콘솔 관리 서버
VTS 시리즈

사용 설명서

버전 1.7.0

2005-5-25

VTS 시리즈 사용 설명서
버전 v1.7.0
펌 웨어 버전 v1.7.0
Printed in Korea

등록 상표
HelloDevice™은 세나테크놀로지의 상표입니다.
Windows R는 Microsoft 사의 등록 상표입니다.
Ethernet R은 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) 573-5422
팩스: (02) 573-7710
email: support@sena.com
웹 사이트: http://www.sena.com

개정 요약

Revision	Date	Name	Description
V1.1.0	2003-06-11	J.W. Woo	Firmware v1.1.0 update 반영
V1.2.0	2003-08-28	O.J. Jung	Firmware v1.2.0 update 반영
V1.3.2	2003-10-07	H.R. Joe	Firmware v1.3.2 update 반영
V1.4.1	2003-12-16	H.R. Joe	Firmware v1.4.1 update 반영
V1.5.1	2004-06-03	H.R. Joe	Firmware v1.5.1 update 반영
V1.5.3	2004-07-15	H.R. Joe	Firmware v1.5.3 update 반영
V1.6.0	2004-10-01	H.R. Joe	Firmware v1.6.0 update 반영
V1.6.1	2004-12-01	Kumar	Updates in the package checklist in this manual
V1.6.5	2005-02-24	K.T Lee	Firmware v1.6.5 update 반영
V1.7.0	2005-05-25	H.R. Joe	Firmware v1.7.0 update 반영

목차

1: 서론

1.1 개요

VTS는 임베디드 Linux 기반 콘솔 관리 서버입니다. 이 제품은, Linux 상에서 구현된 각종 최신 프로토콜을 구비하고 있으며, 1개의 PC 카드 인터페이스 슬롯을 제공함으로써, 사용자의 응용에 있어서의 유연성을 극대화하였습니다.

IT 전문가, 네트워크 관리자 그리고 유틸리티 관리자들은 VTS를 이용하여 네트워크를 통해 시리얼 콘솔 포트가 있는 서버, 라우터, 스위치 및 기타 랙 시스템과 같은 IT/Telco 장비를 원격 관리할 수 있습니다.

VTS 장비는 콘솔 포트 접속을 위해, 4/816/32 개의 시리얼 포트를 가지고 있습니다. VTS는 각 시리얼 포트에 RS232를 지원함으로써 거의 모든 RS232 시리얼 장치를 네트워크를 통해 접속할 수 있게 합니다.

VTS는 TCP/IP, UDP 및 PPPoE (PPP-Over-Ethernet)와 같은 네트워크 프로토콜을 지원함으로써, DSL 기반의 초고속 인터넷 연결 또는 기존 LAN 환경 상에서의 동시 장비 관리 기능을 제공합니다.

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 VTS에 접근 가능하도록 하는 규약을 지원합니다.

VTS는 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

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

1.2 패키지 체크 리스트

- VTS 외장 박스
- 전원 케이블
- 19 인치 랙 설치 키트
- 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
- HelloDevice Manager, HelloDevice VirtualCOM 및 매뉴얼이 포함된 CD-ROM

1.3 제품 사양

	VTS400	VTS800	VTS1600	VTS3200	VTS4800
시리얼 인터페이스	4-포트	8-포트	16-포트	32-포트	48-포트
	RJ45 커넥터가 있는 RS232				
	시리얼 속도 1200bps ~ 230Kbps				
	흐름 제어: none, 하드웨어 RTS/CTS, 소프트웨어 Xon/Xoff				
	신호: RS232 Rx, Tx, RTS, CTS, DTR, DSR, DCD, GND				
	모뎀 제어: DTR/DSR 및 RTS/CTS				
네트워크 인터페이스	RJ45 Ethernet 커넥터를 장착한 10/100 Base Ethernet				
	고정 및 유동 IP 주소 지원				
프로토콜	ARP, IP/ICMP, TCP, telnet, SSH v1 & v2, DNS, Dynamic DNS, HTTP, HTTPS, Authentication, SMTP,DHCP client, NTP, PPPoE, SNMP v1 및 v2 (MIB II), RIP, Static routing				
PC 카드 인터페이스	다음 PC 카드 지원: ATA/IDE fixed disc card / PSTN/CDMA 모뎀 카드 LAN 카드/ 802.11b 무선 LAN 카드				
포트 기능	Host mode 콘솔 서버, 터미널 서버, 전화 모뎀 접속, 전화 접속 터미널 서버				
	포트 버퍼링 및 로깅: RAM 디스크 또는 ATA 메모리 카드 또는 NFS 서버 또는 syslog 서버				
	장비 경고 메시지에 따른 email 또는 SNMP trap 통지				
보안	사용자 ID 및 암호				
	보안 터미널 인터페이스: 공개 키가 있는 SSH				
	포트에 대한 사용자 그룹 관리 및 사용자 접속 관리				
	RADIUS, TACACS+, LDAP, Kerberos Authentication				
	IP 주소 필터링				
Clustering	NAT-기반의 효율적이고 Secure Clustering 지원				
	최대 544개의 장비를 동시에 관리 가능				
관리	시리얼 콘솔 포트, telnet, 웹, HelloDevice Manager				
	시스템 로깅 시스템 로그를 자동으로 email/SNMP 전달 RAM 디스크 또는 ATA 메모리 카드 또는 NFS 서버 또는 syslog 서버				
	시스템 상태 다양한 시스템 상태 표시 기능				
	펌웨어 telnet, 시리얼 콘솔 또는 웹 인터페이스를 통한 다운로드 가능 기능				
전원	5VDC		110 ~ 240VAC		110 ~ 240VAC Dual power (Option)
크기 LxWxH(mm)	245 x 153 x 30		432 x 193 x 44.5		443 x 253 x 44
			19 인치 랙에 탑재 가능		
무게(kg)	1.5		2.8		3.0(Single Power) 3.1(Dual Power)
인증	FCC, CE, MIC				
품질보증 기간	5년				

1.4 용어 및 약어

이 섹션은 본 매뉴얼에서 일반적으로 사용되는 용어를 정의합니다. 이 용어들은 인터넷과 관련이 있으며 VTS의 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. VTS의 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 VTS를 처음 설치하고 설정하는 방법에 대하여 설명합니다

- *2.1 패널 배치*에서는 패널 배치 및 LED 표시 등을 설명합니다.
- *2.2 하드웨어 연결하기*에서는 VTS의 전원, 네트워크 및 장치 연결 방법을 설명합니다.
- *2.3 시스템 콘솔에 접속하기*는 시스템 콘솔 또는 telnet 또는 웹 메뉴를 사용하여 VTS의 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 VTS3200 패널 배치

VTS3200은 그림 2-1(예, 시스템, Ethernet 및 시리얼 포트)에서와 같이 상태 표시를 위한 LED 표시등이 3개 있습니다. 왼쪽에 있는 처음 3개의 표시등은 전원, 준비, PC Card 인터페이스를 나타냅니다. 다음 3개의 표시등은 Ethernet 100Mbps, 링크, 활성에 대한 상태를 나타냅니다. 다음 표시등은 시리얼 포트의 사용, 수신 및 송신 상태를 나타냅니다. 표 2-1은 각 LED 표시등의 기능을 설명합니다. 패널 뒷부분은 RJ45 커넥터, Ethernet 포트, VTS3200 콘솔 포트, 전원 소켓의 시리얼 포트들을 보여주고 있습니다.

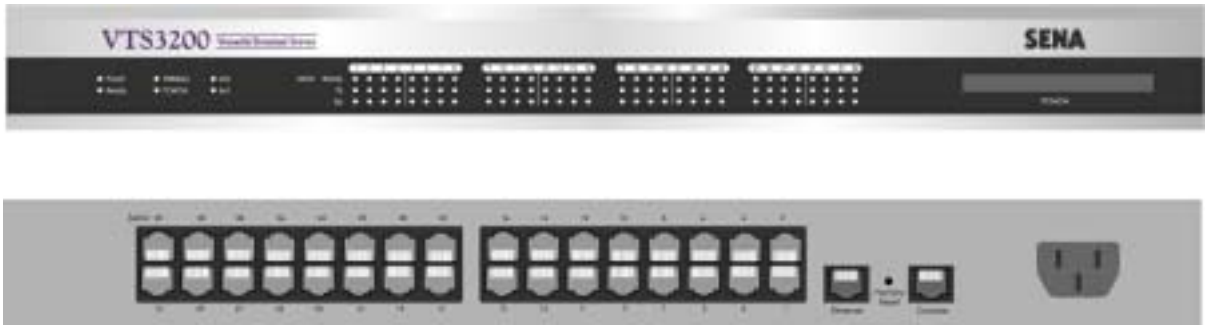


그림 2-1. VTS3200의 패널 배치

표 2-1. VTS3200의 LED 지시 램프

표시등		기능
시스템	Power	전원이 공급되는 경우 점등 됩니다.
	Ready	시스템 작동이 준비되는 경우 점등 됩니다
	PC Card	PC Card 장치가 작동되는 경우 점등 됩니다
Ethernet	100Mbps	100Base-TX 연결되는 경우 점등 됩니다
	LINK	Ethernet 네트워크에 연결되는 경우 점등 됩니다
	Act	Ethernet 포트를 통해 패킷이 들어오고 나가는 경우 깜박거립니다
시리얼 포트	InUse	시리얼 포트가 사용 중인 경우 점등 됩니다 (포트 버퍼링이 가능 상태 또는 포트 접속 기능이 사용 중인 경우)
	Rx/Tx	시리얼 포트를 통해 들어오고 나가는 데이터 흐름이 있을 때, 깜박거립니다.

2.1.2 VTS1600 패널 배치

VTS1600의 전면 패널은 VTS3200의 전면 패널과 거의 유사합니다. 단지, VTS1600은 16개의 시리얼 포트 표시등을 가지고 있는 반면 VTS3200는 32개의 시리얼 포트 표시등을 가지고 있습니다. 자세한 정보는 ***2.1.1. VTS3200 패널 배치***를 참조하십시오.

2.1.3 VTS800 패널 배치

VTS800의 전면 패널은 VTS3200의 전면 패널과 거의 유사합니다. 단지, VTS800은 8개의 시리얼 포트 표시등을 가지고 있는 반면 VTS3200는 32개의 시리얼 포트 표시등을 가지고 있습니다. 자세한 정보는 ***2.1.1. VTS3200 패널 배치***를 참조하십시오.

2.1.4 VTS400 패널 배치

VTS400의 전면 패널은 VTS3200의 전면 패널과 거의 유사합니다. 단지, VTS400은 4개의 시리얼 포트 표시등을 가지고 있는 반면 VTS3200는 32개의 시리얼 포트 표시등을 가지고 있습니다. 자세한 정보는 ***2.1.1. VTS3200 패널 배치***를 참조하십시오.

2.1.5 VTS4800 패널 배치

VTS4800은 그림 2-2에서와 같이 크게 두 종류(예, 시스템 및 Ethernet)의 상태 표시를 위한 LED 표시등이 있습니다. 왼쪽에 있는 처음 4(5)개의 표시등은 전원 1(2), 준비, PC Card 인터페이스 및 파인드미(finde Me)를 나타냅니다. 다음 3개의 표시등은 Ethernet 100Mbps, 링크, 활성에 대한 상태를 나타냅니다. VTS4800에는 다른 모델과 달리 시리얼 포트에 대한 표시등은 없습니다. 표 2-2는 각 LED 표시등의 기능을 설명합니다. 패널 뒷부분은 RJ45 커넥터, Ethernet 포트, VTS4800 콘솔 포트, 전원 소켓의 시리얼 포트들을 보여주고 있습니다.

(듀얼 파워 모델의 전면 패널)

(싱글 파워 모델의 전면 패널)

(후면 판넬)

그림 2-2. VTS4800 의 패널 배치

표 2-2. VTS4800의 LED 지시 램프

표시등		기능
시스템	Power	전원이 공급되는 경우 점등 됩니다.
	Ready	시스템 작동이 준비되는 경우 점등 됩니다
	PC Card	PC Card 장치가 작동되는 경우 점등 됩니다
	Find Me	사용자가 HD manger 를 통하여 장치를 probing 할 경우 깜박거립니다
Ethernet	100Mbps	100Base-TX 연결되는 경우 점등 됩니다
	LINK	Ethernet 네트워크에 연결되는 경우 점등 됩니다
	Act	Ethernet 포트를 통해 패킷이 들어오고 나가는 경우 깜박거립니다

2.2 하드웨어 연결하기

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

- VTS에 전원 공급 장치를 연결합니다.
- VTS를 Ethernet 허브 또는 스위치에 연결합니다.
- 해당 장치에 연결합니다.

2.2.1 전원 연결하기

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

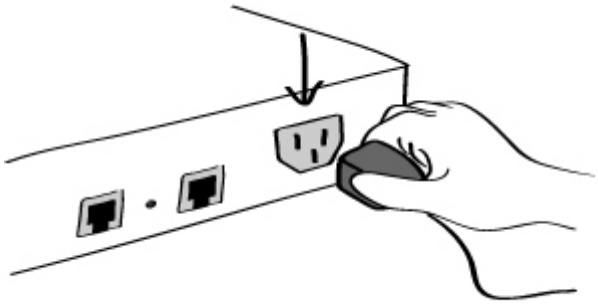


그림 2-3. VTS에 전원 연결하기

2.2.2 네트워크에 연결하기

Ethernet 케이블의 한쪽 끝을 VTS Ethernet 포트에 연결하고, 나머지 다른 Ethernet 케이블의 종단면을 네트워크 포트에 연결합니다. 케이블이 올바르게 연결된 경우, VTS와 Ethernet 네트워크간의 연결표시는 다음과 같이 나타납니다.

- [Link] 표시등은 녹색 점등 상태를 유지합니다.
- [Act] 표시등은 계속해서 깜박거리면서 Ethernet 패킷의 송수신이 여부를 나타냅니다.
- VTS가 100Base-TX 네트워크에 연결되는 경우 [100Mbps] 표시등은 녹색 점등 상태를 유지합니다.
- 현재의 네트워크 연결이 10Base-T인 경우 [100Mbps] 표시등은 켜지지 않습니다.

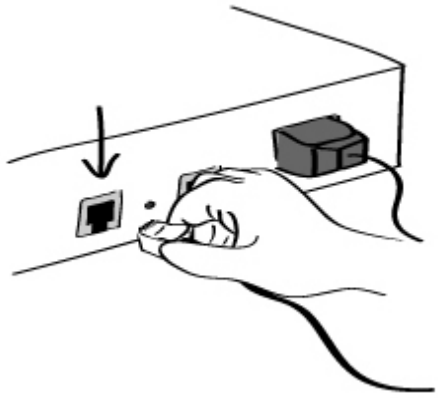


그림 2-4. VTS에 네트워크 케이블 연결하기

2.2.3 해당 장치에 연결하기

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

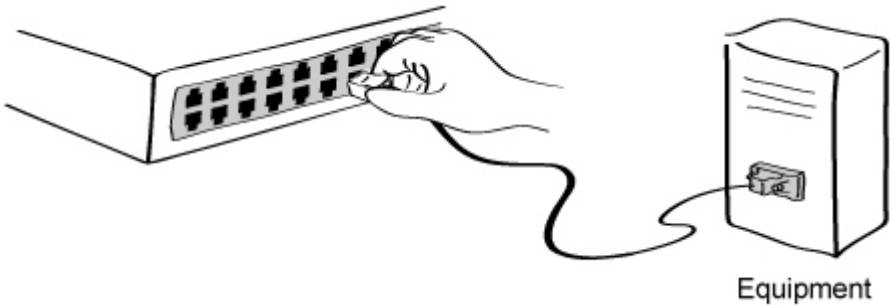


그림 2-5. 장비를 VTS에 연결하기

2.3 시스템 콘솔에 접속하기

VTS에 접속하는 방법은 여러 가지가 있습니다. 이는, 사용자의 위치가 현지 또는 원격이냐 여부에 따라 달라집니다. 또한, VTS는 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 VTS의 시스템 콘솔 포트에 직접 연결할 수 있습니다.
- 원격 콘솔:
텍스트 메뉴 인터페이스를 요구하는 원격 사용자는 터미널 에뮬레이터를 사용해 VTS의 telnet(TCP 포트 23) 또는 SSH(TCP 포트 22)에 접속할 수 있습니다.
- 웹:
웹 브라우저를 사용하여 VTS를 설정하려는 원격 사용자는 Internet Explorer 또는 Netscape Navigator와 같은 웹 브라우저를 사용하여 VTS에 연결할 수 있습니다.

위의 방법들은 모두 VTS 시스템으로의 로그인을 요구합니다.

2.3.1 시스템 콘솔 사용하기

1) 콘솔/Ethernet 케이블의 한쪽 끝을 VTS의 콘솔 포트에 연결합니다.

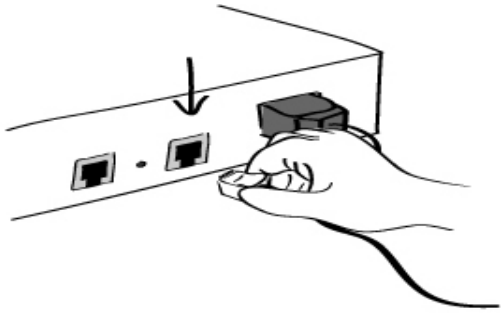


그림 2-6. VTS에 시스템 콘솔 케이블을 연결하기

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 VTS에 로그인 합니다. 다음과 같이 디폴트 값 사용자 설정을 합니다.

   Login: root Password: root

   Login: admin Password: admin

```
192.168.161.5 login: root
Password:****
root@192.168.161.5:~#
```

```
192.168.161.5 login: admin
Password:

 Welcome to VTS-3200 Configuration
 Press Enter
```

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 2-6에 있는 메뉴 화면이 나타납니다.

```
192.168.161.5 login: admin
Password:

------------------------------------------------------------------------------
 Welcome to VTS-1600 configuration page
 Current time : 02/25/2003 16:46:34    F/W REV.    : v1.0.0
 Serial No.   : vts32000302-00001     MAC Address  : 00-01-95-a1-89-b7
 IP mode      : Static IP             IP Address   : 192.168.161.5
------------------------------------------------------------------------------
 Select menu
 1. Network Configuration
 2. Serial Port Configuration
```

```
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
   <ENTER> Refresh
----->
```

그림 2-7. 메인 메뉴 화면(VTS 3200)

메인 메뉴 화면의 사용자는 메뉴 번호를 입력하거나 [ENTER] 키를 눌러 VTS 파라미터 설정에 필요한 메뉴 항목을 선택할 수 있습니다. 하위 메뉴 화면에 있는 사용자는 온라인 설명을 통해 제공된 필수 파라미터를 설정할 수 있습니다. 모든 파라미터는 VTS의 비휘발성 메모리 공간에 저장되며, 이는 사용자가 *메뉴 8. Save Changes*을 선택하여 저장할 수 있습니다. *메뉴 a. Exit and Apply Changes* 또는 *b. Exit and Reboot* 을 선택한 다음 모든 변경 사항을 설정할 수 있습니다.

2.3.2 원격 콘솔 사용하기

사용자는 원격 콘솔을 사용하는 VTS에 접속하기 전에 반드시 VTS의 IP 주소를 알아야 합니다. (자세한 내용은 ***3. 네트워크 설정***을 참조하십시오). VTS의 공장 출하시 기본 IP 주소는 192.168.161.5입니다.
원격 콘솔 기능은 원격 호스트 접속 옵션에서 disable 될 수 있습니다.(자세한 내용은 섹션 3.5의 ***IP 필터링***을 참조하십시오). VTS는 원격 콘솔을 위한 telnet 및 SSH 프로토콜 모두를 지원합니다.

다음의 지침에 따라 VTS 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 VTS와 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.

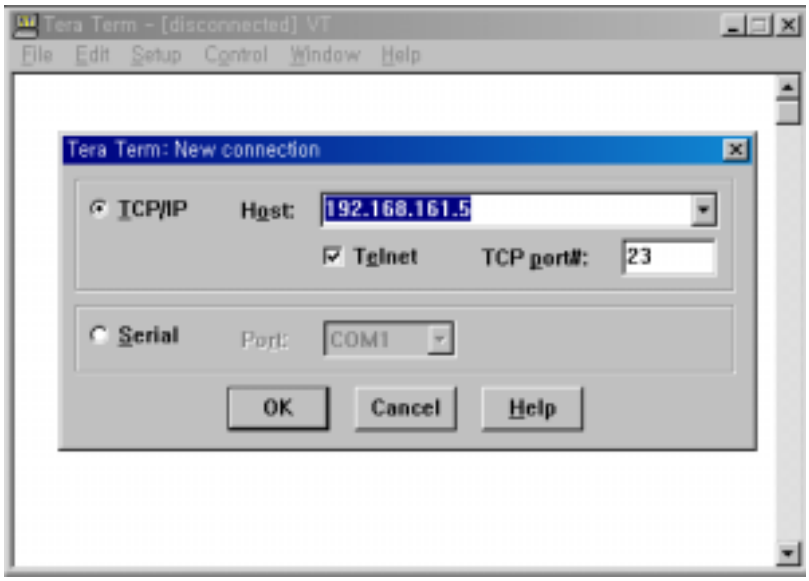


그림 2-8. Telnet 프로그램 설정 예제 (TeraTerm Pro)

2) 사용자는 반드시 VTS로 로그인해야 하며, 이때 사용자 이름과 암호를 입력합니다. 사용자 이름 및 암호의 디폴트 설정은 시스템 root를 위한 **root** 및 시스템 관리자를 위한 **admin** 두 가지입니다(섹션 ***9.1. 사용자 관리를*** 참조하십시오).

3) VTS가 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

VTS는 HTTP 및 HTTPS(HTTP Over SSL) 프로토콜 모두를 지원합니다. VTS는 또한 HTTP 프로토콜을 지원하며, 자체 웹 관리 페이지가 있습니다. VTS 웹 관리 페이지에 접속하려면, VTS의 IP 주소, 또는 유효한 호스트 이름을 웹 브라우저 URL/Location 필드에 입력해야 합니다. 이를 통해 사용자는 VTS 로그인 화면으로 직접 이동할 수 있습니다. 사용자는 정확한 사용자 이름과 비밀번호를 사용하여 로그인 함으로써 인증을 받아야 합니다. 기본 설정은 다음과 같습니다.

Login: root Password: root

Login: admin Password: admin

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

그림 2-9. VTS 웹 관리 페이지 로그인 화면

그림 2-10은 VTS 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. 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]를 선택해야 합니다. 이 옵션은 메뉴 바 하단에서 사용할 수 있습니다. 사용자가 [Apply changes]를 선택한 경우에 한해, 새로운 파라미터 값이 VTS 설정에 적용됩니다. 사용자는 [Save & apply]를 선택하여 동시에 변경 사항을 저장하고[Save to flash] 적용[Apply changes]할 수 있습니다. 사용자가 새로운 파라미터 값을 저장하지 않고자 하는 경우, [Cancel]을 선택합니다. 모든 변경 사항은 손실되며 이전 값은 저장됩니다.

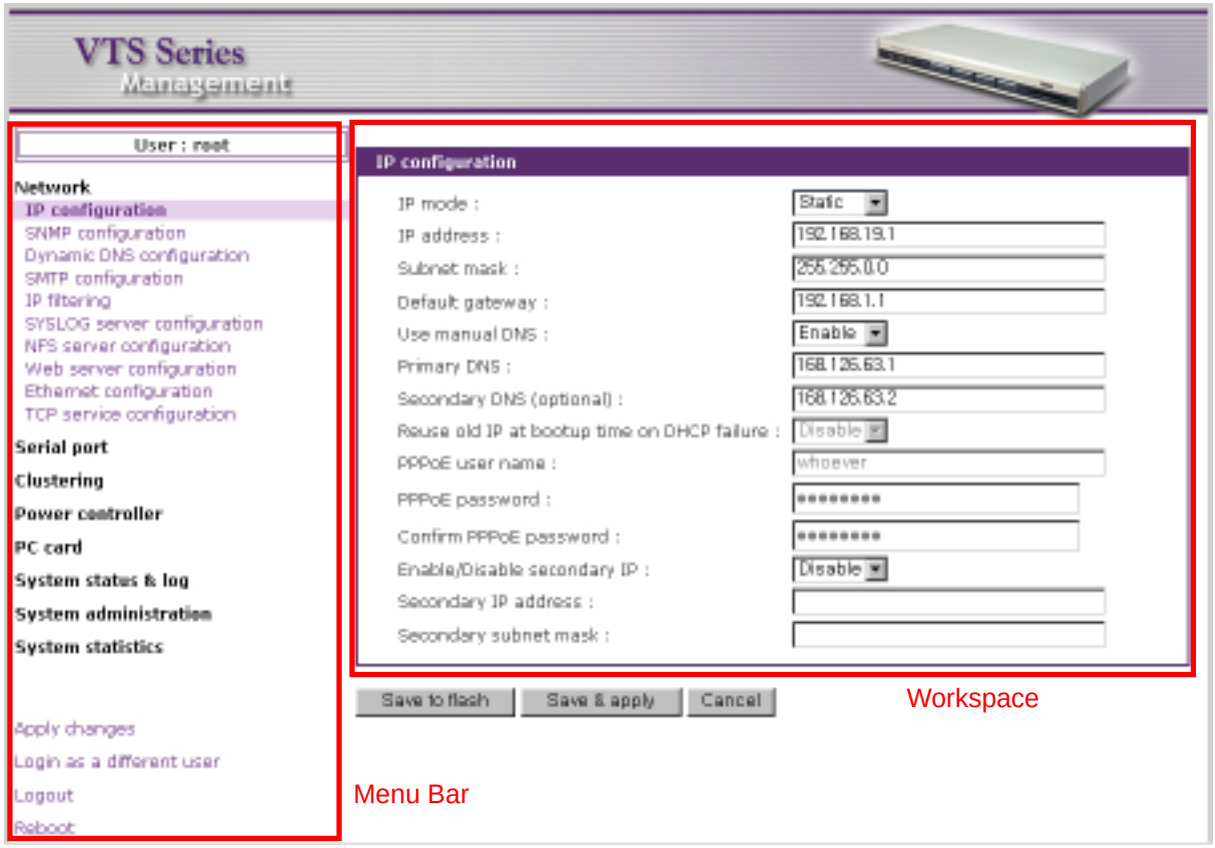


그림 2-10. VTS 웹 관리 화면

3: 네트워크 설정

3.1 IP 설정

사용자 네트워크 환경에서 VTS를 사용하려면, 유효한 IP 주소가 필요합니다. IP 주소가 준비되지 않은 경우, 시스템 관리자에게 문의하여 VTS를 위한 유효한 IP 주소를 할당 받습니다. 네트워크에 VTS를 연결하려면, 고유 IP 주소가 있어야 한다는 사실을 명심해야 합니다.
VTS IP 주소 설정 시, 사용자는 다음과 같은 3개의 인터넷 프로토콜 중의 하나를 선택할 수 있습니다.

- **Static IP**
- **DHCP** (Dynamic Host Configuration Protocol)
- **PPPoE** (Point-to-Point Protocol over Ethernet)

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

표 3-1. IP 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	Use manual DNS/Primary DNS/Secondary DNS (Optional)
	Reuse old IP at bootup time on DHCP failure
	Enable/Disable secondary IP/Secondary IP address/Secondary subnet mask
PPPoE	PPPoE User name
	PPPoE password
	Use manual DNS/Primary DNS/Secondary DNS (Optional)
	Enable/Disable secondary IP/Secondary IP address/Secondary subnet mask

IP mode를 **Disable**로 설정하여 네트워크에 VTS를 연결하지 않을 수도 있습니다.

Enable/Disable secondary IP가 Enabled로 설정되고, Secondary IP address와 Secondary subnet mask가 Static IP 프로토콜의 유효한 IP 주소가 설정되면, 사용자는 이 2차 IP 주소를 통하여 VTS로 연결할 수 있습니다. 2차 IP 주소를 설정하는 방법은 **3.1.1 Static IP 주소 사용하기**를 참조하시기 바랍니다.

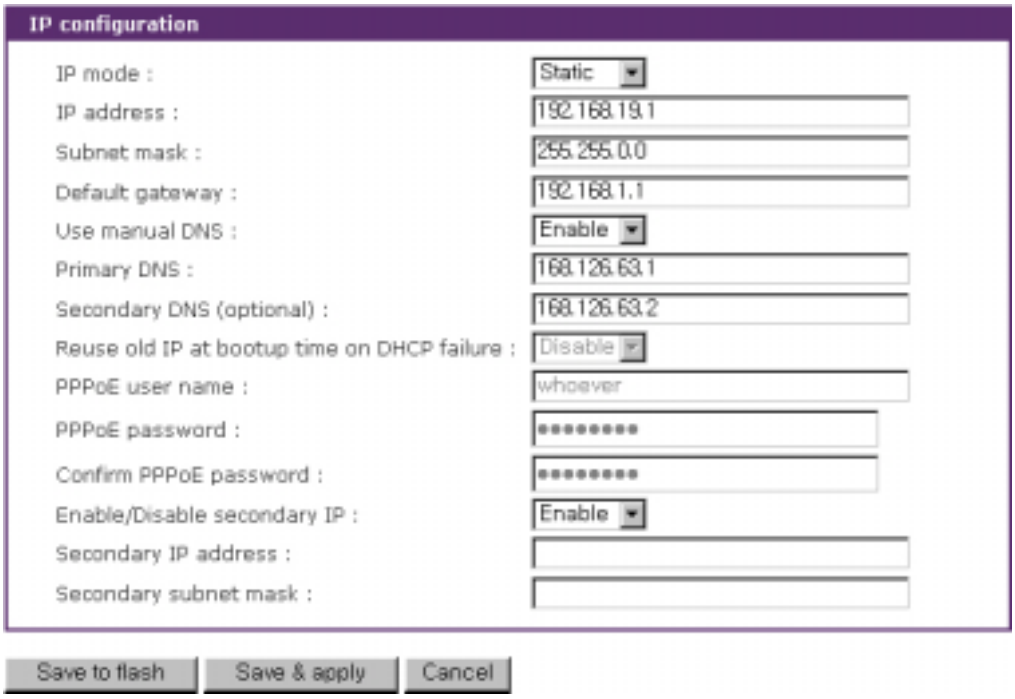


그림 3-1. IP 설정

3.1.1 Static IP 주소 사용하기

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

참고: *VTS는 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 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 시리즈는 패킷이 지정한 TCP/IP 호스트가 로컬 네트워크 영역에 있는지 서브넷 마스크를 통해 확인합니다. 주소가 VTS 시리즈와 동일한 네트워크 영역에 있다면 VTS 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 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 시리즈의 DNS 기능을 사용하려면 도메인 네임으로 호스트에 접속할 수 있도록 이 DNS 서버의 IP 주소를 설정해야 합니다. VTS 시리즈는 **Primary DNS server**와 **Secondary DNS server** 같은 DNS 서버의 IP 주소를 설정하는 방법을 제공합니다. Secondary DNS 서버는 Primary DNS 서버를 사용할 수 없을 때 사용하기 위해 지정합니다.

3.1.2 DHCP 사용하기

동적 호스트 설정 통신 규약(DHCP)은 네트워크 관리자가 IP 주소의 할당을 조직의 네트워크에 서 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.

VTS가 재설정될 때마다 VTS는 네트워크 상에서 DHCP 요청을 발송합니다. DHCP 서버의 응답에는

IP 주소를 비롯하여 서브넷 마스크, 게이트웨이 주소, DNS 서버 및 “대여” 시간이 포함되어 있습니다. VTS는 즉시 이런 정보를 자체 메모리에 저장합니다. “대여”가 만료되는 경우, VTS는 DHCP 서버로부터 ”대여” 시간의 연장을 요청합니다. DHCP 서버가 대여 연장을 승인할 경우, VTS는 계속해서 현재 IP 주소로 작동할 수 있습니다. DHCP 서버가 대여 연장을 승인하지 않는 경우, VTS는 DHCP 서버로부터 새로운 IP 주소 요청 절차를 시작합니다.

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

DHCP 서버는 네트워크 관리자가 관리하고 있는 IP 주소 풀에서 IP 주소를 동적으로 할당합니다. 이는 DHCP 클라이언트, 예를 들어 VTS가 작동될 때마다 다른 IP 주소를 수신합니다. DHCP 서버에서 IP 주소를 예약하여 사용자가 새롭게 할당된 VTS 주소를 항상 인식할 수 있도록 보장해야 합니다. DHCP 네트워크에서 IP 주소를 예약하려면 관리자는 VTS의 하단 부분에 있는 라벨 스티커에 있는 VTS의 MAC 주소를 알아야 합니다.

Reuse old IP at bootup time on DHCP failure을 **Enable**로 설정하면, VTS가 부팅될 때 DHCP 서버에서 VTS의 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.

