPS Port	ACCEPT

IP 필터링 규칙에 대한 자세한 내용은 ***3.5 IP 필터링***을 참조하시기 바랍니다.

All ports

모든 시리얼 포트 및 원격 포트의 연결을 제공할 지 여부를 설정합니다. 다음의 IP 필터링 규칙을

추가하거나 변경하여 지원합니다.

상태	Interface	Option	IP address/Mask	Protocol	Port	Chain rule
Disable	all	Normal	anywhere	PORT	All ports	DROP
Enable	all	Normal	anywhere	PORT	All ports	ACCEPT

IP 필터링 규칙에 대한 자세한 내용은 ***3.5 IP 필터링***을 참조하시기 바랍니다.

Set all ports to

Port access menu와 시리얼 포트 및 원격 포트로 연결할 수 있는 프로토콜을 설정합니다. Telnet 또는 SSH로 설정되면 포트 액세스 메뉴 설정의 **Port access menu protocol** 파라미터와 시리얼 포트 및 원격 포트의 Host mode 설정 중 **Protocol** 파라미터를 Telnet 또는 SSH로 변경합니다. RawTCP로 설정되면 Port access menu는 변경하지 않고 시리얼 포트와 원격 포트의 설정만 RawTCP로 변경합니다. 자세한 내용은 ***4.2 Port access menu 설정***과 ***4.5.5 Host mode 설정***을 참조하시기 바랍니다.

Stealth mode

Stealth mode가 Enable로 설정되면, 클라이언트가 지원하지 않는 포트로 연결을 시도할 경우 VTS II가 연결 거부하지 않고 응답을 하지 않습니다.

9.7.2 Password Security

사용자 패스워드 관리를 통한 보안 정책을 설정합니다. 그림 9-12은 패스워드 시큐리티 설정 화면입니다.

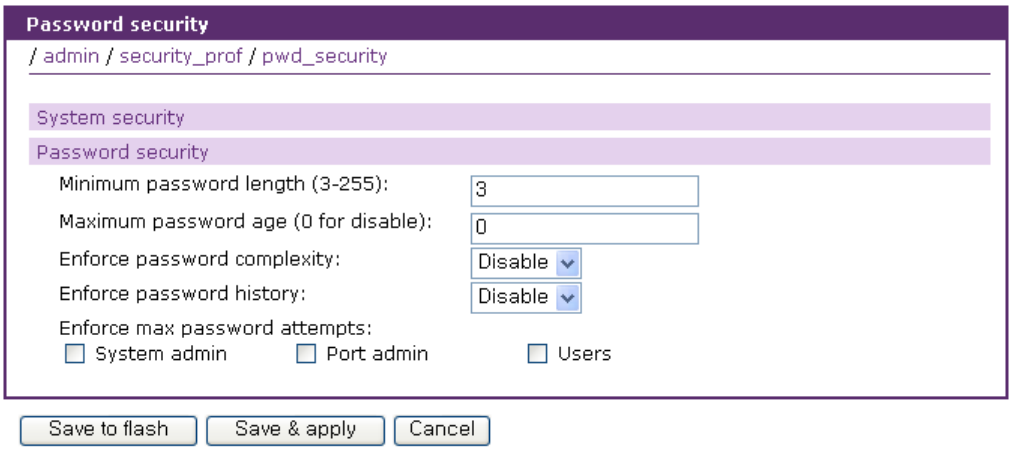


그림 9-12. Security profile – Password security

설정 가능한 파라미터는 다음과 같습니다.

Minimum password length

Maximum password age

Enforce password complexity

Enforce password history

Enforce max password attempts

Minimum password length

패스워드 변경시 패스워드 길이의 최소값을 설정합니다.

Maximum password age

패스워드 유효기간을 설정합니다. 이 유효기간이 지나면 패스워드 변경할 때까지 VTS II 이용이 제한됩니다.

Enforce password complexity

단순한 패스워드 사용을 제한하는데 사용합니다. Enable로 설정되면 패스워드는 다음의 조건을 만족해야 합니다.

1. 길이가 최소 8자 이상이어야 합니다.
2. 적어도 한 자 이상의 대문자, 소문자, 숫자, 특수문자를 포함해야 합니다.
3. 6자 이상의 문자는 2번 이상 사용되지 않아야 합니다.
4. 연속된 문자나 숫자는 사용되지 않아야 합니다.
5. 사용자 이름을 포함해서는 안 됩니다.

Enforce password history

패스워드 변경시 이전 10개의 패스워드 목록에 있는 패스워드와 일치하는 패스워드 사용을 제한합니다.

Enforce max password attempts

사용자 그룹별로 패스워드 인증 시도 횟수를 제한합니다. 설정된 사용자 그룹의 사용자가 3번이상 패스워드를 잘못 입력하면 해당 사용자는 관리자가 유효한 조치를 취하기 전까지 VTS II 이용이 제한됩니다.

9.8 Firmware Upgrade

Firmware는 시스템 콘솔, Telnet 콘솔 또는 웹 인터페이스를 통해 업그레이드할 수 있습니다. 세나 웹 사이트의 다운로드 페이지(**http://www.sena.com/korean/support/downloads**)에서 항상 최신의 firmware를 업그레이드를 할 수 있습니다. VTS II는 부팅시 자동으로 Firmware 및 설정을 자동으로 업그레이드하는 기능을 제공합니다. automatic firmware and configuration 부분을 설정하면 VTS II는 부팅할 때 Firmware와 설정이 새로운 버전인지 확인한 후 필요하면 새로운 버전 으로 업그레이드 합니다. 그림 9-13에 firmware upgrade 웹 인터페이스 화면을 나타내었습니다.

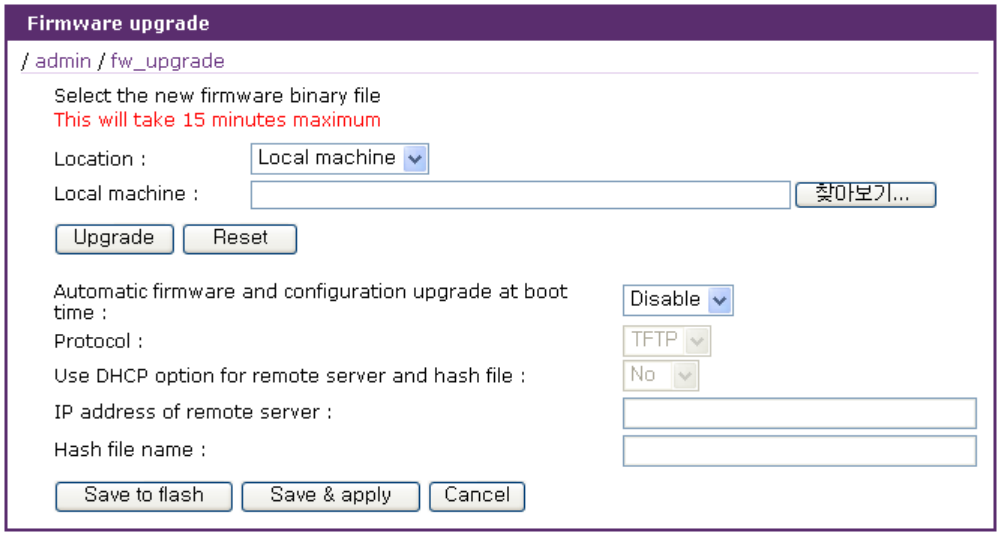


그림 9-13. Firmware upgrade

웹을 통해 firmware를 업그레이드하려면 다음을 수행하십시오.

1. Firmware 를 세나 다운로드 사이트에서 다운로드하여 사용자의 PC에 저장합니다.
2. “Location”을 “Local machine”으로 선택합니다.
3. “찾아보기” 버튼을 클릭하여 다운받은 Firmware 파일을 선택합니다.
4. “Upgrade” 버튼을 선택하여 업그레이드합니다..
5. 업그레이드가 완료되면 시스템이 재부팅되고 변경 사항이 적용됩니다.

VTS II의 CF card를 이용해 업그레이드하려면 다음을 수행하십시오.

1. “Location”을 “CF card”로 선택합니다.
2. “----- Select File -----“ 리스트 박스에서 Firmware를 선택합니다.
3. “Upgrade” 버튼을 선택하여 업그레이드합니다.
4. 업그레이드가 완료되면 시스템이 재부팅되고 변경 사항이 적용됩니다.

VTS II의 USB storage를 이용해 업그레이드하려면 다음을 수행하십시오.

1. “Location”을 “USB storage”로 선택합니다.
2. “----- Select File -----“ 리스트 박스에서 Firmware를 선택합니다.
3. “Upgrade” 버튼을 선택하여 업그레이드합니다.
4. 업그레이드가 완료되면 시스템이 재부팅되고 변경 사항이 적용됩니다.

사용자가 firmware를 업그레이드 하기 위해 원격 또는 시리얼 콘솔을 사용하려면 Telnet/SSH 또는 터미널 에뮬레이션 프로그램이 반드시 Zmodem 전송 프로토콜을 지원해야 합니다. Firmware upgrade가 되더라도 사용자의 설정은 그대로 유지됩니다.

콘솔을 통해 Firmware를 업그레이드하려면 다음을 수행하십시오.

1. Firmware 를 세나 다운로드 사이트에서 다운로드하여 사용자의 PC에 저장합니다.
2. 터미널 에뮬레이션 프로그램을 사용하여, Telnet/SSH 또는 시리얼 콘솔 포트에 연결합니다. (시리얼 콘솔 포트를 이용할 경우 상당히 오래 걸리므로, Telnet 또는 SSH를

사용하기를 권장합니다.)

3. 그림 9-14과 같이 Firmware upgrade 메뉴를 선택합니다.
4. 그림 9-15과 같이 지침에 따라 Zmodem 프로토콜을 사용하여 firmware 파일을 전송합니다. CF card 혹은 USB storage를 통해 업그레이드 하려면 “Location”을 “CF Card”나 “USB storage”로 선택하고 파일명을 입력하면 됩니다.
5. 업그레이드가 완료되면, 시스템을 재부팅하여 변경 사항을 적용합니다.

```
Sena_VTSII login: admin
Password:

------------------------------------------------------------------------------
 Welcome to VTSII-4800 configuration page
 Current time   : 09/06/2006 03:31:05    Serial No.     :
 F/W Rev.       : v1.0.1rc1              Bios Ver.      : v1.0.0
 MAC addr.(eth0): 00-AA-95-AA-AA-AA      IP addr.(eth0) : 192.168.21.48
------------------------------------------------------------------------------
 1. Network
 2. Serial port
 3. Clustering
 4. Power controller
 5. Peripherals
 6. System status & log
 7. System administration
 8. Activate Locator LED

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 7

------------------------------------------------------------------------------
 System administration
 /admin
------------------------------------------------------------------------------
 1. User administration
 2. Access lists
 3. Change password
 4. Device name              : Sena_VTSII
 5. Date and time
 6. Configuration management
 7. Security profile
 8. Firmware upgrade
 9. CLI configuration

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 8

------------------------------------------------------------------------------
 Firmware upgrade
 /admin/fw_upgrade
------------------------------------------------------------------------------
 1. Firmware upgrade
 2. Automatic firmware and configuration upgrade at boottime : Disable

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 1

------------------------------------------------------------------------------
 Firmware upgrade
 /admin/fw_upgrade/fw_upgrade
------------------------------------------------------------------------------
 1. Location               :
```

```
 2. Upgrade

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 1

-------------------------------------------------------------------------------
 Location
 /admin/fw_upgrade/fw_upgrade/location
-------------------------------------------------------------------------------
 1. Local machine
 2. CF Card
 3. USB storage

SELECT> 1

-------------------------------------------------------------------------------
 Firmware upgrade
 /admin/fw_upgrade/fw_upgrade
-------------------------------------------------------------------------------
 1. Location                : Local machine
 2. Upgrade

[h]elp, [s]ave, [a]pply, e[x]it, [r]eboot
COMMAND (Display HELP : help)> 2
Do you want to upgrade firmware? (y, n) : y
Preparing for firmware upgrade. Wait a moment...
 Now starting firmware upgrade...
 Please log out and Do NOT access system.
Transfer firmware by zmodem using your terminal application.
** B0ff000005b157
```

그림 9-14. 원격/시리얼 콘솔을 이용한 firmware upgrade

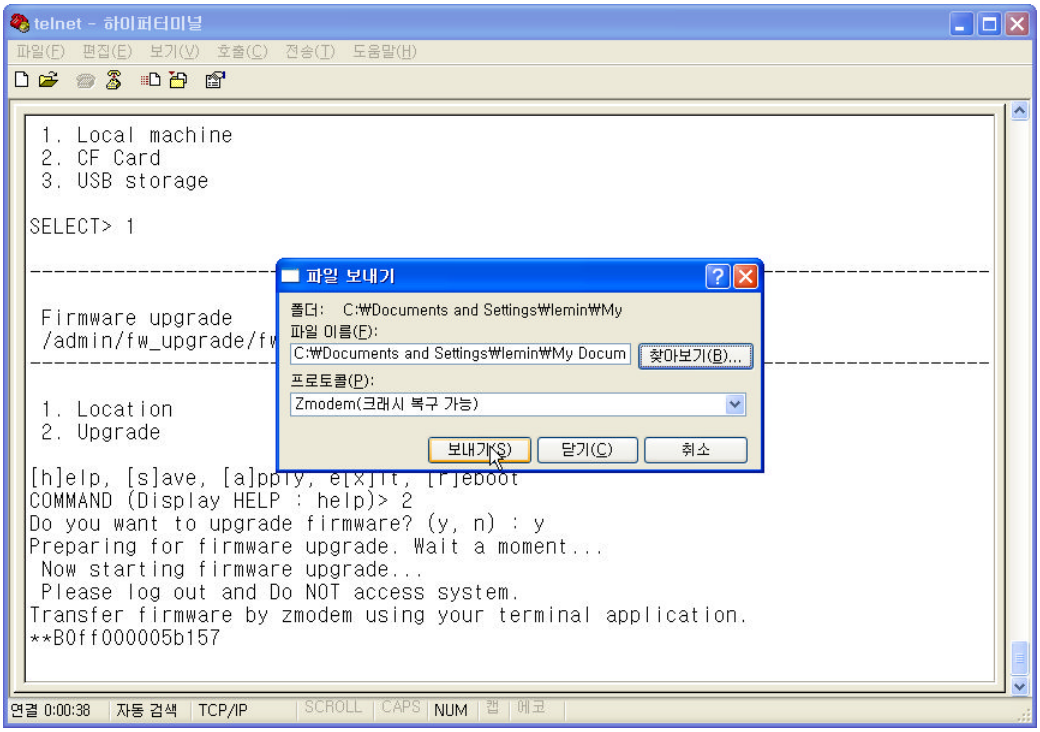


그림 9-15. Zmodem을 이용한 firmware 파일 전송 (Hyper Terminal)

부팅할 때 Firmware 및 설정을 업그레이드하거나 사용자가 원하는 파일을 업로드하거나 지정한 명령을 실행하는 기능을 제공합니다. 이 기능을 사용하려면 사용자는 다음의 파라미터를 설정해야 합니다.

Automatic firmware and configuration upgrade at boot time

자동 업그레이드 기능을 사용할 지 여부를 결정합니다.

Protocol

업그레이드할 때 원격호스트와 통신하기 위해 VTS II가 어떤 프로토콜을 사용할 지를 결정합니다.

Use DHCP option for remote server and hash file

자동 업그레이드할 때 요구되는 원격 호스트의 IP 주소와 해쉬 파일 이름을 찾는 방법을 설정합니다. Yes로 설정되면 VTS II의 DHCP 요청에 대한 DHCP 응답에서 찾은 원격호스트 IP 주소와 해쉬 파일 이름을 이용하고, No로 설정되면 **IP address of remote server**와 **Hash file name**의 설정을 이용하여 자동 업그레이드를 실행합니다.

IP address of remote server

VTS II가 해쉬 파일, Firmware 이미지 파일 및 설정 파일을 얻기 위해 접속해야 하는 원격 호스트의 IP 주소를 설정합니다.

Hash file name

업그레이드할 Firmware 이미지 파일과 설정 파일을 명시하는 해쉬 파일의 이름을 설정합니다. VTS II는 해쉬 파일에 기록된 모델이름, 버전을 대상 VTS II의 모델이름, Firmware 버전과 비교하여 업그레이드가 필요한지 아닌지를 결정합니다. 해쉬 파일의 형식은 다음과 같습니다.