3.1.3 PPPoE 사용하기

PPPoE는 모뎀 또는 유사 장치를 통해 Ethernet LAN(근거리 통신망)상의 여러 컴퓨터 사용자를 원격 사이트에 연결하기 위한 규격입니다. 여러 컴퓨터 사용자는 PPPoE를 사용해 인터넷에 ADSL, 케이블 모뎀 또는 무선 연결을 할 수 있습니다.
PPPoE 모드에서 VTS를 사용하려면 사용자는 PPPoE 계정 및 ADSL 모뎀과 같은 PPPoE 접속용 장비가 있어야 합니다. VTS가 PPPoE 프로토콜을 지원하기 때문에 ADSL 연결을 통해 인터넷 상의 원격 호스트에 접속할 수 있습니다. 사용자는 VTS에 대한 PPPoE 계정의 사용자 이름 및 암호를 설정해야만 합니다.
시동될 때마다 VTS는 PPPoE 서버와 PPPoE 연결을 시작합니다. 연결을 시작하는 동안 VTS는 IP 주소, 게이트웨이, 서브넷 마스크 및 DNS 서버와 같은 인터넷 연결에 필요한 정보를 수신합니다. 연결이 되면 VTS는 연결을 가능한 한 오래 유지하려 합니다. 연결이 종료되면 VTS는 새로운 연결을 요청하여 새로운 PPPoE 연결을 시도합니다.

***참고**: PPPoE 모드에서는 DNS 서버를 포함한 VTS의 모든 네트워크 관련 파라미터는 자동으로 설정됩니다. DNS 서버가 자동으로 설정되지 않은 경우, 사용자는 primary 및 secondary DNS IP*

주소를 입력함으로써 수동적으로 설정할 수 있습니다. DNS 주소를 자동 설정하려면, primary 및 secondary DNS IP 주소를 0.0.0.0 (권장됨)으로 설정합니다.

3.2 SNMP 설정

VTS는 SNMP v1 및 v2 프로토콜을 지원하는 SNMP(Simple Network Management Protocol)에이전트가 있습니다. NMS 또는 SNMP 브라우저와 같은 네트워크 관리자는 VTS로 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 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 3-2는 웹 인터페이스를 통한 SNMP 설정 화면을 보여줍니다.

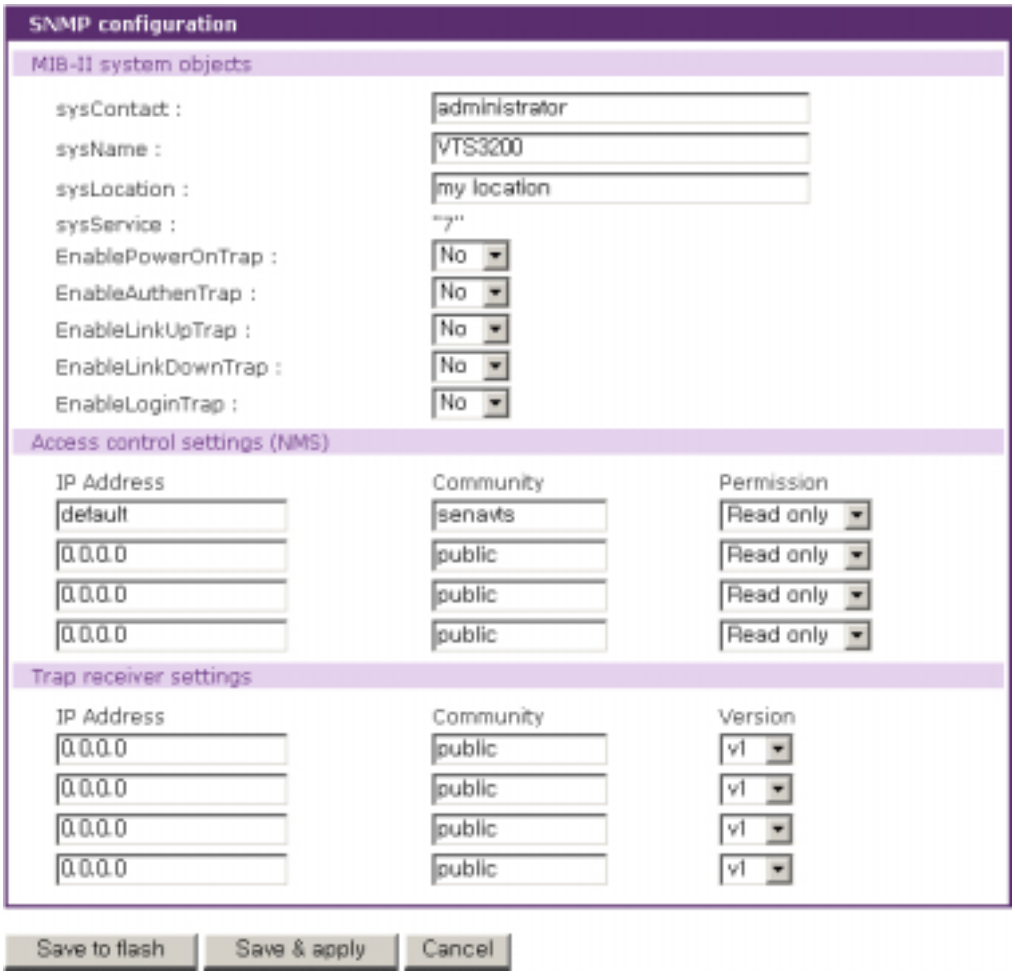


그림 3-2. SNMP 설정

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

MIB-II 시스템 객체 설정을 통해 시스템 연락, 이름, 위치 및 VTS의 SNMP 에이전트가 사용하는 인증 실패 정보(Authentication-failure traps)를 설정할 수 있습니다. 이러한 설정은 MIB-II sysName, sysContact, sysLocation, snmpEnableAuthenTraps, snmpEnablePowerOnTrap, snmpEnable AuthenTrap, snmpEnableLinkUpTrap, snmpEnableLinkDownTrap 그리고 snmpEnableLoginTrap 객체 식별정보 (OID)가 사용하는 값을 제공해 줍니다.

각 OID의 간단한 설명은 다음과 같습니다.

- sysContact: 관리 시스템(VTS)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 VTS는 응용 프로그램(7) 레벨만을 지원합니다.
- EnablePowerOnTrap: SNMP 에이전트 프로세스가 시스템이 시작되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다..
- EnableAuthenTrap: 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: SNMP 에이전트 프로세스가 Ethernet 연결이 되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.
- EnableLinkDownTrap: SNMP 에이전트 프로세스가 Ethernet 연결이 단절 되었는지에 관한 정보 생성을 허용할 것인지 여부를 나타냅니다.
- EnableLoginTrap: 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 SNMP 에이전트에 대한 관리자의 접속 가능성을 정의하고 있습니다. 이 메뉴 상에 설정된 관리자만이 VTS 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 SNMP 에이전트에 접속할 수 있습니다.

3.2.3 트랩 수신기 설정(Trap receiver settings)

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

3.2.4 SNMP를 이용한 관리

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

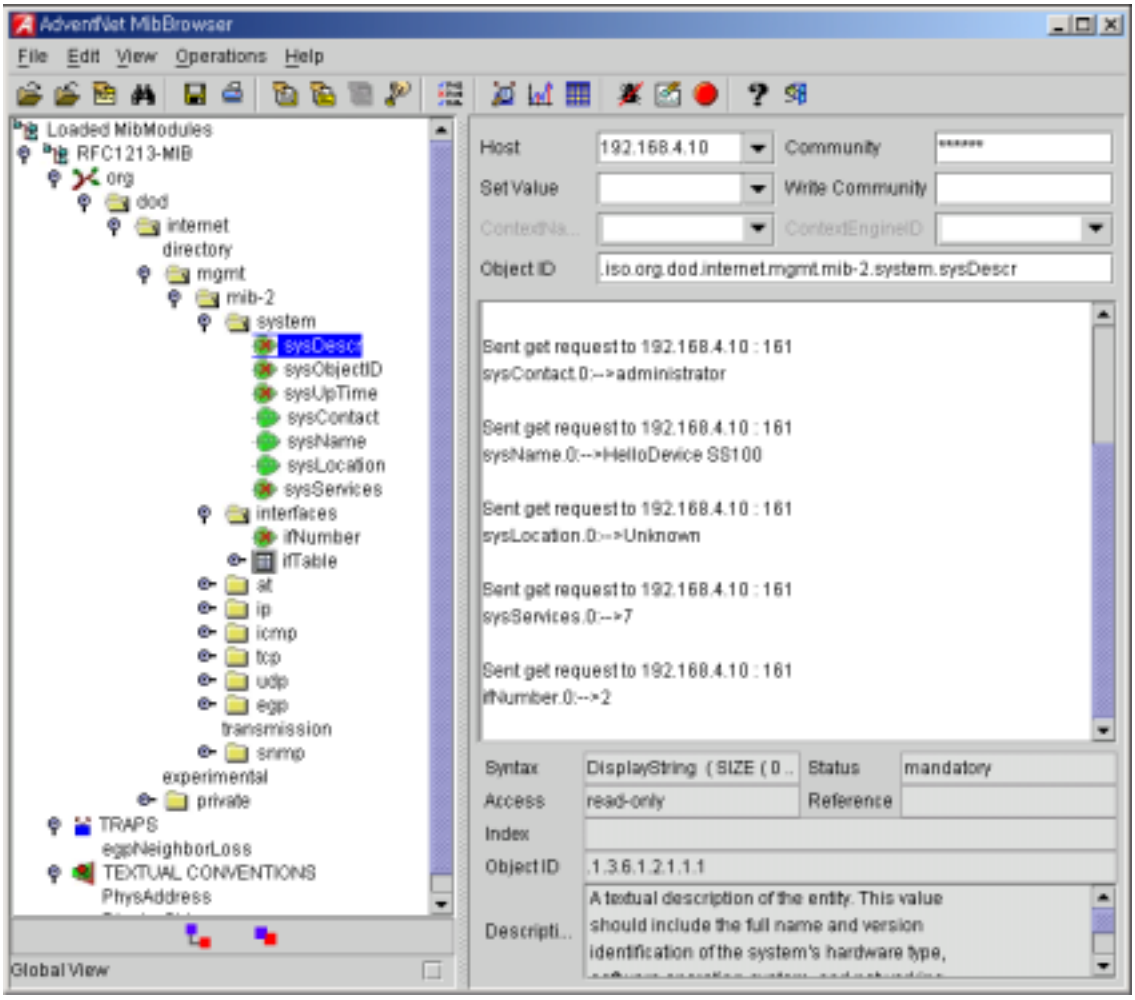


그림 3-3. SNMP 브라우저를 사용한 VTS SNMP 에이전트의 MIB-II OID 브라우징 (AdventNet MIB브라우저)

3.3 동적 DNS(Dynamic DNS) 설정

사용자가 VTS를 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 VTS에 접속할 수 있습니다.

일반적으로, VTS는 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 VTS에 접속할 수 있습니다.

그림 3-4는 동적 DNS 설정 웹 인터페이스를 보여줍니다.

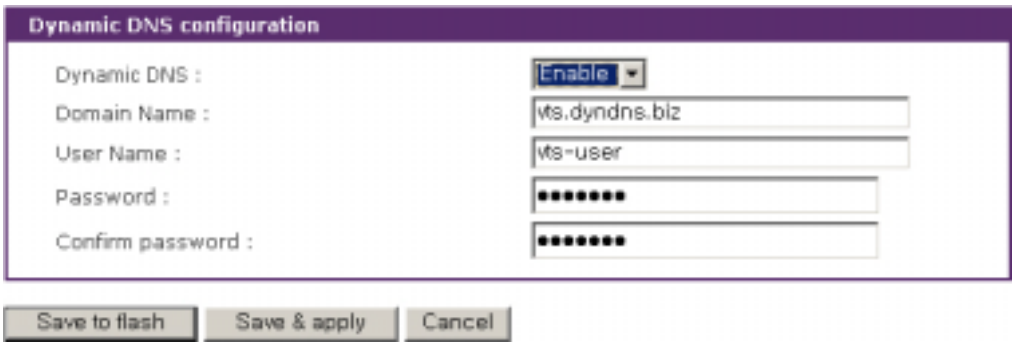


그림 3-4. 동적 DNS 설정

3.4 SMTP 설정

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

- 인증이 없는 SMTP
- 인증이 있는 SMTP
- 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

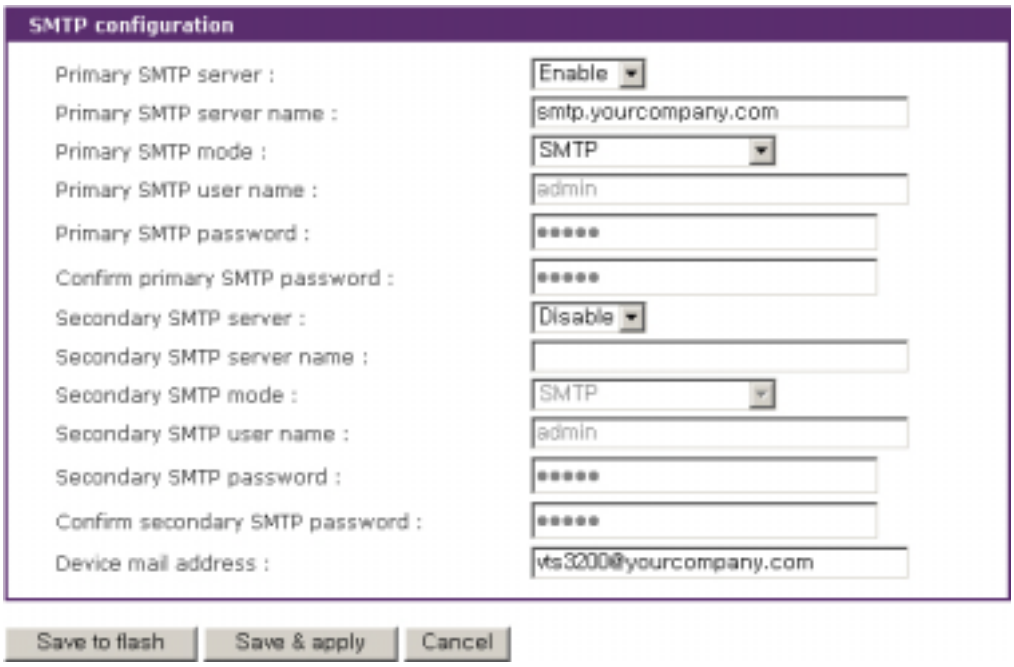


그림 3-5. SMTP 설정

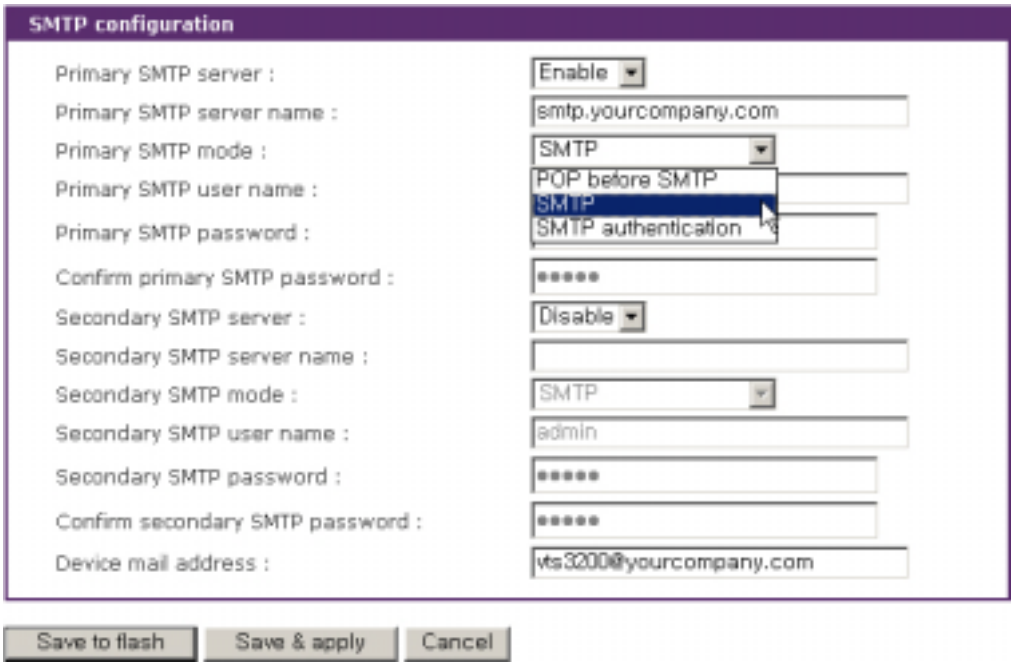


그림 3-6. SMTP 설정에서 SMTP 모드 선택

Device mail address는 모든 로그 및 경고 전달 email 위한 발신자, 즉, VTS의 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.

인증이 있는 SMTP 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

VTS는 IP 주소 기반의 필터링 규칙을 사용하여 승인 권한이 없는 호스티가 VTS에 접속하는 것을 막는 기능이 있습니다. IP 필터링 규칙을 설정하기 위한 항목에는 **Interface**, **Option**, **IP address/Mask**, **Port**와 **Chain rule**등이 있습니다.

Interface

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

- eth0 : VTS 기본 인터페이스
- eth1 : 네트워크 PC 카드나 무선 네트워크 PC 카드를 설정하여 생기는 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 3-2. IP 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
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

Port

호스트가 접속하려는 VTS의 포트번호나 포트번호 범위를 설정합니다. 포트범위를 입력하려면 port1:port2의 형식으로 입력합니다. port1은 포트범위의 시작 포트 번호이고 port2는 마지막 포트 번호입니다.

Chain rule

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

- ACCEPT : 접근 허용
- DROP : 접근 거부

그림 3-7은 IP 필터링 설정 웹 인터페이스를 보여줍니다.

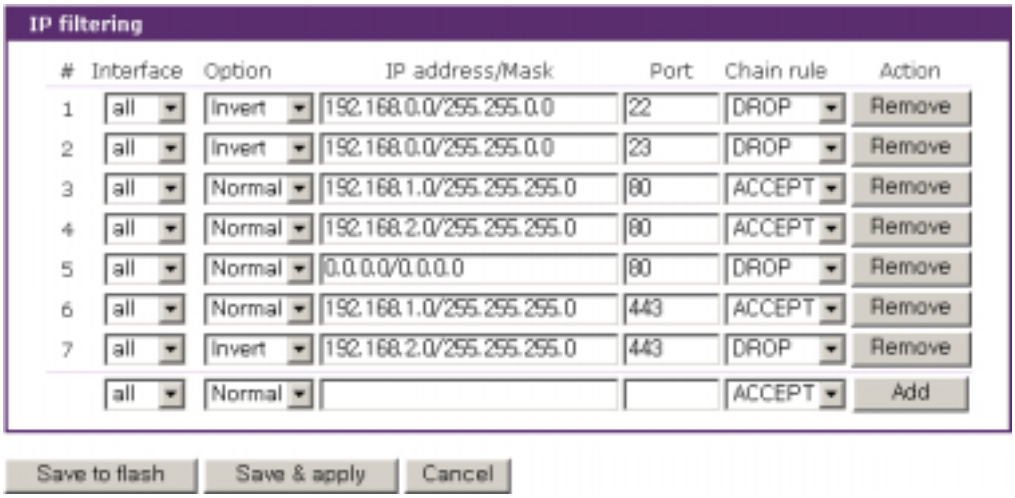


그림 3-7. IP 필터링 설정

그림 3-7에서 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 VTS에 접속을 시도할 때 접속이 거부된다는 것을 의미합니다. 즉, 1번 규칙은 192.168.x.x 서브넷에 속한 호스트만 SSH 프로토콜로 VTS에 접속할 수 있도록 허용합니다. 2번 규칙은 192.168.x.x 서브넷에 속한 호스트의 eth0나 eth1 인터페이스를 통해 VTS로 텔넷 접속을 허용함을 의미합니다.

5번 규칙에 의해 어떠한 호스트도 http 프로토콜(Port : 80)로 VTS에 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 VTS에 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 VTS에 접속할 수 있게 됩니다.

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 VTS에 적용되지 않습니다.

3.6 SYSLOG 서버 설정

VTS는 원격 메시지 로깅 서비스, 시스템 및 포트 데이터 로깅을 위한 SYSLOG service를 지원합니다. 원격 SYSLOG service를 사용하려면, 사용자는 SYSLOG 서버의 IP주소 또는 도메인 이름과 사용할 facility를 반드시 지정해야 합니다. 그림 3-8은 웹 인터페이스의 SYSLOG server configuration 화면을 보여줍니다. VTS는 최대 두 개의 SYSLOG 서버를 제공합니다. 보조 SYSLOG 서버가 설정된 경우, VTS는 이 두 서버에 동일한 SYSLOG 메시지를 전송합니다.

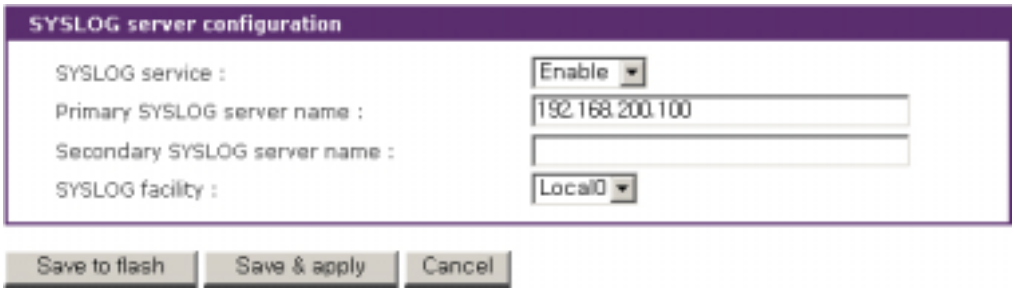


그림 3-8. SYSLOG 서버 설정

로그 메시지를 VTS로부터 수신하려면 VTS 설정에서 지정된 SYSLOG 서버는 “remote reception allowed”으로 설정되어야 합니다. VTS 및 SYSLOG 서버 사이에 방화벽이 있는 경우, 사용자는 나가고 들어오는 UDP 패킷이 자유롭게 이동할 수 있는 규칙을 반드시 추가해야 합니다.
VTS는 local0 에서 local7까지 SYSLOG Facility들을 지원합니다. 사용자는 이러한 Facility들을 사용하여, SYSLOG 메시지의 형태로 VTS 메시지를 저장할 수 있습니다.
SYSLOG service가 가능한 상태에 있고 SYSLOG 서버 설정이 적절히 설정된 경우에만, 사용자는 VTS 시스템 로그 또는 시리얼 포트들의 데이터 로그 설정 화면에서 로그 저장 위치를 SYSLOG 서버로 지정할 수 있습니다. 포트/시스템 로그 저장 등에 대한 자세한 정보는 ***4.3.6 포트 로깅*** 및 ***8.2 시스템 로그 설정*** 을 참조하십시오.

3.7 NFS 서버 설정

VTS는 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 로그 데이터를 NFS 서버에 저장하려면, VTS 설정에 지정된 NFS 서버를 “read and write allowed”으로 설정해야 합니다. VTS 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 VTS의 시스템 로그 또는 포트 데이터 로그로 NFS 서버로 저장할 수 있습니다. 또, 보조 NFS 서버가 설정된

경우, VTS는 동일한 LOG 메시지를 보조 NFS 서버에도 저장합니다. 포트/시스템 로그 저장 위치에 대한 자세한 정보는 ***4.3.6 포트 로깅*** 및 ***8.2 시스템 로그 설정*** 섹션을 참조하십시오.

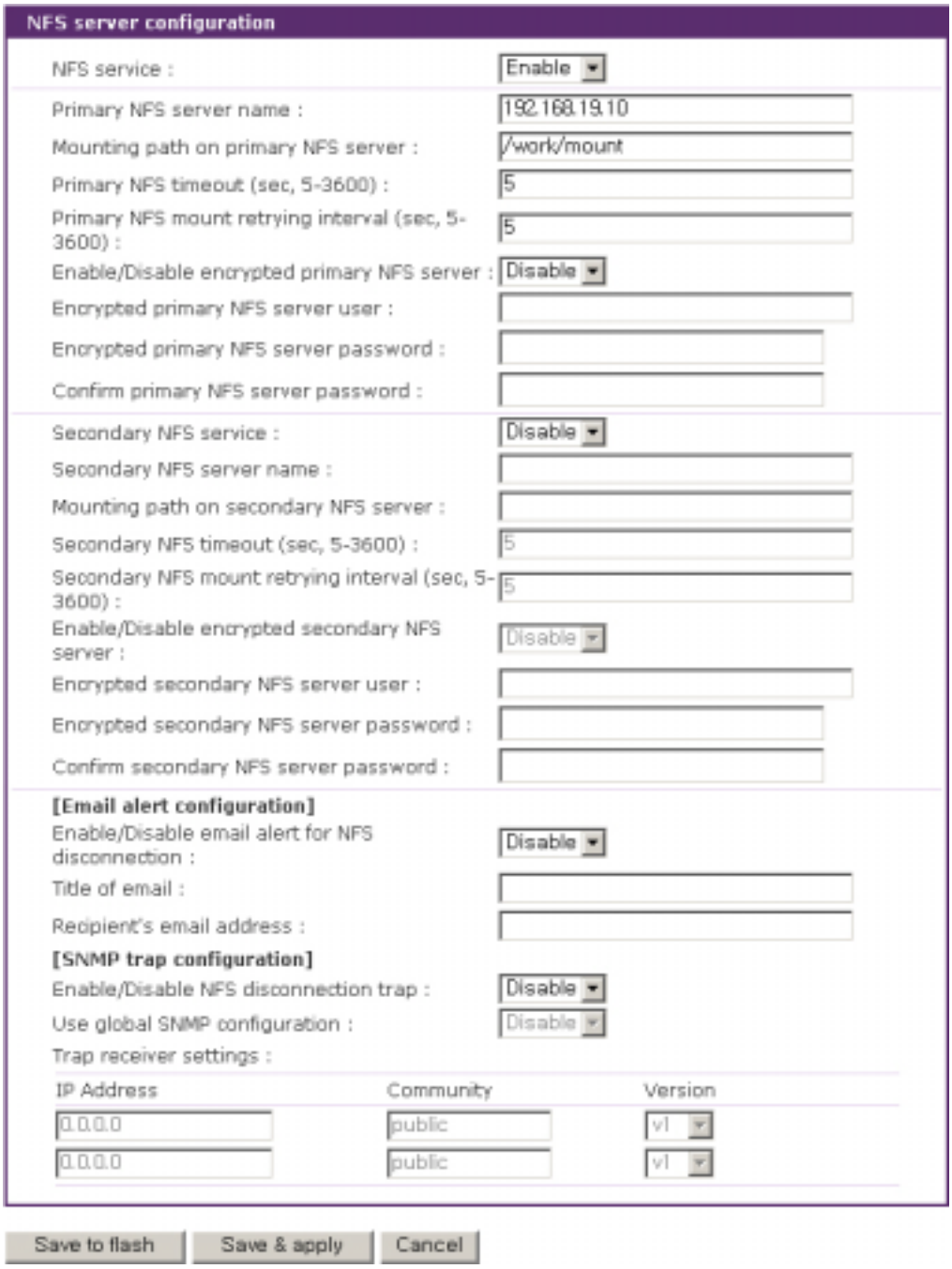


그림 3-9. NFS 서버 설정

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, VTS가 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

VTS가 NFS server로의 연결이 가능한지를 점검하는 주기를 설정합니다. 설정된 주기마다 VTS는 NFS server로 연결이 가능한지를 점검합니다. 가능하다면, VTS는 VTS의 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 serve로 사용될 호스트에는 SSH 데몬이 실행되고 있어야 합니다. 마지막으로, VTS 제품과 함께 제공되는 pause.exe 라는 유틸리티 프로그램을 SSH 데몬 프로그램이 위치한 디렉토리로 복사해야 합니다. 이 기능의 보다 자세한 설명은 **부록 F. 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 VTS는 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 VTS는 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

VTS의 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 시큐리티 프로파일**을 참조하시기 바랍니다. 그림 3-10은 웹 서버 설정 페이지를 보여줍니다.

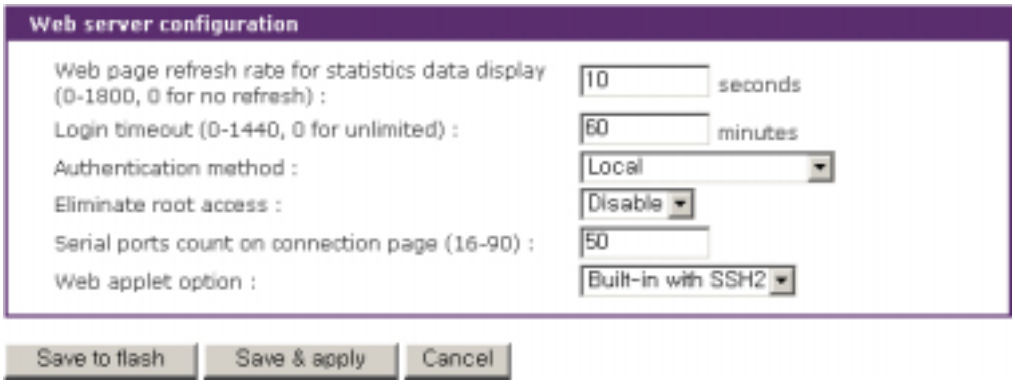


그림 3-10. 웹 서버 설정

본 설정 페이지에서 웹 페이지 업데이트 주기(**web page refresh rate**)는 조정될 수 있습니다. 업데이트 주기는 시리얼 포트 연결 페이지와 네트워크 인터페이스, 시리얼 포트, IP, ICMP, TCP 및 UDP와 같은 시스템 상태 등을 나타내는 페이지 및 파워 컨트롤러 관리 페이지에 적용됩니다. 그 외의 웹 페이지에서는 자동으로 새로 고침(Refresh)이 적용 되지 않습니다. 포트 연결에 대한 자세한 내용은 섹션 ***4.5. Serial port 연결***을 참조하시고, 시스템 통계에 대한 자세한 내용은 섹션 ***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.

Authentication method 선택 메뉴에서는 웹에 로그인할 때 사용자 인증 방법을 선택할 수 있습니다. 현재 VTS 웹서버는 Local, RADIUS server, RADIUS down - Local, TACACS+ server, LDAP server, Kerberos Server, Custom PAM등의 인증 방법을 지원합니다. 인증 방법에 대한 자세한 내용은 **4.3.9 Authentication** 설정을 참조하시기 바랍니다.

Eliminate root access 항목을 **Enabled**로 설정하여 VTS의 root 사용자의 웹 인터페이스 접근을 제한할 수 있습니다. VTS의 root 사용자가 텔넷/SSH 프로토콜의 원격 또는 시리얼 컨솔 접근을 제한하려면 *11. CLI Guide 11.1 Introduction* 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* ***4.3.9 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 ***4.5. 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. VTS가 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. VTS가 제공하는 SSH 버전1를 지원하는 Java applet을 선택한 경우, 시큐리티 프로파일의 SSH 버전1을 사용 불가능하도록 설정(**9.7 시큐리티 프로파일**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.

3.9 Ethernet 설정

VTS는 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, VTS가 네트워크 환경에서 동작하지 않을 수 있습니다.

그림 3-11. 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, VTS는 TCP keep-alive 기능을 제공합니다. VTS는 네트워크가 여전히 keep alive되어 있는지 확인하기 위해 주기적으로 상대 호스트에 패킷을 전송합니다. 반응이 없으면 상대 호스트에 이상이 있는 것으로 간주하고, 세션을 종료하게 됩니다.

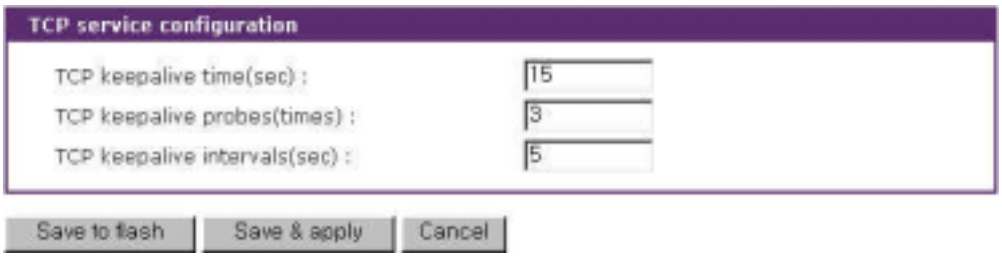


그림 3-12. TCP keep-alive 설정

VTS로 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 15 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 3 회로 설정되어 있습니다.

- TCP keepalive intervals (sec):
  Keepalive 패킷 전송의 시간 간격을 나타냅니다. 기본값은 5 초로 설정되어 있습니다.

공장 초기 설정일 때, VTS 는 데이터가 통신이 없는 상태부터 15 초가 지난 후 5 초 간격으로 3 회 keepalive 패킷을 전송합니다.

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 VTS의 시리얼 포트에 접속할 수 있습니다.
- **Terminal server mode**: 연결 요청은 시리얼 포트로부터 전송됩니다. 이를 통해 네트워크 상의 원격 호스트에 접속하거나 VTS의 쉘 프로그램을 실행할 수 있습니다.
- **Dial-in modem mode**: 모뎀 연결을 통해 VTS에 접속할 수 있습니다.
- **Dial-in terminal server mode**: 모뎀 연결을 통해 네트워크 상의 원격 호스트에 접속할 수 있습니다.

VTS는 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 VTS의 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.

VTS는 또한 **port access menu**를 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 logging** 기능 상태에서, 시리얼 포트를 통해 전송되는 데이터는 **MEMORY, SYSLOG server, NFS server ' s storage** 또는 PC 카드 슬롯을 사용하는 **ATA/IDE fixed disk card**로 전달됩니다. 사용자는 포트 별로 키워드 메시지들을 등록할 수 있으며, 이때 VTS는 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 VTS에 전원이 들어와 동작할 경우에만 유효합니다. 시리얼 포트 로그 데이터를 보존하려면 **SYSLOG server, NFS server** 또는 **ATA/IDE fixed disk card** 를 사용합니다.

제공된 유용한 기능 중의 하나는 **port sniffing** 기능입니다. 즉, 여러 사람이 동시에 한 포트에 접속하여, 협업을 통해 교육 또는 troubleshooting을 수행할 수 있는데, 사용자는 최대

15명까지의 sniff 사용자를 등록할 수 있습니다.

시리얼 포트와 원격 포트는 개별적으로 또는 한꺼번에 모두 설정할 수 있습니다. 표4-1에 시리얼 포트 설정과 관련한 설정 파라미터를 요약하였습니다.

표 4-1. 시리얼 포트 설정 파라미터

Port Access Menu	Port access menu Enable/Disable		
	Port access menu port number (listening TCP port)		
	Port access menu protocol (Telnet or SSH)		
	Port access menu inactivity timeout (seconds)		
	Port access menu local IP		
	Port access menu quick connect via (Web applet or Local client)		
	Port access menu web applet encoding – Web applet only (English (latin1), Korean (KSC5601), Japanese (eucjp), Unicode (UTF8))		
	Login on port access Enable/Disable		
	Port access menu authentication method (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	
		Version	
All ports setting **Or** **Individual serial port setting #1~#4 (8, 16, 32, 48)** **Or** **Remote port**	**Port Enable/Disable**	Enable/Disable port	
		Reset port (except all ports setting)	
		Set port as factory default (except all ports setting)	
	Port title	Automatic detection Enable/Disable	
		Use detected port title Enable/Disable	
		Port title	
		Probe string	
		Detected OS (Read only)	
		Device detection method (Active or Passive)	
		Detection initiation (Periodically, If new device is detected)	
		Detection delay	
	Apply all port settings (except all ports setting)		
	Host mode configuration		Enable/Disable assigned IP
			Assigned IP
			Listening TCP port
			Protocol (Telnet/SSH/RawTCP)
			Inactivity timeout (0 for unlimited)
		Console server	Enable/Disable port escape sequence
			Port escape sequence
			Port break sequence
			Use comment
			Quick connect via
			Web applet encoding (same as Port access menu web applet encoding)
		Terminal server (except	Terminal server option (Remote connection / Shell program)
			Terminal server shell program path

		remote port)	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)	Destination IP
			Destination port
			Protocol (Telnet/SSH/ RawTCP)
			Inactivity timeout (0 for unlimited)
			Modem init string
	Serial Port Parameters (except remote port)	Baud rate	
		Data bits	
		Parity	
		Stop bits	
		Flow control	
		DTR behavior (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)	IP address	
		Port	
		Protocol	
	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	
		Port log buffer size	
		Port log file name (User port title / Specify below + 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	
		Monitoring interval (sec.)	
	Port event handling (only provided on port logging enabled)	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
			Version
	Port IP filtering (console server mode only)	Allowed base hosts IP	
		Subnet mask to be applied	
	Authentication	None	
		Local	
		RADIUS	First RADIUS authentication server

		server	Second RADIUS authentication server	
			First RADIUS accounting server	
			Second RADIUS accounting server	
			RADIUS timeout (0-300 sec.)	
			RADIUS secret	
			RADIUS retries (0-50 times)	
		TACAS+ server	First TACAS+ authentication server	
			Second TACAS+ authentication server	
			First TACAS+ accounting server	
			Second TACAS+ accounting server	
			TACAS+ secret	
		LDAP server	First LDAP authentication server	
			Second LDAP authentication server	
			LDAP search base	
			Domain name for active directory	
		Kerberos server	First Kerberos authentication server	
			Second Kerberos authentication server	
			Realm for first Kerberos server	
			Realm for second Kerberos server	
		Custom PAM		
	User access control	**<<Everyone>> or individual user's or access list's access**	Port	
			Monitor	
			Power	
		Sniff session	Enable/Disable sniff mode	
			Sniff session display mode (Server output / User input / Both)	
			Display data direction arrows Enable/Disable	
			Permit monitoring only mode Enable/Disable	
	Alert configuration	**Console server**	Email alert for port login	
			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	
			Port login trap	
			Device connection trap	
			Active detection trap	
			Use global SNMP configuration	
			First / Second Trap receiver settings	IP Address
				Community
				Version
		Dial-in modem (Dial-in modem test enabled)	Email alert for dial-in modem test	
			Title of email	
			Recipient's email address	
			Dial-in modem test trap	
			Use global SNMP configuration	
			First / Second Trap receiver settings	IP Address
				Community
				Version
	Power control configuration	Power controller		
		Outlet		

그림 4-1은 웹-기반 시리얼 포트 설정 화면을 보여줍니다.

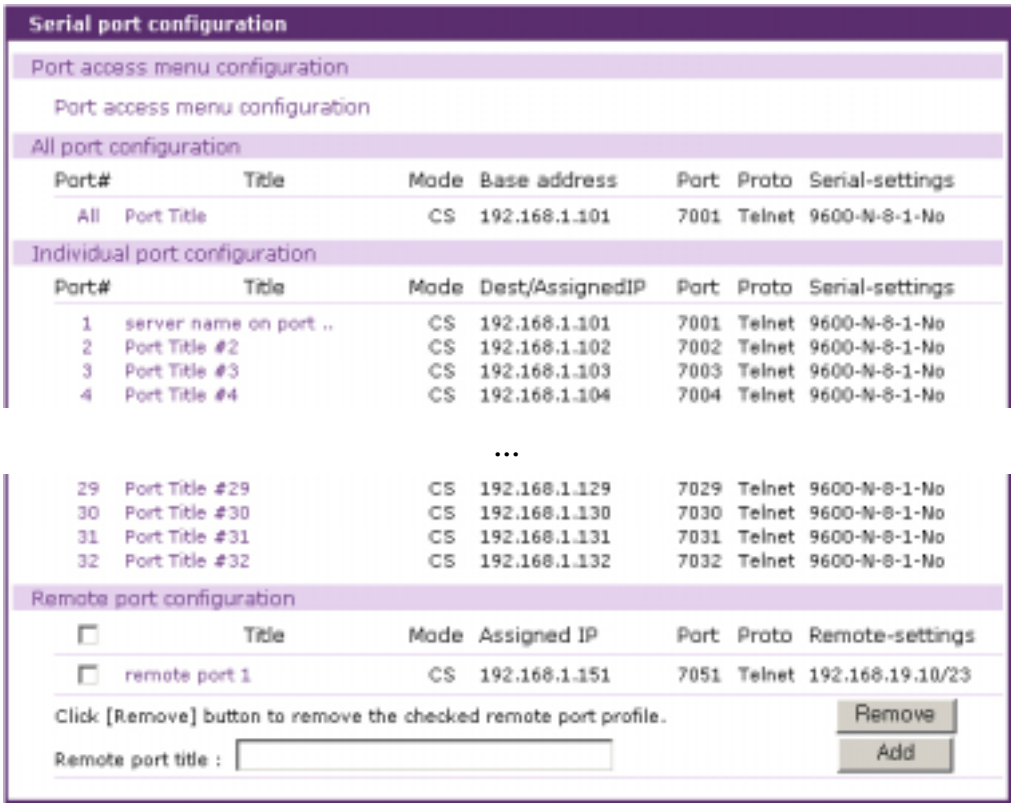


그림 4-1. 시리얼 포트 설정 메인 화면

개별적으로 시리얼 포트 또는 원격 포트를 선택하고 설정하려면 포트 번호 또는 타이틀을 클릭합니다. 시리얼 포트와 원격 포트를 한꺼번에 모두 설정하려면,[All port configuration] 라벨 아래에 위치한 [All] 또는 [Port Title]을 클릭합니다.

사용자는 원격 포트 설정에서 원격 포트 타이틀을 입력하고 [Add] 버튼을 클릭하여 원격 포트를 추가할 수 있고, 원격 포트들을 선택한 후 [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. 사용자는 **Individual port connection**에 있는 터미널 Icon을 선택해야 합니다.
3. 사용자는 현재 **port access menu connection**에 제공된 시리얼 포트 링크를 사용할 수도 있습니다.

***참고**: 포트 연결에 대한 자세한 사항은 **4.5 Serial port 연결**을 참고하시기 바랍니다.*

4.2 Port access menu 설정

4.2.1 개요

VTS는 **port access menu**와 telnet/SSH 클라이언트 연결을 통해 지정된 가상 포트로 연결할 수 있습니다. **port access menu**와 연결되면, VTS는 **port access menu** 를 통해 모든 시리얼 포트와 원격 포트로의 연결 경로를 보여줍니다. 이는 또한 포트 번호, 포트 타이틀 및 시리얼 포트 모드를 포함합니다. VTS는 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 4-2은 윈도우 telnet 프로그램을 사용하여 **port access menu**에 접속한 화면을 보여줍니다.

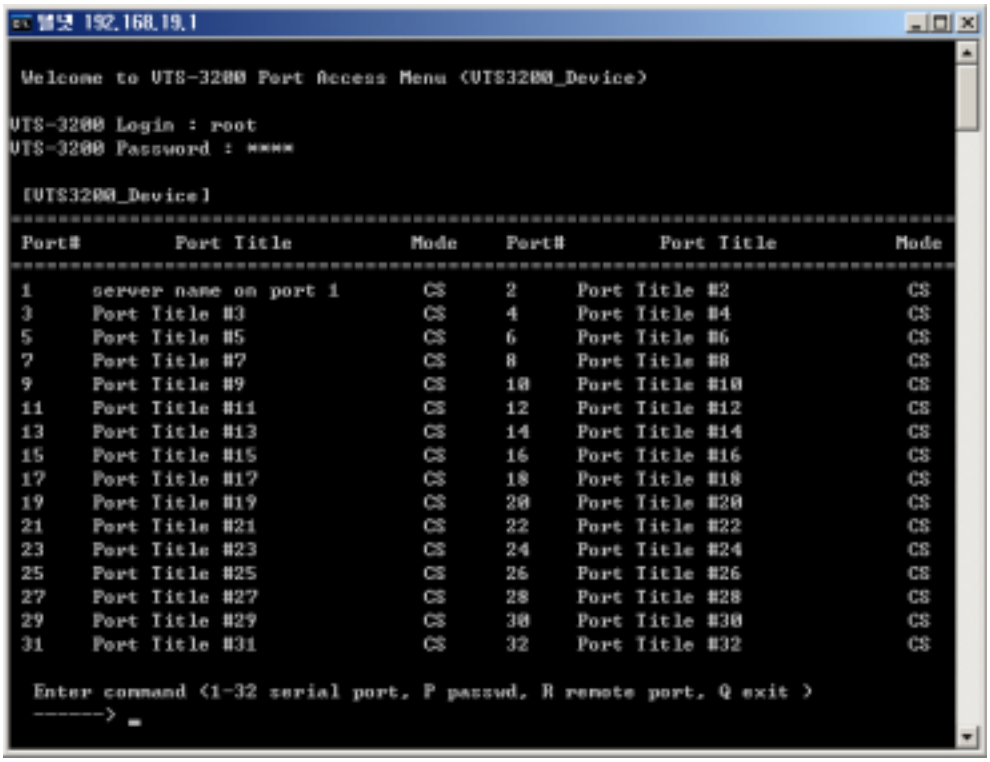


그림 4-2. Telnet을 이용하여 포트 액세스 메뉴에 접속하기

VTS는 다음을 수행함으로써 사용자가 가상 포트에 연결되도록 합니다.

- VTS 의 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 IP 주소가 192.168.1.100이고, **port access menu** 의 TCP 포트 번호가 6000인 경우, 사용자는 윈도우 명령 프롬프트에서 다음 명령을 입력할 수 있습니다.

```
telnet 192.168.1.100 6000 <ENTER>
```

port access menu 의 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 4-3는 **port access menu** 설정 화면을 보여줍니다.

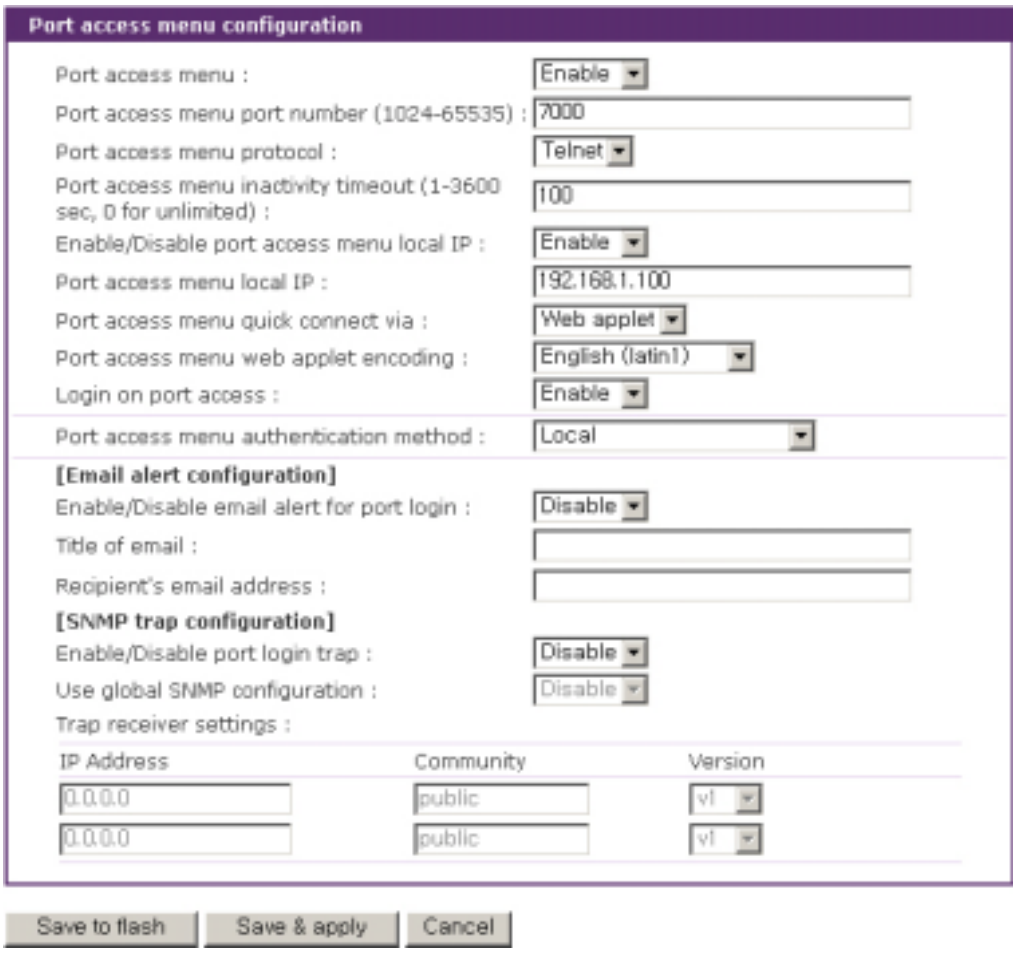


그림 4-3. 포트 액세스 메뉴 설정

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

Enable/Disable email alert를 Enable로 설정하면, 사용자가 port access menu로 로그인 또는 로그 아웃 할 때 설정된 주소로 설정된 제목의 이메일이 전송됩니다. Enable/Disable port login trap을 Enable로 설정하면, trap receive settings의 설정에 따라 SNMP trap을 전달합니다.

***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. Local IP를 disable 시키거나 local IP를 0.0.0.0으로 하면 해당 시리얼 포트에 IP를 할당하지 않으며 해당 포트는 VTS의 IP address 와 포트 번호를 통해서만 접속이 가능 합니다.*

4.2.2 Port access menu에 대한 인증

사용자가 VTS의 **port access menu**에 접속하기 위해서는 이중적인 인증 절차를 걸쳐야 한다. **port access menu**에 접속하려면 사용자는 우선 **port access menu** 에 인증을 받아야 한다. 다음에 **port access menu**에서 시리얼 포트를 선택하면 해당되는 시리얼 포트 접속을 위한 인증을 받아야 합니다. 만일 "port access menu authentication" 방법이 [none]으로 설정된 경우, 모든 사용자는 **port access menu** 의 시리얼 포트에 접속할 수 있습니다. "serial port authentication" 방법이 [none]으로 설정된 경우에만, 사용자는 인증 없이 시리얼 포트에 접속할 수 없습니다.
만일 "port access menu authentication" 방법이 [Local]로 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, "콘솔 서버 모드"로 설정되어 있는 시리얼 포트에만 접속할 수 있습니다. 다른 모드로 설정된 시리얼 포트에는 접속할 수 없습니다. 인증을 받은 경우, **port access menu**에 접속하는 사용자는 모든 연결 보다 우선 순위를 가집니다. 사용자가 현재 사용 중인 포트로 연결을 시도하면, 사용 중인 연결은 종료되고 인증된 사용자를 위한 새로운 세션이 생성됩니다.
인증 방법에 대한 자세한 내용은 **4.3.9 Authentication** 설정을 참조하시기 바랍니다.

4.2.3 Port access menu 프로토콜

Telnet 또는 SSH를 사용하려면 **port access menu** 프로토콜을 설정해야 합니다. **port access menu**의 프로토콜이 각각의 시리얼 포트의 프로토콜과 일치하지 않을 수도 있습니다. 시리얼 포트의 프로토콜은 원격 호스트로부터 VTS로의 연결 방법을 명시하는 것이므로, 사용자가 **port access menu**를 통해 VTS로 로그인 했다면 각각의 시리얼 포트의 프로토콜은 의미가 없습니다. **port access menu**의 프로토콜이 각각의 시리얼 포트의 프로토콜 설정에 우선하게 되며, 이 경우 각 시리얼 포트의 설정은 무시되게 됩니다.

4.2.4 Port access menu options

“**Port access menu quick connect via**” option은 웹 페이지의 connection 메뉴를 통한 접속 시 사용할 client 프로그램을 지정할 수 있게 합니다. “**Port access menu quick connect via**” option이 Web applet으로 설정되어 있다면, 웹 애플릿은 서버로부터 받은 데이터를 화면에 표시하기 위해 “**Port access menu web applet encoding**” option을 이용하여 설정된 문자모음으로 변환합니다. “**Enable/Disable email alert for port login**” option이 “Enable”로 설정되면 사용자가 Port access menu로 로그인 또는 로그아웃 할 때마다 VTS는 이메일 경보 설정(Email alert configuration)에 따라 이메일을 전송합니다. “**Enable/ Disable port log in trap**” option이 “Enable”로 설정되고, 트랩 수신기 설정(Trap receiver settings)에서 IP 주소가 트랩 수신기로 바르게 설정되면, 사용자가 Port access menu로 로그인 또는 로그아웃 할 때마다 VTS는 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.

4.2.5 Clustering시의 port access menu

Clustering(5절 참조)을 사용하는 경우 Master unit의 **port access menu**를 통하여 slave unit을 access하게 됩니다. **port access menu**의 메인 메뉴에서 S를 입력하고 Slave unit 선택메뉴에서 A~P까지의 입력을 통해 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. 상단의 IP 주소는 현재 접근하고 있는 Unit의 주소를 보여줍니다.

```
[VTS3200_Device]
================================================================================
 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  ( 1-32 serial port, P passwd, S slave unit
                   R remote port, Q exit )
```

```
------> S

[VTS3200_Device]
================================================================================
 Unit #        IP                    Unit #        IP
================================================================================
   A      192.168.19.3                B        ----------
   C      ----------                  D        ----------
   E      ----------                  F        ----------
   G      ----------                  H        ----------
   I      ----------                  J        ----------
   K      ----------                  L        ----------
   M      ----------                  N        ----------
   O      ----------                  P        ----------

  Enter command ( A-P slave unit, L serial port, R remote port, Q exit )
  ------>
```

4.3 개별 포트 설정

VTS의 시리얼 포트와 원격 포트는 개별적으로 또는 한꺼번에 설정될 수 있는데, 개별 및 모든 포트 설정에 대한 파라미터는 동일합니다. 개별 포트 설정은 다음과 같이 12개 그룹으로 분류됩니다.

1. Port enable/disable
2. Port title
3. Apply all port settings
4. Host mode configuration
5. Serial port parameters: *Only available for serial port*
6. Port logging: *Only available if the host is set to Console Server Mode.*
7. Port event handling: *Only available if the host is set to Console Server Mode and Port logging is enabled.*
8. Port IP filtering: *Only available if the host is set to Console Server Mode.*
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. Power control configuration : *Only available if a power controller is added.*

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

4.3.1 Port Enable/Disable

각 시리얼 포트와 원격 포트는 enable 또는 disable 될 수 있습니다. 만약 시리얼 포트 또는 원격 포트가 disable 상태가 되면 사용자는 해당 시리얼 포트로 접속할 수 없습니다. 그림 4-4는 포트 enable/disable 화면을 보여줍니다.

각 stuck된 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.

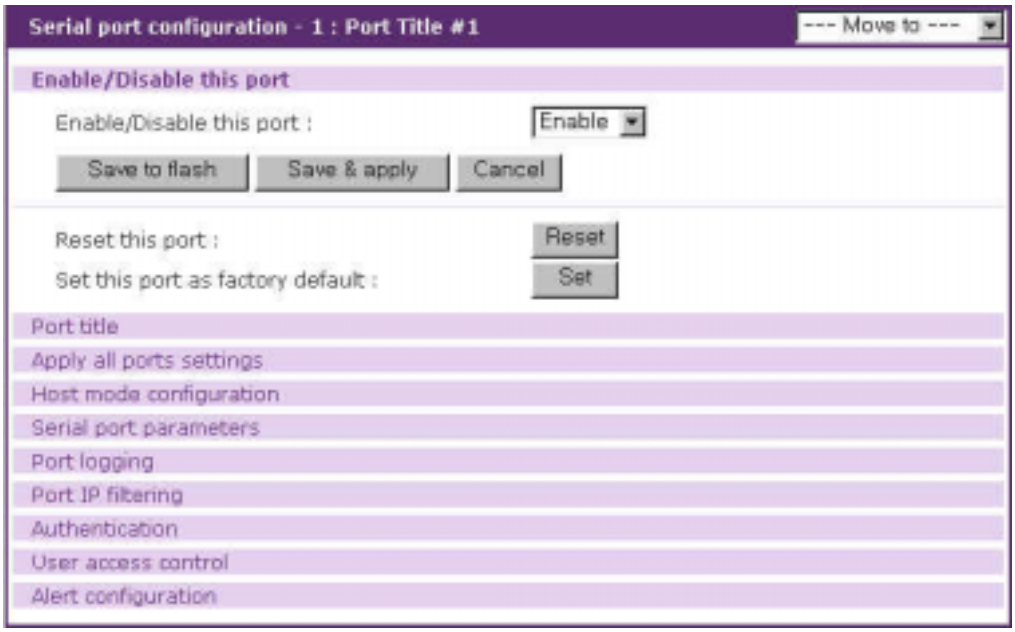


그림 4-4. 포트 enable/disable

4.3.2 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**에 대한 설명으로도 이용됩니다.

Port title에서 필요한 파라미터는 다음과 같습니다.

Automatic detection

Use detected port title

Port title

Probe string

Device detection method

Detection initiation

Detection delay

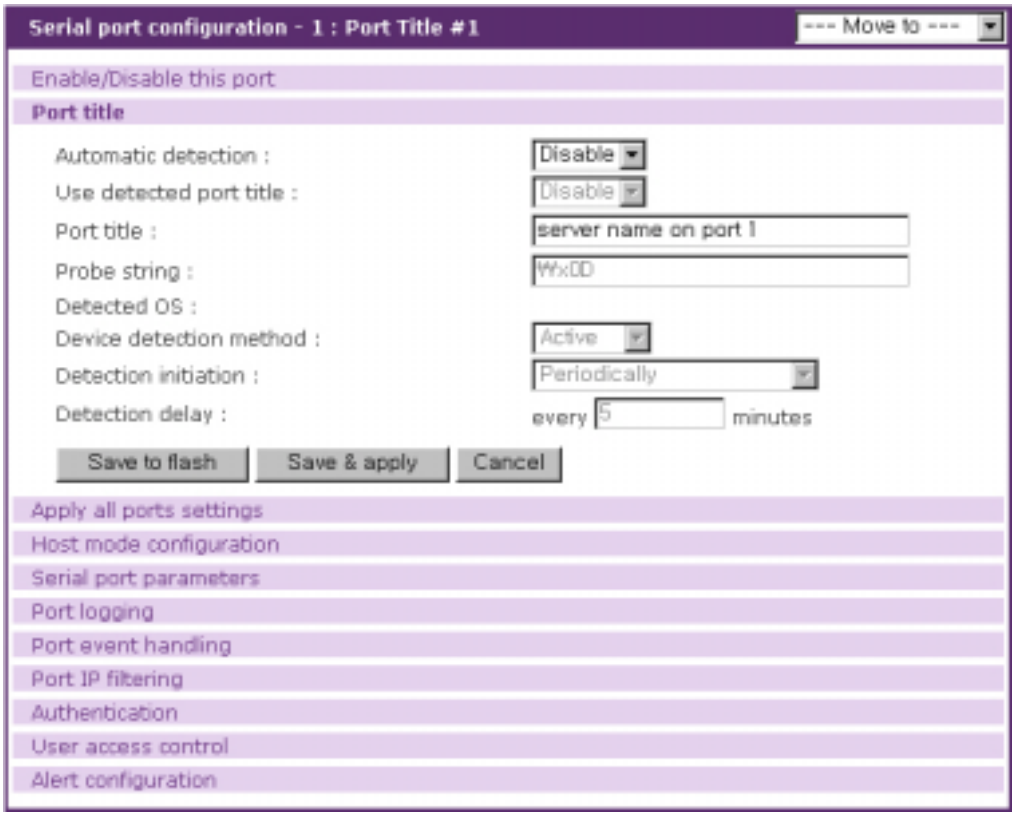


그림 4-5. 포트 타이틀 설정

Automatic detection

시리얼 포트에 연결된 장치의 운영체제나 호스트 이름 등의 정보를 자동으로 수집할 지 여부를 설정합니다. **Host mode**가 **Console server** 모드이고 연결된 장치가 파워 컨트롤러가 아닐 때에만 **Enable/Disable** 중에서 선택 가능하고 그렇지 않으면 **Disable**로 자동 설정됩니다. 원격 포트의 경우에는 항상 Disable로 설정되고 변경될 수 없습니다.

Use detected port title

자동으로 수집된 장치의 정보를 이 포트의 포트 타이틀로 사용할 것인지를 설정합니다. **Automatic detection**이 **Enable**로 설정된 경우에만 나타납니다.

Port title

포트 타이틀을 표시합니다. 장치 정보를 자동으로 수집(**Automatic detection**이 **Enable**로 설정)하고 수집된 정보를 포트 타이틀로 사용(**Use detected port title**이 **Enable**로 설정)하는 경우에는 포트 타이틀을 변경할 수 없고 자동 수집된 정보가 포트 타이틀로 사용됩니다. 그 외의 경우에는 이 파라미터에 입력한 값이 포트타이틀로 사용됩니다.

Probe string

Automatic detection이 **Enable**로 설정된 경우에만 입력 가능합니다. 장치 정보를 수집하기 위해

VTS가 장치에게 보내는 명령을 설정합니다.

Device detection method

Automatic detection이 **Enable**로 설정된 경우에만 설정 가능합니다. **Active**와 **Passive**중에서 설정할 수 있습니다. **Active**는 VTS가 장치 정보 수집을 위해 명령을 보내면 장치에서 전송하는 데이터를 바로 분석하여 장치의 운영체제와 호스트 이름 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 기록됩니다. 여기서, xx는 포트번호를 나타냅니다.

Detection initiation

Device detection method가 **Active**인 경우에 **Periodically**와 **If new device is detected** 중에서 선택할 수 있으나, **Passive**인 경우에는 **Periodically**가 설정됩니다. **Periodically**는 **Detection delay**에 설정된 시간마다 주기적으로 VTS가 장치정보를 분석합니다. **If new device is detected**는 시리얼 포트에 새로운 장치가 연결되었다는 이벤트가 발생할 때마다 장치정보를 분석합니다.
Automatic detection이 **Enable**로 설정되고 **Device detection method**가 **Active**로 **Detection initiation**이 **Periodically**로 설정된 경우 VTS가 장치정보를 분석한 결과를 **Alert 설정**에서 설정한 데로 email이나 SNMP trap을 전송합니다. 자세한 내용은 **4.3.11 Alert 설정**을 참조하시기 바랍니다.

Detection delay

Detection initiation이 **Periodically**인 경우 입력 가능합니다. VTS가 장치 정보를 분석하는 주기를 설정합니다.

4.3.3 Apply all ports settinigs

사용자가 all ports settings 를 수행하여 모든 포트의 설정을 한꺼번에 수행하다가, 변경해서는 안 되는 기존 포트 설정 값들을 초기화하는 것을 막기 위해, VTS는 개별 포트 설정에서 이를 허용할 지 말지 여부를 설정할 수 있게 합니다. 만일 설정이 disable 상태인 경우, 기존의 포트 설정 값은 all ports setting을 수행하더라도 유지되게 됩니다. 그림 4-6은 **apply all ports settings** 설정 화면을 보여줍니다.

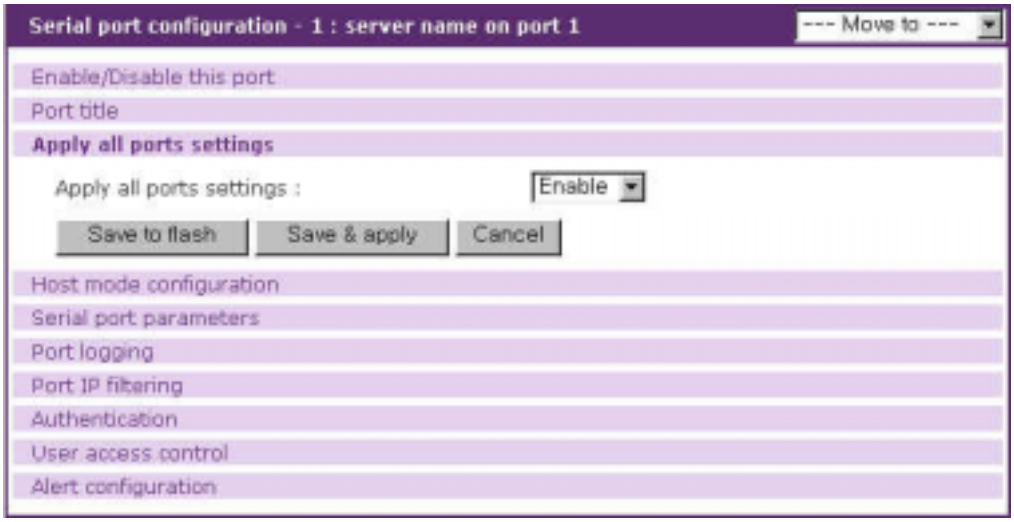


그림 4-6. Apply all ports settings 설정

4.3.4 Host mode 설정

VTS 작동 모드는 "host mode"라고도 합니다. 다음과 같은 4개의 host mode가 사용 가능합니다.

console server mode
terminal server mode
dial-in modem mode
dial-in terminal sever.

Console Server Mode
이 모드에서는, telnet 또는 SSH 클라이언트의 연결을 대기하고 있는 TCP 서버 소켓이 실행됩니다. telnet 또는 SSH 클라이언트가 VTS에 접속하면, VTS에 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 VTS의 시리얼 포트에 연결된 장치에서 원격 호스트로 telnet 또는 SSH를 이용하여 접속하거나 VTS의 쉘 프로그램을 실행하게 됩니다. 원격 포트에서는 지원되지 않습니다.

Dial-in Modem Mode
VTS는 외장형 모뎀을 사용하여 망외(out-of-band) 접속 기능을 지원합니다. 시리얼 포트가 **dial-**

in modem mode로 설정된 경우, VTS는 시리얼 포트가 외장형 모뎀과 연결된 것으로 간주하고, 원격 지로부터 전화 접속 연결을 기다립니다. 터미널 에뮬레이션 프로그램을 사용하여 모뎀에 접속하면 VTS에 접속을 인증하기 위한 로그인 화면이 표시됩니다. 원격 포트에서는 지원되지 않습니다.