<TYPE>,<NAME>,<MODEL>,<VERSION>

또는

<TYPE>,<NAME>,<Options for file uploading>,<Path to upload>

또는

<TYPE><COMMAND>

여기서 <TYPE> - 1:Firmware 이미지 2:설정 (1 byte)

<NAME> - Firmware 이미지 파일 또는 설정 파일의 이름

<MODEL> - VTSII800, VTSII1600, VTSII3200, VTSII4800등의 VTS II의 모델 이름

<VERSION> - Firmware 또는 설정파일의 버전

Firmware 이미지의 경우 Firmware 이미지 파일의 버전과 같은 버전을 표시해야 하고, 설정의 경우 Firmware 버전과 유사한 형식으로 사용자가 할당한 버전을 표시합니다.

또는 <TYPE> - 3:사용자 파일 업로드

<NAME> - 업로드 대상 파일이름

<Options to file uploading> - [F][X][X]U

F : forced copy(remove if there is same file already)

X : uncompress the file to the specified location

Z : unzip the file to the specified location

U : default option for file uploading

<Path to upload> - 대상 파일이 업로드 되어야 할 디렉토리 경로

또는 <TYPE> - 4:사용자 명령 실행

<COMMAND> - 실행할 명령

다음은 해쉬 파일의 예를 보여줍니다.

```
1,vtsII32.img,VTSII3200,v1.5.0
2,vtsII32.syscm,VTSII3200,v1.0.0
3,test_hash.tar,FXU,/mnt/flash
3,active_detect.tar.gz,FXZU,/mnt/flash
4,mkdir /tmp/test
```

9.9 CLI 설정

시리얼 콘솔, Telnet/SSH 원격 콘솔등의 CLI에 로그인할 때 사용자 인증 방법을 선택합니다. 현재 VTS II는 Local, RADIUS server, RADIUS server – Local, Local - RADIUS server, RADIUS down – Local, TACACS+ server, TACACS+ server – Local, Local - TACACS+ server, TACACS+ down – Local, LDAP server, LDAP server – Local, Local - LDAP server, LDAP down – Local, Kerberos server, Kerberos server – Local, Local - Kerberos server 등의 Linux-PAM (Pluggable Authentication Modules for Linux)을 이용한 다양한 인증 방법을 지원합니다.
인증 방법에 대한 자세한 내용은 ***4.5.10 Authentication 설정***을 참조하시기 바랍니다.

그림 9-16는 웹 인터페이스를 통한 CLI 설정 화면을 보여줍니다.
CLI configuration menu를 일정 시간이 경과할 동안 사용하지 않으면 프로그램을 종료하도록 Timeout for CLI configuration menu를 설정할 수 있습니다. 0으로 설정되면 프로그램이 종료되지 않습니다.

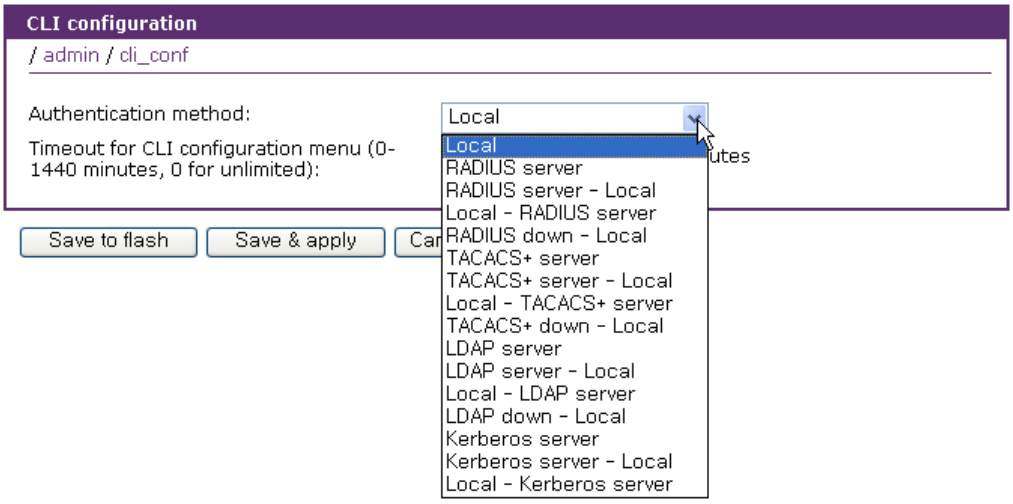

CLI configuration
/ admin / cli_conf
Authentication method:
Local
Timeout for CLI configuration menu (0-1440 minutes, 0 for unlimited):
utes
Local
RADIUS server
RADIUS server - Local
Local - RADIUS server
RADIUS down - Local
TACACS+ server
TACACS+ server - Local
Local - TACACS+ server
TACACS+ down - Local
LDAP server
LDAP server - Local
Local - LDAP server
LDAP down - Local
Kerberos server
Kerberos server - Local
Local - Kerberos server
Save to flash
Save & apply
Can

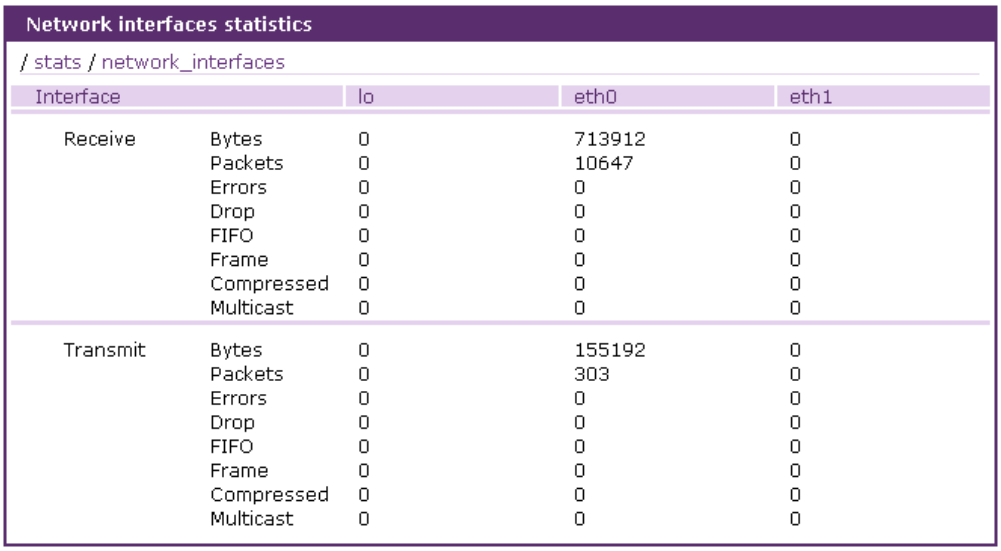
그림 9-16. CLI 설정

10: 시스템 통계

VTS II의 웹 인터페이스는 시스템 통계 화면을 제공합니다. 사용자는 시스템 통계 화면을 참조하여 VTS II 메모리에 저장된 통계 데이터를 확인할 수 있습니다. 네트워크 인터페이스 및 시리얼 포트 통계는 link layer, **lo**, **eth** 와 시리얼 포트에 대한 사용 통계를 나타냅니다. IP, ICMP, TCP 및 UDP 통계는 TCP/IP 프로토콜의 4개의 기본 구성 요소들에 대한 사용 통계를 나타냅니다.

10.1 네트워크 인터페이스 (Network interfaces) 통계

네트워크 인터페이스 통계는 VTS II의 local loop back interface 인 **lo** 및 VTS II의 기본 네트워크 인터페이스인 **eth0** 대한 기본 네트워크 인터페이스 사용을 나타냅니다.



Network interfaces statistics

/ stats / network_interfaces

Interface		lo	eth0	eth1
Receive	Bytes	0	713912	0
	Packets	0	10647	0
	Errors	0	0	0
	Drop	0	0	0
	FIFO	0	0	0
	Frame	0	0	0
	Compressed	0	0	0
	Multicast	0	0	0
Transmit	Bytes	0	155192	0
	Packets	0	303	0
	Errors	0	0	0
	Drop	0	0	0
	FIFO	0	0	0
	Frame	0	0	0
	Compressed	0	0	0
	Multicast	0	0	0

그림 10-1. 네트워크 인터페이스 상태

10.2 시리얼 포트 통계

시리얼 포트 통계는 시리얼 포트의 사용 통계, Baud rate 설정 및 각 포트의 핀 상태를 나타냅니다. (: On : Off)

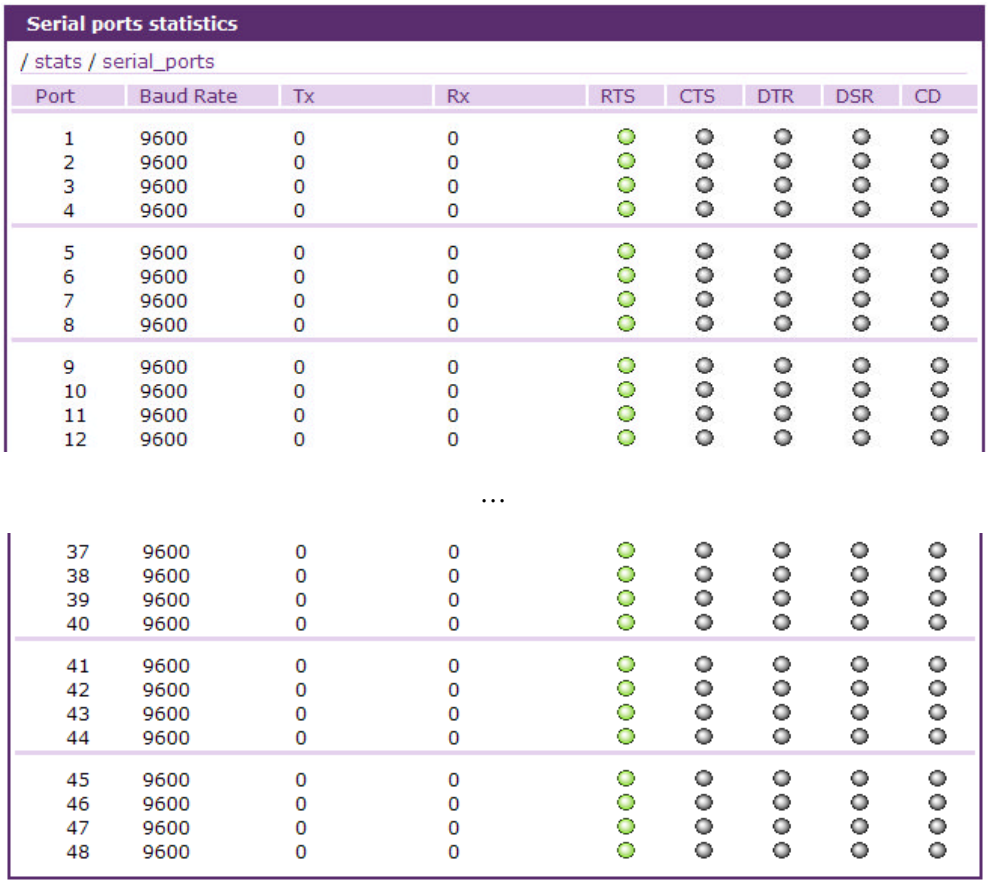


그림 10-2. 시리얼 포트 상태

10.3 IP 통계

IP 통계 화면은 IP 프로토콜을 사용하여 패킷/연결에 대한 상태 정보를 제공합니다.
지원되는 각각의 파라미터에 대한 정의 및 설명은 다음과 같습니다

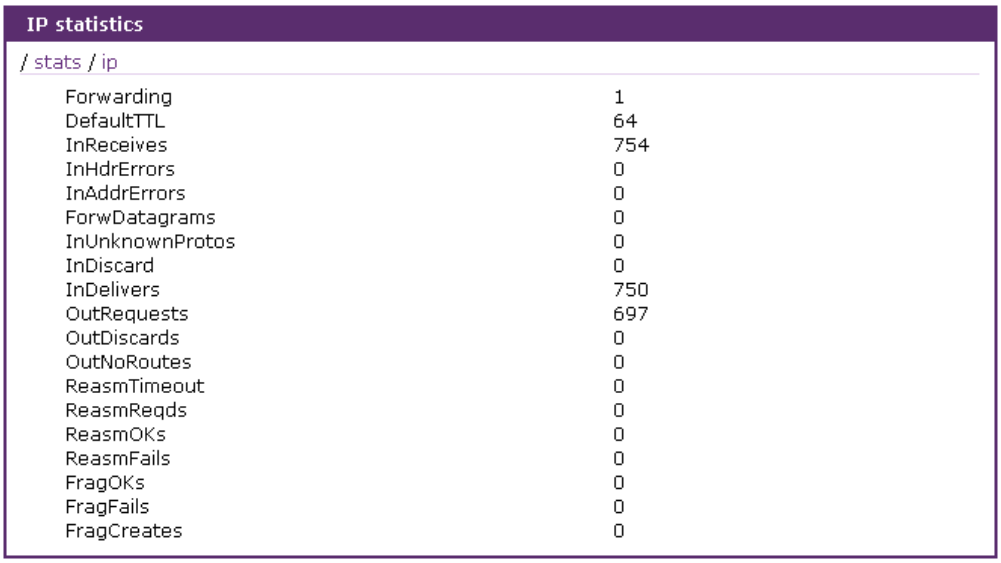


그림 10-3. IP 상태

Forwarding:

IP forwarding이 Enable 또는 Disable 상태인지 여부

DefaultTTL :

기본 TTL(Time To Live)

InReceives :

수신된 데이터그램 수

InHdrErrors :

헤더 오류가 있다고 수신된 데이터그램의 수

InAddrErrors :

주소 오류가 있다고 수신된 데이터그램의 수

ForwDatagrams :

Forwarding 된 데이터그램의 수

InUnknownProtos :

인식되지 않고 또는 지원되지 않은 프로토콜이기 때문에 무시되었지만 성공적으로 수신된 데이터그램의 수

InDiscard :

프로토콜 상의 별 문제는 발견되지 않았지만 무시된(예를 들어, 버퍼 공간의 부족의 원인) 입력 IP 데이터그램의 수

InDelivers :

전달된 수신 데이터그램의 수

OutRequests :

전송하도록 요청된 출력 데이터그램의 수. Forwarding 된 데이터그램의 수는 제외함.

OutDiscards :

무시된 출력 데이터그램의 수

OutNoRoutes :

destination IP 주소에 전송하기 위한 경로가 발견되지 않은 데이터그램의 수. 이런 데이터그램은 폐기 처분됩니다.

ReasmTimeout :

데이터그램 일부가 도착한 후, 나머지 데이터그램들이 도착해야하는 허용 시간. 전부가 해당 시간에 도착하지 않은 경우, 데이터그램은 폐기 처분됨.

ReasmReqds :

재생이 필요한 데이터그램의 수

ReasmOKs :

성공적으로 재생된 데이터그램의 수

ReasmFails :

재생될 수 없는 데이터그램의 수.

FragOKs :

성공적으로 fragmentation 된 데이터 그램의 수

FragFails :

fragmentation 실패한 데이터그램의 수

FragCreates :

생성된 fragment 수

10.4 ICMP 통계

ICMP 통계 화면은 ICMP 프로토콜의 사용 통계 정보를 제공합니다. 각 파라미터의 정의 및 설명은 다음과 같습니다.