Dial-in Terminal Server

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

그림 4-7 ~ 그림 4-10은 각 모드별 Host mode 설정 화면을 보여줍니다.

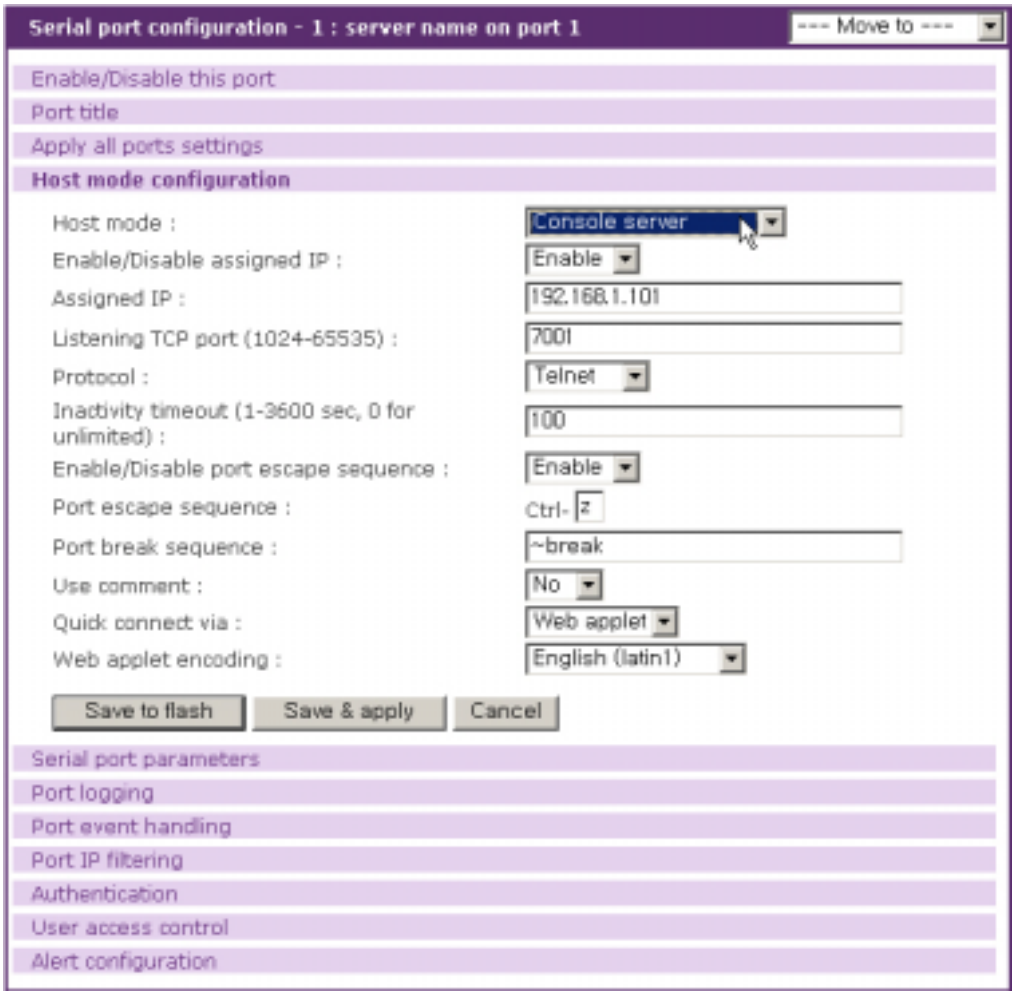


그림 4-7. Host mode 설정 - console server mode

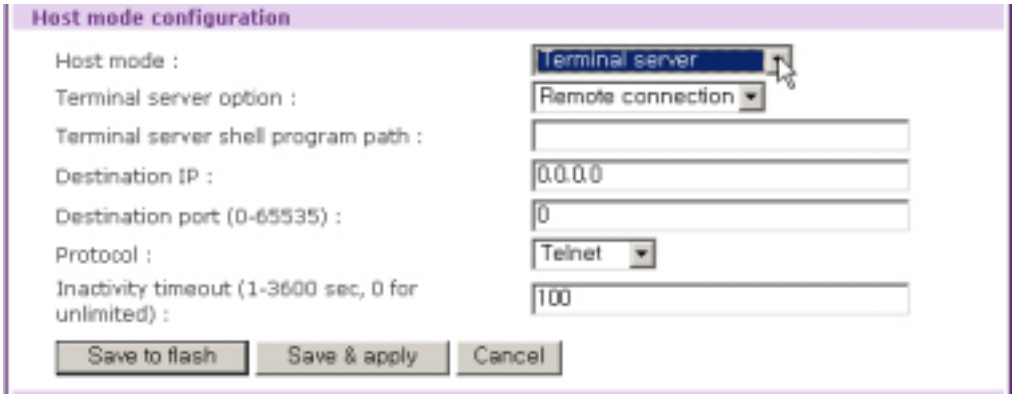


그림 4-8. Host mode 설정 - terminal server mode

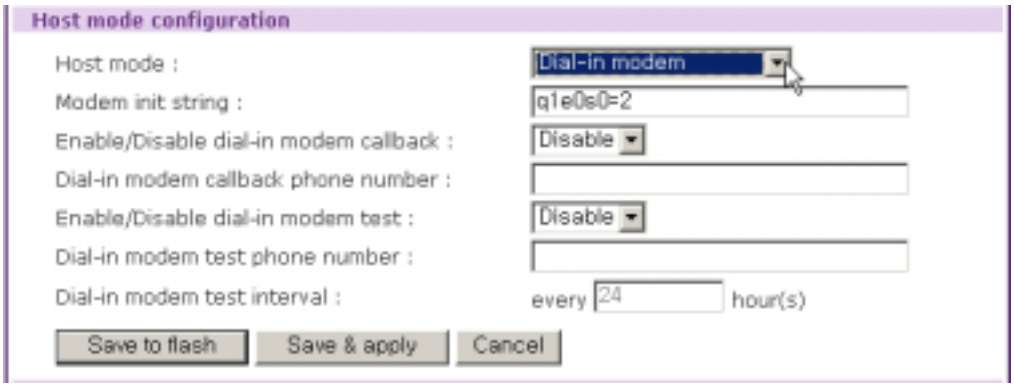


그림 4-9. Host mode 설정 - dial-in modem mode

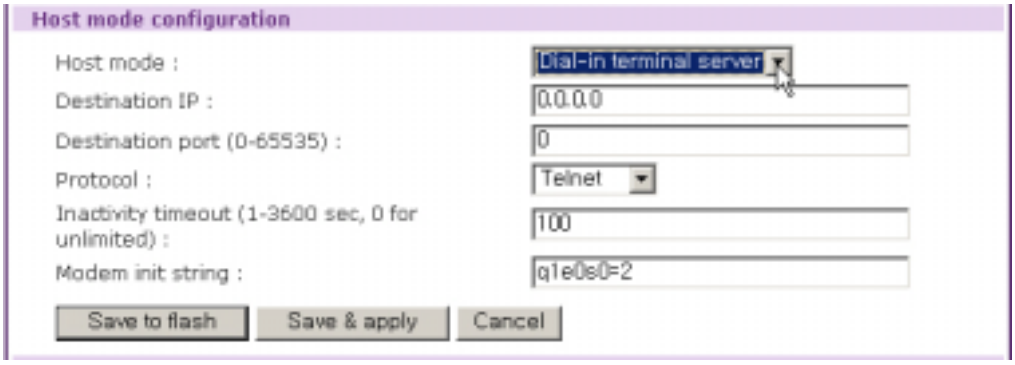


그림 4-10. Host mode 설정 - dial-in terminal server mode

Console server mode 설정

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

Enable/Disable assigned IP
Assigned IP address
Listening TCP port number
Protocol
Inactivity timeout

Enable/Disable port escape sequence

Port escape sequence

Port break sequence

Use comment

Quick connect via

Web applet encoding

Eanble/Disable assigned IP

Assigned IP address를 사용할 지 여부를 결정하는데 사용합니다.

Assigned IP address

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 포트 또는 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 number

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

VTS의 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 VTS와 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, VTS는 "keep alive" 패킷을 주기적으로 전송하여 telnet/SSH 클라이언트와 VTS 사이의 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 또는 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], Sniff 사용자를 위한 [enter as a slave session], 메인 세션 사용자를 위한 [send break], Port와 Monitor 접근권한을 모두 가진 Sniff 사용자의 [take over main session] 그리고 Port와 Monitor 접근권한을 모두 가진 사용자의 [disconnect a sniff session] 메뉴 등이 있습니다. 시리얼 포트 또는 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. (섹션 **4.5 Serial port 연결**을 참조하십시오.)

Quick connect via

Quick connect via로 VTS 웹의 연결 페이지에서 구동 될 Client의 종류를 Web applet 또는 Local client로 선택합니다. 이 설정은 Protocol이 Telnet 또는 SSH인 경우에만 적용됩니다. 시리얼 포트 연결 페이지에서 사용자가 연결 아이콘을 선택할 경우, 사용자가 VTS가 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.

Web applet encoding

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

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 address**
- **Destination TCP port number**
- **Protocol**
- **Inactivity timeout**

Terminal server option

Remote connection으로 설정된 경우, VTS의 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, VTS의 시리얼 포트로 접속하면 VTS에서 **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 VTS가 실행할 쉘 프로그램을 지정합니다.

Destination IP 주소 및 Destination TCP port number

Terminal server option이 **Remote connection**으로 설정된 경우, Destination IP 주소 및 Destination TCP port number는 VTS에 연결된 장치가 접속하고자 하는 원격지 호스트의 IP 주소 및 TCP port number를 의미한다.

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 와 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**
- **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’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 VTS는 연결을 끊고 나서 **Dial-in modem callback phone number**에 명시된 전화 번호로 연결하여 통신합니다.

Dial-in modem callback phone number

Dial-in modem callback이 활성화된 경우 VTS가 연결할 전화번호를 명시합니다.

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 **4.3.11 Alert 설정**을 참조하시기 바랍니다.

Dial-in modem test phone number
모뎀이 정상 동작하는지 점검하기 위해 VTS가 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.

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

4.3.5 Serial port parameters / Remote port parameters

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

시리얼 통신에서 필요한 파라미터는 다음과 같습니다.

Baud rate
Data bits
Parity
Stop bits
Flow control
DTR behavior
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)

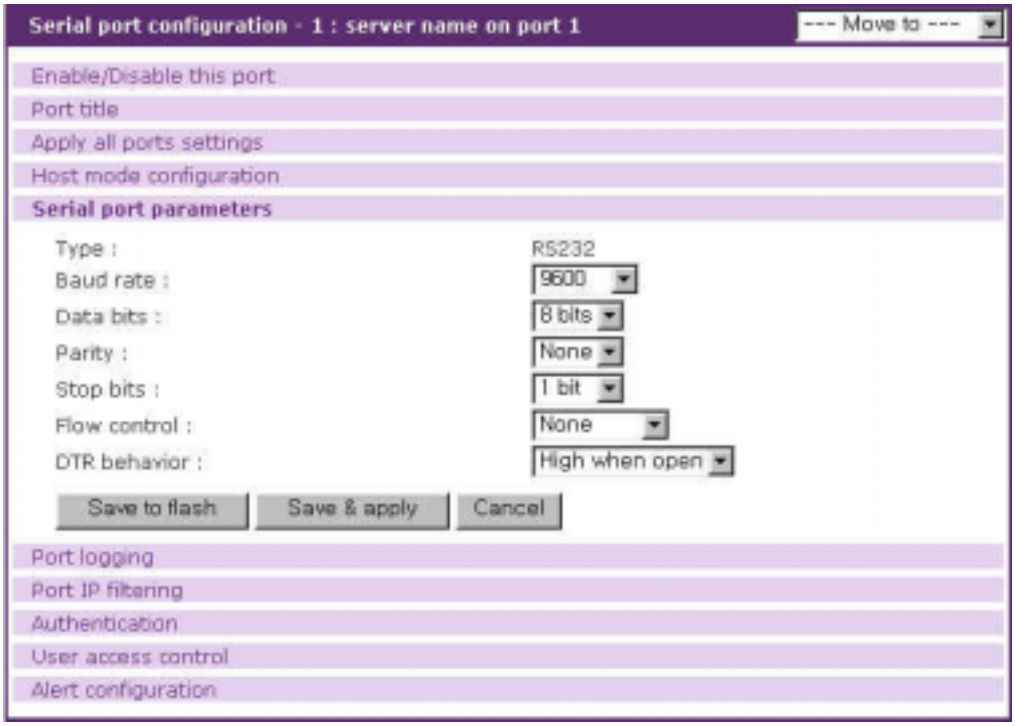


그림 4-11. Serial port parameters 설정

Baud rate

VTS에서 지원하는 baud rate는 다음과 같습니다.

1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200 및 230400

공장 출하시의 기본값은 9600입니다.

Data bits

Data bits는 7 bit와 8bit 중에서 하나를 선택할 수 있습니다. 공장 출하시의 기본값은 8 bits입니다.

Parity

Parity는 **none, even** 또는 **odd** 중에서 선택할 수 있습니다. 공장 출하시의 기본값은 none입니다.

Stop bits

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

Flow control

흐름 제어 값은 none, 소프트웨어(Xon/Xoff) 또는 하드웨어(RTS/CTS) 중에서 선택할 수 있습니다. 공장 출하시의 기본값은 none입니다.

DTR behavior

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 mode”로 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 않으면 클라이어트로 데이터를 전송합니다.

rc.user 스크립트를 수정하면 컨솔 포트에 다이얼인 모뎀을 연결할 수 있습니다. rc.user 파일에 다음과 같은 스크립트를 추가하십시오.

```
echo 57600 > /var/run/mgetty.console
```

57600은 컨솔 포트에 연결된 모뎀의 baudrate 입니다. rc.user 파일을 수정한 후 재부팅해야 컨솔 포트에 연결된 다이얼인 모뎀이 정상 동작합니다.

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

원격 포트에서 필요한 파라미터는 다음과 같습니다.

IP address

Port

Protocol

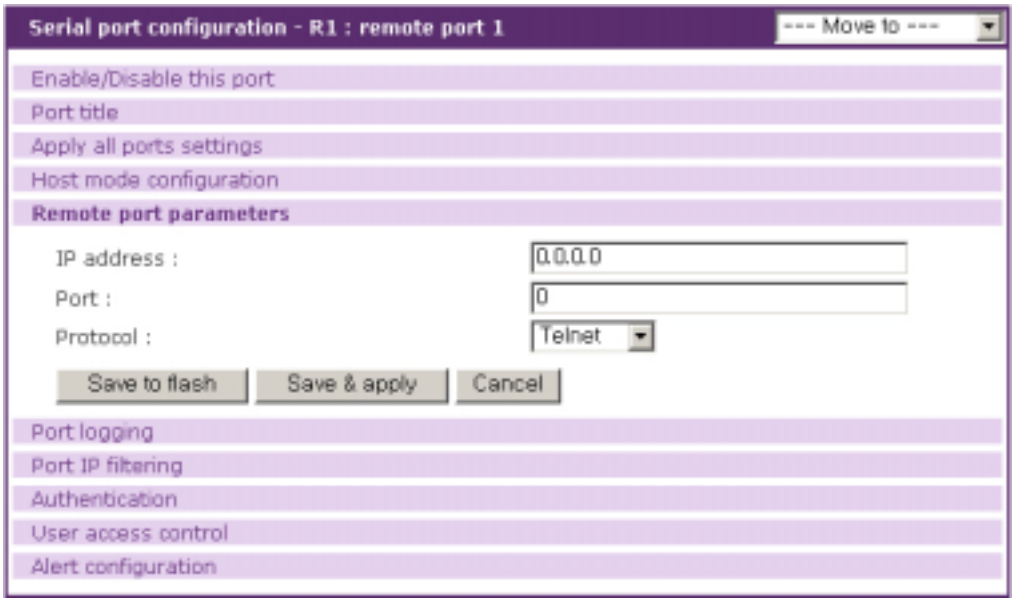


그림 4-12. Remote port parameters 설정

IP address
접속할 원격 호스트의 IP 주소를 설정합니다.

Port
원격 호스트에 접속하는데 사용할 TCP port number를 설정합니다.

Protocol
원격 호스트에 접속하는데 사용되는 프로토콜을 설정합니다.

4.3.6 Port Logging

Console Server 모드에서 Port Logging 이 Enable 되면, VTS의 시리얼 포트 또는 원격 포트로 전송되는 데이터를 메모리, ATA/IDE fixed disk card 또는 NFS 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 **4.3.7. Port event handling 설정**을 참조하십시오.
시리얼 포트 또는 원격 포트의 host mode가 console server mode 로 설정된 경우에만 Port Logging 기능이 유효합니다. 시리얼 포트가 terminal server 또는 dial-in modem mode로 설정된 경우 Port Logging 기능으로 접속할 수 없습니다.

Port Logging에 대한 설정 파라미터는 다음과 같습니다.

Enable/Disable port logging

Logging direction

Port log storage location

Port log to SYSLOG server

Port log buffer size

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

Monitoring interval

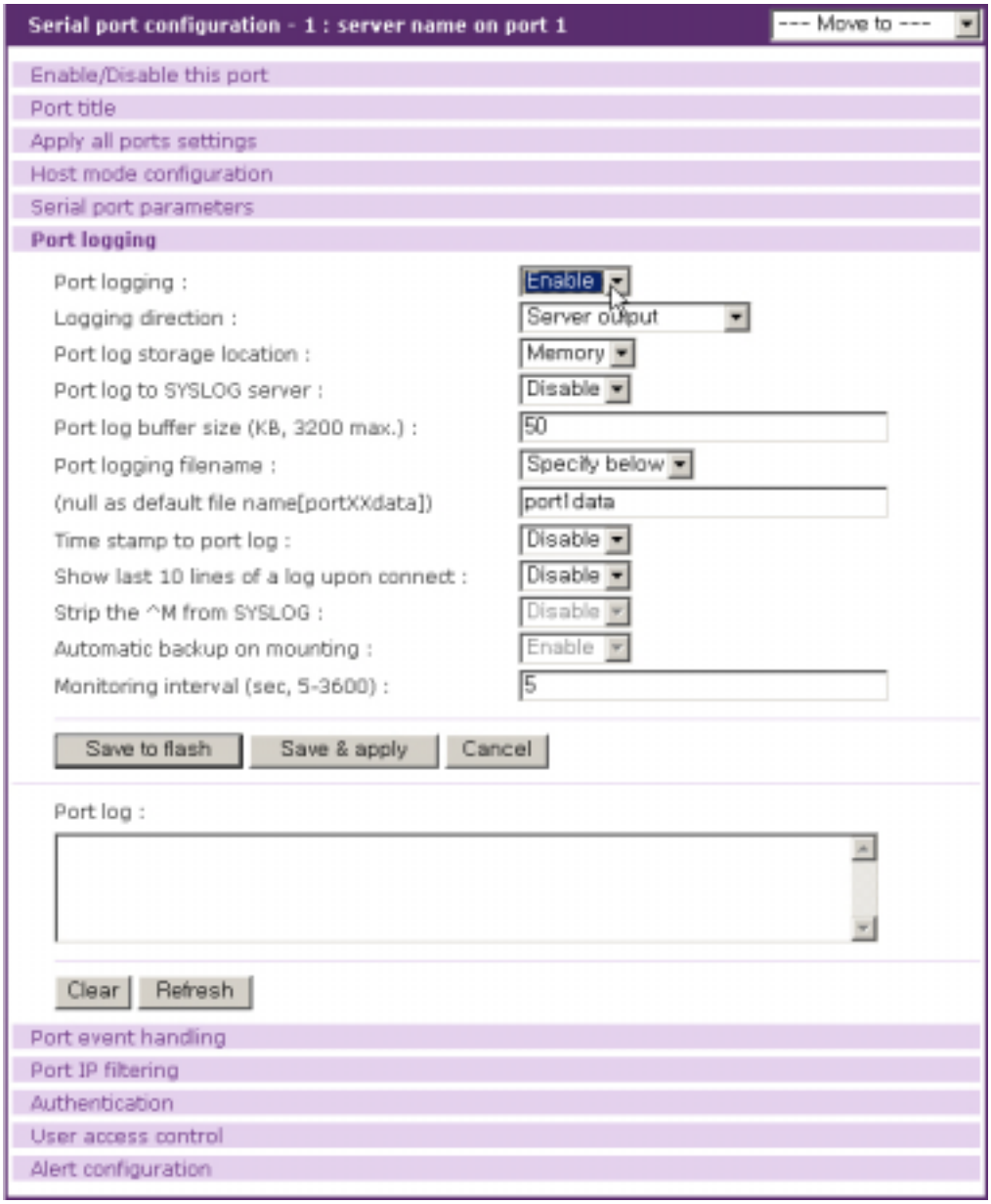


그림 4-13. 포트 로깅 설정

Enable/disable 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 output입니다.

Port log storage location

포트 로그 데이터는 VTS의 내부 메모리, ATA/IDE fixed disk card 또는 NFS 에 저장할 수 있습니다. 포트 로그가 메모리에 저장되는 경우, VTS가 꺼질 때 포트 로그 데이터는 삭제됩니다. 시리얼 포트 로그 데이터를 보존하려면, 저장 위치를 ATA/IDE fixed disk card 또는 NFS 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

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

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 4Kbytes입니다.

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

로그 데이터를 저장하기 위해 NFS 서버를 사용하는 경우, 최대 port buffer size는 서버의 환경에 따르게 되며, 사용자는 NFS 서버를 설정하여 port logging 시스템이 적절히 작동할 수 있도록 해야 합니다.

Port log file name

이 파라미터는 logging되는 포트 로그 파일의 이름를 정의합니다. **Port logging file name**이 **Use port title**로 설정되면 포트 타이틀이 포트 로그 파일 이름으로 사용됩니다. **Specify below**로 설정되면 아래에 입력된 파일 이름이 로그 파일 이름으로 사용됩니다. 로그 파일 이름이 입력되어 있지 않을 경우에 는 기본 설정 값인 portXXdata 라는 이름이 사용 됩니다. 여기서 XX은 해당 시리얼 포트의 번호를 표시합니다.

Time stamp to port log

이 파라미터 값이 설정되면 logging되는 포트 로그는 줄마다 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 10줄이 표시됩니다. 기본값은 **Disable**입니다.

Strip the ^M from SYSLOG

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 또는 NFS server로 설정된 경우에만 설정할 수 있습니다. 이 설정이 enable되면 해당 저장 공간이 다시 마운트될 경우 로그를 저장하는 백업 파일을 만듭니다.

Monitoring interval

Port logging이 설정되고 port event handling(4.3.7 참조)이 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 최대한 큰 값을 설정하는 것이 가장 좋습니다.

4.3.7 Port event handling 설정

Port logging 이 enable이 되면 포트로 들어 오는 메시지를 검사해서 기 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.

Port event handling을 위한 키워드 별 파라미터는 다음과 같습니다.

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 IP address

First/Second SNMP trap community

First/Second SNMP trap version

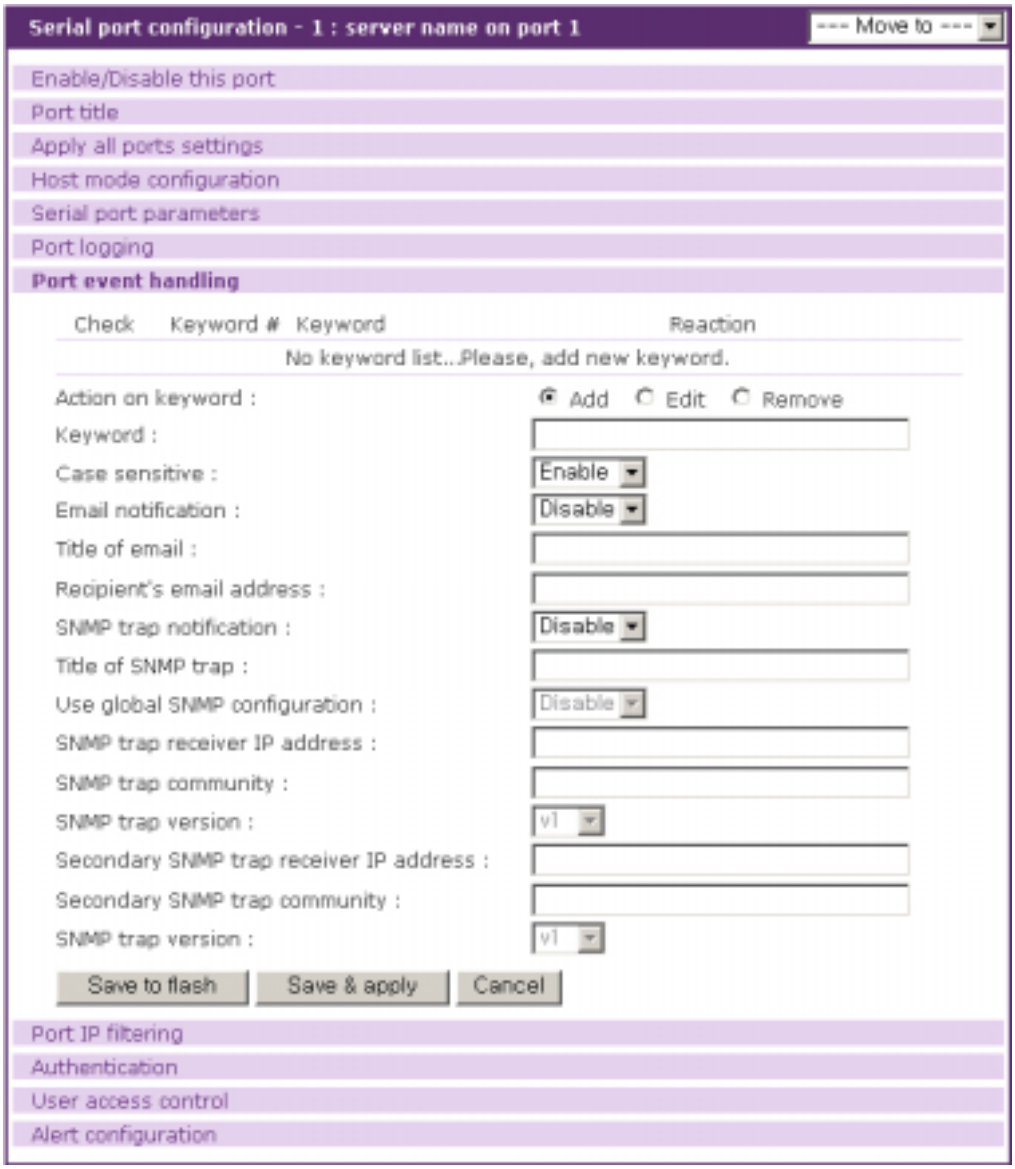


그림 4-14. 포트 이벤트 핸들링 설정

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 각각 및 **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, VTS는 이 키워드가 발생하는지 감시합니다. 키워드가 발생하고 어느 사용자도 이 포트에 연결하지 않으면, 사용자가 포트에 연결할 때까지 시리얼 포트 연결 페이지의 포트 타이틀 좌측에 경고 아이콘이 표시됩니다. 그림 4-15은 포트 타이틀이 server name on port1인 1번 포트에 경고 아이콘이 표시된 상황을 보여줍니다.

그림 4-15. 경고 아이콘을 포함한 시리얼 포트 연결 페이지

4.3.8 Port IP Filtering 설정

VTS 시리얼 포트 또는 원격 포트에 접속을 허용하는 원격 호스트는 IP 주소 filtering 규칙에 기초하여 지정할 수 있습니다. 사용자는 유효한 IP 주소 및 subnet mask를 제공하여 특정 호스트가 VTS 시리얼 포트 또는 원격 포트에 접속할 수 있도록 허용합니다. 자세한 내용은 섹션 3.5를 참조하십시오.

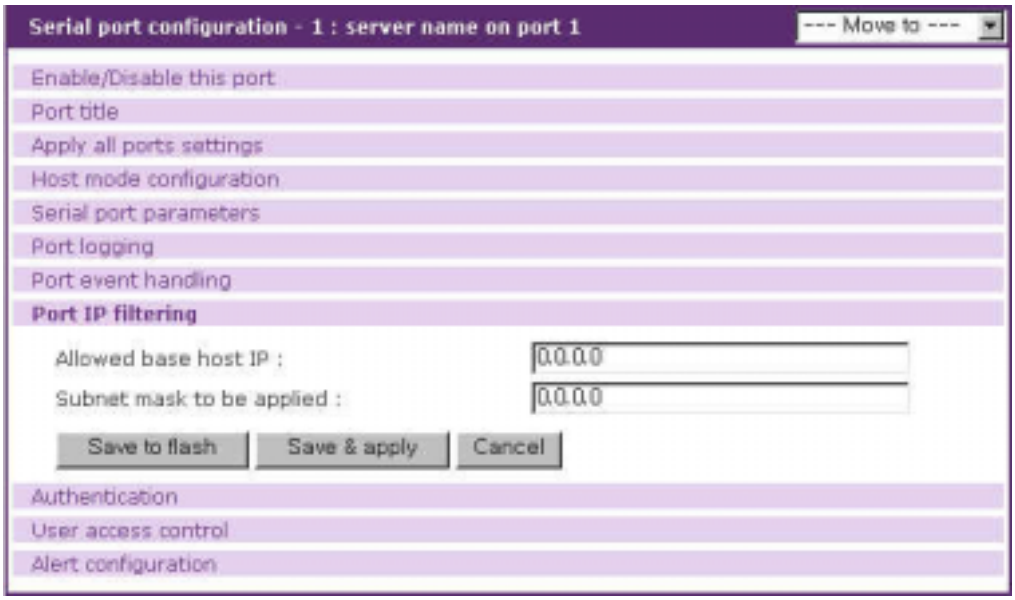


그림 4-16. 포트 IP 필터링

4.3.9 Authentication 설정

인증(Authentication)은 일반적으로 사용자 이름 및 비밀 번호를 기초로 하여 개별적으로 식별하는 과정입니다. VTS는 시리얼 포트에 접속하는 사용자를 인증하기 위한 **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, VTS는 사용자를 인증하기 위해 VTS 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, VTS는 외부 인증 서버(예. RADIUS, Kerberos, TACACS+ 및 LDAP 서버) 에 사용자 인증을 요청할 것입니다. 그림 4-17는 외부 인증 서버를 사용할 때의 사용자 인증 프로세스를 개념적으로 보여줍니다.

사용자는 또한 인증 방법을 조합하여 선택할 수 있습니다. 이 경우에는, 처음의 방법으로 VTS가 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, VTS는 RADIUS를 우선 사용하여 외부 RADIUS 서버에 인증을 요청하고, 실패한 경우에는 VTS 자신의 사용자 목록을 통해 인증을 시도합니다.
“**RADIUS down - Local**" 인증 방법의 경우에는, 외부 RADIUS 서버에 인증을 요청하고, RADIUS 서버가 다운되었을 때만 VTS는 자신의 사용자 목록을 통해 인증을 시도합니다.

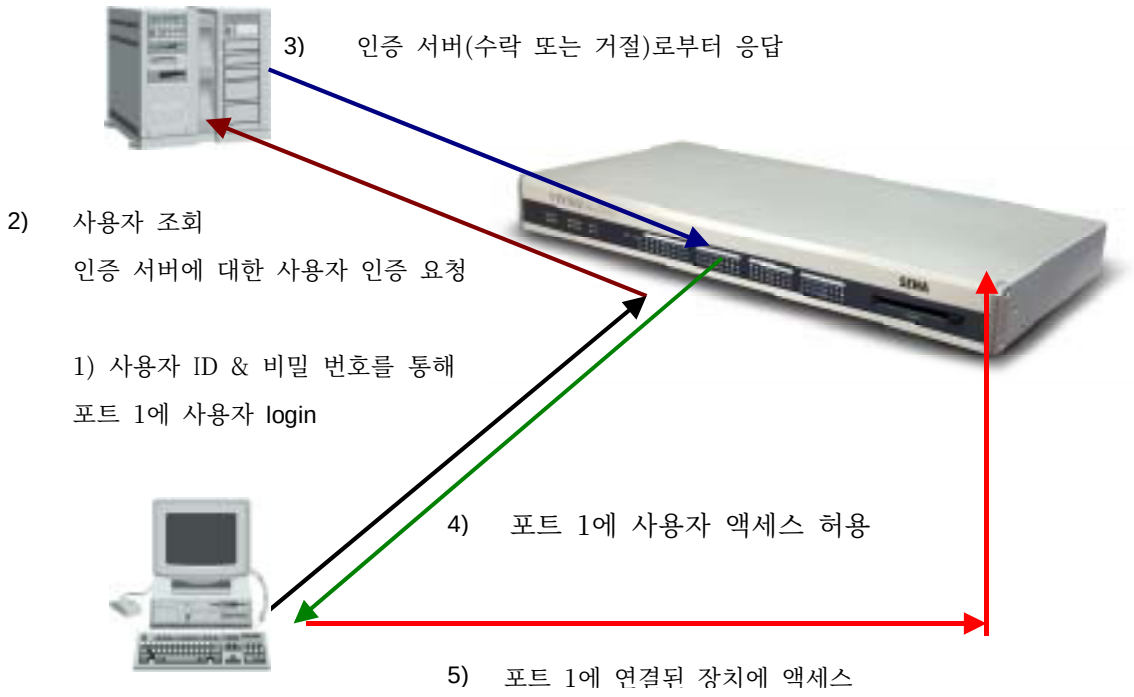


그림 4-17. 외부 서버에 의한 사용자 인증 개념

주의 *:*

1. *VTS v1.7.0에서는 Kerberos 인증을 사용하기 위해서는 /usr2에 kinit 바이너리를 복사해 놓아야 합니다.*
2. *Custom PAM은 Linux-PAM을 지원합니다. 이를 사용하려면 /ets/pam.d/custom 파일을 생성해야합니다. (Linux-PAM에 대한 자세한 내용은* ***11.9.2 CLI 로그인에 대한 RADIUS 인증하기****와* ***11.9.3 CLI 로그인에 대한 TACACS+ 인증하기****를 참조하시기 바랍니다.)*

다음은 VTS 각 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
LDAP server
LDAP server - Local
Local - LDAP server
Kerberos server

Kerberos server - Local

Local - Kerberos server

Custom PAM

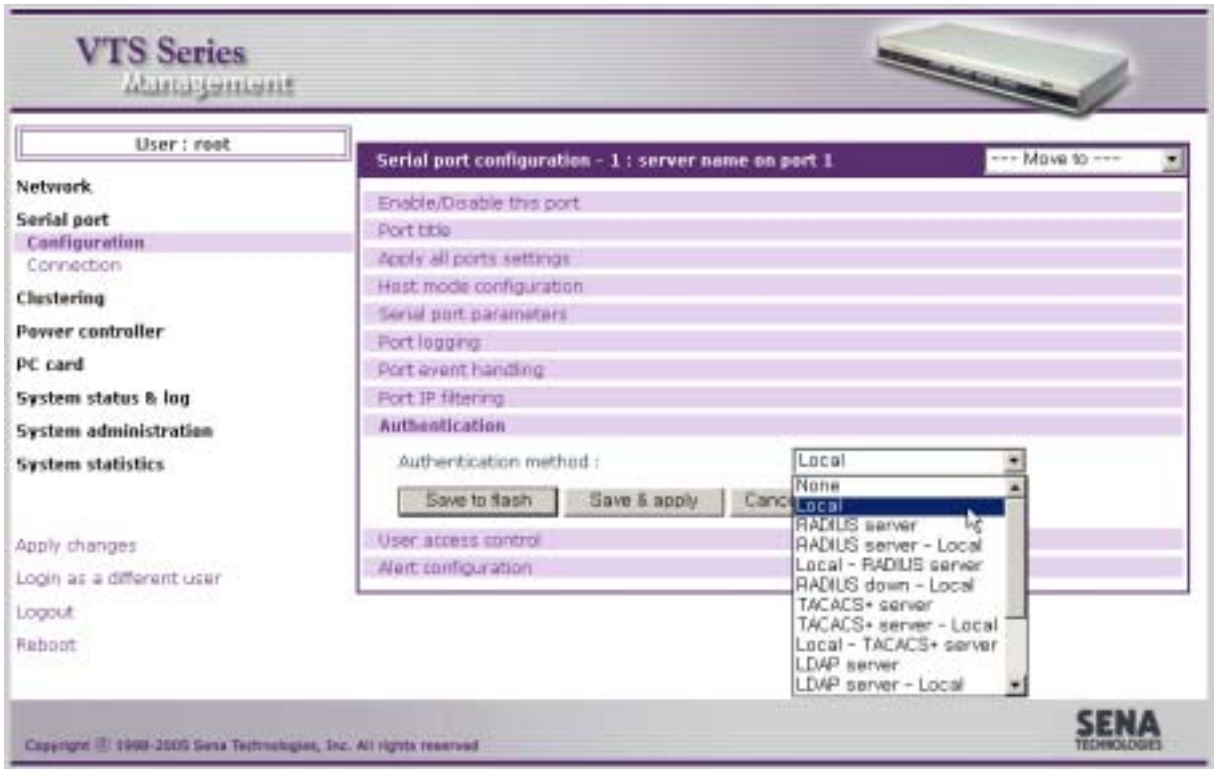


그림 4-18. 시리얼 포트에 대한 인증 옵션

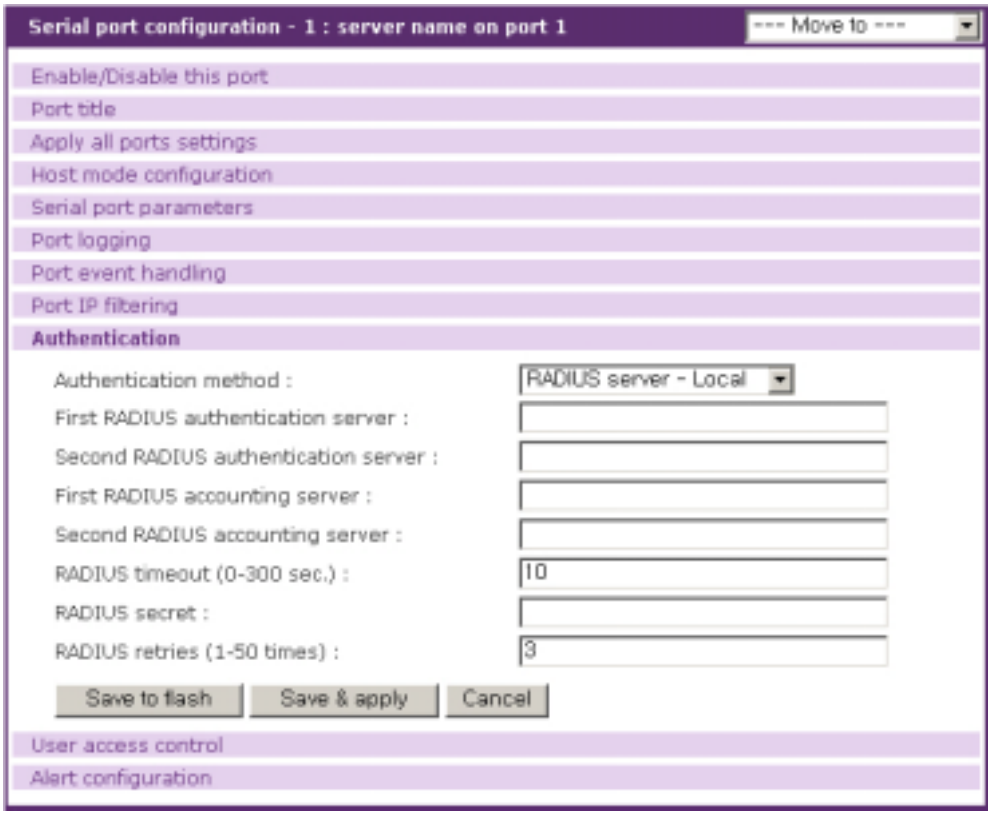


그림 4-19. RADIUS 서버 – local 에 대한 인증 설정

4.3.10 User access control 설정

VTS 시리얼 포트/원격 포트의 연결과 Sniff session 연결 또는 파워 컨트롤러 아웃렛을 제어하려는 사용자의 접근권한을 설정합니다. Sniff session 부분에서는 Sniff session을 어떻게 운용할 것인지를 설정합니다.

Port 접근권한은 시리얼 포트/원격 포트로의 연결을 제한하거나 허용하는데 사용됩니다. **Monitor** 접근권한은 시리얼 포트로의 Sniff session 연결의 접근을 제어합니다. **Power** 접근권한은 파워 컨트롤러 아웃렛에 연결된 시리얼 포트의 전원을 제어하는 것을 제한하거나 허용하는데 사용됩니다.

<<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.
Sniff session이 허용되지 않는 포트의 경우에는 Monitor 접근권한 설정은 아무런 영향을 미치지 않습니다. 포트가 파워 컨트롤러 아웃렛에 연결되지 않은 경우 Power 접근권한도 사용되지 않습니다.

Sniff session이 허용된 경우라면 포트로 연결할 수 있는 사용자는 세 가지 그룹으로 나뉠 수 있습니다. Port / Monitor 접근권한 모두를 가진 사용자, Port 접근권한만 가진 사용자, Monitor 접근권한만 가진 사용자입니다.
Port / Monitor 접근권한 모두를 가진 사용자 그룹은 메인 세션으로 포트에 연결할 수도 있고, 메인 세션 / Sniff session으로서 다른 sniff session으로 연결된 사용자의 연결을 종료할 수도 있고, Sniff session 상태에서 메인 세션으로 전환할 수도 있습니다.
Port 접근권한만 가진 사용자 그룹은 메인 세션 또는 Sniff session으로 포트에 연결할 수는 있지만 다른 Sniff session 사용자의 연결을 종료하거나 Sniff session으로 연결했을 경우 메인 세션으로 전환할 수는 없습니다.
Monitor 접근권한만 가진 사용자 그룹은 Sniff session으로만 시리얼 포트에 연결이 가능하고 다른 Sniff session의 연결을 끊거나 메인 세션으로의 전환은 불가능합니다.

사용자가 Authentication 설정에 따라 VTS나 인증 서버의 인증을 거쳐야 하는 것은 물론이고, User access control 설정에 따라 접근권한이 부여되어야만 시리얼 포트에 연결이 가능합니다. Authentication 설정에 관한 자세한 내용은 ***4.3.9. Authentication configuration***을 참조하시기 바랍니다.

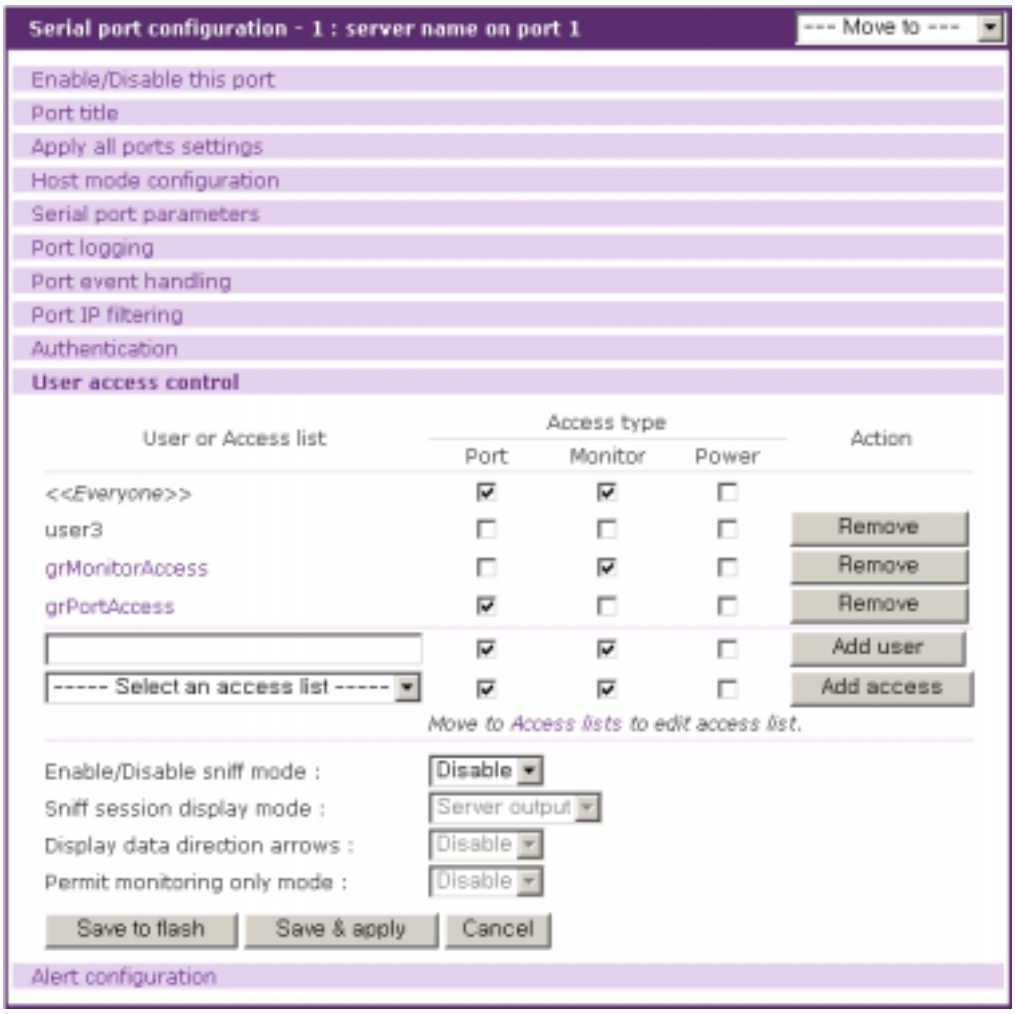


그림 4-20. 시리얼 포트에 대한 액세스 제어 설정

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.

Sniff session

Sniff 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 Sniff user의 개수는 15개로 한정되어 있으며 또한 시스템의 리소스에 의해 제한될 수 있습니다.

사용자의 Sniff session을 인정하려면 **Enable/Disable sniff mode**를 **Enable**로 설정해야 합니다.

Sniff session display mode는 **User input**, **Server output**와 **both**로 설정할 수 있습니다. **User input** 모드로 설정된 경우, sniff 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, sniff 사용자가 다음에 연결하는 경우, 그림 4-21 과 같은 화면이 나타나게 됩니다. 이 때 port escape sequence를 입력하면 port menu가 나타납니다. Port / Monitor 접근권한을 모두 갖고 있는 사용자는 Port 또는 Monitor 접근권한만 가진 일반 사용자보다 높은 권한을 보유하게 되며, 현재 접속되어 있는 메인 세션을 종료하거나 다른 Sniff session을 종료할 권한도 보유하고 있습니다. sniff menu를 통해서 현재 메인 세션을 종료 시키고(**Enter as the main session**) 자신이 메인 세션 사용자가 되거나 현재 메인 세션을 sniff 세션으로 바꾸고(**Take over a main session**) 메인 세션 사용자가 될 수 있습니다.

이외에도 Sniff 사용자는 '**disconnect a sniff session**'을 통해서 다른 sniff 사용자를 선택하여 강제적으로 종료 시킬 수도 있으며, '**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.

메인 세션이 없는 상태에서 Sniff session으로 연결할 수 없고, 메인 세션이 종료되면 Sniff session은 자동으로 종료됩니다. 즉, 메인 세션이 없으면 Sniff session이 존재할 수 없게 됩니다. **Permit monitoring only mode**를 **Enable**로 설정하면 이런 제약이 없어지게 됩니다. 메인 세션없이 Sniff session으로 연결할 수 있고, 메인 세션이 종료되어도 Sniff session에서 계속 모니터링이 가능합니다.

```
  Welcome to VTS-1600 Console Server

VTS-1600 Login : admin
VTS-1600 Password : *****
  Entering server port, ..... type ^z for port menu.

  New sniff session started ...
```

port escape sequence를 입력한 후

```
Port menu:

(server name on port 1) (Port 1) is being used by (sena)
The (admin) is connected in monitoring mode.

m       take over main session
s       enter as a slave session

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

x       close current connection to port
```

그림 4-21. Sniff user 인터페이스 화면

4.3.11 Alert 설정

Host mode가 Console server mode인 경우, 포트 로그인이나 시리얼 포트 연결 이벤트가 발생할 때 이메일 에이전트는 이메일 경보 설정에 따라 이메일을 전송하고, SNMP 에이전트는 SNMP trap 설정에 따라 SNMP trap을 관리자에게 전달합니다.

Port title 설정에서 **Automatic detection**이 활성화 되고 **Device detection method**는 **Active**, **Detection initiation**은 **Periodically**로 설정된 경우 설정에 따라 VTS가 주기적으로 분석한 장치 정보를 이메일이나 SNMP trap을 전송할 수 있습니다. 원격 포트의 경우에는 포트 로그인 이벤트만 지원됩니다.

Alert 설정에 대한 설정 파라미터는 다음과 같습니다.

Enable/Disable email alert for port login
Enable/Disable email alert for device connection
Enable/Disable email alert for active detection
Title of email
Recipient's email address
Enable/Disable port login trap
Enable/Disable device connection trap
Enable/Disable active detection trap
Use global SNMP configuration
Trap receiver settings

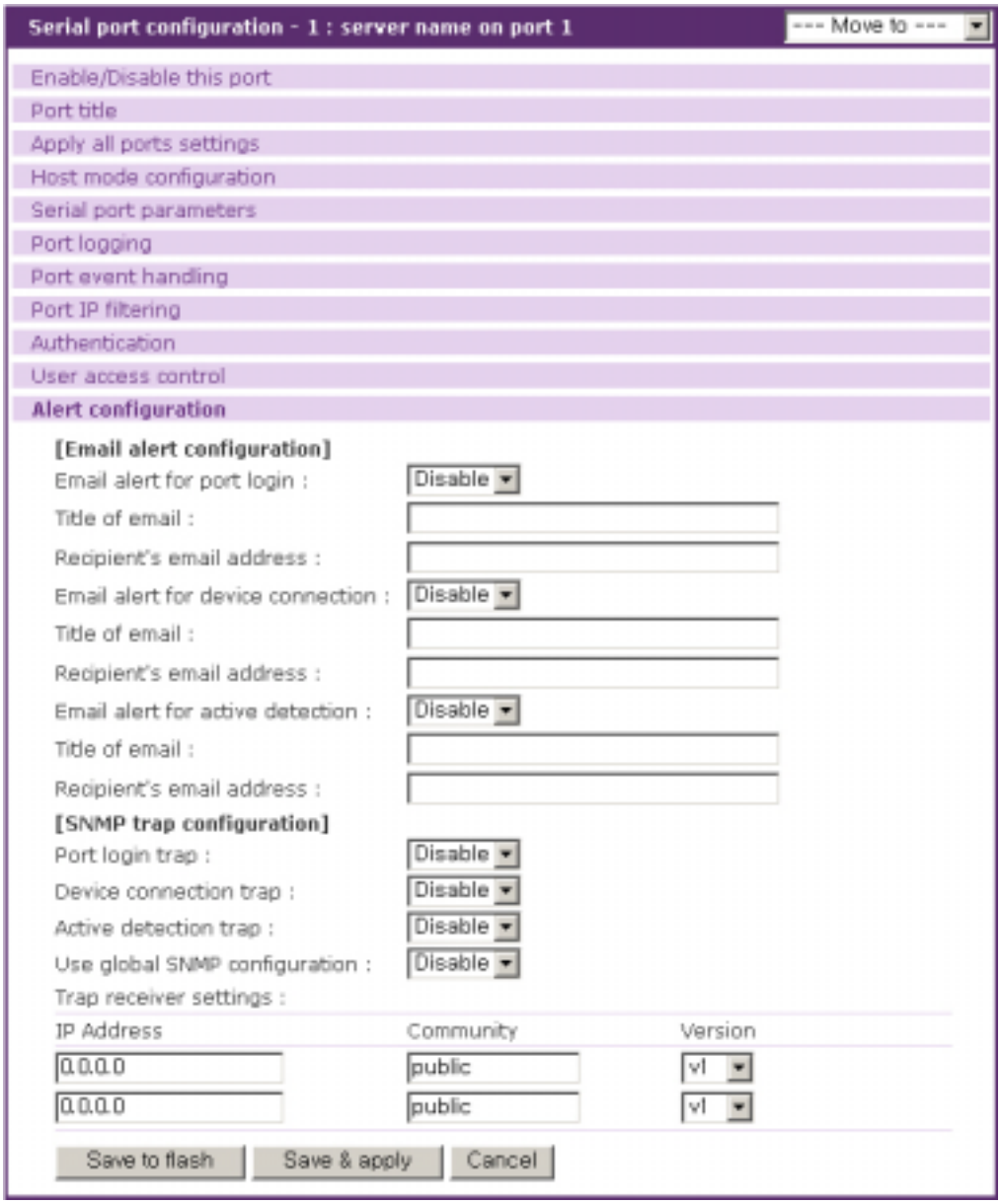


그림 4-22. Console server mode의 Alert 설정

Enable/Disable email alert for port login

사용자가 시리얼 포트 또는 원격 포트로 로그인 또는 로그아웃 할 때 이메일을 전송할지 여부를 설정 합니다.

Enable/Disable email alert for device connection

시리얼 포트가 장비로 연결되거나 연결이 끊길 때 이메일을 전송할지 여부를 설정합니다.

Enable/Disable email alert for active detection

Port title 설정에서 **Automatic detection**이 활성화 되고 **Device detection method**는 **Active**,

Detection initiation은 **Periodically**로 설정된 경우, 주기적으로 분석된 장치정보를 이메일로 전송할 지 여부를 설정합니다.

Title of email
전송되는 이메일의 제목을 설정합니다.

Recipient's email address
전송되는 이메일을 받을 주소를 설정합니다.

Enable/Disable port login trap
사용자가 시리얼 포트 또는 원격 포트로 로그인 또는 로그아웃 할 때 SNMP trap을 발생시킬지 여부를 설정 합니다.

Enable/Disable device connection trap
시리얼 포트가 장비로 연결되거나 연결이 끊길 때 SNMP trap을 발생시킬지 여부를 설정합니다.

Enable/Disable active detection trap
Port title 설정에서 **Automatic detection**이 활성화 되고 **Device detection method**는 **Active**, **Detection initiation**은 **Periodically**로 설정된 경우, 주기적으로 분석된 장치정보에 관한 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 각각 및 **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.

Alert 설정에 대한 설정 파라미터는 다음과 같습니다.

Enable/Disable email alert for dial-in modem test
Title of email
Recipient's email address

Enable/Disable dial-in modem test trap

Use global SNMP configuration

Trap receiver settings

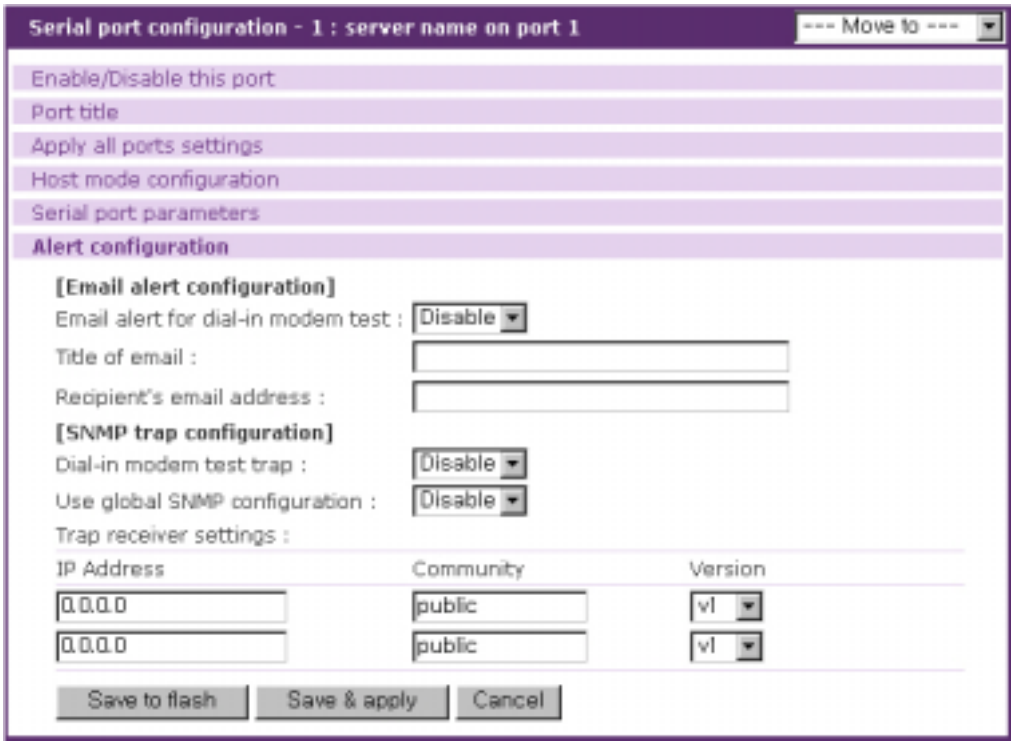


그림 4-23. Dial-in modem mode의 Alert 설정

Enable/Disable email alert for dial-in modem test

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

Enable/Disable dial-in modem test trap

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

4.3.12 Power control 설정

파워 컨트롤러가 VTS에 연결되어 있다면, 시리얼 포트가 그 파워 컨트롤러의 어느 아웃렛에 연결되어 있는지를 설정한다. 시리얼 포트의 전원은 이 설정을 이용하여 관리된다.

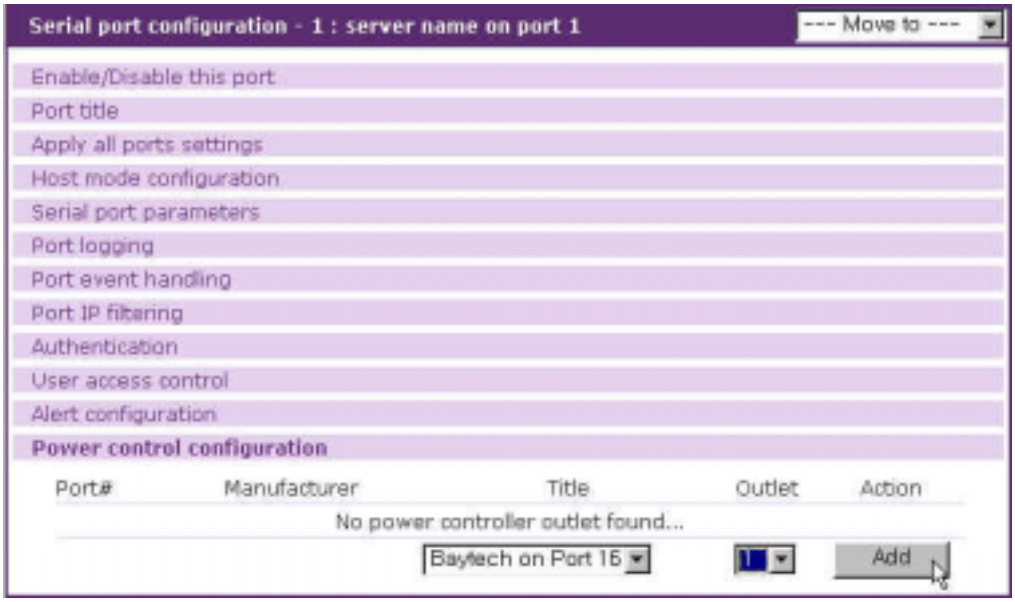


그림 4-24. Power control 설정

4.4 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 enable/disable
2. Port title
3. Host mode configuration
4. Serial port parameters: *Invalid for remote port*
5. Port logging*: Only valid and visible if host mode set to Console Server Mode.*
6. Port event handling: *Only available if the host is set to Console Server Mode and Port logging is enabled.*
7. Port IP filtering: *Only available if the host is set to Console Server Mode.*
8. Authentication
9. User access control: *Only available if the host is set to Console Server Mode.*
10. Alert configuration: *Only available if the host is set to Console Server Mode.*

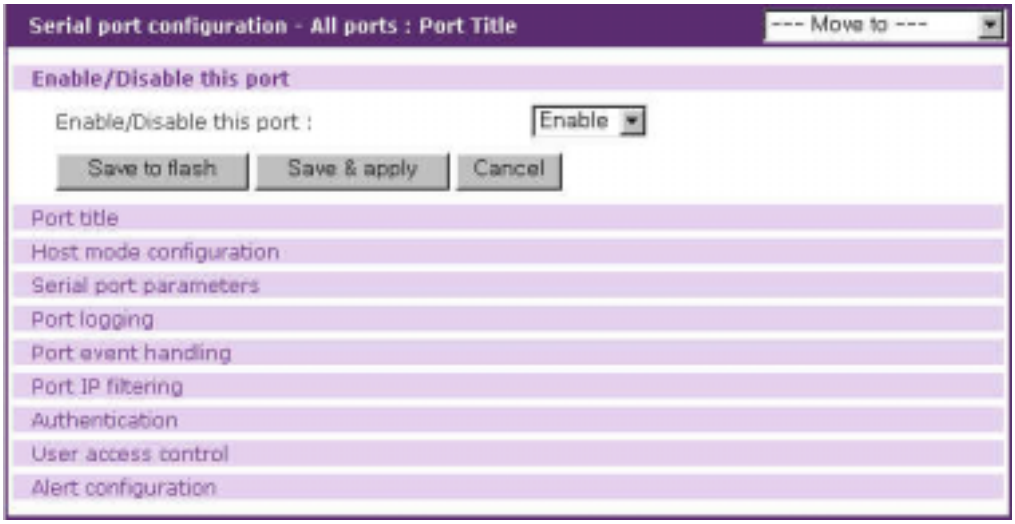


그림 4-25. 모든 포트 설정

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 server #1"로 설정되고 포트 #2의 포트 타이틀은 "my server #2"로 자동으로 설정됩니다. 원격 포트 #1은 "my server #R1"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. VTS3200인 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.

Serial port parameters, Port logging, Port event handling, Port IP filtering, Authentication, User access control, Alert configuration
위 그룹의 파라미터의 경우, “**apply all ports settings**” 설정 값은 모든 시리얼 포트 또는 원격 포트에서 동일하게 설정됩니다. 다만, Serial port parameters 설정의 경우에는 원격 포트에 영향을 미치지 않습니다.

4.5 Serial port 연결

VTS 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 4-26과 같은 화면이 나타납니다.

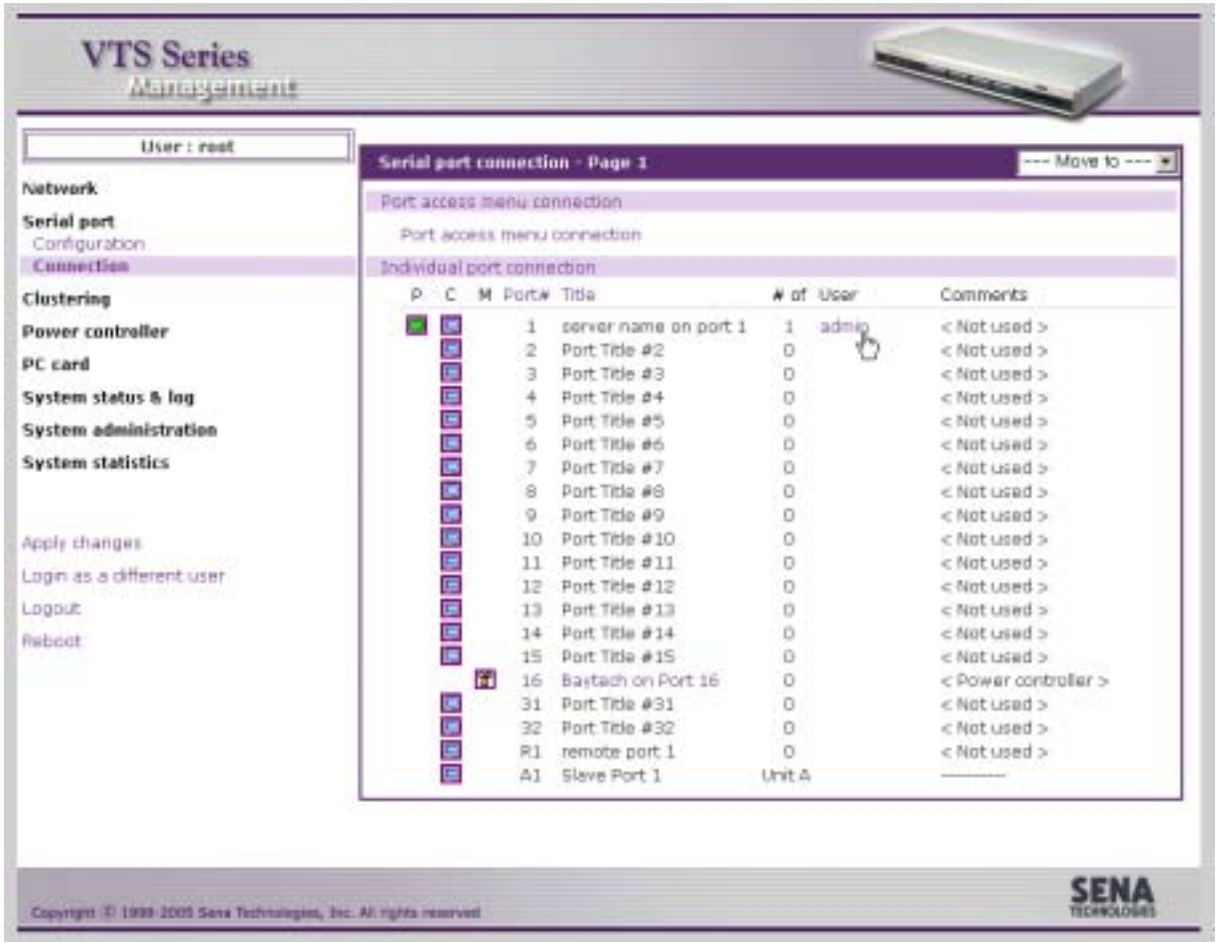


그림 4-26. 시리얼 포트 연결 페이지

이 페이지에서는 **port access menu**, **시리얼 포트, 원격 포트** 및 클러스터링 슬레이브 장치의 사용가능한 모든 **시리얼 포트**에 대한 연결 기능을 제공합니다. 사용자는 자신들이 접속하려는 포트의 C(Connect) 열에 있는 터미널 아이콘을 클릭함으로써 포트에 접속할 수 있습니다. 사용자가 해당 포트의 터미널 아이콘을 클릭하면 터미널 에뮬레이션 팝업 창이 나타나 사용자에게 시리얼 포트 접속에 대한 권한을 부여합니다.
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.
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 원격 포트 번호 앞에 R이 붙어 표시되고, 클러스터링 슬레이브 장치의 경우에는 포트 번호 앞에 슬레이브 장치 번호가 붙습니다.
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.