InMsgs, OutMsgs :

수신 또는 전송된 메시지 수

InErrors, OutErrors :

수신 또는 전송된 오류 수

InDestUnreachs, OutDestUnreachs :

수신 또는 전송된 목적지에 도달하지 못한 메시지의 수

InTimeExcds, OutTimeExcds :

time-to-live(TTL)를 초과하는 수신 또는 전송된 메시지의 수

InParmProbs, OutParmProbs :

수신 또는 전송된 메시지 중 파라미터에 오류가 발생한 메시지의 수

InSrcQuenchs, OutSrcQuenchs :

수신 또는 전송된 소스 Quench 메시지의 수

InRedirects, OutRedirects :

수신 또는 전송되는 Redirection 메시지의 수

InEchos, OutEchos :

송신 또는 수신된 echo 요청의 수

NEchoReps, OutEchoReps :

송신 또는 수신된 echo 응답의 수

InTimestamps, OutTimestamps :

수신 또는 전송된 time-stamp 요청의 수

InTimestampReps, OutTimestampReps :

수신 또는 전송된 time-stamp 응답의 수

InAddrMasks, OutAddrMasks :

수신 또는 전송된 주소 마스크의 수

InAddrMaskReps, OutAddrMaskReps :

수신 또는 전송된 주소 마스크 응답의 수

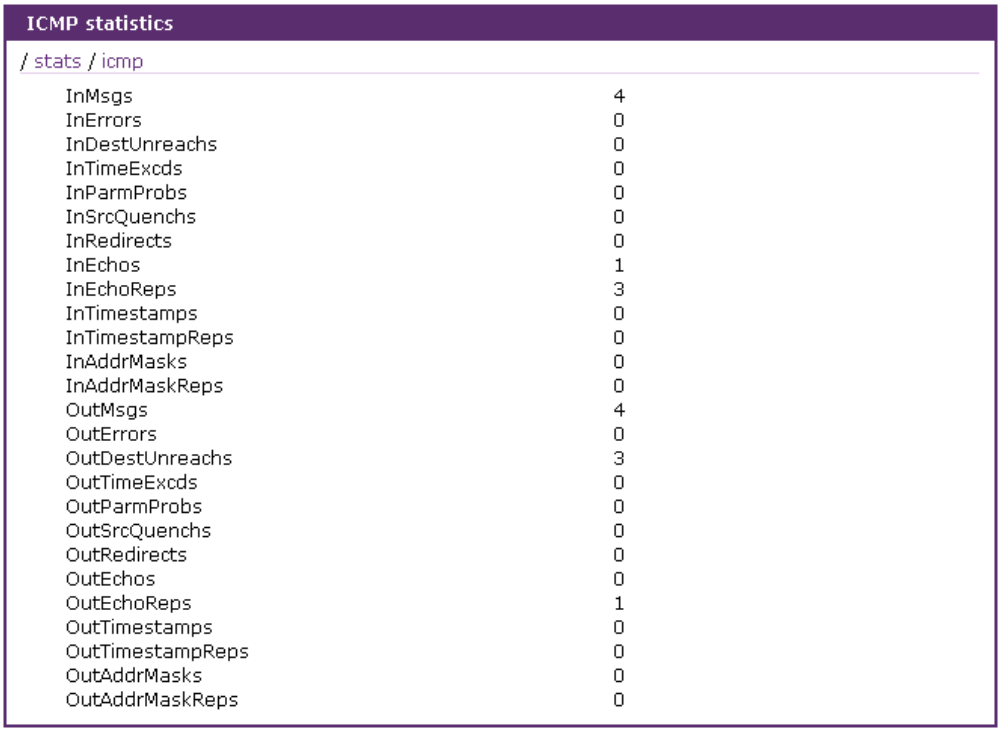


그림 10-4. ICMP 상태

10.5 TCP 통계

TCP 통계 화면은 TCP 프로토콜의 사용 통계 정보를 제공합니다. 각 파라미터의 정의 및 설명은 다음과 같습니다.

RtoAlgorithm :

사용 중인 retransmission time-out (RTO) 알고리즘. 재전송 알고리즘은 다음의 값 중 하나를 가짐.

0 : CONSTANT - Constant Time-out

1: RSRE - MIL-STD-1778 Appendix B

2: VANJ - Van Jacobson's Algorithm

3: OTHER - Other

RtoMin :

최소 RTO 값 (ms).

RtoMax :

최대 RTO 값 (ms)

MaxConn :

최대 연결 세션 수

ActiveOpens :

능동적인 연결의 수. 능동적인 연결은 클라이언트의 경우.

PassiveOpens :

수동적인 연결의 수. 수동적인 연결은 서버의 경우.

AttemptFails :

실패한 연결 시도에 대한 수

EstabResets :

재설정으로 성립된 연결의 수

CurrEstab :

현재 성립된 연결 수

InSegs :

수신된 segment 수

OutSegs :

전송된 segment 수. 재전송된 segment는 포함되지 않음.

RetransSegs :

재전송된 세그먼트 수

RetransSegs :

재전송된 세그먼트 중 오류의 개수

OutRsts :

Reset 플래그가 설정되어 전송된 세그먼트의 수

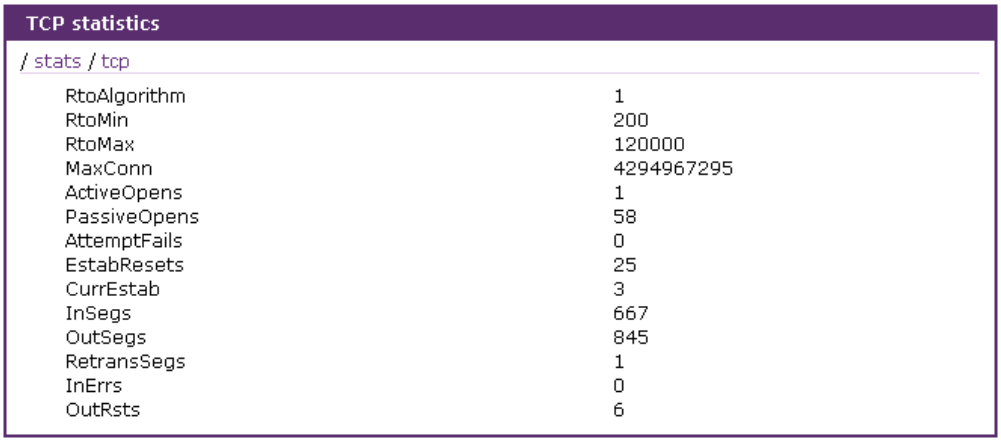


그림 10-5. TCP 상태

10.6 UDP 통계

UDP 상태 화면은 UDP 프로토콜의 사용 통계 정보를 제공합니다. 각 파라미터의 정의 및 설명은 다음과 같습니다.

InDatagrams :

수신된 데이터그램의 수

NoPorts :

지정된 포트가 유효하지 않아 폐기 처분된 수신 데이터그램의 수

InErrors :

수신된 오류 데이터그램의 수

OutDatagrams :

전송된 데이터그램의 수

그림 10-6. UDP 상태

11: CLI 안내서

11.1 서론

root 또는 **System admin** 은 시스템 콘솔 또는 Telnet/SSH 원격 콘솔을 통해 VTS II의 Linux 콘솔 커맨드라인 인터페이스(CLI)에 접속 할 수 있습니다. CLI 에서 인증된 사용자는 표준 Linux 명령을 통하여 VTS II 상태를 감시하고, 설정을 편집하고 변경 사항을 적용하고, 사용자 정의 script를 실행하며 원격 호스트로부터 파일을 다운로드 받을 수도 있습니다.
VTS II는 내부 플래시 메모리에서 읽고/쓸 수 있도록 /usr2에 16 MB의 사용자 공간을 제공합니다. 사용자 공간에서, 사용자는 자신이 제작한 shell script를 실행할 수 있으며, 작성한 프로그램를 실행할 수도 있습니다.
root 사용자는 시스템 콘솔 또는 Telnet/SSH 클라이언트를 사용하여 CLI 에 접속할 수 있습니다. **System admin**은 CLI에 제한된 권한을 가지고 접속할 수 있습니다.
root 사용자의 Telnet 원격/시리얼 콘솔 연결을 제한하려면 /etc/pam.d/login 파일에 있는 아래 줄을 추가하십시오.

```
auth       requisite  pam_securetty.so
```

root 사용자의 SSH 원격/시리얼 콘솔 연결을 제한하려면 /etc/ssh/sshd_config 파일에 있는 아래 설정을 변경하십시오.

```
#PermitRootLogin yes => PermitRootLogin no.
```

위의 설정을 SSH 데몬에 적용하기 위해 다음의 명령을 실행하십시오.

```
[root@loclahost ~] killall –HUP sshd
```

시스템 콘솔에 다이얼인 모뎀을 연결하여 모뎀 접속을 통해 CLI에 접속할 수도 있습니다. 이 기능을 이용하려면, ***11.8 모뎀을 이용하여 시리얼 콘솔에 연결하기***와 같이 rc.user 파일을 수정한 후 시스템을 재부팅 하여 변경 내용을 반영해야 합니다.

11.2 플래시 구성

VTS II 내부 플래시는 아래의 표와 같이 구성됩니다. 사용자는 Mtdblock5에 자유롭게 접속할 수 있는데, 이는 /usr2에 마운트되어 있습니다. 사용자는 /etc, /var 및 /temp 파일에 접근할 수 있습니다. 재부팅한 후 이런 파일에 단순히 접근하는 것은 VTS II에 영향을 주지 않습니다. 그러나, 만일 사용자가 파일들에 접근을 하고 saveconf 명령을 실행한다면, 설정 파일은 변경되어 내부 플래시 메모리 영역으로 저장되며, 재부팅하면 이 내용이 적용되게 됩니다. 따라서, 유효하지 않게 변경하면 VTS II가 올바르게 동작하지 않을 수 있습니다. 최악의 경우, VTS II가 작동하지 않을

수도 있습니다.

블록	유형	마운트 지점	크기(KB)
Mtdblock0	Bootloader	none	384
Mtdblock1	Kernel	none	2048
Mtdblock2	램 디스크 이미지(7.5MB)	/etc, /home, /tmp, /var	256
Mtdblock3	CRAMFS (읽기 전용)	/	30080
Mtdblock4	CRAMFS (읽기 전용)	/opt	16384
Mtdblock5	JFFS2 (R/W)	/usr2	16384
합계			65536

Note : CLI에서 `mount` 또는 `dd` 명령어를 사용하여 각각의 `mtdblock`에 접근하지 마십시오. VTS II가 작동하지 않을 수도 있습니다.

11.3 지원되는 Linux 유틸리티

11.3.1 Shell 및 Shell 유틸리티:

```
sh, ash, bash, echo, env, false, grep, more, sed, which, pwd
```

11.3.2 파일 및 디스크 유틸리티:

```
ls, cp, mv, rm, mkdir, rmdir, ln, mknod, chmod, touch, sync,
gunzip, gzip, zcat, tar, dd, df, du, find, cat, vi, tail,
mkdosfs, mke2fs, e2fsck, fsck, mount, umount, scp
```

11.3.3 시스템 유틸리티:

```
date, free, hostname, sleep, stty, uname, reset,
insmod, rmmod, lsmod, modprobe,
kill, killall, ps, halt, shutdown, poweroff, reboot, telinit, init,
useradd, userdel, usermod, whoami, who, passwd, id, su
```

11.3.4 네트워크 유틸리티:

```
ifconfig, iptables, route, telnet, ftp, ssh, ping
```

11.4 CLI 접속하기

11.4.1 root 로 CLI 접속하기

시스템 콘솔:

1) PC의 시리얼 포트와 VTS II의 콘솔 포트를 연결합니다.
2) PC용 터미널 에뮬레이션 프로그램을 실행합니다.
3) PC의 시리얼 포트를 다음과 같이 설정합니다: 9600-8-N-1 No flow control

4) <enter>를 누릅니다.

5) VTS II root 계정으로 로그인합니다.

Telnet/SSH 콘솔:

1) `telnet VTSII_ip_address or`

2) `ssh root@VTSII_ip_address`

11.4.2 System admin 으로 CLI 접속하기

System admin 설정

1) 접속 웹: **System administration > Users administration**

2) [Add user] 또는 [Edit user]

3) 선택 그룹 = System admin

4) shell 프로그램 = CLI

5) **[Add]** 또는 **[Submit]**

6) **System admin** 으로 로그인하여, 시리얼 콘솔 또는 SSH/Telnet 콘솔에 접속합니다.

11.5 CLI의 VTS II 설정 편집하기

11.5.1 설정 파일 저장/로드 동작:

1) VTS II는 부팅 시, `/home/config/cnf.tar.gz` 파일을 `/tmp/cnf/` 에 압축을 풀어 저장합니다.

2) 사용자가 설정을 변경하면, `/tmp/cnf/` 에 있는 파일들의 내용을 변경하게 됩니다.

3) 사용자가 웹에서 **[Save to flash],** 또는 CLI 내의 `saveconf` 명령을 이용하여, 설정을 저장하는 경우, VTS II는 변경된 파일들을 `/home/config/cnf.tar.gz` 로 다시 압축합니다.

11.5.2 CLI에서 설정 변경 방법:

CLI에서 VTS II의 설정을 변경하려면, 텍스트 기반의 메뉴 설정 유틸리티인 `configmenu` 를 실행하거나 다음과 같이 수동으로 설정합니다.

1) `vi` 명령을 사용해 해당되는 설정 파일을 편집합니다.
(설정 파일의 각 파라미터에 대한 자세한 설명은 부록 D: ***VTS II 설정 파일***을 참조하세요)

2) `saveconf` 유틸리티를 사용해 설정 파일을 플래쉬 메모리에 저장합니다.

3) `applyconf` 유틸리티를 사용해 모든 변경 사항을 시스템에 적용합니다.

```
[root@Sena_VTSII ~]# configmenu
or

[root@Sena_VTSII ~]# cd /tmp/cnf
[root@Sena_VTSII cnf]# vi ports/port1/portinfo.cnf
[root@Sena_VTSII cnf]# saveconf
[root@Sena_VTSII cnf]# applyconf
```

11.6 사용자 Script 실행하기

Shell script /usr2/rc.user는 VTS II가 부팅되면 자동으로 호출되어 실행됩니다. 사용자는 사용자 정의 script 또는 실행 프로그램을 실행하기 위해 rc.user 파일을 수정할 수 있습니다.

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#
#PATH=/bin:/usr/bin:/sbin:/usr/sbin
# Add shell command to execute from here

echo ‘This is the welcome message defined by users’exit 0
```

11.7 File 전송

사용자는 파일 전송을 위해 ftp 클라이언트 프로그램을 사용할 수 있고 프로그램을 다운받아 /usr2 디렉토리에 저장할 수 있습니다.

```
[root@Sena_VTSII ~]# cd /usr2
[root@Sena_VTSII usr2]# ftp 192.168.2.3
Connected to 192.168.2.3.
220 lxtoo.senalab.co.kr FTP server (Version wu-2.6.1-16) ready.
Name (192.168.2.3:root): sena
331 Password required for sena.
Password:
230 User sena logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get test.tgz
local: test.tgz remote: test.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for test.tgz (350 bytes).
226 Transfer complete.
350 bytes received in 0.04 secs (9.6 kB/s)
ftp> bye
```

또한 사용자는 scp 클라이언트 프로그램을 이용하여 Encrypt 된 상태로 파일을 복사할 수 있습니다. 사용자의 PC 에서 VTS II(192.168.0.120)에 있는 특정 파일을 복사하고 싶을 경우에는 다음과 같은 명령을 사용자 PC에서 실행 시켜 주면 됩니다.

```
[root@localhost work]# scp root@192.168.0.120:/usr2/rc.user /work
The authenticity of host '192.168.0.120 (192.168.0.120)' can't be established.
RSA key fingerprint is c1:70:ab:52:48:ab:e5:dc:47:9c:94:ed:99:6f:94:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.120' (RSA) to the list of known hosts.
root@192.168.0.120's password:
rc.user           100% |*****************************|   173      00:00
[root@localhost work]#
```

11.8 모뎀을 이용하여 시리얼 콘솔에 연결하기

사용자는 시리얼포트에 연결된 모뎀을 통해 시리얼 콘솔에 접근할 수 있습니다. /usr2/rc.user 에 다음과 같은 스키립트를 추가한 후 재부팅하여 스크립트가 자동 실행되도록하면 됩니다.

```
echo 9600 > /var/run/mgetty.console
```

여기서 9600은 시리얼 포트와 모뎀의 baud rate 입니다.

US Robotics 모뎀등과 같이 일부 모뎀에서는 다음의 스크립트를 추가해야 합니다.

```
echo “9600 &F&B1”> /var/run/mgetty.console
```

부록 A: 연결

A.1 Ethernet Pin out

VTS II는 AT&T 258 규격을 준수한 커넥터인 표준 Ethernet 커넥터를 사용합니다. 표 A-1은 핀 할당 및 전선 색상을 보여줍니다.

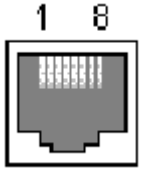


그림 A-1 RJ45 커넥터의 핀 배치

표 A-1 Ethernet용 RJ45 커넥터의 핀 할당

핀	설명	색상
1	Tx+	주황색과 흰색
2	Tx-	주황색
3	Rx+	녹색과 흰색
4	NC	청색
5	NC	청색과 흰색
6	Rx-	녹색
7	NC	갈색과 흰색
8	NC	갈색

A.2 콘솔 및 시리얼 포트 Pin out

VTS II는 콘솔 및 시리얼 포트 용 RJ45 커넥터를 사용합니다. 시리얼 포트용 RJ45 커넥터의 핀 지정은 표 A-2에 요약되어 있습니다. 각 핀에는 시리얼 통신 설정에 따른 기능이 있습니다.

표 A-2 시리얼 포트용 RJ45 커넥터 핀 할당

핀	설명
1	CTS
2	DSR
3	RxD
4	GND
5	DCD
6	TxD
7	DTR
8	RTS

A.3 케이블 다이어그램

장치	시리얼 포트 유형	용도
Cisco 장비  Sun Netra 서버 	RJ45	콘솔/Ethernet 케이블
Nortel 장비 기타 DB9 DTE 장치	DB9 male형	콘솔/Ethernet 케이블 + RJ45-DB9F cross-over 어댑터
Sun Sparc 서버  기타 DB25 DTE 장치	DB25 female형	콘솔/Ethernet 케이블 + RJ45-DB25M cross-over 어댑터
시리얼 프린터 DB25 DTE 장치	DB25 male형	콘솔/Ethernet 케이블 + RJ45-DB25F cross-over 어댑터
모뎀 ISDN 터미널 어댑터	DB25 male형	콘솔/Ethernet 케이블 + RJ45-DB25M straight 어댑터

RJ45-DB9 female adapter

Using RJ45 to DB9(Female) ***Cross-over*** *Cable*

Description (RJ45)	Internal Cable Color	RJ45 Pin No.	DB9 Pin No.	Description (DB9)
CTS	Blue	1	7	RTS
DSR	Orange	2	4	DTR
RXD	Black	3	3	TXD
GND	Red	4	5	GND
DCD	Green	5	1	DCD
TXD	Yellow	6	2	RXD
DTR	Brown	7	6	DSR
RTS	White	8	8	CTS

콘솔 케이블 + RJ45-DB9F 어댑터

RJ45-DB25 female adapter

Using RJ45 to DB25(Female) ***Cross-over*** *Cable*

Description (RJ45)	Internal Cable Color	RJ45 Pin No.	DB25 Pin No.	Description (DB25)
CTS	Blue	1	4	RTS
DSR	Orange	2	20	DTR
RXD	Black	3	2	TXD
GND	Red	4	7	GND
DCD	Green	5	8	DCD
TXD	Yellow	6	3	RXD
DTR	Brown	7	6	DSR
RTS	White	8	5	CTS

RJ45-DB25 male adapter

Using RJ45 to DB25(Male) ***Cross-over*** *Cable*

Description (RJ45)	Internal Cable Color	RJ45 Pin No.	DB25 Pin No.	Description (DB25)
CTS	Blue	1	4	RTS
DSR	Orange	2	20	DTR
RXD	Black	3	2	TXD
GND	Red	4	7	GND
DCD	Green	5	8	DCD
TXD	Yellow	6	3	RXD
DTR	Brown	7	6	DSR
RTS	White	8	5	CTS

RJ45-DB25 male adapter

Using RJ45 to DB25(Male) ***Straight*** *Cable*

Description (RJ45)	Internal Cable Color	RJ45 Pin No.		DB25 Pin No.	Description (DB25)
CTS	Blue	1	⟷	5	CTS
DSR	Orange	2	⟷	6	DSR
RXD	Black	3	⟷	3	RXD
GND	Red	4	⟷	7	GND
DCD	Green	5	⟷	8	DCD
TXD	Yellow	6	⟷	2	TXD
DTR	Brown	7	⟷	20	DTR
RTS	White	8	⟷	4	RTS

콘솔 케이블 + RJ45-DB25F/M 어댑터

부록 **B: VTS II**가 지원하는 **PC** 카드

VTS II 시리즈는 다음의 PC 카드를 지원합니다.

표 B-1 네트워크 카드

제조 업체	모델 이름	VTS II Probe 모델 이름	규격
3COM	3CXE589ET-AP	3Com Megahertz 589E TP/BNC LAN PC Card	10 Mbps LAN 카드
Linksys	Linksys EtherFast 10/100 Integrated PC Card (PCM100)	Linksys EtherFast 10/100 Integrated PC Card (PCM100) Ver 1.0	10/100 Mbps LAN 카드
Netgear	16bit PCMCIA Notebook Adapter FA411	NETGEAR FA411 Fast Ethernet	10/100 Mbps LAN card

표 B-2 무선 네트워크

제조 업체	모델 이름	VTS II Probe 모델 이름	규격

표 B-3 ATA/IDE Fixed Disk Card

제조 업체	모델 이름	VTS II Probe 모델 이름	규격
Advantech	CompactFlash	CF 48M	48 MB 저장 카드
SanDisk	SDP series	SunDisk SDP 5/3 0.6	64 MB 저장 카드
SanDisk	SDP series	SanDisk SDP 5/3 0.6	256 MB Storage card
Kingston	CompactFlash Storage Card	TOSHIBA THNCF064MAA	64 MB 저장 카드
Viking	CompactFlash	TOSHIBA THNCF064MBA	64 MB 저장 카드

표 B-4 HDD 카드

제조 업체	모델 이름	VTS II Probe 모델 이름	규격
Toshiba	MK5002MPL		Type II PC card 5GB HDD

표 B-5 시리얼 모뎀 카드

제조 업체	모델 이름	VTS II Probe 모델 이름	규격
Billionton Systems Inc.	FM56C series	PCMCIA CARD 56KFaxModem FM56C-NFS 5.41	Ambient (Intel) V.90 FAX/MODEM PC 카드
Viking	PC Card Modem 56K	Viking V.90 K56flex 021 A	MODEM PC 카드
KINGMAX	KIT PCMCIA 56K Fax/Modem Card	CIRRUS LOGIC 56K MODEM CL-MD56XX 5.41	V.90 FAX/MODEM PC 카드
U.S. Robotics	USR0756-XJ/USR0756-CB		56K Fax/Modem 카드
3COM	3CXM576/3CCM576		56K Fax/Modem 카드

부록 C: VTS II가 지원하는 USB 장치

VTS II 시리즈는 다음의 USB 장치를 지원합니다.

표 C-1 무선 네트워크 카드

제조 업체	모델 이름	VTS II Probe 모델 이름	규격
Linksys	WUSBF54G	ZyDAS USB2.0 WLAN	802.11b/g USB2.0
TRENDNET	TEW429UB	ZyDAS USB2.0 WLAN	802.11b/g USB2.0
AIRLINK	AWLL3026	ZyDAS USB2.0 WLAN	802.11b/g USB2.0
IOGEAR	GWU523	ZyDAS USB2.0 WLAN	802.11b/g USB2.0

부록 D: VTS II 설정 파일

D.1 VTS II 설정 파일의 구성

Web UI 또는 콘솔 UI 를 통하여 설정된 VTS II의 설정값들은 VTS II의 `/tmp/cnf` 디렉토리에 저장되어 있습니다. (부팅시 복원되는 실제 저장값은 flash 메모리상에 저장됩니다. UI 상에서 `save` 명령을 실행시키거나 CLI 상에서 `saveconf` 명령을 실행시키게되면 `/tmp/cnf` 디렉토리 상의 변수 값들이 flash 메모리에 저장되게 됩니다.)
`/tmp/cnf` 디렉토리에는 다음과 같은 하위 디렉토리들이 존재하며

```
.ssh    bin    cluster    etc    ports    power    sys
```

각 디렉토리에 저장되는 설정값들의 내용은 표 D-1과 같습니다.

표 D-1 VTS II 설정 파일의 구성

디렉토리	설정파일 및 하위 디렉토리	설명
.ssh		사용자의 ssh public key 저장 디렉토리
bin	active_detect	Active automatic detection 에 사용 되는 script 파일
	passive_detect	Passive automatic detection 에 사용 되는 script 파일
	rportcon	Remote Port connection 에 사용 되는 script 파일
cluster	cluster.cnf	master cluster unit 의 설정 파일
	unitxx.cnf	slave cluser unit xx 의 설정 파일
etc	client.pem	Client 인증 파일
	interfaces	네트워크 설정 파일
	passwd	Password 파일
	snmpd.conf	SNMP 설정 파일
	dhcpcd.opt	DHCP 옵션 설정 파일
	ip6tables.save ppp	IPv6 패킷 필터 설정 파일
	sshd_config	PPP 관련 설정 디렉토리
	group	SSH 데몬 설정 파일
	iptables.save	Group 파일
	resolv.conf	IPv4 패킷 필터 설정 파일
	syslog-ng.conf	Name server 설정 파일
	hostname	Syslog-ng 서비스 설정 파일
	nsswitch.conf	Hostname 설정 파일
	server.pem	Name Service Switch 설정 파일

	timezone	Client 인증 파일
	hosts	시스템 Timezone 설정 파일
	pam.d	호스트 Name 설정 파일
	shadow	PAM 모듈 설정 디렉토리
	xinetd.d	Shadow password 파일
		Extendted internet service daemon 설정 디렉토리
ports	allports	시리얼 포트 공통 설정 디렉토리
	master.cnf	마스터 포트 설정 파일
	portxx	시리얼 포트 xx 설정 디렉토리
	rport.default	리모트포트 기본 설정 파일
power	power.cnf	파워 유닛 설정 파일
sys	autobk.cnf	자동 설정 백업 설정 파일
	cliauth.cnf	CLI 인증 설정 파일
	modem.cnf	내장 모뎀 설정 파일
	pccard.cnf	PC CARD 설정 파일
	syslog-ng.cnf	Syslog-ng 서비스 설정 파일
	autofwup.cnf	자동 Firmware Upgrade 설정 파일
	datetime.cnf	날짜/시간 설정 파일
	network	네트워트 설정 관련 디렉토리
	security.cnf	Security 변수 설정 파일
	system.cnf	시스템 변수 설정 파일

부록 E: 잘 알려진 포트 번호

포트 번호는 다음과 같은 3가지 범위로 잘 알려진 포트(Well Known Port), 등록된 포트(registered port), 동적(Dynamic) 또는 사설 포트(private port)고 나눌 수 있습니다. 잘 알려진 포트는 0~1023번까지 이며, 이미 등록된 포트는 1024부터 49151까지의 포트입니다. 동적 및 사설 포트는 49152부터 65535까지의 포트입니다.

잘 알려진 포트는 IANA가 지정한 것으로서, 대부분의 시스템에서는 시스템 프로세스나 특별히 허가된 사용자가 실행한 프로그램에 의해서만 사용될 수 있습니다. 표 E-1은 잘 알려진 포트 번호 중의 일부를 보여줍니다. 자세한 내용은 IANA 웹사이트를 방문하시기 바랍니다.
http://www.iana.org/assignments/port-numbers

표 E-1 잘 알려진 port number

Port number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure SHell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

부록 F: Bios 메뉴 프로그램 안내

F.1 개요

Bios 메뉴는 비상 시, 복구 옵션으로 VTS II를 복구하고 시스템 하드웨어를 진단하는 방법을 제공합니다. VTS II 장치에 전원이 공급된 후 3초 이내에 사용자가 <ESC> 키를 누르면, bios 메뉴 프로그램을 입력할 수 있습니다. 이 메뉴 프로그램으로부터, 사용자는 다양한 시스템 파라미터를 설정할 수 있고, 하드웨어 시스템 테스트 및 Firmware 업그레이드를 수행할 수 있습니다.

F.2 메인 메뉴

Bios 메뉴 프로그램에 들어가면, 사용자는 그림 F-1과 같은 페이지를 볼 수 있습니다.

```
*******************************************************************************
 MPC88x Bios v1.0.1
*******************************************************************************
Please wait for initializing the board.
Board initializing.............................OK
CPU checking...................................OK
DRAM checking..................................OK.
FLASH checking.................................OK.
Power checking.................................OK
(Power1 : OK, Power2 : OK)

CPU is the MPC880 at 132Mhz(DRAM:128MB,FLASH:64MB)

Now starting the main program!!!
Press <ESC> key to enter the bios menu :  0
-------------------------------------------------------------------------------
 Welcome to Bios Configuration page
-------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Feb 09 06 -  12:14:57 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.0.1]
 4. Exit and boot from flash
 5. Exit and boot from flash in emergency mode
 6. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-1 Bios 메인 프로그램의 메인 메뉴 페이지

F.3 RTC 설정 메뉴

RTC 설정 메뉴를 사용함으로써, 사용자는 VTS II의 시스템 시간을 설정할 수 있습니다.

```
--------------------------------------------------------------------------------
 RTC configuration
--------------------------------------------------------------------------------
 Select menu
 1. Date(mm/dd/yy) : 02/14/03
 2. Time(hh:mm:ss) : 13:27:12
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Enter Current Date (mm/dd/yy) : 02/15/03
press the ENTER key to continue

--------------------------------------------------------------------------------
 RTC configuration
--------------------------------------------------------------------------------
 Select menu
 1. Date(mm/dd/yy) : 02/15/03
 2. Time(hh:mm:ss) : 13:27:20
  <ESC> Back, <ENTER> Refresh
 -----> 2
 Enter Current Time (hh:mm:ss) : 13:25:00
press the ENTER key to continue

--------------------------------------------------------------------------------
 RTC configuration
--------------------------------------------------------------------------------
 Select menu
 1. Date(mm/dd/yy) : 02/15/03
 2. Time(hh:mm:ss) : 13:25:01
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-2 Bios 메뉴 프로그램 내의 RTC 설정

F.4 하드웨어 테스트 메뉴

F.4.1 테스트 설정

사용자는 하드웨어 테스트 메뉴를 사용하여 하드웨어 구성 장치들을 테스트할 수 있습니다. 다음과 같은 3가지의 하드웨어 테스트 모드가 있습니다.

- One time
- Looping(without External test in Auto test)
- Looping(with External test in Auto test)

사용자가 **One time** 또는 **Looping(with External test in Auto test)** 모드를 선택하는 경우, 원격 호스트(서버 IP 주소)로의 Ping 테스트와 UART 테스트(내부 루프백 테스트 및 외부 케이블 루프백 테스트), 모뎀 테스트(내부 AT 테스트 및 외부 전화걸기)를 포함하는 전체 테스트가 수행됩니다.

One time 또는 **Looping(with External test in Auto test)** 모드 테스트를 수행하기 위해서는 이더넷 포트에 LAN 케이블, 시리얼 포트에 루프백 케이블, 모뎀포트에 전화 라인이 각각 연결되어 있어야 합니다.

또한 동일한 네트워크 상에 서버 IP 로 설정되어 있는 IP 와 같은 주소를 가지는 호스트가 존재하여야 합니다. 이 서버 IP는 기본적으로 192.168.0.128 로 설정되어 있으며, **Firmware Upgrade** 메뉴에서 변경할 수 있습니다.

모뎀 테스트는 타겟 모뎀에 전화 걸기를 시도하여 그 응답을 체크하기 때문에 반드시 타겟 모뎀의 번호가 설정되어 있어야 합니다. 타겟 모뎀의 번호는 Hardware test 메뉴의 하위 메뉴인 **Modem test > External modem test** 에서 변경할 수 있습니다.

사용자가 **Looping(with External test in Auto test)**모드를 선택하는 경우, 보드 내부의 장치에 대해서만 테스트를 수행하기 때문에 VTSII에 어떠한 케이블의 연결 없이도 테스트가 가능합니다.

F.4.2 테스트 모드 및 메뉴 리스트

하드웨어 테스트 메뉴에서는 각 구성 장치들에 대한 테스트를 수행할 수 있습니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-3 하드웨어 테스트 메뉴(Dual Power / Modem)

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
```

```
2. DRAM test
3. FLASH test
4. EEPROM test
5. UART test
6. USB test
7. Ethernet test
8. LED test
9. PC card test
10. Power test
11. Summary for test result
 <ESC> Back, <ENTER> Refresh
----->
```

그림 F-4 하드웨어 테스트 메뉴(Dual Power)

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Summary for test result
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-5 하드웨어 테스트 메뉴(Single Power)

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Modem test
 11. Summary for test result
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-6 하드웨어 테스트 메뉴(Single Power / Modem)

사용자가 **One time** 테스트 모드를 선택하면, 각 하드웨어 구성 장치들에 대하여 단 한번의 테스트만이 수행됩니다. 이 모드에서는 외부 호스트 장비로의 ping 테스트 및 외부 UART 테스트,

모뎀 테스트를 포함한 모든 테스트가 수행됩니다.
사용자가 **Looping(without External test in Auto test)** 테스트 모드를 선택하면, <ctrl+c> 키를 누를때까지 각 하드웨어 장치에 대한 테스트가 주기적으로 반복 실행됩니다. 그러나 이 모드에서는 외부 호스트(서버 IP 주소)로의 Ping 테스트, 외부 UART 테스트, target 모뎀에 대한 전화 접속 테스트는 수행되지 않습니다.
사용자가 **Looping(without External test in Auto test)** 테스트 모드를 선택하면 <ctrl+c> 키를 누를때까지 각 하드웨어 장치에 대한 테스트가 주기적으로 반복 실행됩니다.
이 모드에서는 외부 호스트 장비로의 ping 테스트 및 외부 UART 테스트, 모뎀 테스트를 포함한 모든 테스트를 수행합니다.