시리얼 포트/원격 포트의 전원 제어에 대한 연결 기능을 제공합니다. P(power control) 열에 있는 on/off 상태 표시 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. VTS에 추가된 파워 컨트롤러를 관리할 수 있는 파워 컨트롤러 관리(**Power controller management**) 페이지로의 연결 기능을 제공합니다. M(power Management) 열에 표시된 아이콘을 클릭하면, 파워 컨트롤러 관리 페이지로 이동하여 파워 컨트롤러를 제어할 수 있습니다. 자세한 내용은 **6.3.4 파워 컨트롤로 관리 – 시리얼 포트 연결** 을 참조하시기 바랍니다.

***참고**: 해당 포트의 프로토콜이 Telnet 또는 SSH로 설정 되어 있을 경우에는 팝업되는 터미널 에뮬레이션 창의 종류는 **4.3.4 Host mode 설정** 에서 기술된 바와 같이 Quick connect via 메뉴의 설정값에 따라 달라집니다.*

Java Applet은 serial port에 접속하기 위한 텍스트 기반의 사용자 인터페이스를 제공합니다. Java 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 Applet 창이 나타나게 되고, 사용자는 그 포트에 접속하기 위해 필요한 자신의 사용자 ID 및 비밀번호를 입력하라는 요청을 받게 됩니다. 인증을 받은 경우, 사용자는 현재 시리얼 포트, 원격 포트 또는 슬레이브 장치의 시리얼 포트에 접속할 수 있습니다. Java Applet 창의 타이틀 바는 telnet 또는 SSH의 연결 상태, 포트 번호와 포트 타이틀과 같은 정보를 보여줍니다. 창 아래의 버튼들은 연결, 종료 또는 브레이크 전달 등의 기능에 제공하고 있습니다.

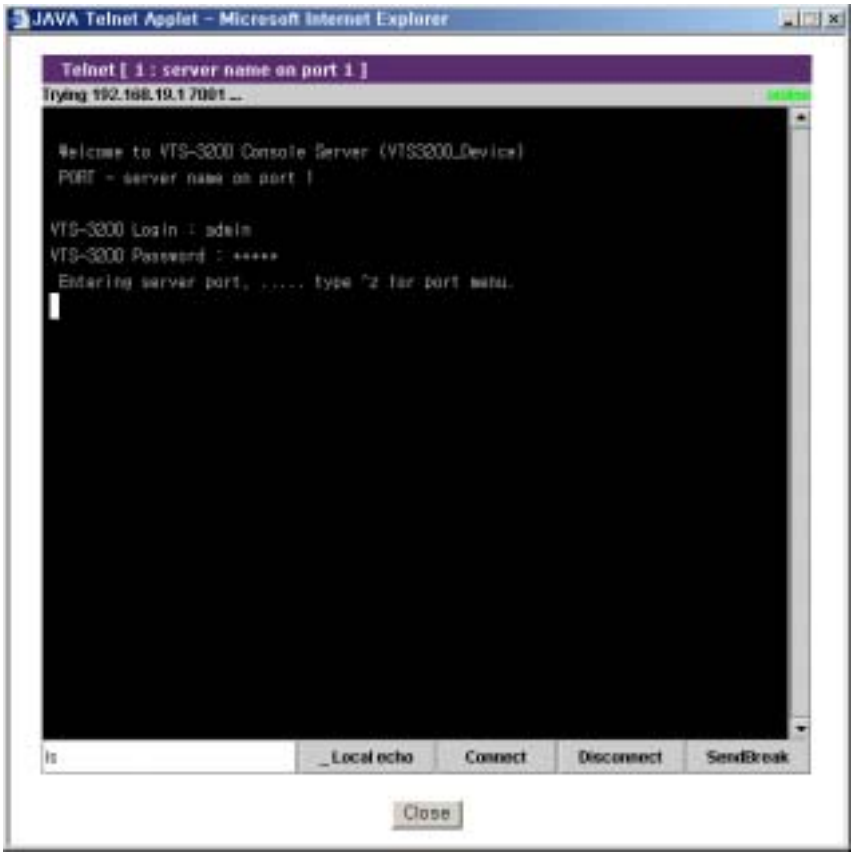


그림 4-27. JTA telnet 윈도우

그림 4-28. JTA SSH 윈도우

VTS가 SSH 버전 1을 지원할 지 여부는 시큐리티 프로파일의 SSH V1 항목에서 설정합니다. (**9.7 시큐리티 프로파일** 참조). Java 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 Applet 이 SSH 공개 키 인증을 제공하지 않기 때문에 웹을 통해 포트에 접속할 수 없습니다.*

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 클릭하면 그림 4-29 로그인 중인 시리얼 포트 사용자 리스트 화면이 나타납니다.
이 화면의 사용자 리스트 중인 연결 종료하려는 사용자들을 체크한 후 **Kill** 버튼을 누르면 해당 사용자들의 연결을 강제로 종료할 수 있습니다.

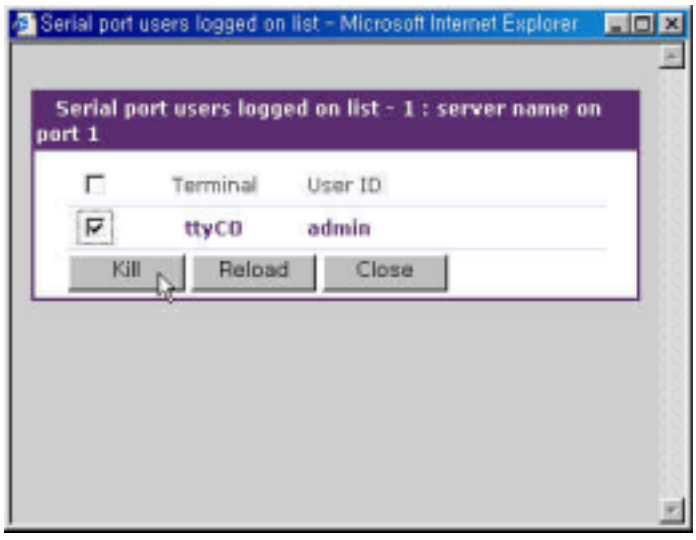


그림 4-29. 로그인 중인 시리얼 포트 사용자 리스트

VTS는 웹 인터페이스에 로그인하지 않고 직접 시리얼 포트, 원격 포트 또는 슬레이브 장치의 시리얼 포트에 접근하는 웹 페이지를 제공합니다. 웹브라우저의 주소창에 다음과 같이 입력하면 시

리얼 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 VTS의 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.

그림 4-30와 그림 4-31는 <port number>와 <port title>을 사용하여 직접 시리얼 포트로 연결하는 예를 보여줍니다.

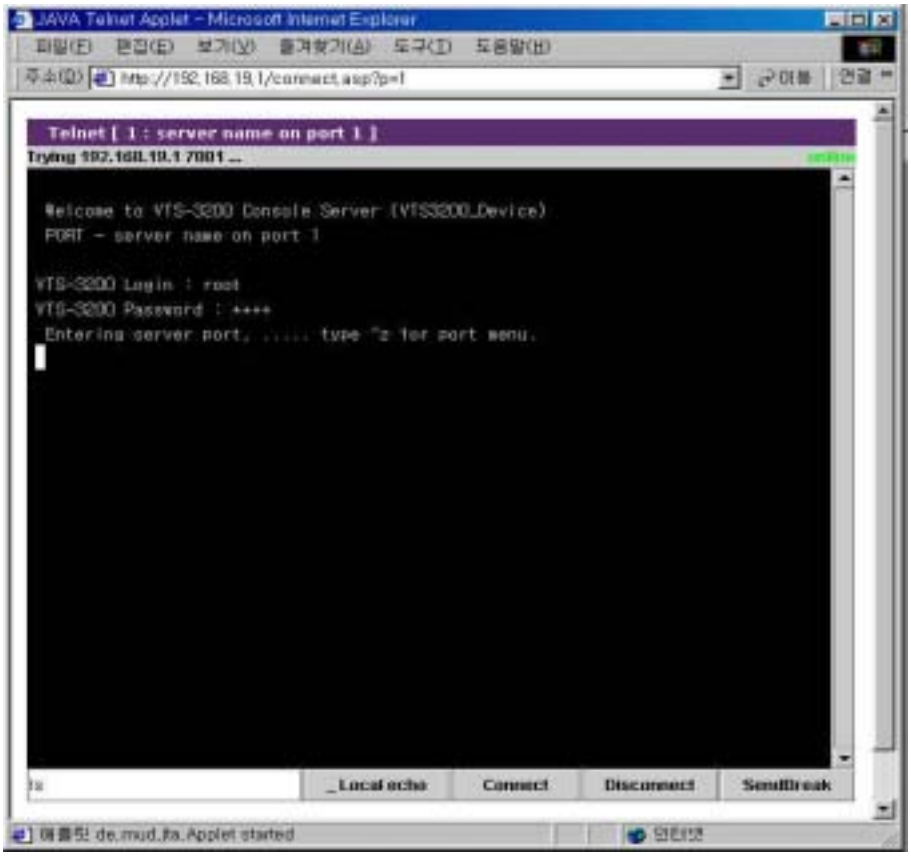


그림 4-30. Port number로 시리얼 포트에 직접 연결

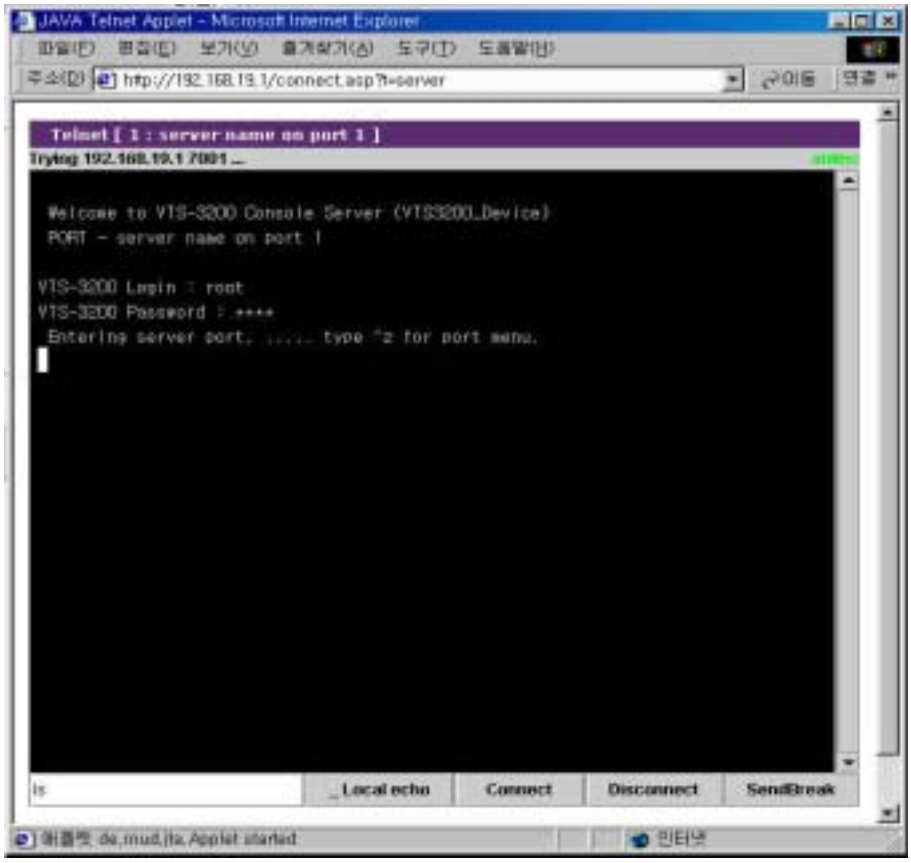


그림 4-31. Port title로 시리얼 포트에 직접 연결

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

<user>:p=<port number>
또는
<user>:t=<port title>

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. 그림 4-32과 그림 4-33은 리눅스에서 <port number>과 <port title>을 이용하여 SSH 원격 시리얼 컨솔을 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 4-32. SSH 원격 시리얼 컨솔을 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 4-33. SSH 원격 시리얼 컨솔을 통한 포트 연결 - port title

5: Clustering 설정

5.1 개요

VTS는 Clustering 기능을 사용하여 하나의 VTS를 통해, 다른 여러 VTS들의 시리얼 포트들도 접속할 수 있습니다. 사용자는 하나의 마스터 VTS를 통해 최대 816개까지의 시리얼 포트(*=48 포트 * 16 개의 슬레이브 장치 + 마스터 장치의 48 포트*)를 접속할 수 있습니다.
슬레이브 장치의 시리얼 포트로 접근하기 위해 VTS는 NAT(Network Address Translation)에 기반한 방법론을 사용합니다. 커널 기반의 간단한 IP forwarding 방식을 사용하여, VTS는 효율적이고 유연하고 빠르면서 안전한 접근 방법을 제공합니다. 만약, 사용자가 현재 환경을 반영하는 IP forward-ing 규칙을 수동으로 설정한다면, VTS는 다른 터미널 서버들도 또한 관리할 수 있게 됩니다.
마스터 VTS의 TCP port로 전송되는 데이터는 슬레이브 VTS 의 (IP 주소: TCP 포트)에 전달됩니다. 따라서, 사용자가 마스터 VTS 에서 IP forwarding 규칙만 설정해 주면, 마스터 VTS를 통해 슬레이브 VTS 들에게 접속할 수 있게 됩니다. 슬레이브 VTS 에는 추가적인 설정이 필요 없습니다.
사용자가 마스터 VTS 를 경유하여 슬레이브 VTS 의 시리얼 포트에 접속을 시도한다고 생각해봅시다. 다음은 현재 사용자의 응용 환경입니다.

- 사용자 컴퓨터의 IP 주소: 192.168.0.100
- 마스터 VTS 의 IP 주소: 192.168.0.2
- 슬레이브 VTS 의 IP 주소: 192.168.0.3.
- 마스터 VTS의 TCP 포트 6033 을 슬레이브 VTS 의 시리얼 포트 1 (TCP 포트, 6001)를 위해 따로 지정합니다.

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

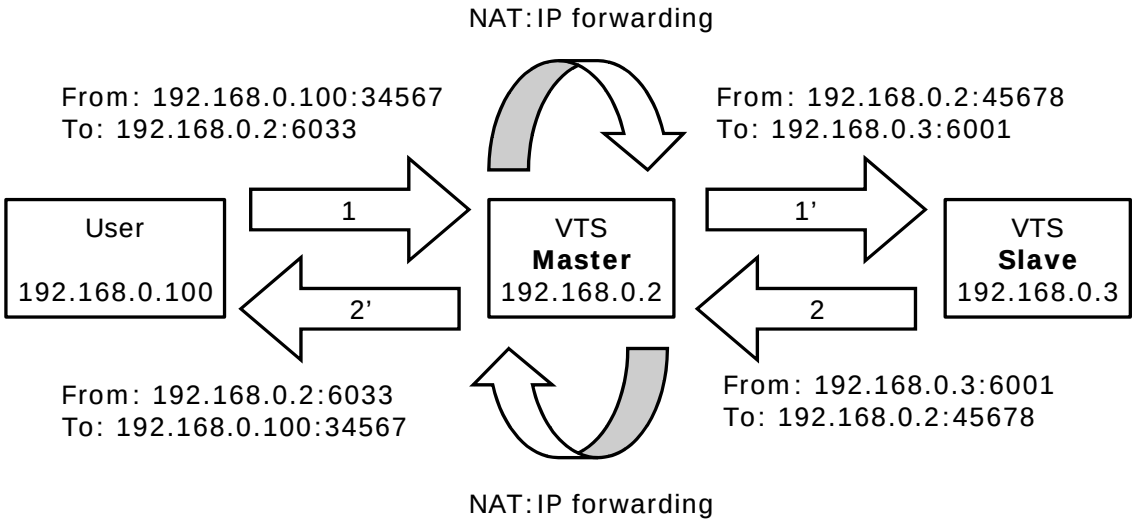


그림 5-1. VTS Clustering 작동 개념

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

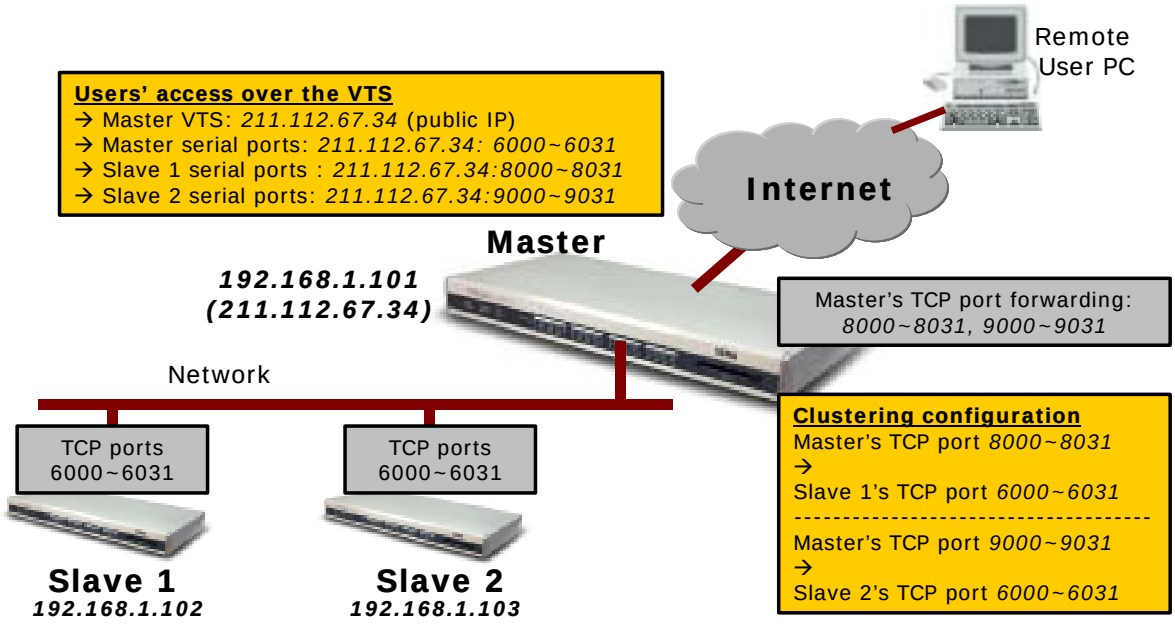


그림 5-2. VTS Clustering 예제

5.2 Clustering 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. VTS의 **Clustering mode**가 **Master**로 설정되면 **Authentication mode**와 **Update master on changes** 항목은 비활성화 됩니다.

사용자가 한 VTS를 마스터로 설정하기 원하는 경우, **Clustering 설정** 화면에서 설정해야 하는데, 장치를 미스터로 설정하면 마스터 설정에 관련된 설정 화면이 나타납니다. 그림 5-3은 Clustering mode를 마스터로 설정한 Clustering 설정 화면을 보여줍니다. 사용자가 Clustering mode를 마스터로 설정하고 저장하면, 마스터 장치를 위한 Clustering 설정 화면이 표시됩니다. 그림 5-4는 마스터 장치를 위한 Clustering 설정 화면을 보여줍니다.

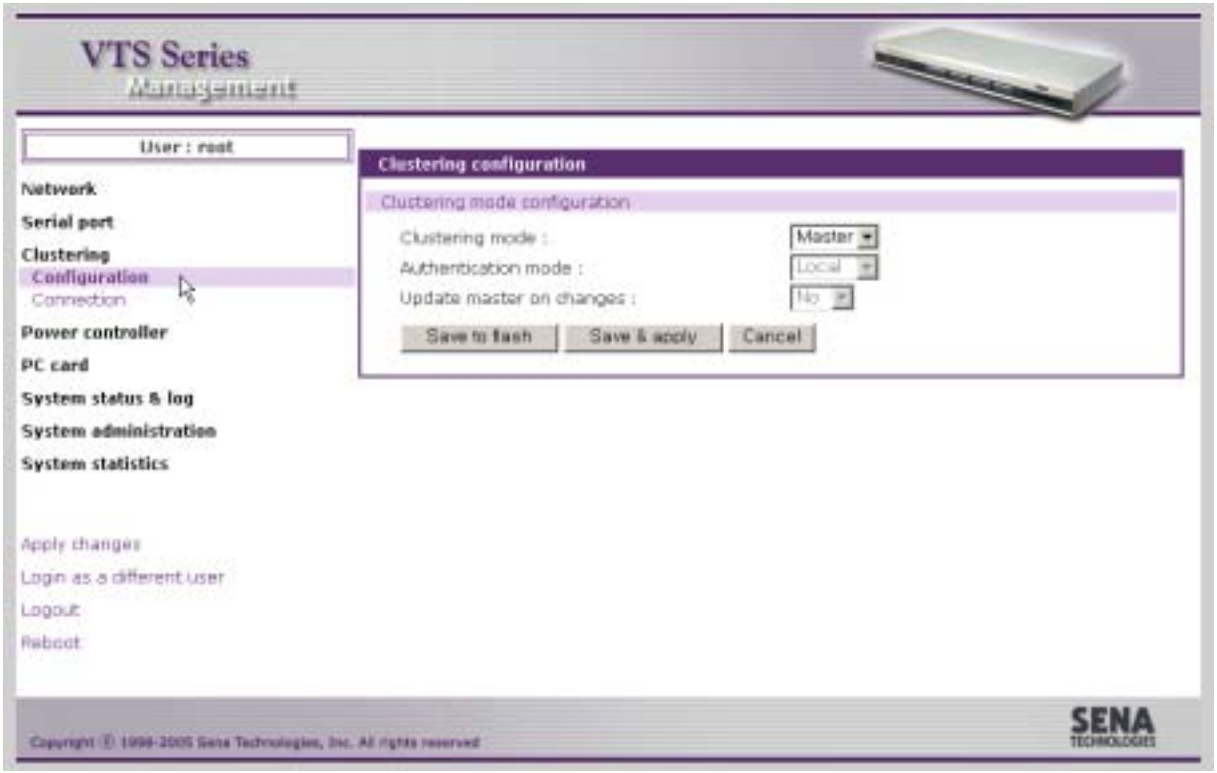


그림 5-3. 마스터로 VTS Clustering 설정

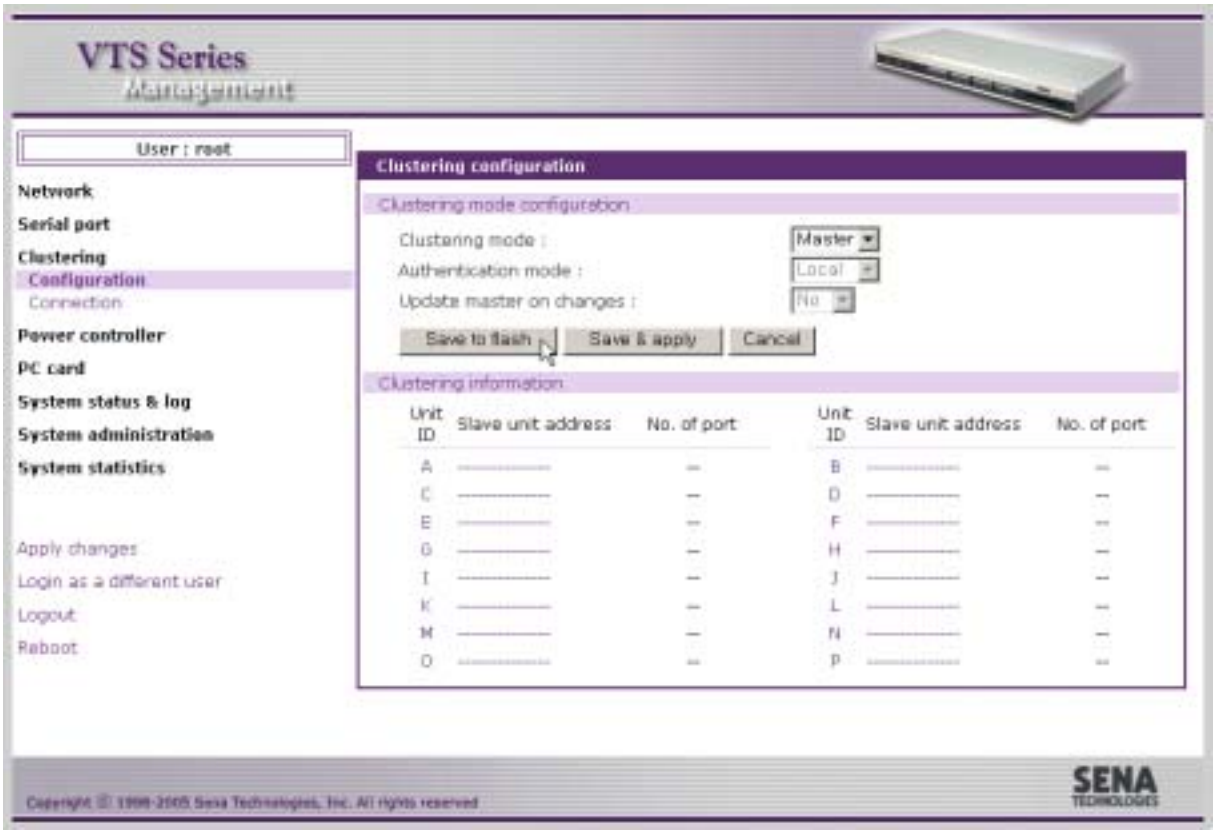


그림 5-4. 마스터 VTS Clustering 설정

슬레이브를 추가하기 위해, 사용자는 슬레이브 번호 또는 IP 주소를 클릭하여 추가적인 설정을 할 수 있습니다. 그림 5-5는 슬레이브 장치를 설정하기 위한 화면을 보여줍니다. 이 화면에서 슬레이브 장치를 enable로 설정하면, 지정 슬레이브 장치에 대한 추가적인 설정을 위해 IP forwarding 테이블 화면으로 이동합니다. 그림 5-6은 슬레이브 장치의 Clustering 설정을 위한 IP forwarding 화면을 보여줍니다.

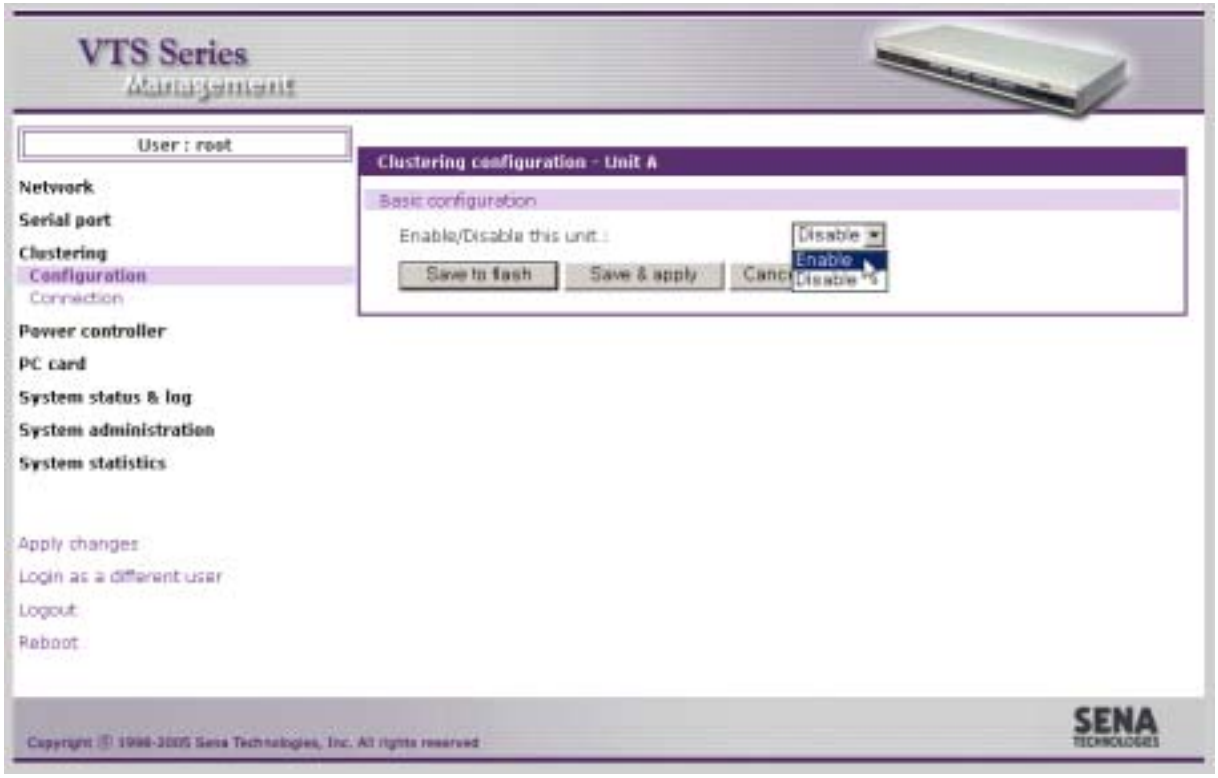


그림 5-5. 슬레이브 장치에 대한 설정

사용자는 수동으로 IP forwarding 테이블을 설정할 수도 있고 자동으로 슬레이브 장치의 시리얼 포트 설정을 import 할 수 있습니다. **Port access menu** 및 시리얼 포트에 접속하기 위한 IP forwarding 테이블이 제공됩니다. Source port는 마스터 장치의 TCP 포트 번호이며, Destination Port는 Source port 포트로 전송되는 데이터가 전달될 슬레이브 장치의 TCP 포트 번호입니다.
포트 forwarding 테이블을 자동으로 설정하려면 슬레이브 장치의 IP 주소 또는 도메인 이름을 입력한 다음 [Auto Config] 버튼을 클릭합니다. 마스터 장치는 슬레이브 장치의 시리얼 포트 정보를 자동으로 import하고 그에 대한 마스터의 소스 포트 정보를 자동으로 설정합니다. 그림 5-7은 자동 설정 실행 후 결과를 보여줍니다. 마스터는 장치가 슬레이브로 설정되어 있고 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 마스터의 시리얼 포트의 기존의 설정과 충돌되도록 설정하지 말아야 합니다. 충돌되는 경우, Clustering 기능이 비활성 상태가 됩니다.*