각각의 테스트 모드는 **Hardware Test** 메뉴에서 0번을 선택함으로써 사용할 수 있습니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 -----> 0
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - Looping(without External test in Auto test)
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 -----> 0
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - Looping(with External test in Auto test)
 1. Auto test
 2. DRAM test
 3. FLASH test
```

```
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 -----> 0
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-7 테스트 모드 변경

F.4.3 자동 테스트(Auto test)

Hareware Test 메뉴에서 1번을 선택하면 모든 하드웨어 구성 장치에 대한 테스트가 자동적으로 수행됩니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. LED test
 9. PC card test
 10. Power test
 11. Modem test
 12. Summary for result
  <ESC> Back, <ENTER> Refresh
 -----> 1

              ******** Hardware auto-detect and auto-test ********

[DRAM]
```

```
Writing the DRAM at the address for starting offsets of 20 with value 1's
writing ------------------------------------------------------------[OK     ]
Writing the DRAM at all other location with a value 0's
writing ------------------------------------------------------------[OK     ]
Check every 20th location from the staring address
Reading ------------------------------------------------------------[OK     ]
Writing the DRAM at the address for starting offsets of 20 with value 0's
writing ------------------------------------------------------------[OK     ]
Writing the DRAM at all other location with a value 1's
writing ------------------------------------------------------------[OK     ]
Check every 20th location from the staring address
Reading ------------------------------------------------------------[OK     ]
Memory test is successed.

[FLASH]
Flash Test Status---------------------------------------------------[KERNEL ]
Flash Test Status---------------------------------------------------[INITRD ]
Flash Test Status---------------------------------------------------[CRAMFS1]
Flash Test Status---------------------------------------------------[CRAMFS2]
FLASH Test ---------------------------------------------------------[OK     ]

[EEPROM]
[testing]-----------------------------------------------------------[SUCCESS]

[UART]
<--Internal Uart Test-->
Port #  1 test in progressing(Read/Write)--------------------------[SUCCESS]
Port #  2 test in progressing(Read/Write)--------------------------[SUCCESS]
Port #  3 test in progressing(Read/Write)--------------------------[SUCCESS]

.......

Port # 30 test in progressing(Read/Write)--------------------------[SUCCESS]
Port # 31 test in progressing(Read/Write)--------------------------[SUCCESS]
Port # 32 test in progressing(Read/Write)--------------------------[SUCCESS]

[UART]
<--External Uart Test-->
Port #  1 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]
Port #  2 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]
Port #  3 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]
                                  .......
Port # 30 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]
Port # 31 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]
Port # 32 test in progressing(Read/Write)--------------------------[SUCCESS]
                            (RTS/CTS)------------------------------[SUCCESS]
                            (DTR/DSR)------------------------------[SUCCESS]

[USB TEST]
Test is OK.

[ETHERNET1]
host 192.168.4.54 is alive

[ETHERNET2]
host 192.168.4.54 is alive
```

```
[LED]
LED On/OFF------------------------------------------------------ 1 time(s)
LED On/OFF------------------------------------------------------ 2 time(s)
LED On/OFF------------------------------------------------------ 3 time(s)
LED TEST OK.

[PCMCIA]
Lucent Technologies WaveLAN/IEEE Version 01.01
          Network Adapter Card

[POWER1 TEST]
Test is OK.

[POWER2 TEST]
Test is Fail.

[Internal MODEM TEST]
Modem status is OK.

[External MODEM TEST]
Dialing to 205. Please wait a moment.
Received correct answer from the modem(BUSY).
Modem status is OK.

      *******  Hardware auto-detect and auto-test  SUMMARY *******
1. DRAM Test-------------------------------------------------[SUCCESS]
2. FLASH Test------------------------------------------------[SUCCESS]
3. EEPROM Test-----------------------------------------------[SUCCESS]
4. UART Test Summary
 Port NO |  exist status  |   exist status  |  exist status  | exist  status
-------------------------------------------------------------------------------
Port 01-04|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 05-08|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 09-12|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 13-16|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 17-20|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 21-24|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 25-28|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 29-32|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
5. USB Test--------------------------------------------------[SUCCESS]
6. ETHERNET1 Test--------------------------------------------[SUCCESS]
   ETHERNET2 Test--------------------------------------------[SUCCESS]
7. PCMCIA Test-----------------------------------------------[SUCCESS]
8. POWER1 Test-----------------------------------------------[SUCCESS]
   POWER2 Test-----------------------------------------------[SUCCESS]
9. Internal MODEM Test---------------------------------------[SUCCESS]
   External MODEM Test---------------------------------------[SKIPPED]

PRESS any key to continue!!!
```

그림 F-8 하드웨어 자동 테스트(Auto test)결과(One time)

각 장치에 대하여 사용자는 <ESC> 키를 사용하여 테스트를 건너 뛸 수 있습니다.

```
-------------------------------------------------------------------------------
 Hardware Test
-------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
```

```
 6. USB test
 7. Ethernet test
 8. PC card test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 -----> 1

          *******  Hardware auto-detect and auto-test *******
[DRAM]
Writing the DRAM at the address for starting offsets of 20 with value 1's
writing ------------------------------------------------------------------[SKIPPED]

[FLASH]
Flash Test Status--------------------------------------------------------[Kernel ]
FLASH Test ---------------------------------------------------------------[SKIPPED]
```

그림 F-9 하드웨어 자동 테스트(Auto test) (Skipped)

looping 모드에서 **Auto test**를 수행하는 중에 하드웨어 장치에서 Fail이 발생하면, 실행중이던 테스트가 정지됩니다. 또한 하드웨어 테스트에 이상이 있음을 알려주기 위하여 FINDME LED가 점등됩니다. 사용자가 메뉴 페이지로 돌아가려고 한다면 <ctrl+c>키를 눌러야만 합니다.
이 후에 **Hardware Test**페이지에서 **Summery for Test result**를 선택하여 이상이 있는 장치를 확인할 수 있습니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - Looping(with External test in Auto test)
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. PC card test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 -----> 1

              ******** Hardware auto-detect and auto-test ********

[DRAM]
Writing the DRAM at the address for starting offsets of 20 with value 1's
writing ------------------------------------------------------------------[SKIPPED]

[FLASH]
Flash Test Status--------------------------------------------------------[Kernel ]
Flash Test Status--------------------------------------------------------[INITRD ]
Flash Test Status--------------------------------------------------------[CRAMFS1]
Flash Test Status--------------------------------------------------------[CRAMFS2]

FLASH Test ---------------------------------------------------------------[OK     ]

[EEPROM]
```

```
[testing]-------------------------------------------------------------[SUCCESS]

[UART]
<--Internal Uart Test-->
Port #  1 test in progressing(Read/Write)-----------------------------[SUCCESS]
Port #  2 test in progressing(Read/Write)-----------------------------[SUCCESS]
Port #  3 test in progressing(Read/Write)-----------------------------[SUCCESS]
 .......
Port # 30 test in progressing(Read/Write)-----------------------------[SUCCESS]
Port # 31 test in progressing(Read/Write)-----------------------------[SUCCESS]
Port # 32 test in progressing(Read/Write)-----------------------------[SUCCESS]

[UART]
<--External Uart Test-->
Port #  1 test in progressing(Read/Write)-----------------------------[SUCCESS]
                            (RTS/CTS)---------------------------------[SUCCESS]
                            (DTR/DSR)---------------------------------[SUCCESS]
Port #  2 test in progressing(Read/Write)-----------------------------[SUCCESS]
                            (RTS/CTS)---------------------------------[SUCCESS]
                            (DTR/DSR)---------------------------------[SUCCESS]
.......

Port # 30 test in progressing(Read/Write)-----------------------------[SUCCESS]
                            (RTS/CTS)---------------------------------[SUCCESS]
                            (DTR/DSR)---------------------------------[SUCCESS]
Port # 31 test in progressing(Read/Write)-----------------------------[SUCCESS]
                            (RTS/CTS)---------------------------------[SUCCESS]
                            (DTR/DSR)---------------------------------[SUCCESS]
Port # 32 test in progressing(Read/Write)-----------------------------[FAILED ]
Press the Ctrl+C key to continue. =>  <ctril-C> 키를 눌러서 메뉴 페이지로 이동
Hardware Test is Failed!!!
-------------------------------------------------------------------------------
 Hardware Test
-------------------------------------------------------------------------------
 Select menu
 0. Test Mode - Looping(with External test in Auto test)
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. PC card test
 7. Ethernet test
 8. USB test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 -----> 12

      *******  Hardware auto-detect and auto-test  SUMMARY *******
1. DRAM Test----------------------------------------------------------[SUCCESS]
2. FLASH Test---------------------------------------------------------[SUCCESS]
3. EEPROM Test--------------------------------------------------------[SUCCESS]
4. UART Test Summary
 Port NO |  exist status  |   exist status  |  exist status  | exist  status
-------------------------------------------------------------------------------
Port 01-04|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 05-08|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 09-12|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 13-16|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 17-20|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 21-24|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 25-28|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 29-32|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES    FAIL
5. USB Test -----------------------------------------------------------[  N/A  ]
```

```
6. ETHERNET1 Test-----------------------------------------------------[  N/A  ]
   ETHERNET2 Test-----------------------------------------------------[  N/A  ]
7. PCMCIA Test -----------------------------------------------------[  N/A  ]
8. POWER1 Test------------------------------------------------------[  N/A  ]
   POWER2 Test------------------------------------------------------[  N/A  ]
9. Internal MODEM Test ---------------------------------------------[  N/A  ]
   External MODEM Test ---------------------------------------------[  N/A  ]

  Press any key to continue!!!
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - Looping(with External test in Auto test)
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. PC card test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-10 테스트 결과 확인(looping test mode)

F.4.4 하드웨어 장치별 테스트

Hardware Test 메뉴에서 테스트를 원하는 장치에 대한 번호를 선택하면 각 장치에 대한 독립적인 테스트가 수행됩니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. PC card test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 -----> 5
--------------------------------------------------------------------------------
 Hardware Test  --> UART test
--------------------------------------------------------------------------------
 Select menu
 1. Internal Loopback port test
 2. External Loopback port test
```

```
 <ESC> Back, <ENTER> Refresh
 -----> 2
```

그림 F-11 UART 테스트

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. EEPROM test
 5. UART test
 6. USB test
 7. Ethernet test
 8. PC card test
 9. LED test
 10. Power test
 11. Modem test
 12. Summary for test result
  <ESC> Back, <ENTER> Refresh
 -----> 11
--------------------------------------------------------------------------------
 Hardware Test  --> Modem test
--------------------------------------------------------------------------------
 Select menu
 1. Internal modem test
 2. External modem test
  <ESC> Back, <ENTER> Refresh
 -----> 1
[Internal MODEM Test]
Modem status is OK.
--------------------------------------------------------------------------------
 Hardware Test  --> Modem test
--------------------------------------------------------------------------------
 Select menu
 1. Internal modem test
 2. External modem test
  <ESC> Back, <ENTER> Refresh
 -----> 2
--------------------------------------------------------------------------------
 Hardware Test  --> Modem test
--------------------------------------------------------------------------------
 Select menu
 1. Phone number to dial [211]
 2. Start modem test
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Enter the phone number : 213
--------------------------------------------------------------------------------
 Hardware Test  --> Modem test
--------------------------------------------------------------------------------
 Select menu
 1. Phone number to dial [213]
 2. Start modem test
  <ESC> Back, <ENTER> Refresh
 -----> 2
 [MODEM]
Dialing to 213. Please wait a moment.
Received correct answer from the modem(BUSY).
Modem status is OK.
--------------------------------------------------------------------------------
 Hardware Test  --> Modem test
```

```
--------------------------------------------------------------------------------
Select menu
1. Phone number to dial [213]
2. Start modem test
 <ESC> Back, <ENTER> Refresh
----->
```

그림 F-12 모뎀(Modem) 테스트

F.5 Firmware upgrade 메뉴

사용자는 **Fimware upgrade** 메뉴에서 각 VTS II 장비의 업그레이드를 수행할 수 있습니다. 펌웨어 업그레이드를 하기 전에, 사용자는 메인 메뉴 페이지에서 3번을 선택해서 현재 펌웨어 버전을 확인할 수 있습니다.

```
--------------------------------------------------------------------------------
Welcome to Bios Configuration page
--------------------------------------------------------------------------------
Select menu
1. RTC configuration [ Feb 09 2006 - 15:31:09 ]
2. Hardware test
3. Firmware upgrade [S/W Version : v1.0.0]
4. Exit and boot from flash
5. Exit and boot from flash in emergency mode
6. Exit and reboot
 <ESC> Back, <ENTER> Refresh
-----> 3
```

그림 F-13 펌웨어 업그레이드 메뉴 선택

VTS II는 펌웨어 업그레이드를 위하여 2가지 프로토콜을 지원합니다.
초기 설정된 프로토콜은 DHCP 환경을 위한 BOOTP 입니다. 사용자는 이 외에 **Firmwave upgrade** 메뉴에서 1번을 선택하여 프로토콜을 변경할 수 있습니다. 이 메뉴에서 **TFTP**를 선택한다면, 사용자는 **Firmwave upgrade** 메뉴에서 2번을 선택하여 반드시 VTS II 유닛에 대한 IP를 설정해야 합니다. 초기 IP 어드레스는 192.168.161.5로 설정되어 있습니다.

사용자는 **Firmware upgrade** 메뉴에서 7번을 선택하여, 펌웨어 업그레이드를 즉시 수행할 수 있습니다. 펌웨어 업그레이드를 올바르게 수행하기 위해서는 **Server's IP address**에서 설정된 IP를 가지는 서버에 **Firmware File Name**에서 설정된 파일 이름을 가지는 펌웨어 파일이 반드시 존재하여야 합니다.

만약 2번째의 이더넷 인터페이스를 이용하여 펌웨어 업그레이드를 수행할 경우, **Firmware upgrade** 메뉴에서 4번을 선택하여 이더넷 인터페이스를 변경해 주어야만 합니다.
(ETHERNET1 -> ETHERNET2 로 변경)

```
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET1]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select protocol ( 1 = BOOTP, 2 = TFTP) : 2
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [TFTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET1]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-14 펌웨어 업그레이드 메뉴 (프로토콜 선택)

```

--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET1]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 4
 Select default Ethernet interface(1 = Ethernet1, 2 = Ethernet2) : 2
```

그림 F-15 펌웨어 업그레이드 메뉴 (이더넷 인터페이스 선택)

사용자는 **Firmware upgrade** 메뉴에서 6번을 선택하여 **Auto firmware Upgrade on next boot**를 설정 할 수 있습니다. **Auto firmware Upgrade on next boot** 메뉴에서 1번을 선택하여 **ON**으로 설정한다면, 펌웨어 업그레이드는 즉시 수행되지 않고, 다음 부팅시 수행될 것입니다. 만약 사용자가 **Auto firmware upgrade on next boot** 옵션을 **ON**으로 설정하였으나, 부팅시 자동 펌웨어 업그레이드를 수행하지 않기를 원한다면 VTS II의 전원이 인가(cold booting,warm booting)된 후 3초 안에 <ESC> 를 누르면 됩니다. 그러면 VTS II는 업그레이드를 수행하지 않고 메인 메뉴로 들어가게 됩니다.

이 때 **Auto firmware upgrade on next boot**의 설정은 **ON** 상태를 유지하고 있는데, 더 이상 부팅

시 자동 업그레이드를 원하지 않는다면 **Auto firmware upgrade on next boot**에서 2번을 선택하여 설정을 **OFF**로 설정하여야 합니다.

만약 **Auto firmware upgrade on next boot**이 한번 수행되었다면, 펌웨어 업그레이드의 성공 여부와는 별도로 **Auto firmware upgrade on next boot** 설정은 **OFF**로 변경됩니다. 그래서 다음 부팅부터는 정상적인 부팅 과정을 수행하게 됩니다.

펌웨어 업그레이드를 수행하는 도중 업그레이드가 실패하였을 경우, VTS II는 정상적으로 부팅되지 않고 사용자가 어떠한 키 입력을 줄 때까지 프로그램을 정지 시킵니다. 이 때 VTSII는 사용자가 업그레이드 실패를 인지할 수 있도록 FINDME LED를 깜빡입니다.

이 때는 펌웨어 업그레이드의 실패 원인을 해결한 후, 다시 펌웨어를 시도하여야 합니다.

```
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET2]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 6
  Select auto firmware Upgrade on next boot(1 = ON, 2 = OFF) : 1
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET2]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[ON]
 7. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 F-16 Auto firmware upgrade on next boot

```
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET1]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade
 -----> 7
Firmware upgrade cannot be stopped until finished.
And all configuration parameters are restored to default values.
Do you really want to start firmware upgrade(y/n)?
BOOTP broadcast 1
DHCP client bound to address 192.168.220.7
TFTP from server 192.168.161.13; our IP address is 192.168.220.7
Filename 'pp.bin'.
```

```
Load address: 0x100000
Loading: ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################
done
Bytes transferred = 5838194 (591572 hex)

Erase Flash Sectors 9-20 in Bank # 1
BLOCK 1 : Copy to Flash... done
Erase Flash Sectors 21-115 in Bank # 1
BLOCK 2 : Copy to Flash... done
Erase Flash Sectors 116-116 in Bank # 1
BLOCK 3 : Copy to Flash... done
BLOCK 4 : Erase Flash Sectors 117-117 in Bank # 1
Firmware upgrade is finished successfully.
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Default Ethernet interface [ETHERNET1]
 5. Firmware File Name [pp.bin]
 6. Auto firmware Upgrade on next boot[OFF]
 7. Start firmware upgrade

 ----->
```

그림 F-17 수동 펌웨어 업그레이드

펌웨어 업그레이드가 성공적으로 수행된 후에, 프로그램은 펌웨어 업그레이드 성공에 대한 메시지 (Firmware upgrade is finished successfully)를 출력한 후 메인 메뉴를 실행 시킵니다. 만약 바이오스 이미지를 포함한 펌웨어의 업그레이드라면, VTS II는 자동적으로 재부팅 됩니다.

F.6 Emergency 모드

VTS II가 정상적인 부팅이 안되는 경우 사용자는 bios 메뉴상에서 emergency 모드로 VTS II 를 부팅시킬수 있습니다. emergency 모드로 VTS II 를 부팅 시키면 그림 F-18 과 같이 사용자는 VTS II 의 콘솔을 암호 없이 Access가 가능합니다. 단, 이 경우 VTS II 의 네트워크 기능을 포함한 일반적인 기능이 모두 사용 불가능 하게 되므로 VTS II의 콘솔을 통하여 이상 상황을 복구시키기 위한

기본적인 명령 수행(factory_reset 등) 이외에는 다른 작업이 불가능 합니다.

```
--------------------------------------------------------------------------------
 Welcome to Boot Loader Configuration page
--------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Feb 09 2006 - 15:31:09 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.0.0]
 4. Exit and boot from flash
 5. Exit and boot from flash in emergency mode
 6. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 -----> 5


   <Loading Kernel Image>
   Image Name:   Kernel 2.6.12 for MPC880(Linux Kernel)
   Data Size:    1491774 Bytes
   Verifying Checksum ... OK
   Uncompressing Kernel Image ... OK
   <Loading RAMDisk Image>
   Image Name:   RAMDISK(Linux RAMDisk Image)
   Data Size:    122373 Bytes
   Verifying Checksum ... OK
   Loading Ramdisk ...OK
Linux version 2.6.12 (root@localhost.localdomain) (gcc version 4.0.0 (DENX ELDK
4.0 4.0.0)) #1190 Mon Jul 17 00:04:18 KST 2006
...
...
Attached scsi removable disk sda at scsi0, channel 0, id 0, lun 0

             Welcome to Passport Embedded Linux Environment
Mounting user space
Telling INIT to go to emergency mode.
INIT: Going single user
INIT: Sending processes the TERM signal
INIT: Sending processes the KILL signal
cat: /etc/timezone: No such file or directory
[root@(none) /]#
```

그림 F-18 emergency 모드 부팅

부록 G: 암호화된 NFS 기능 안내

G.1 개요

NFS는 네트워크를 통하여 파일들을 공유하는데 널리 사용되는 프로토콜이다. 그러나 일반적으로 NFS는 UDP 프로토콜을 사용하므로 다음과 같은 보안상의 문제점을 가지고 있습니다.

- NFS server 와 client 사이의 data는 암호화 되기 어렵다.
- NFS server에 접속하려는 사용자의 ID에 따른 인증 방법을 마련하기가 어렵다.
- NFS server 와 client 사이의 방화벽이 있는 경우 NFS 기능을 사용하기가 어렵다.

이와 같은 보안상의 문제점을 보완하기 위하여 암호화된 NFS (Encrypted NFS 또는 Secure NFS) 라는 기능을 이용할 수 있습니다. VTS II에서 암호화된 NFS 기능은 SSH 터널링 (SSH tunneling) 기능을 이용하여 구현되었습니다. 이 절에서는 암호화된 NFS 기능을 이용하기 위한 NFS server 의 설치 및 설정에 대하여 설명을 하였습니다.

G.2 NFS server의 설치

암호화된 NFS 기능을 사용하기 위하여 사용자는 TCP 프로토콜을 지원하는 NFS server를 이용하여야 합니다. 마이크로소프트사의 Windows 계열 OS에서 동작하는 대부분의 NFS server 는 TCP 프로토콜을 지원 합니다. 여기에서는 Xlink Technology 사의 Omni-NFS server v4.2를 사용한 경우에 대하여 설명하도록 하겠습니다. Omni-NFS server 의 평가판은 Xlink Technology 사의 Web Site 에서 Download 받을 수 있습니다. (http://www.xlink.com/eval.htm)

Omni-NFS server 를 설치 하기 위해서는 다음 과정들을 수행하도록 하십시오.

Step 1. Omni-NFS server v4.2를 Download 받습니다.

Step 2. "nfserver.exe" 프로그램을 실행시키고 이때 나타나는 지시에 따릅니다.

Step 3. Omni-NFS server 설치를 완료한 후에, “시작 -> 프로그램 -> Omni-NFS Server V4.” 에서 NFS server를 선택합니다.

Step 4. XLink NFS Server 창에서, Action 메뉴 밑의 New Entry 를 선택합니다.

Step 5. NFS Server Export 창의 Browse 버튼을 선택하여 NFS로 mount 될 폴더를 선택합니다.

주의 *: 1. 사용자는 export 될 폴더의 "Exported Alias" 를 기억하고 있어야 합니다. 이것은 VTS II 에서 NFS server 상의 mounting path로 사용 됩니다.*

2. 일반적으로 Linux는 NTFS 파일 시스템을 인식하지 못합니다.

VTS II 또한 NTFS 파일 시스템을 인식하지 못하므로 mount 될 폴더는 FAT 또는 FAT32 파일 시스템 상에 있는 폴더를 지정하시기 바랍니다.

Step 6. NFS Server Export 창의 Directory Access Rights 를 설정하는 부분에서 "Read/Write" 를 check 하도록 하십시오.

G.3 OpenSSH 패키지의 설치

VTS II상의 암호화된 NFS 기능은 SSH tunneling 기능을 이용합니다. 그러므로 NFS server 가 설치된 호스트에 SSH daemon이 실행 되고 있어야 암호화된 NFS 기능을 이용 할 수 있습니다. 이 절에서는 OpenSSH for Windows v3.6.1 패키지를 이용한 예를 설명하도록 하겠습니다. OpenSSH for Windows 는 무료 소프트웨어로써 다음 URL,에서 download 받을 수 있습니다.

http://lexa.mckenna.edu/sshwindows/download/releases/

OpenSSH for Windows를 설치하기 위해서 다음 절차들을 따라 주시기 바랍니다.

Step 1. OpenSSH for Windows package 를 download 받습니다.

Step 2. "setupssh361-20030512.exe" 를 실행 시킵니다.

Step 3. command prompt(Dos 창)을 실행 시켜고 OpenSSH 가 설치된 디렉토리로 이동합니다. (`Program Files\OpenSSH`가 기본 설정입니다.)

Step 4. `bin` 디렉토리로 이동합니다.

Step 5. mkgroup 프로그램을 이용하여 group permissions 파일을 만듭니다.

```
C:\Program Files\OpenSSH\bin> mkgroup -l >> ..\etc\group
```

Step 6. mkpasswd 프로그램을 이용하여 passwd 파일에 인증된 사용자를 추가합니다. 이 경우 Windows 상의 모든 사용자를 추가 하려면 `'-u username'` 옵션을 사용하지 말아야 합니다.

```
C:\Program Files\OpenSSH\bin> mkpasswd -l >> ..\etc\passwd
```

Step 7. OpenSSH server 를 실행합니다.