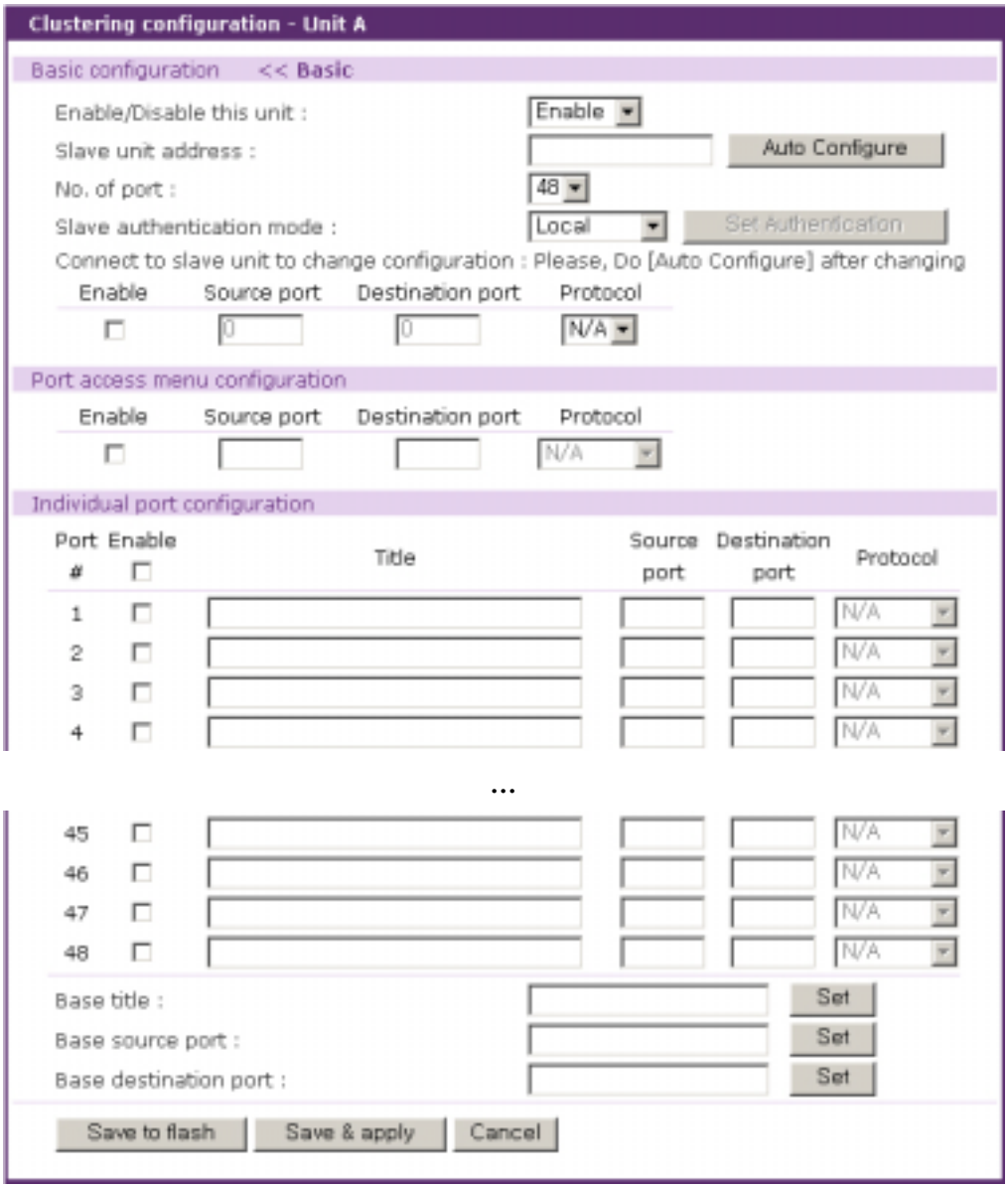


그림 5-6. 슬레이브 장치의 Clustering 설정을 위한 IP forwarding 테이블

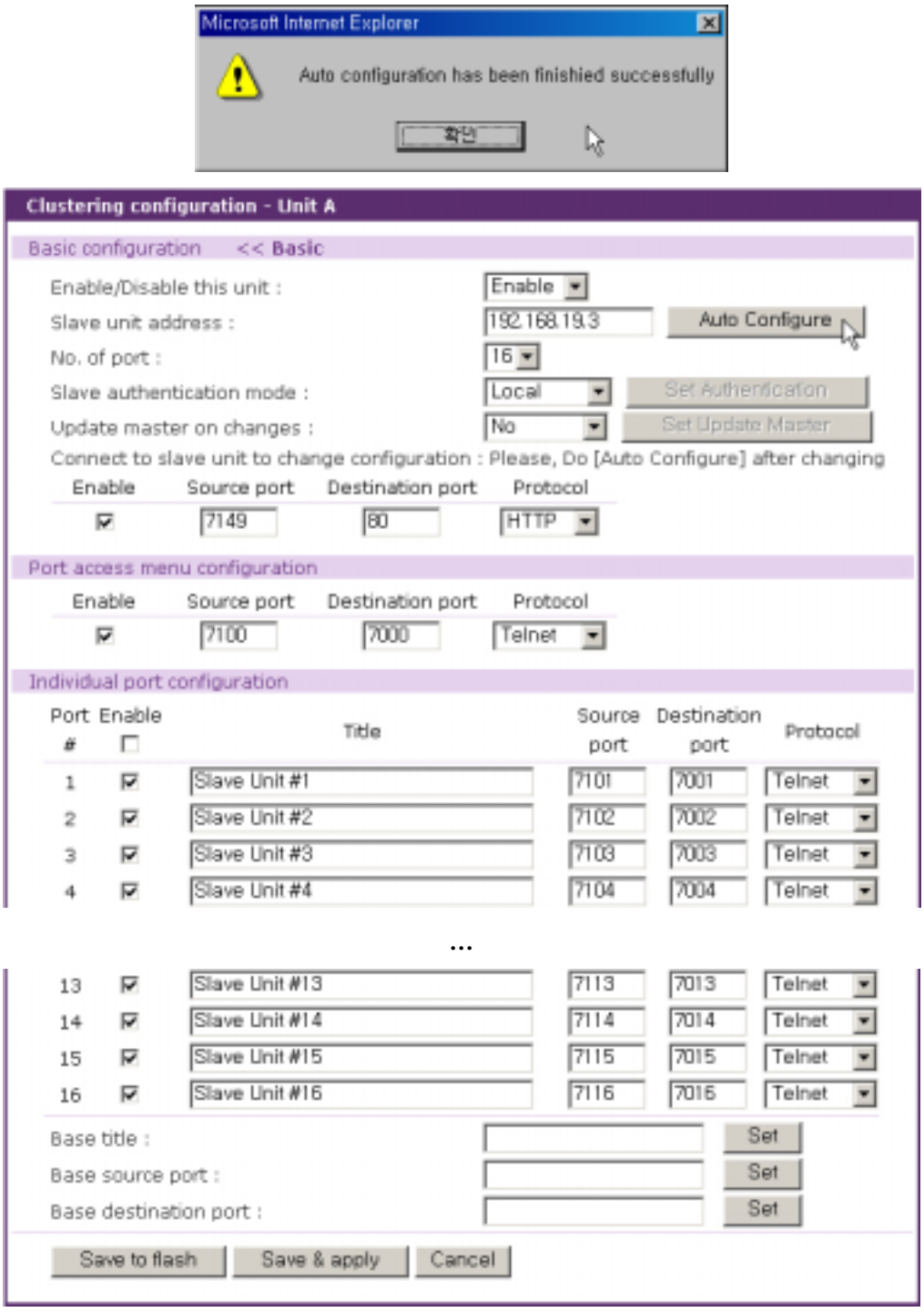


그림 5-7. VTS 자동 Clustering 설정 결과

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 5-8. VTS Clustering 설정 오류 메시지

슬레이브 장치의 포트 정보가 정확하게 설정되었는지 확인하십시오. 그런 다음 슬레이브 장치에 대한 Clustering 설정을 완료하기 위해 [Save to flash] 및 [Apply changes] 버튼을 선택하십시오. 그림 5-9는 Clustering 설정을 저장하고 적용한 결과를 보여줍니다.

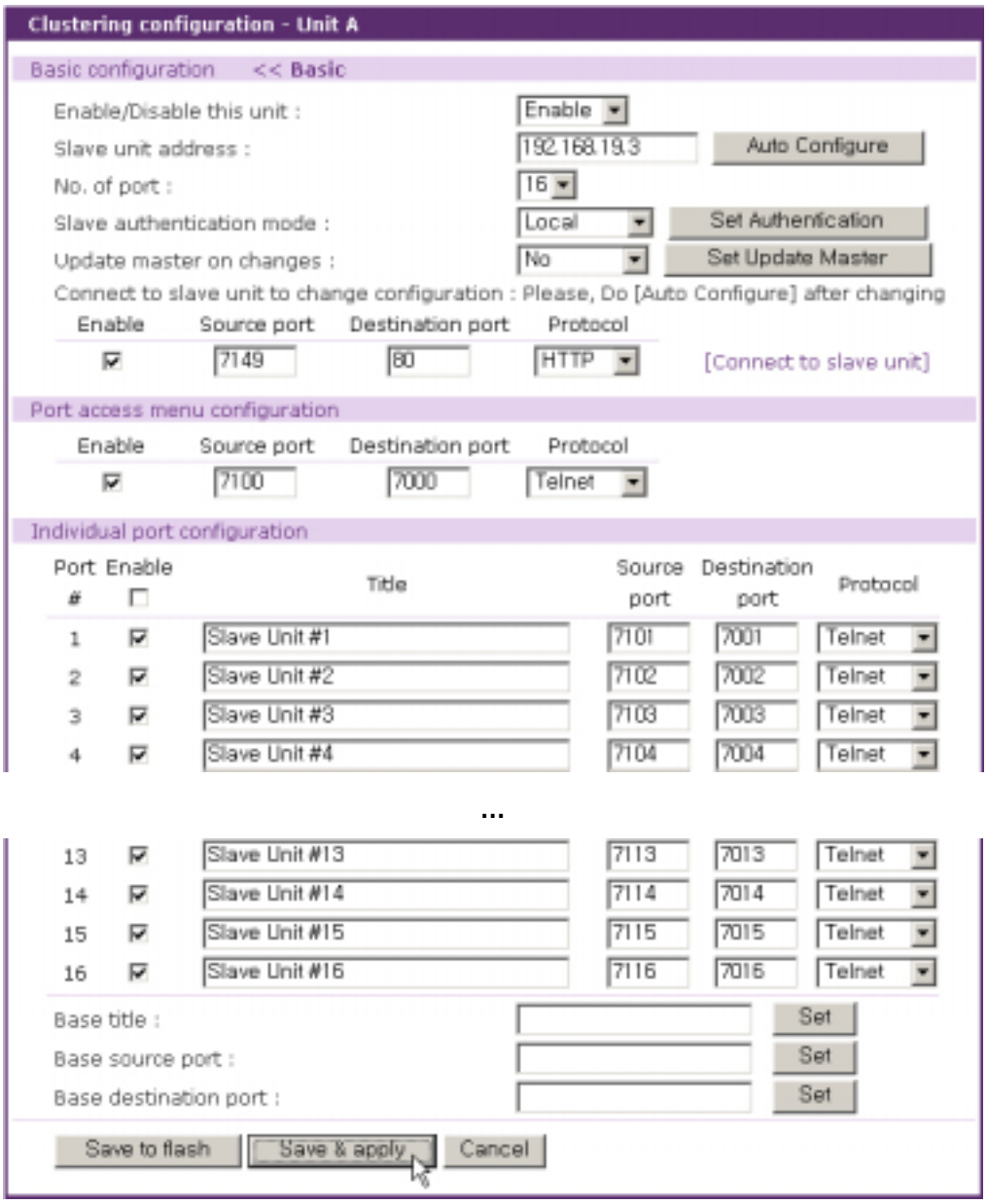


그림 5-9. 저장 적용 후 VTS clustering 설정

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.

Clustering 설정이 완료되면, 사용자는 메뉴 바의 [Clustering – Connection] 메뉴 항목을 선택하여 슬레이브 장치들의 포트에 연결을 시도할 수 있습니다. 그림 5-10은 Clustering 연결 화면을 보여줍니다. 사용자는 Clustering - Connection 화면에서 슬레이브 장치의 번호 또는 IP 주소를 선택하여 슬레이브 장치의 포트 연결 화면으로 이동할 수 있습니다. 이 화면에서 슬레이브 장치의 모든 연결 가능한 시리얼 포트가 표시됩니다.

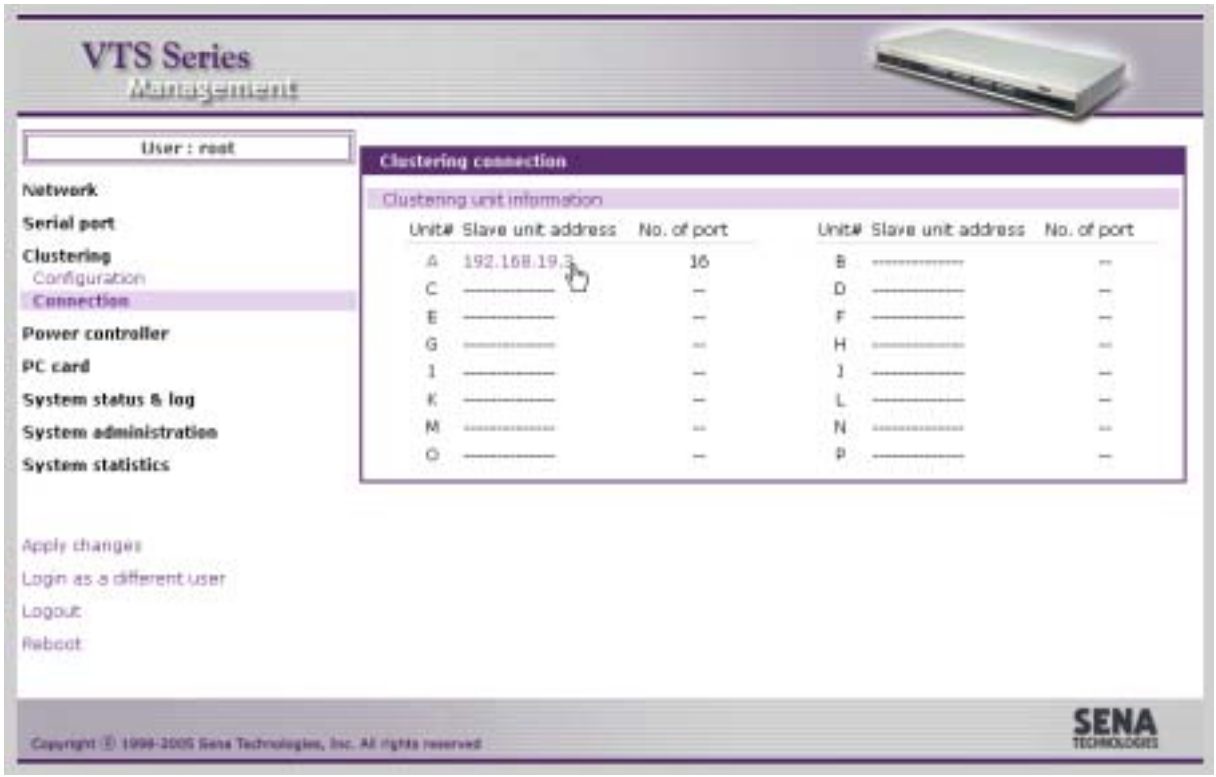


그림 5-10. VTS Clustering 연결 페이지 – 슬레이브 정보

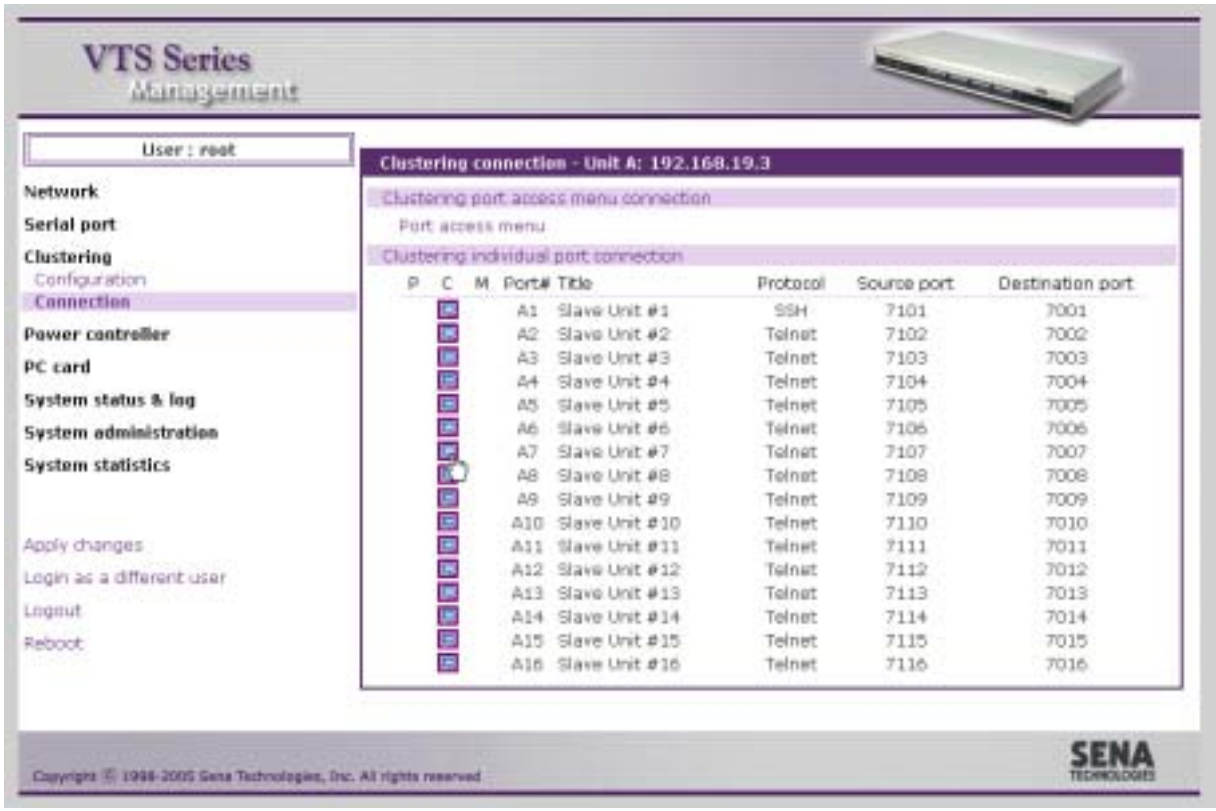


그림 5-11. VTS Clustering 연결 페이지 – 슬레이브 장치

그림 5-11은 슬레이브 장치에서 사용 가능한 모든 시리얼 포트를 표시하는 화면입니다. 이는 Serial Port – Connection의 시리얼 포트 연결과 유사하게 동작합니다. 사용자가 접속하려는 포트의 C(Connect) 열에 있는 터미널 아이콘을 클릭하면, 포트 접속을 위한 Java Applet 윈도우가 나타나게 되고, 사용자는 슬레이브 장치의 해당되는 포트를 접속할 수 있습니다. 시리얼 포트 연결 페이지에도 슬레이브 장치의 모든 연결한 가능한 포트들이 표시됩니다. 마스터 장치의 시리얼 포트 또는 원격 포트처럼 슬레이브 장치의 포트에 연결할 수 있습니다. (**4.5 Serial port 연결** 참조)

telnet 또는 SSH 클라이언트 프로그램을 이용하여 슬레이브 장치의 시리얼 포트에 접속하려면 Destination port에 해당되는 마스터 장치의 Source port에 접속하면 됩니다.

마스터 장치의 시리얼 포트 또는 원격 포트 연결과 같이, VTS는 웹 인터페이스에 로그인하지 않고 직접 슬레이브 장치의 시리얼 포트에 접근하는 웹 페이지도 제공하고, SSH 원격 시리얼 컨솔을 통하여 슬레이브 장치의 시리얼 포트에 연결하는 방법도 제공합니다. (**4.5 Serial port 연결** 참조)

그림 5.-12는 Java Applet 윈도우로 슬레이브 장치의 시리얼 장치에 연결했을 때의 화면입니다.

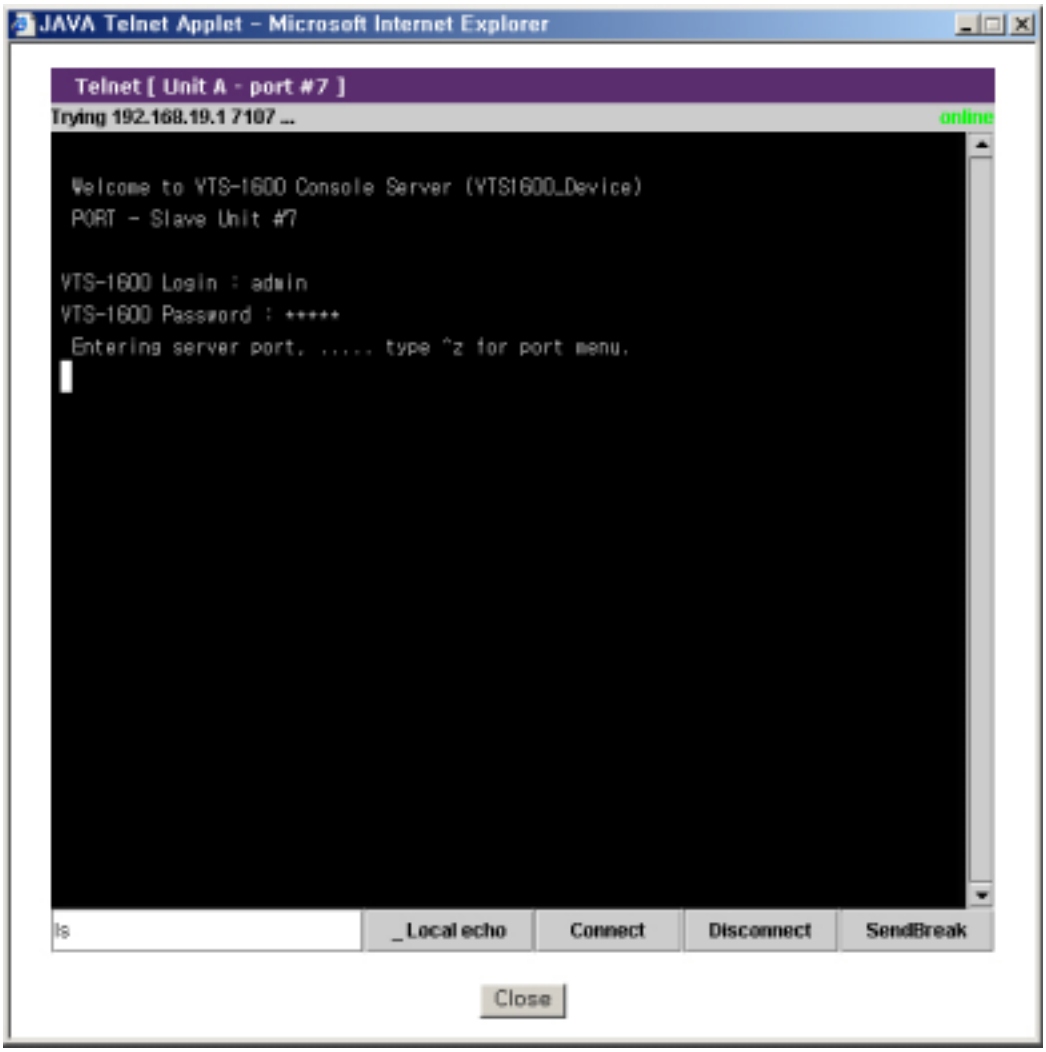


그림 5-12. 슬레이브 장치의 시리얼 포트에 연결

6: Power Controller

6.1 개요

SENA PM 시리즈, Baytech RPC 시리즈 같은 파워 컨트롤러를 VTS에 추가하고 설정하고 제어할 수 있습니다. 사용자가 VTS에 파워 컨트롤러를 추가하고 VTS의 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 ***4.3.12. Power control configuration*** 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.
VTS의 파워 컨트롤러 기능의 특징은 사용자가 VTS 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.

지원하는 파워 컨트롤러
- SENA PM 시리즈
- Baytech RPC 시리즈

6.2 파워 컨트롤러 설정

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

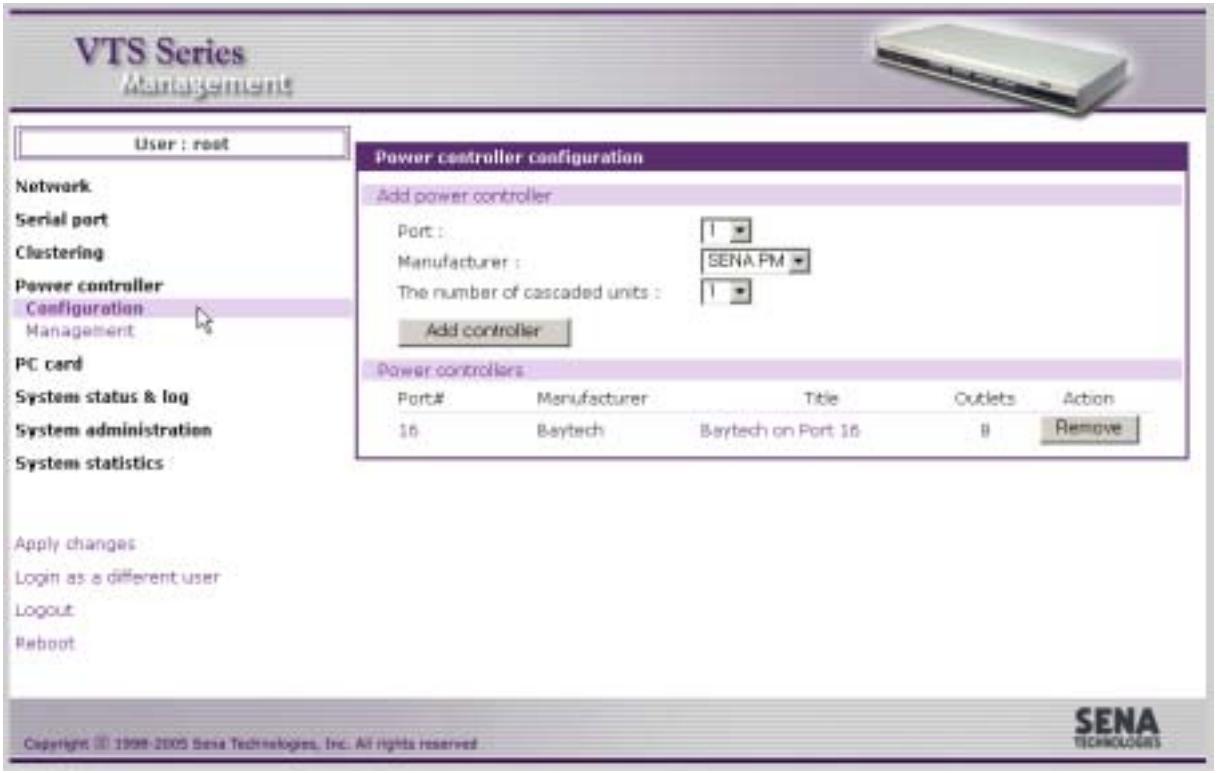


그림 6-1. 파워 컨트롤러 설정

6.2.2 파워 컨트롤러 편집 – 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 6-2 파워 컨트롤러 설정 – power controller 탭 참조) 화면이 표시됩니다.

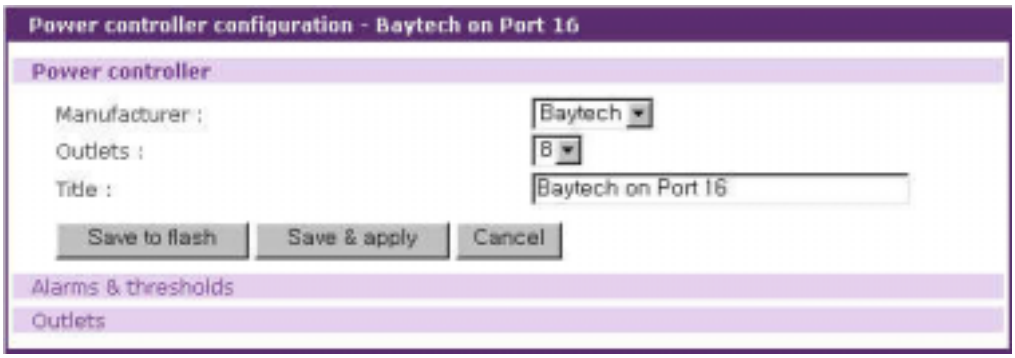


그림 6-2. 파워 컨트롤러 설정 – power controller 탭

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 편집 – Alarms & thresholds 탭

파워 컨트롤러 편집 화면(그림 6-1 파워 컨트롤로 편집 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 6-3 파워 컨트롤로 설정 – alarms & thresholds 탭 참조)이 표시됩니다. 여기서 설정하는 항목들은 파워 컨트롤러의 종류에 따라 달라질 수 있습니다.

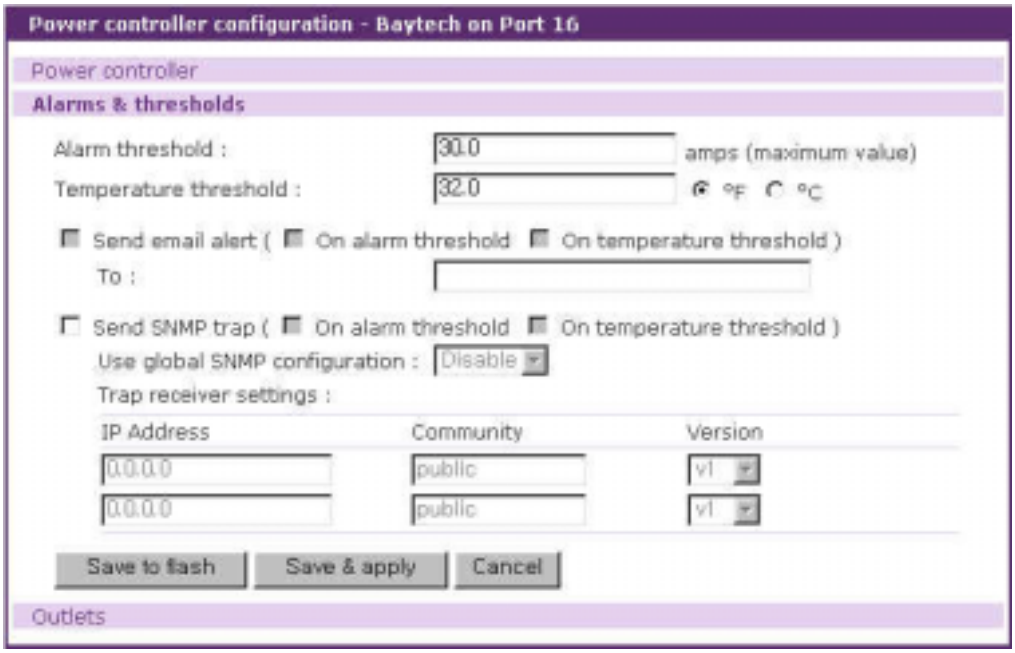


그림 6-3. 파워 컨트롤러 설정 – alarms & thresholds 탭

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 : 퍄워 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 : 퍄워 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 각각 및 **3.2 SNMP 설정** 을 참고하십시오.

6.2.4 파워 컨트롤러 편집 – Outlets 탭

파워 컨트롤러 편집 화면(그림 6-1 파워 컨트롤로 편집 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 6-4 파워 컨트롤로 설정 - outletss 탭 참조)이 표시됩니다.

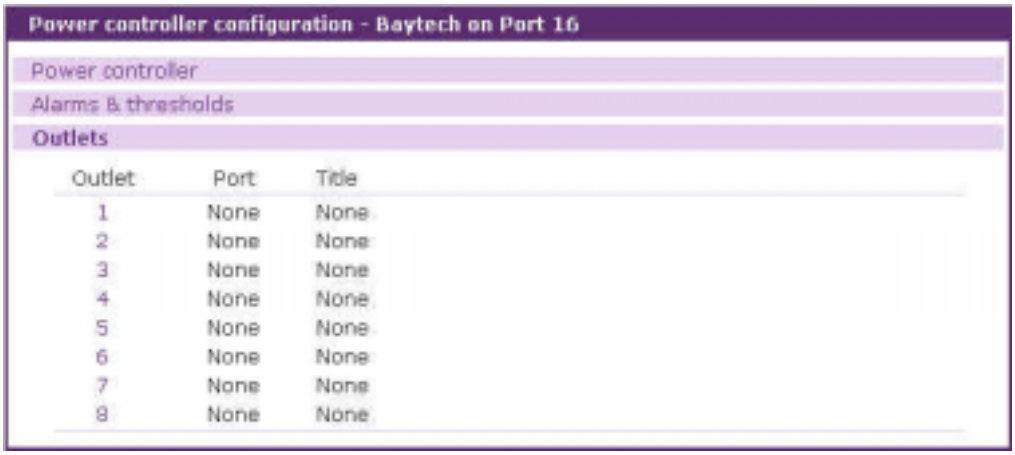


그림 6-4. 파워 컨트롤러 설정 - outlets 탭

사용자는 아웃렛 번호를 클릭하여 아웃렛 설정 부분을 펼칠 수도 있고, 펼쳐진 아웃렛의 번호를 클릭하여 아웃렛 설정 부분을 다시 접을 수도 있습니다. 그림 6-5 펼쳐진 아웃렛 설정 부분을 표시합니다.