```
C:\Program Files\OpenSSH\bin> net start opensshd
```

Step 8. “pause.exe”프로그램을 `"Program Files\OpenSSH\bin"` directory 에 복사합니다.

주의 : 1. “pause.exe” 프로그램은 세나테크놀로지에서 만든 VTS II용 응용프로그램입니다.

2. 이 프로그램은 server와 client 간의 Encrypted TCP 연결을 유지하는 역할을 합니다,

3. 이 프로그램은 VTS II 제품과 같이 제공되는 CD ROM 안에 수록되어 있습니다. 만일 이 프로그램이 없을 경우에는 세나 기술 지원으로 문의 하시기 바랍니다.

G.4 VTS II 에서 Encrypted NFS 기능의 설정

NFS server 와 OpenSSH 의 설치를 완료하면 사용자는 VTS II의 설정 메뉴 상에서 Encrypted NFS 기능을 설정할 수 있습니다. 설정 절차는 다음과 같습니다.

Step 1. VTS II의 Web UI 에 로그인 합니다.

Step 2. NFS server configuration 페이지로 이동합니다.

Step 3. 각 변수들을 다음과 같이 설정합니다.

NFS service : Enabled

Primary NFS server IP address : *Encrypted NFS server 의 IP address를 적습니다.*

Mounting path on primary NFS server : *"Exported Alias" 적습니다.*

Primary NFS timeout (sec, 5-3600) : *원하는 임의의 값을 적습니다.* (*5sec 가 기본값)*

Enable/Disable encrypted primary NFS server : Enabled

Encrypted primary NFS server user : *Encrypted NFS server의 사용자 이름을 적습니다.*

Encrypted primary NFS server password : *해당 사용자의 password를 적습니다.*

Confirm primary NFS server password : *해당 사용자의 password를 다시 적습니다.*

Step 4. **Save & apply**를 선택합니다.

Step 5. System log 나 Port log 의 Location을 NFS server로 설정합니다.

Step 6. 테스트합니다.

Encrypted NFS를 테스트하려면, 사용자는 LanExplorer나 EtherReal과 같은 이더넷 패킷 캡쳐 프로그램을 사용할 수 있어야 합니다. 일반적인 NFS의 경우에는, 단순한 텍스트 형태의 데이터이기 때문에 VTS II와 NFS 서버간의 모든 전송 데이터를 캡쳐할 수 있습니다. 그러나, Encrypted NFS 의 경우에는, 사용자는 CM과 NFS 서버간의 모든 전송 데이터를 캡쳐할 수는 있지만, 암호화된 모든 전송 데이터를 복호화(Decode)할 수는 없습니다.

부록 H: SNMP를 이용한 VTS II 관리

H.1 개요

관리자는 NMS(네트워크 관리 시스템) 또는 SNMP 브라우저를 사용하는 SNMP 프로토콜을 통해 VTS II를 관리할 수 있습니다. VTS II가 NMS 또는 SNMP 브라우저가 실행되고 있는 호스트에 접속을 허용하려면 NMS 또는 SNMP 브라우저를 사용하기 전에, 액세스 제어 설정을 적절히 설정해야 합니다. 그림 H-1 은 VTS II SNMP 에이전트의 MIB-II OID를 브라우징 하고 있는 일반적인 SNMP 브라우저 화면 쇼트를 보여줍니다.

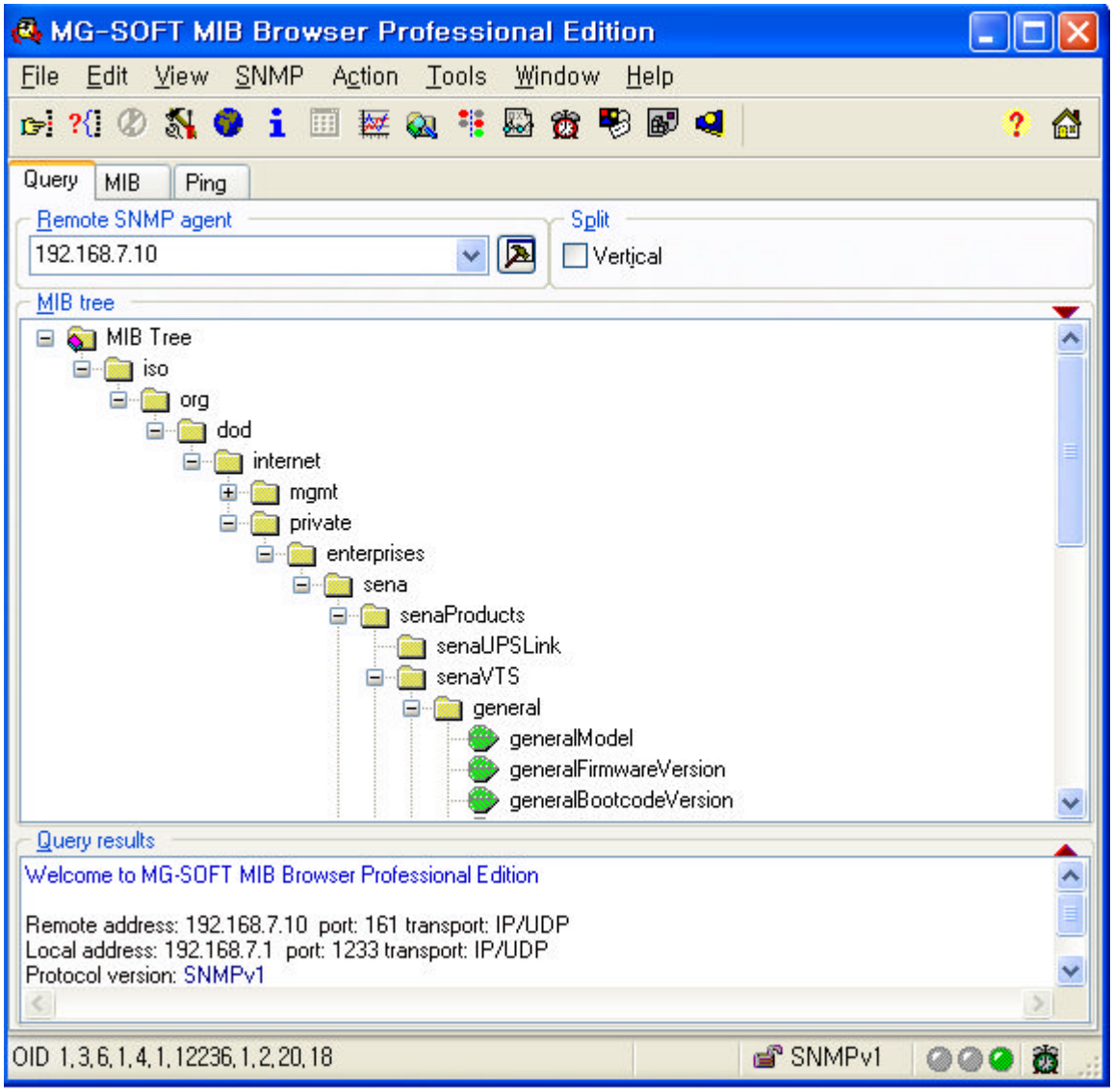


그림 H-1. SNMP 브라우저

H.2 정보 조회

관리자는 SNMP 프로토콜의 Get / Get-Next를 사용하여 VTS II의 정보를 조회할 수 있습니다.

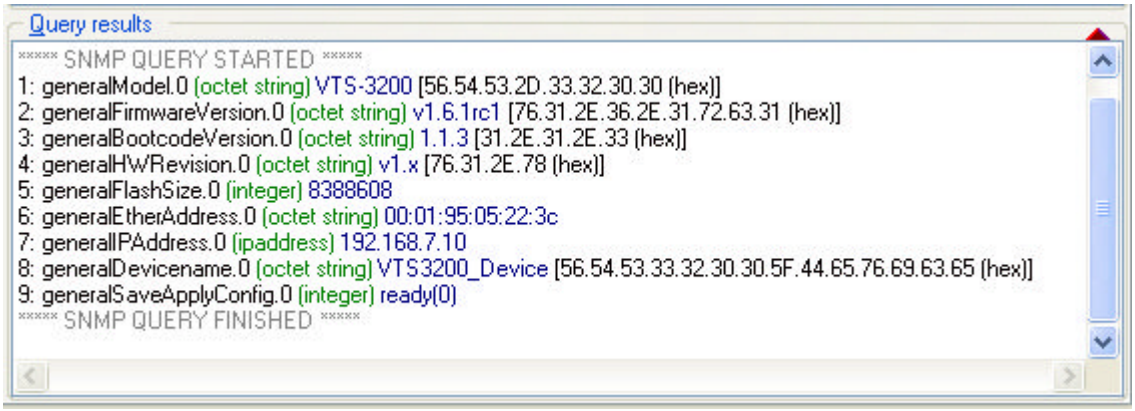


그림 H-2 SNMP를 이용한 정보 조회

H.3 정보 변경

관리자는 SNMP 프로토콜의 Set을 사용하여 VTS II의 정보를 변경할 수 있습니다.

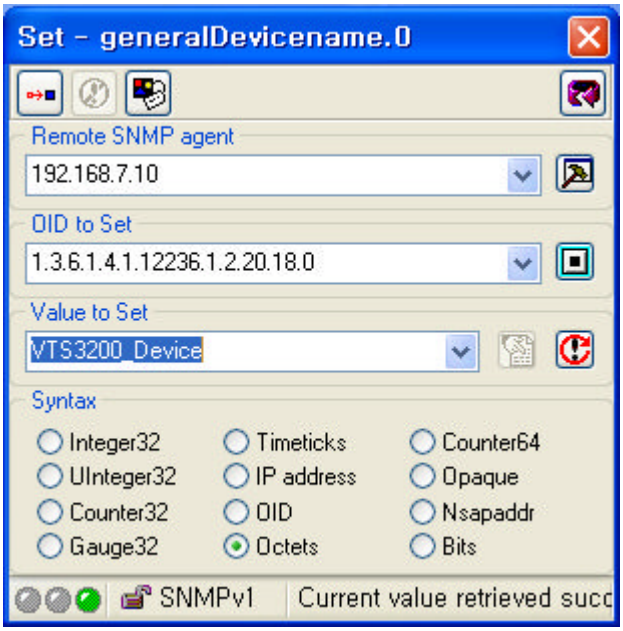


그림 H-3 SNMP를 이용한 정보 변경

H.4 주의사항

- 변경된 정보는 임시로 저장 하기 때문에 정보의 보존을 위해 generalSaveApplyConfig를 save 혹은 saveApply로 변경해야 합니다.

- 포트에 처음으로 키워드를 추가할 때는 default-keyword에서 addRow하고 portIndex를 변경하여 사용합니다.

- 키워드가 있는 포트에 다른 키워드를 추가할 때는 해당 포트의 키워드에서 addRow하여 추가합니다.

- 다른 port에서 addRow한 후에 portIndex를 변경하면 같은 포트에 같은 인덱스를 갖는 키워드가 2개 생성되기 때문에 추가되지 않습니다.

- portsResetFactoryDefault와 같이 excute 하는 정보를 MIB-Browser에서 셋팅하는 경우에는 한번에 하나씩 해야 합니다.

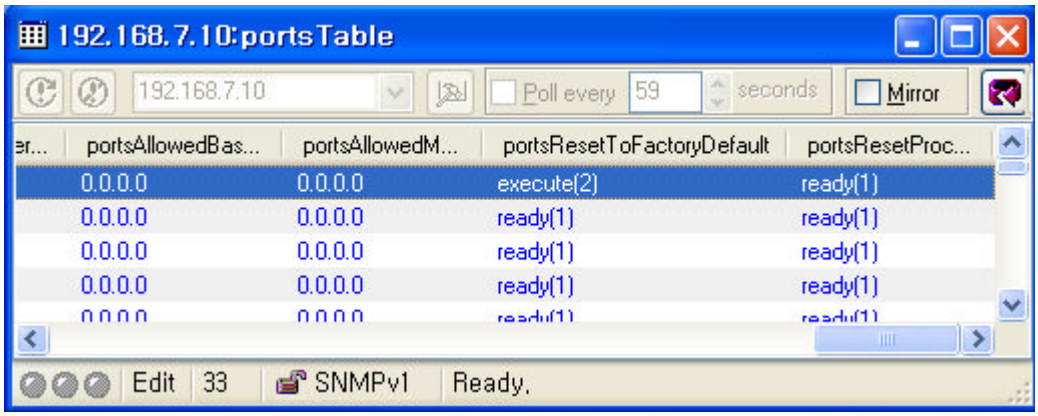


그림 H-4 excute 설정

부록 I: freeKVM Tool

I.1 개요

VTS II 장치의 freeKVM 연결 기능을 이용하여 서버를 관리할 때 사용하는 효율적인 관리를 지원하는 유틸리티 프로그램입니다. 서버가 연결되어 있는 포트의 로그 표시 기능, 시리얼 포트 또는 원격 포트로의 연결 기능, 다른 KVM 클라이언트 프로그램으로의 이동 기능등이 있습니다.

I.2 설치

freeKVM Tool을 사용하려면 사용자 PC에 프로그램을 설치하고 VTS II 장치의 웹인터페이스에서 이 프로그램을 실행할 수 있도록 시스템 패스에 등록해야 합니다. 프로그램은 세나 기술 지원 (email: support@sena.com , 웹 사이트 http://www.sena.com)에 요청하여 구할 수 있습니다.

Windows용 freeKVM Tool의 설치 절차는 다음과 같습니다.

Step 1. 프로그램 실행파일을 사용자 PC로 복사합니다.

Step 2. 프로그램 실행파일이 있는 폴더를 시스템 패스에 추가합니다.

Linux용 freeKVM Tool의 설치 절차는 다음과 같습니다.

Step1. 설치 파일의 압축을 풉니다.

Step 2. 파일 구성은 다음과 같습니다.

connect.xpm	(연결 버튼 이미지)
log.xpm	(로그 버튼 이미지)
exit.xpm	(종료 버튼 이미지)
RDCTool.config	(설정 파일)
RDCTool	(바이너리 파일)

Step 3. `/usr/local/bin`에 바이너리 파일을 복사합니다.

Step 4. `/usr/local/etc/`에 RDCTool 디렉토리를 만듭니다.

Step 5. `/usr/local/etc/RDCTool/`에 바이너리 파일을 제외한 모든 파일을 복사합니다.

I.3 실행

KVM을 지원하는 서버가 연결된 포트에 freeKVM 설정을 하고, Serial Port Connection 화면에서 해당 포트의 작업리스트에 있는 freeKVM 연결 아이콘을 클릭하면 freeKVM Tool 프로그램이 실행되면서 설정된 KVM 클라이언트 프로그램을 실행하여 서버로 KVM 세션을 연결합니다.

다음은 Windows에서 freeKVM Tool 프로그램을 실행하는 예입니다.

Step 1. Port #1에 Windows 2003이 설치되어 있고 Remote desktop 연결이 설정되어 있는 서버를 연결하고, Host mode configuration 화면에서 다음과 같이 설정합니다.

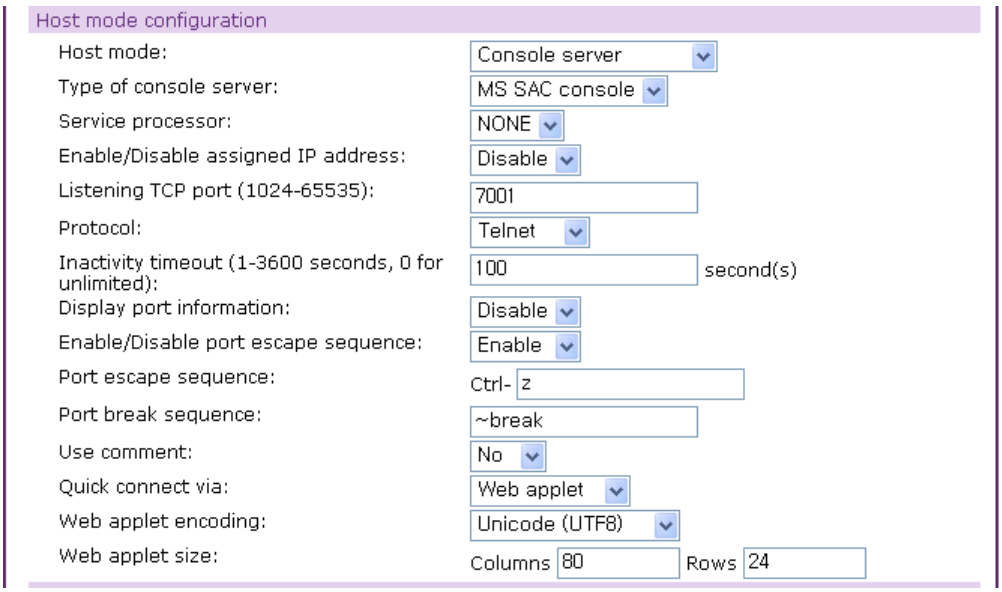


그림 I-1 Host mode configuration of Windows2003 Remote desktop connection

Step 2. Port #1의 freeKVM configuration 화면에서 다음과 같이 설정합니다.

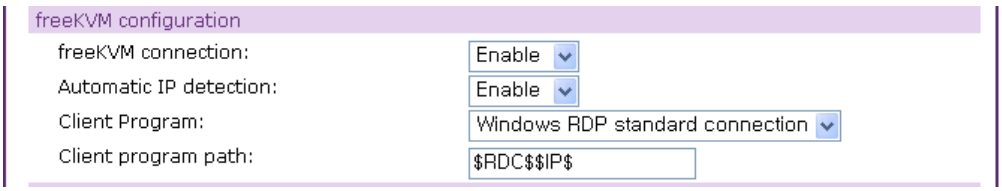


그림 I-2 freeKVM configuration of Windows2003 Remote desktop connection

Step 3. Port #2에 Linux가 설치되어 있고 X window server가 실행되고 있는 서버를 연결하고, freeKVM configuration 화면에서 다음과 같이 설정합니다.

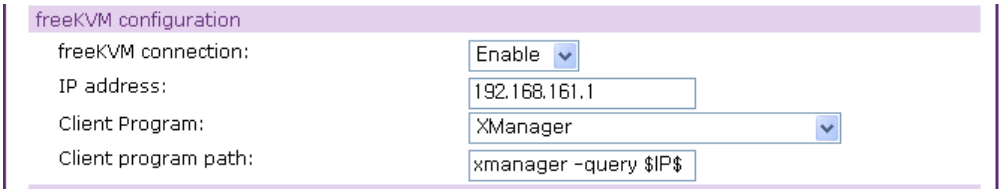


그림 I-3 freeKVM configuration of Linux X window server

Step 4. 왼쪽 메뉴 바에 있는 **Serial port > Connection** 을 선택해서 Seial port connection 화면에 접속한 후 Port #1을 선택합니다.

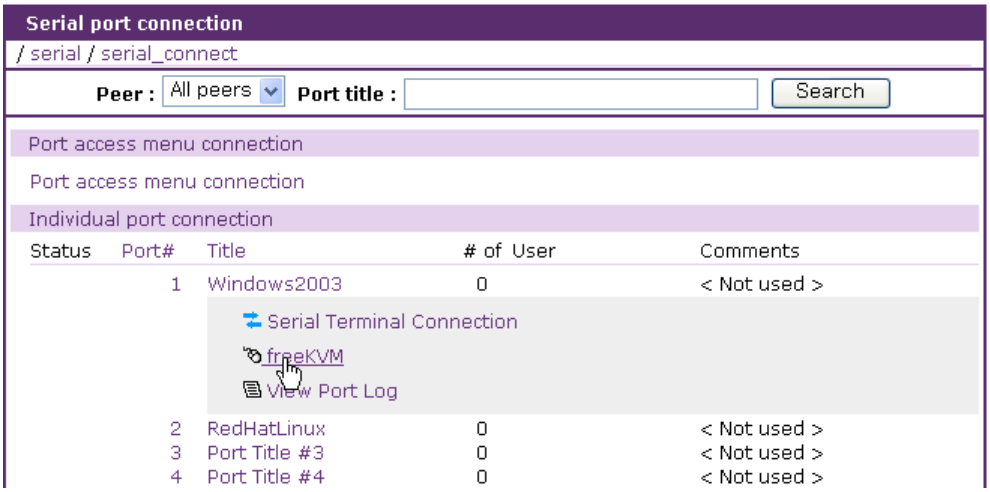


그림 I-4 Serial port connection 화면

Step 5. Serial port connection 화면에서 Port #1의 작업리스트에 있는 freeKVM 연결 아이콘을 클릭하여 freeKVM Tool을 실행합니다.

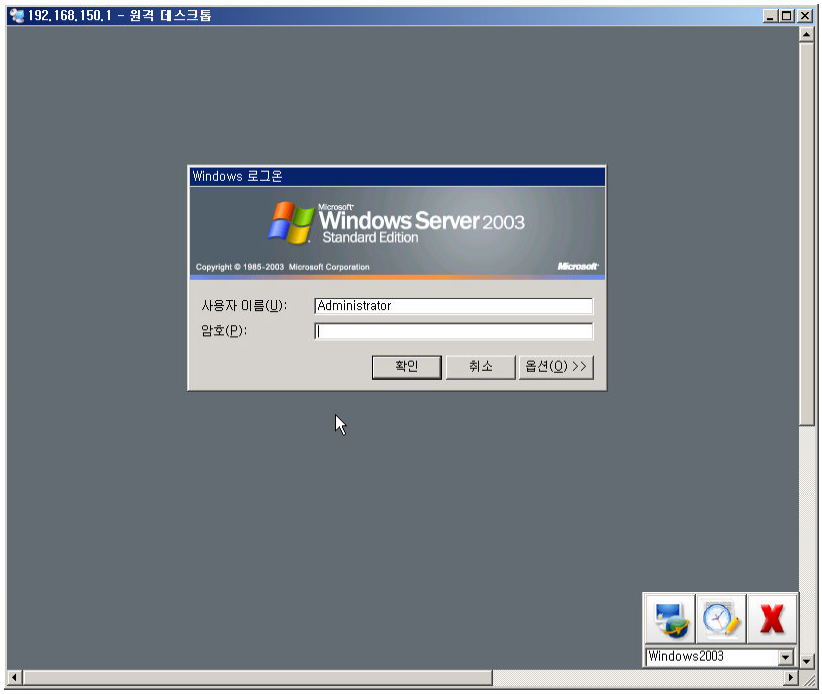


그림 I-5 freeKVM Tool – Remote desktop connection

freeKVM Tool은 설정된 Remote desktop connection 클라이언트 프로그램(mstsc.exe)를 실행하여 서버로 Remote desktop 연결을 합니다. freeKVM Tool의 Port list에 포트 타이틀 Windows2003이 추가됩니다.

Step 6. Serial port connection 화면에서 Port #2의 작업리스트에 있는 freeKVM 연결 아이콘을 클릭하여 freeKVM Tool이 Xmanager통해 X window server로 KVM 연결합니다. freeKVM

Tool의 Port list에 포트 타이틀 RedHatLinux가 추가됩니다.

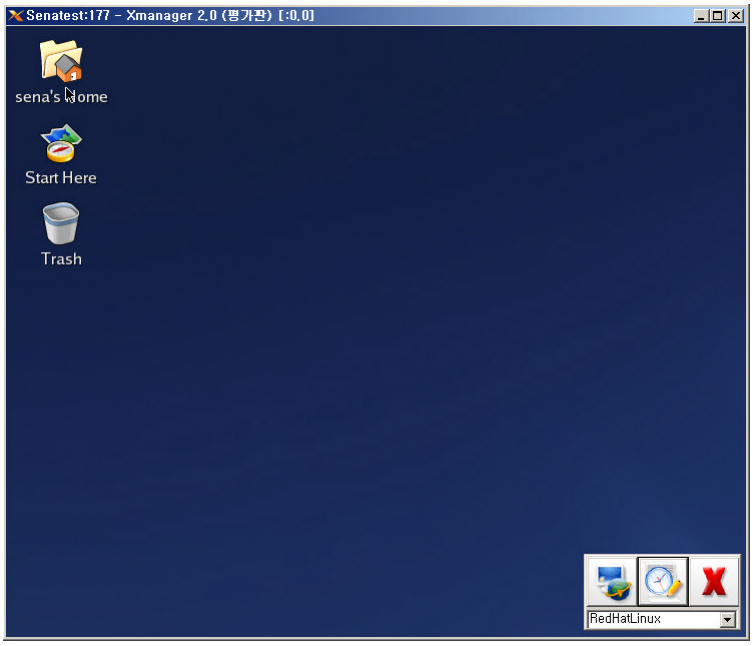


그림 I-6 freeKVM Tool – X window server

I.4 동작 및 기능

freeKVM Tool의 주요 기능은 다음과 같습니다.

1. 시리얼 포트 또는 리모트 포트의 원격 서버로의 연결
2. 시리얼 포트 또는 리모트 포트의 로그 표시
3. VTS II의 Serial port connection 화면에서 연결된 KVM 클라이언트 프로그램으로 이동

참고 :다음은 Windows용 freeKVM Tool에서의 동작 및 기능들입니다. Linux용 freeKVM Tool에서는 지원하지 동작 및 기능이 있습니다. 자세한 내용은 세나 기술 지원에 문의하시기 바랍니다

그림 I-7은 freeKVM Tool이 활성화 되었을 때의 화면입니다.

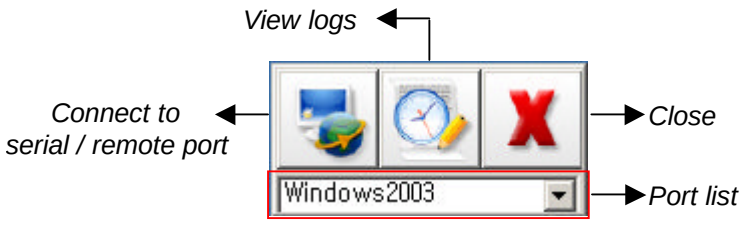


그림 I-7 freeKVM Tool Activated

그림 I-8은 freeKVM Tool이 비활성화 되었을 때의 화면입니다.

그림 I-8 freeKVM Tool Deactivated

Serial port connection 화면에서 연결된 KVM 클라이언트 프로그램이 포커스를 갖게 되면 freeKVM Tool이 활성화됩니다. freeKVM Tool이 활성화 되었을 때 시리얼 포트 또는 리모트 포트로 연결하고, 포트 로그도 표시하는 기능을 사용할 수 있습니다. KVM 클라이언트 프로그램 이외의 다른 프로그램이 포커스를 갖게 되면 freeKVM Tool은 비활성화 되고, 시리얼 포트 / 리모트 포트로 연결과 포트 로그를 표시하는 기능은 사용할 수 없게 됩니다.

freeKVM Tool 활성화되었을 때 Connect 버튼을 클릭하면 해당 시리얼 포트 또는 리모트 포트로 연결합니다. 그림 I-9는 Connect 버튼을 클릭하여 Port #1에 연결했을 때의 화면입니다.

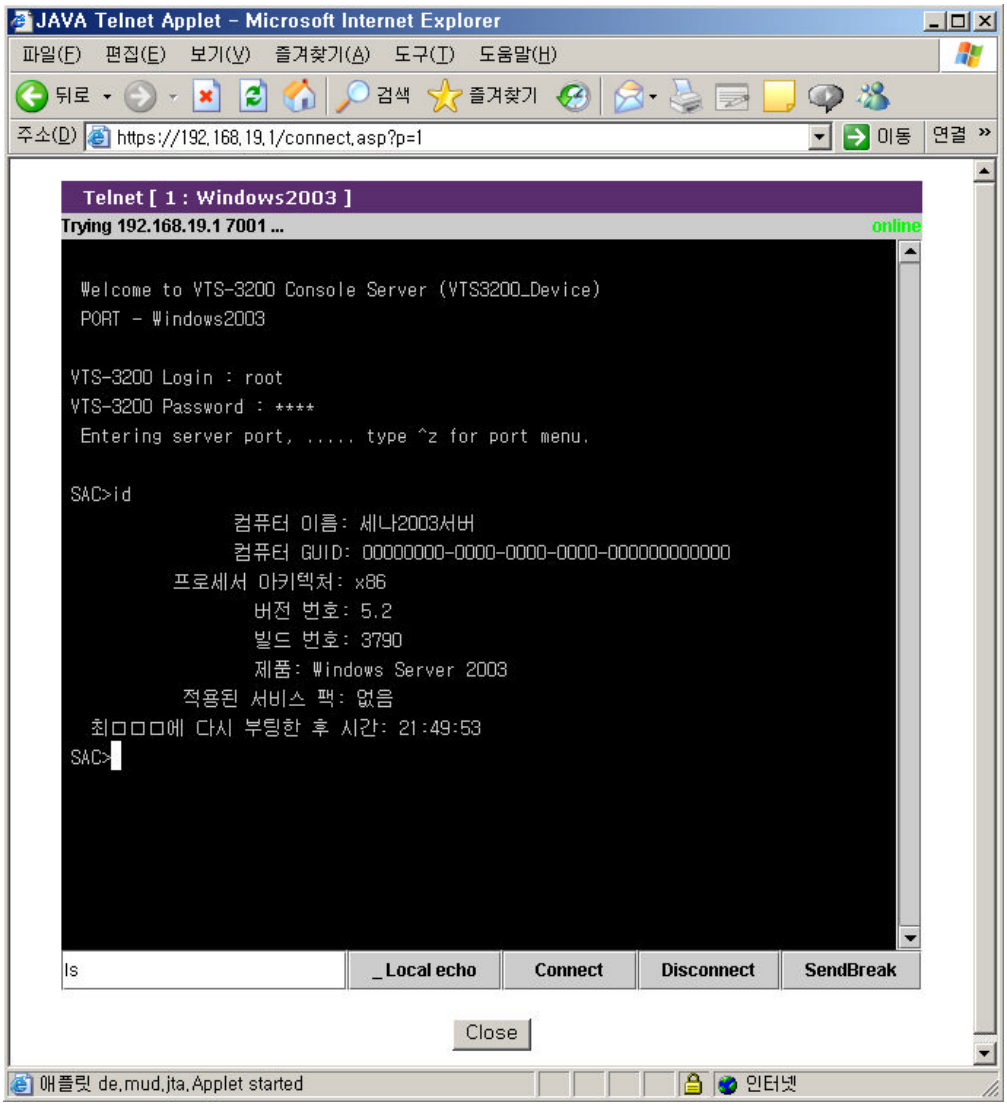


그림 I-9 Connect to serial port

freeKVM Tool 활성화되었을 때 View logs 버튼을 클릭하면 해당 시리얼 포트 또는 리모트 포트의 로그를 표시합니다. 그림 I-10은 View logs 버튼을 클릭하여 Port #1의 로그를 표시한 화면입니다.

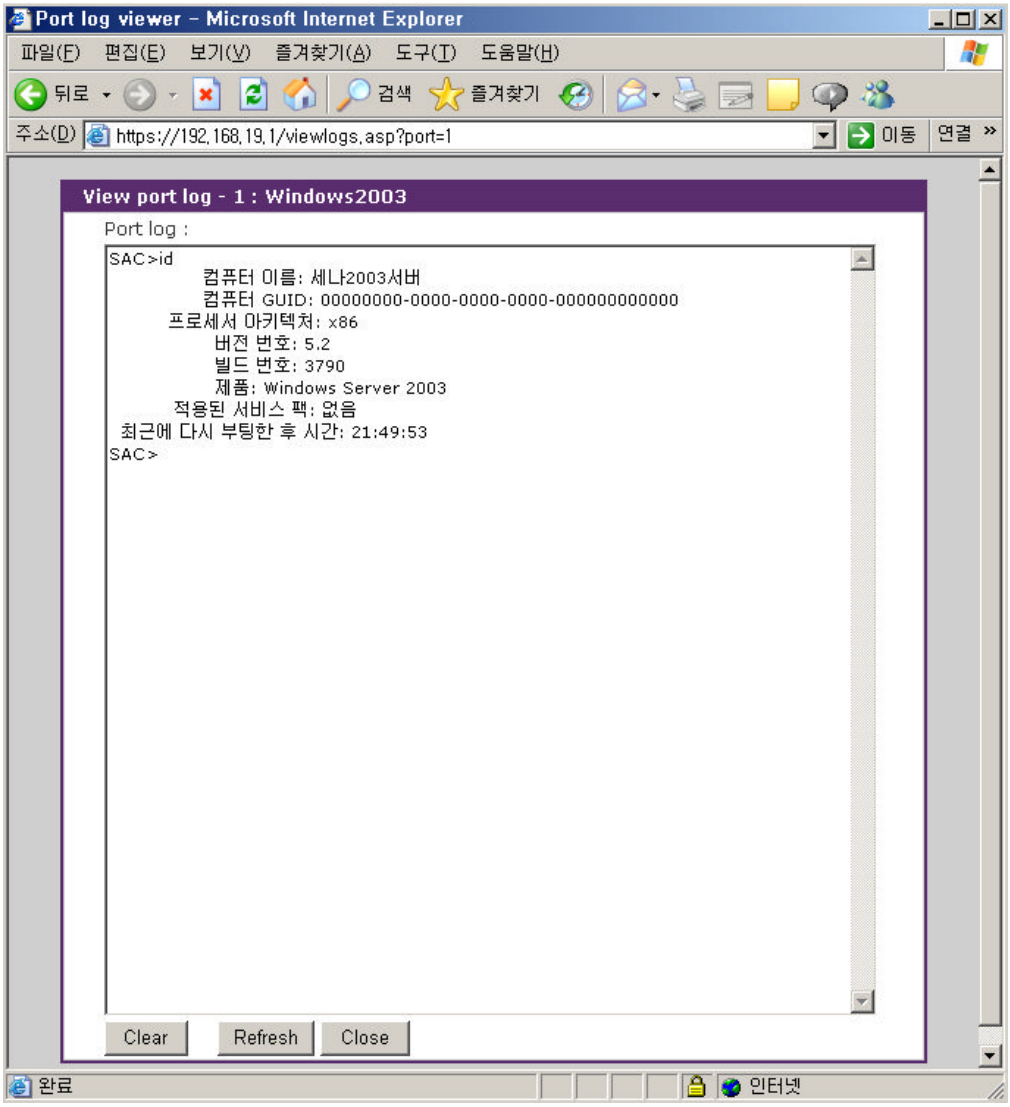


그림 I-10 View port logs

Serial port connection 화면에서 해당 포트의 작업리스트에 있는 freeKVM 연결 아이콘을 클릭하여 KVM 클라이언트 프로그램을 열 때마다 Port list에 포트 타이틀이 추가됩니다. 이 리스트 중의 포트 타이틀을 선택하면 해당 포트의 KVM 클라이언트 프로그램으로 이동할 수 있습니다. 그림 I-11은 I.3의 예에서와 같이 설정하고 실행했을 경우의 Port list를 보여줍니다.

그림 I-11 Port list

freeKVM Tool의 위치를 이동하려면 마우스 오른쪽 버튼을 클릭한 상태에서 원하는 위치로 끌어 놓으면 됩니다.

freeKVM Tool을 종료하려면 Close 버튼을 클릭하면 됩니다.

부록 J: 품질 보증 정책

J.1 제품 품질 보증 정책

주식회사 세나테크놀로지 (이하 “SENA”) 는 제품이 기술명세 및 부속 자료에 명시된 사양에 부합하고 그에 따라 작동하며, 보증 기간 동안 재료 및 공법상 하자가 없음을 보증한다. 보증기간은 제품을 수령하는 시점부터 시작된다.
SENA의 보증 범위는, SENA의 자체적 판단에 따라, 하자 또는 부적합 제품의 수리 또는 교체로 국한되며, (a) 제품을 잘못 적용 또는 사용하는 경우 (b) 사용자가 SENA의 사용 지침을 준수하지 않은 경우; (c) 제품의 관리 소홀, 남용 및 우발적인 사고의 경우; 또는 (d) SENA가 제공하지 않은 장비나 소프트웨어와 관련된 경우에 생기는 기능상 문제에 대해서는 책임지지 않는다.
사용자는 구매 또는 수령일자를 증빙하는 자료와 함께 제품을 SENA 또는 제품을 구매한 해외 딜러에게 보냄으로써 제한적 보증 서비스를 받을 수 있다. 이 때, 사용자는 운송 중 생길 수 있는 제품 분실 또는 파손의 가능성을 인지하고, 운송비를 선지급하며, 원래의 운송 포장 등을 사용하기로 합의한다.

J.2 책임의 한계

SENA는, 본 문서에 명시된 경우를 제외하고는, 본 계약에 따라 제공되는 장비, 부품 또는 서비스에 대해 어느 특정 용도에 대한 상업성이나 적합성 여부를 포함한 어떠한 보증도 명시적이든 묵시적이든 하지 않는다. SENA 또는 그 딜러는, 손해 가능성에 대한 사전 인지 여부와 관계없이 본 계약에 따라 제공되는 장비, 부품 또는 서비스가 기대한대로 동작하지 않는 경우 발생될 수 있는 직접, 간접, 부수, 특별 또는 결과적 손해나 기대 이익의 손실 등 어떠한 다른 손해에 대하여 책임을 지지 않는다.
어떠한 경우에도 SENA 또는 그 딜러의 책임 한도는 제품의 지불된 판매 가격을 초과하지 않는다.

J.3 하드웨어 제품 보증 상세 내용

SENA는 내장 하드웨어 제품을 일(1)년간 보증하고, 외장 하드웨어 제품을 제품에 따라서 삼(3)년간 또는 오(5)년간 보증한다.
보증절차: 하드웨어 제품이 반환된 경우, SENA는 자체 판단에 따라 추가 비용 없이 제품을 수리 또는 교체한다. 단, 아래에 해당되는 경우는 제외한다. 수리 부품과 교체 제품은 일대일 교환 형태로 제공되며, 재생 또는 신제품으로 할 수 있다. 교체된 제품 및 부품은 SENA로 귀속된다. 제품에 대해 보증이 적용되지 않는 것으로 SENA가 판단한 경우, SENA는 고객의 선택에 따라 부품 및 노무에 관한 SENA의 표준 요율에 따라 제품을 수리하거나 또는 제품을 그냥 반환할 수 있다.

보증 제외 경우:
- 사고, 떨어뜨린 경우, SENA 제품에 충격을 가한 경우,
- SENA의 온도 및 습도 명세를 초과한 환경에서 제품을 작동한 경우,
- 전원 불안정, 고압 방전으로 인한 경우,
- 부적절한 접지 및 부정확한 배선으로 인한 경우,
- 고객 등의 오용, 부주의로 인한 경우,
- SENA 사용자 매뉴얼에 따라 제품을 설치 또는 작동하지 않은 경우,
- 고객 또는 제3자의 부적절한 유지보수로 인한 경우,
- 홍수, 번개, 지진으로 인한 경우,
- 물을 쏟은 경우,
- 통상의 마모로 인한 부품 교체,
- 하드웨어가 변경된 경우,
- SENA의 서면 합의 없이 제3자가 수리를 시도한 제품,
- 하드웨어에 SENA 소프트웨어의 변형, 또는 SENA 소프트웨어 이외의 소프트웨어를 사용한 경우, SENA가 변형을 승인한 경우 제외.
- 소모품인 충전용 배터리의 사용 시간이 제품의 사용 방법과 기간에 따라서 최초 구입시보다 현저히 줄어든 경우.

J.4 소프트웨어 제품 보증의 상세

보증기간: 소프트웨어 제품의 보증기간은 일(1)년으로 한다.
보증범위: SENA의 보증은 사용자가 SENA에게 소프트웨어 부적합을 통보한 때로부터 합리적 시간 내에 소프트웨어 버그 픽스 또는 패치를 제공하는 것으로 제한된다.

J.5 제3자 소프트웨어 제품 보증의 상세

제3자 소프트웨어의 보증정책은 해당 벤더의 품질 보증 정책을 따른다.