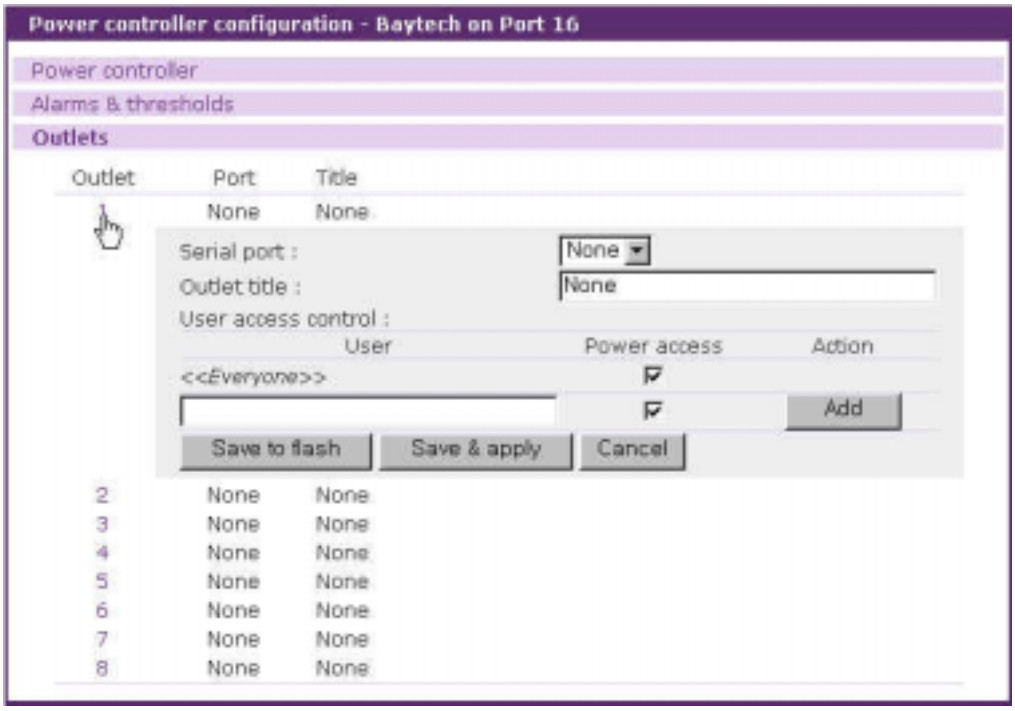


그림 6-5. 파워 컨트롤러 설정 - 아웃렛 설정

아웃렛 설정을 위한 파라미터는 다음과 같습니다:

Serial port

Outlet title

User access control

Serial port

VTS의 시리얼 포트에 연결된 장비에 전원을 제공하는 파워 컨트롤러의 아웃렛을 표시합니다. None은 이 아웃렛이 VTS 시리얼 포트에 연결된 장비가 아닌 다른 장비에 연결되었다는 것을 의미합니다. VTS의 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 6-6 파워 컨트롤러 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 6-6 파워 컨트롤러 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(refer to 6.3.4 Power controller unit management - Serial port connection)에서 전원 상태를 감시할 수 있고, 파워 컨트롤러 유닛 관리 화면(6.3.3 파워 컨트롤러 관리 – Outlets 탭 참조) 또는 시리얼 포트 연결 화면의 P 열에서 연결되는 serial port power control 화면(6.3.5 파워 컨트롤러 유닛 관리 – Serial port power control 참조)에서 파워 컨트롤러 아웃렛을 제어할 수 있습니다.

<<Everyone>> 접근권한이 체크되면, User access control 부분의 사용자 리스트에 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 6-6 파워 컨트롤러 설정 – 시리얼 포트에 연결된 아웃렛 설정 참조)

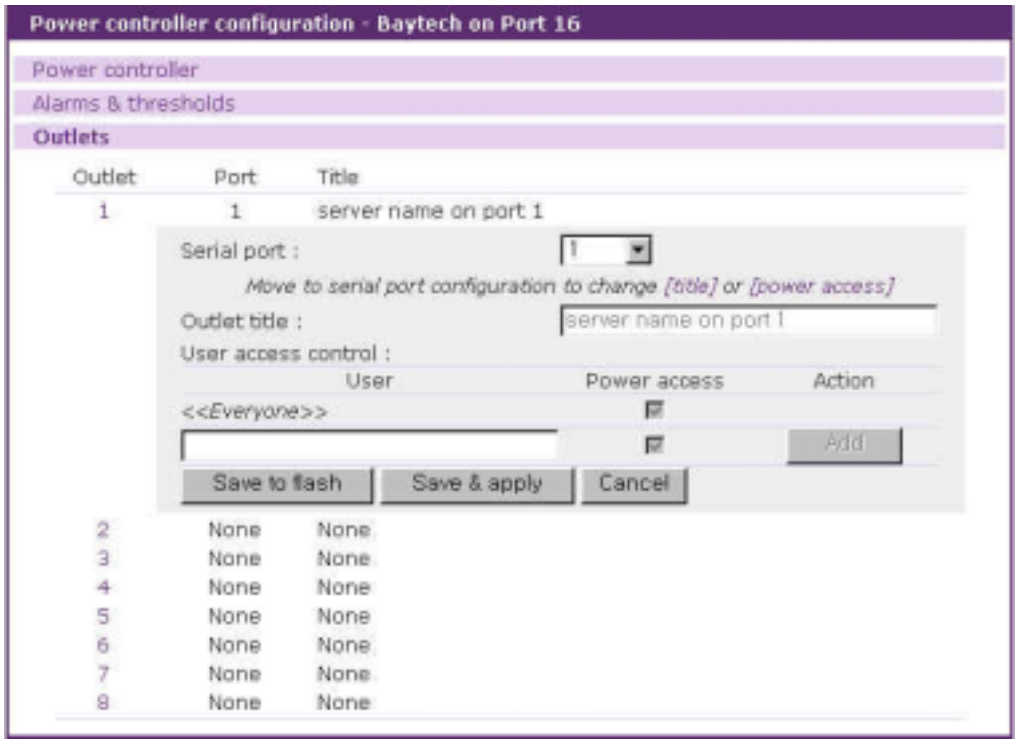


그림 6-6. 파워 컨트롤러 설정 – 시리얼 포트에 연결된 아웃렛 설정

6.2.5 시리얼 포트 설정의 power control 설정 편집

power control configuration 화면은 serial port 설정의 하나입니다. 파워 컨트롤러가 VTS에 추가되면, 각 포트의 시리얼 포트 설정에는 Power control configuration 탭이 추가됩니다. (4.3.12 Power control 설정 참조).

이 화면은 VTS의 시리얼 포트에 연결된 장비를 파워 컨트롤러의 아웃렛에 연결할 수 있도록 도와줍니다. 반면 아웃렛 설정 화면은 파워 컨트롤러 아웃렛을 장비에 연결할 수 있도록 설정합니다. (6.2.4 파워 컨트롤러 편집 - Outlets 탭 참조).

6.3 파워 컨트롤러 관리

사용자는 파워 컨트롤러와 아웃렛을 파워 컨트롤로 관리 화면, 시리얼 포트 연결 화면과 시리얼 포트 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 6-7 파워 컨트롤러 관리 – 파워 컨트롤러 리스트 참조)이 표시됩니다. VTS에 추가된 파워 컨트롤러 리스트가 표시됩니다. VTS에 연결된 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 6-7. 파워 컨트롤러 관리 – 파워 컨트롤러 리스트

6.3.2 파워 컨트롤러 유닛 관리 – Power controller 탭

파워 컨트롤러 관리 화면(그림 6-7 파워 컨트롤러 관리 – 파워 컨트롤러 리스트)의 파워 컨트롤러 리스트에서 파워 컨트롤러를 선택하여 파워 컨트롤러 관리의 파워 컨트롤러 탭화면 (그림 6-8 파워 컨트롤러 유닛 관리 – power controller 탭 참조)을 열 수 있습니다. 이 화면은 시리얼 포트 연결 화면의 M 열에 있는 아이콘을 클릭하여 접근할 수도 있습니다.
파워 컨트롤러의 정보와 상태가 표시됩니다. Clear 버튼을 클릭하여 [Max current detected]등과 같은 재설정 할 수 있습니다. 파워 컨트롤러 종류에 따라 표시되는 값이 달라질 수 있습니다.

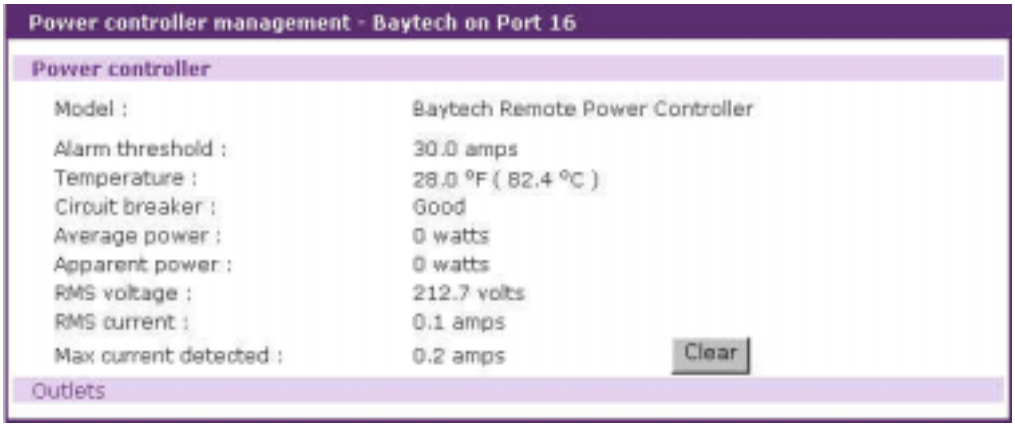


그림 6-8. 파워 컨트롤러 유닛 관리 – power controller 탭

6.3.3 파워 컨트롤러 유닛 관리 – Outlets 탭

파워 컨트롤러 관리 (그림 6-7 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 6-9 파워 컨트롤러 유닛 관리 – outlets 탭 참조)에 접근할 수 있습니다.

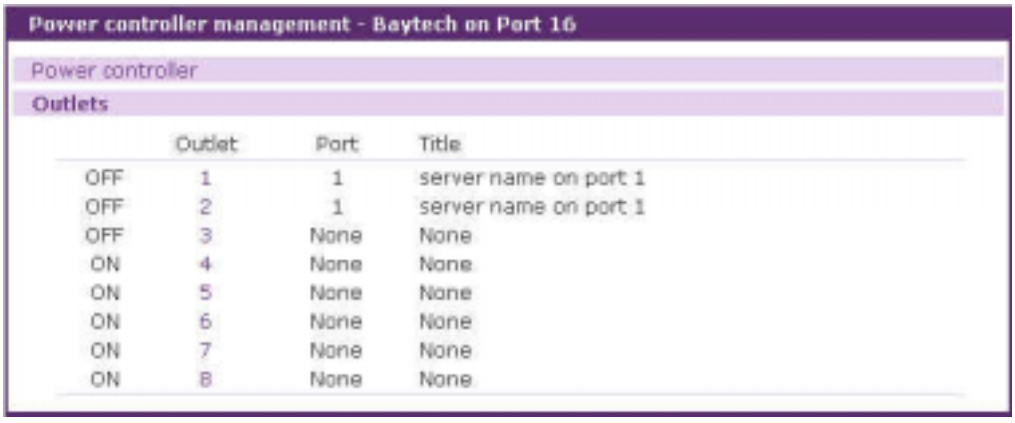


그림 6-9. 파워 컨트롤러 유닛 관리 – outlets 탭

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 6-10이 아웃렛 관리 부분이 펼쳐진 화면입니다.

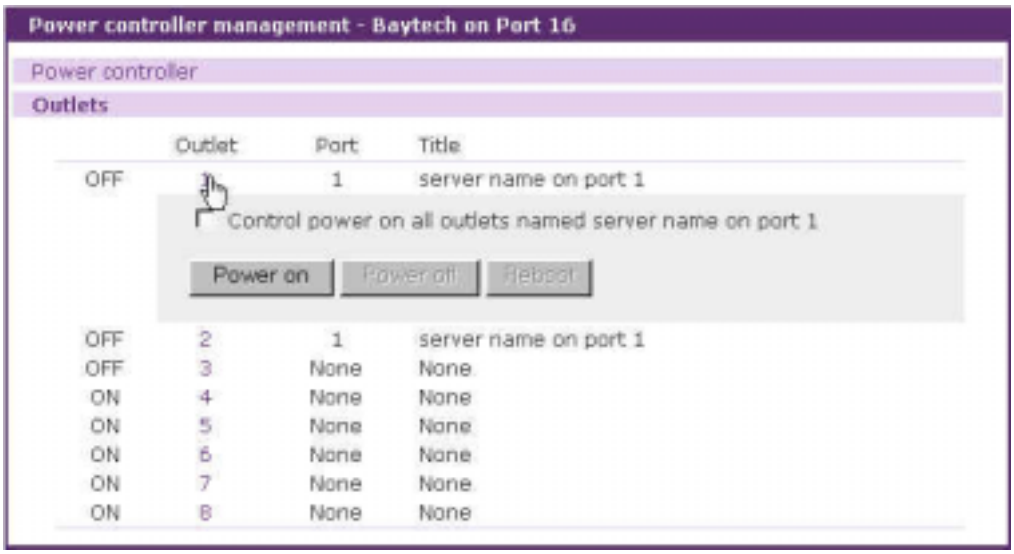


그림 6-10. 파워 컨트롤러 유닛 관리 – 아웃렛 관리

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 6-11 파워 컨트롤러 유닛 관리 – 시리얼 포트 연결 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 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. 전원이 켜짐(녹색 아이콘) 또는 꺼짐(적색아이콘) 상태일 경우에만 P 열의 상태표시 아이콘을 클릭하여 사용자는 serial port power control화면으로 이동할 수 있습니다. 전이(황색아이콘) 상태일 경우에는 연결될 수 없습니다.

파워 컨트롤러가 연결된 시리얼 포트는 M 열에 파워 컨트롤러 유닛 관리 화면으로 이동할 수 있는 아이콘이 표시됩니다. 시리얼 포트 번호와 타이틀도 그 화면으로 연결됩니다.

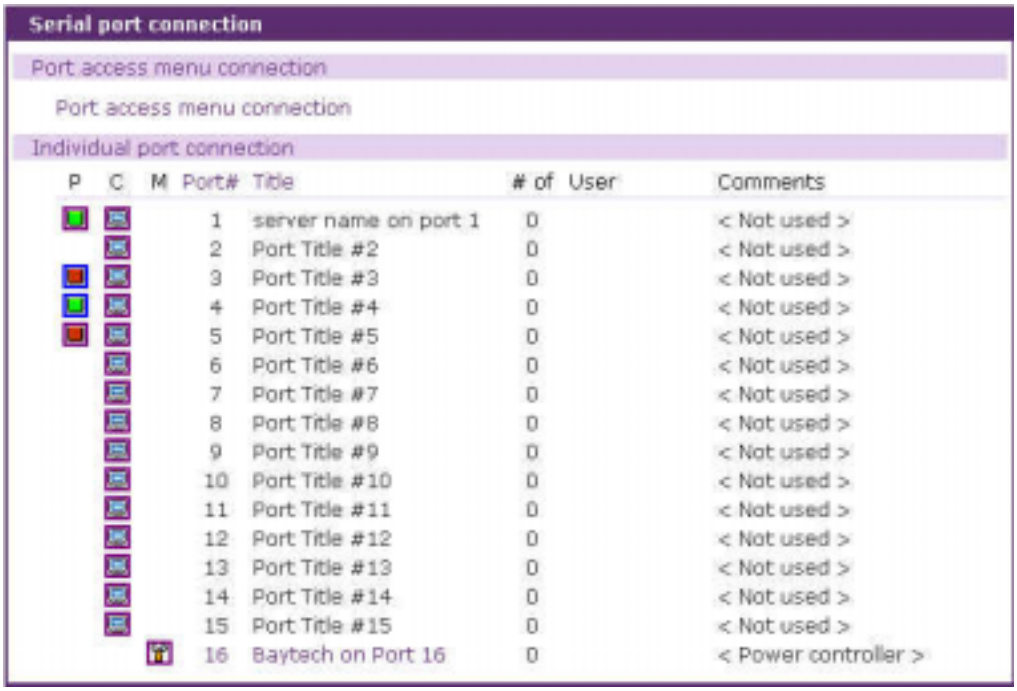


그림 6-11. 파워 컨트롤러 유닛 관리 - 시리얼 포트 연결

6.3.5 파원 컨트롤러 유닛 관리 – Serial port power control

시리얼 포트 연결 화면의 P 열에 있는 켜짐 / 꺼짐 상태 표시 아이콘을 클릭하면 serial port power control 화면(그림 6-12 파워 컨트롤러 유닛 관리 – serial port power control 참조). 파워 컨트롤러 아웃렛 관리 화면이 파워 컨트롤러의 아웃렛을 제어하는 반면, 이 화면은 시리얼 포트에 연결된 장비의 전원을 제어하는데 사용됩니다.

그림 6-12. 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: PC 카드 설정

VTS는 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 VTS에 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 VTS에 망외(out-of-band) 접속을 할 수도 있습니다.

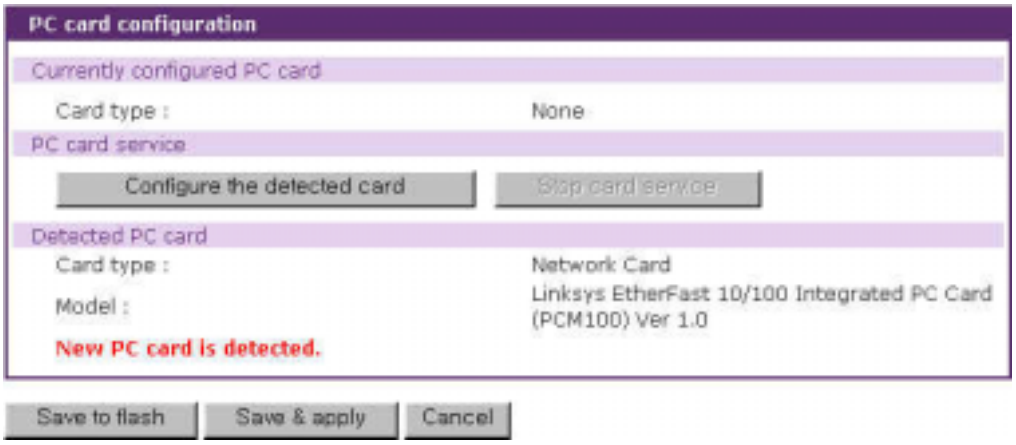


그림 7-1. 초기 PC 카드 설정 메뉴 화면

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. VTS는 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.

VTS가 PC 카드를 발견하는데 실패하면, 다음 오류 메시지가 나타납니다.

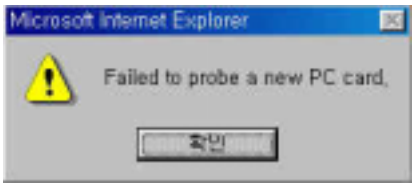


그림 7-2. 발견 실패 오류 메시지

VTS가 지원하는 PC 카드 목록을 보려면 ***부록 B. VTS가 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 LAN 카드 설정

LAN 카드를 PC 카드 슬롯에 설치하면 VTS는 2개의 IP 주소를 보유하게 됩니다. 이때, IP 주소는 반드시 유효한 것을 지정해야 합니다.

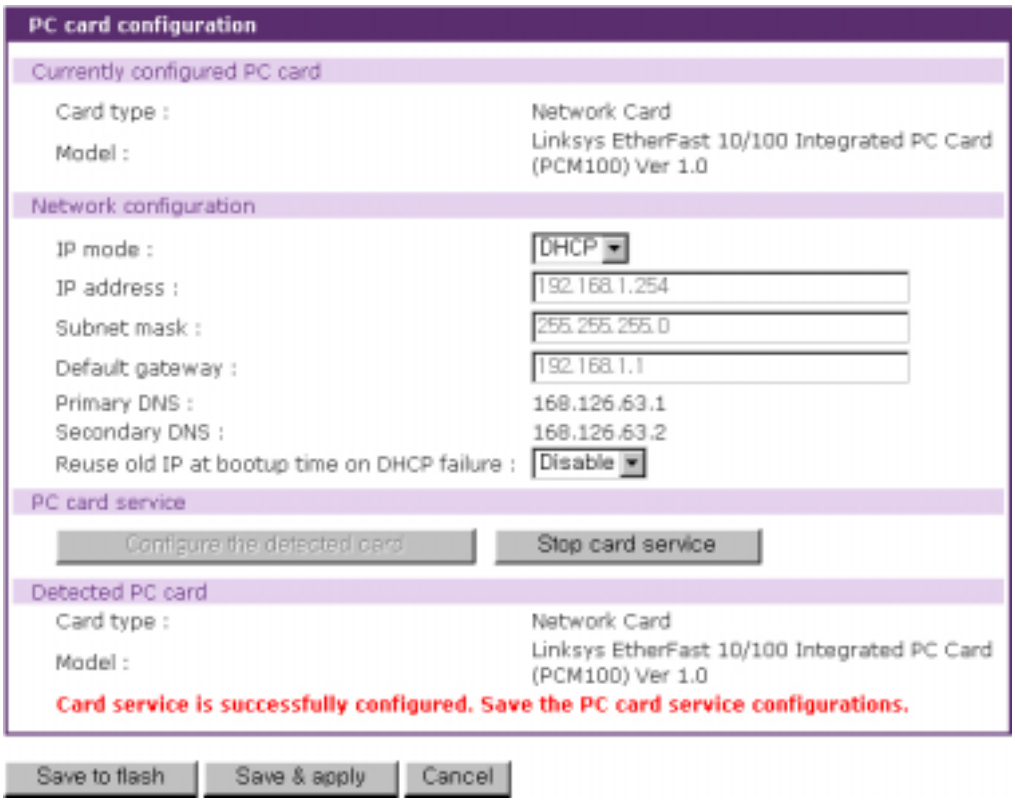


그림 7-3. PC LAN 카드 설정

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. VTS가 지원하는 PC 카드 목록을 보려면 ***부록 B. VTS가 지원하는 PC 카드*** 를 참조하십시오.

7.2 무선 LAN 카드 설정

무선 LAN 카드를 PC 카드 슬롯에 설치하면 VTS는 2개의 IP 주소를 보유하게 됩니다. 이때, IP 주소는 반드시 유효한 것을 지정해야 합니다.

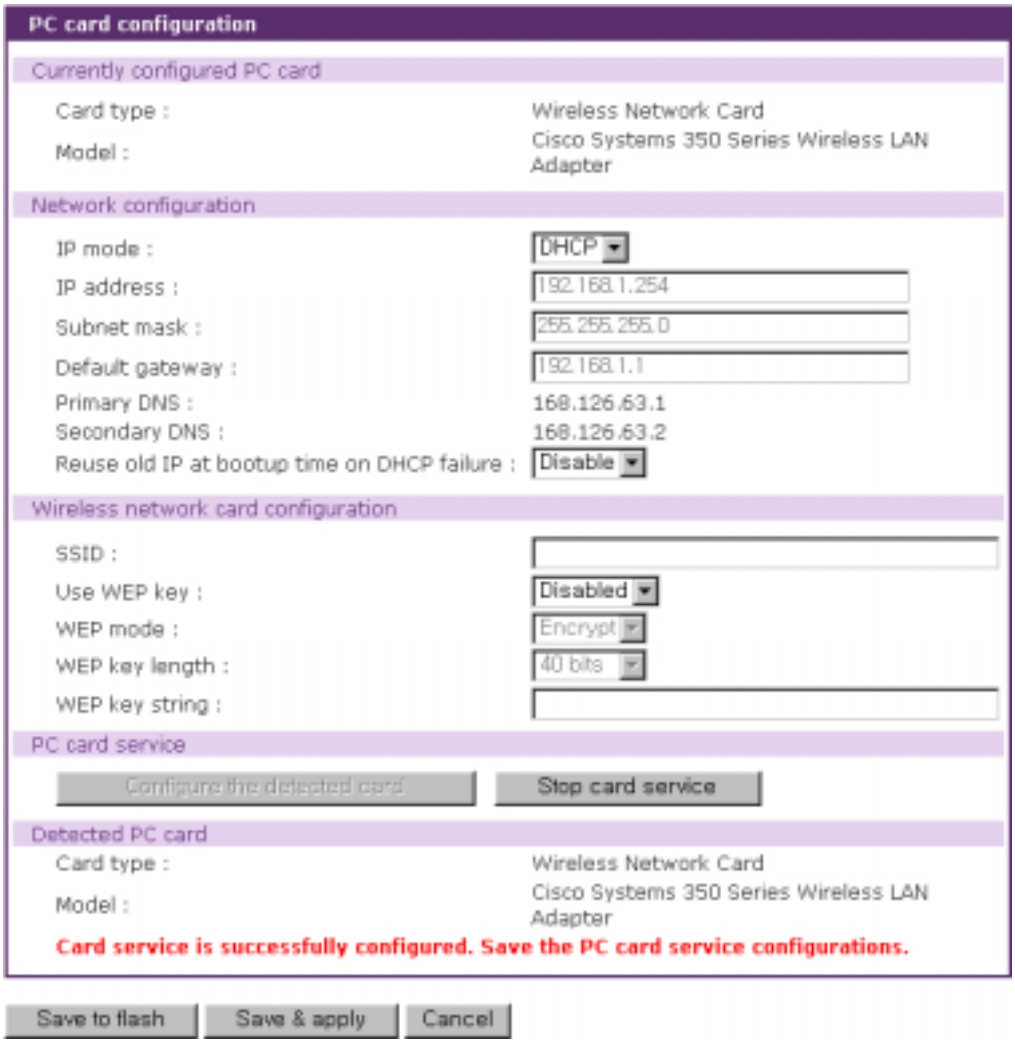


그림 7-4. PC 무선 LAN 카드 설정

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.

VTS는 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

VTS가 지원하는 PC 카드 목록을 보려면 ***부록 B. VTS가 지원하는 PC 카드*** 를 참조하십시오.

7.3 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. VTS가 지원하는 PC 카드 목록을 보려면 ***부록 B. VTS가 지원하는 PC 카드*** 를 참조하십시오.
기본 모뎀 초기화 스트링 값은 “q1e0s0=2”입니다. 이는 모뎀이 무음 모드(quiet mode)(‘q1’), 에코 오프 모드(echo off mode)(‘e0’) 그리고 자동 응답 모드 방식 2(Auto Answer mode equaling two)(“s0=2”)의 설정을 의미합니다. 해당 명령 세트에 대한 자세한 정보는 모뎀 매뉴얼을 참조하십시오.

Callback 항목, Modem test 항목과 Alert 설정은 **4.3.4 Host mode 설정**과 **4.3.11 Alert 설정**의 Dial-in modem mode 부분을 참조하십시오.

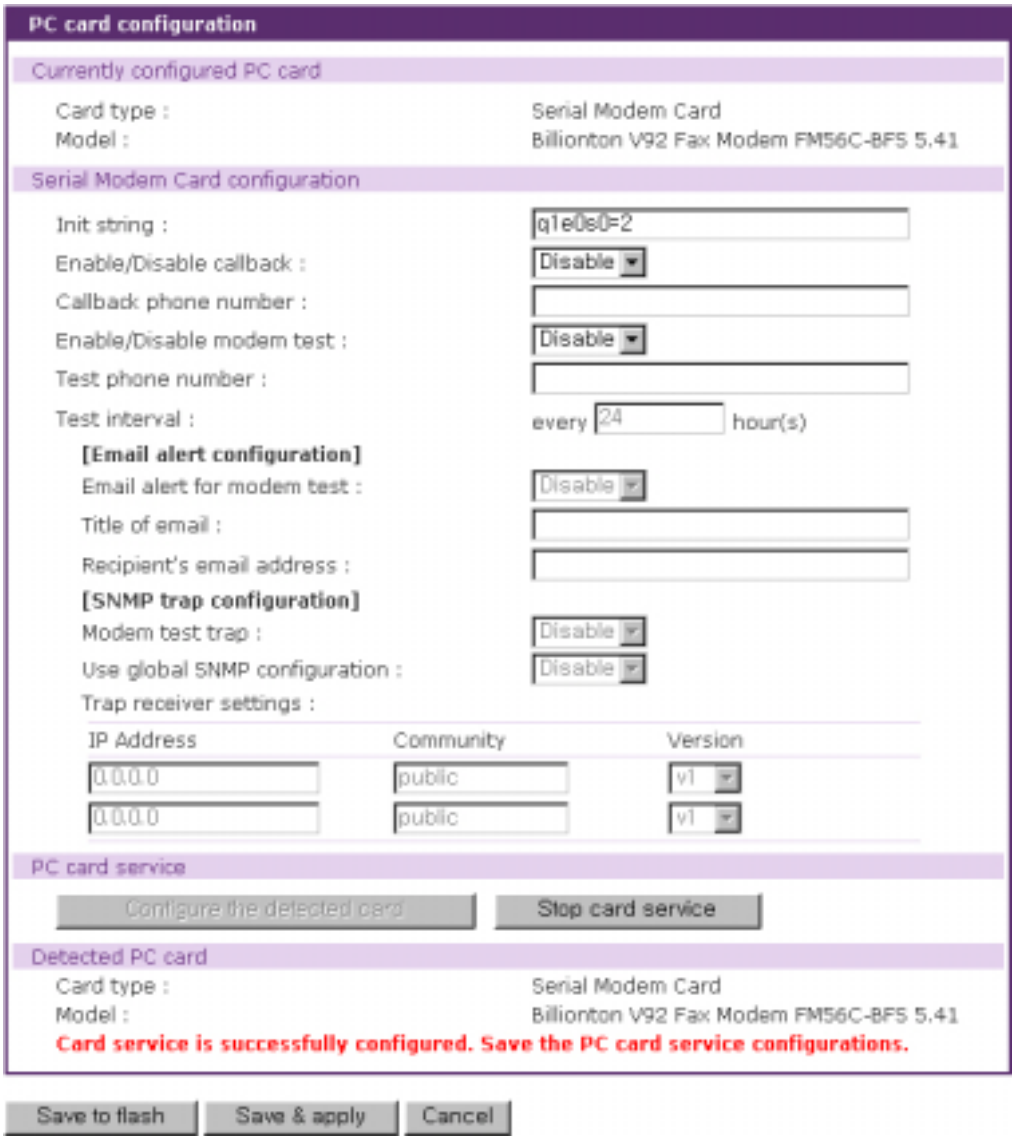


그림 7-5. PC 시리얼 모뎀 카드 설정

7.4 ATA/IDE fixed disk card 설정

사용자는 시스템 및 시리얼 포트 로그를 저장하기 위해 PC ATA/IDE fixed disk card를 사용하는데 필요한 전체 데이터 크기를 반드시 설정해야 합니다. VTS는 전체 저장 크기 및 디스크에서 사용 가능한 디스크 공간을 자동으로 설정합니다.

사용자는 Delete 를 선택하여 카드의 모든 파일을 삭제할 수 있습니다.

사용자는 Format 을 선택하여 카드를 포맷할 수 있습니다. VTS는 디스크 카드의 **EXT2** 및 **VFAT** 파일 시스템을 지원합니다.

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

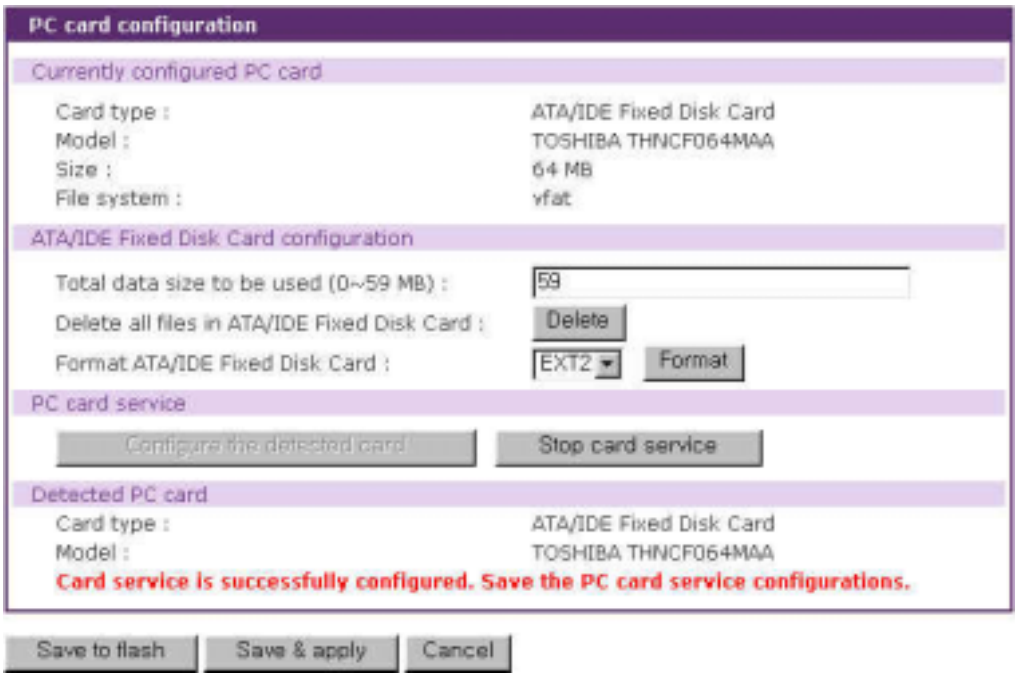


그림 7-6. PC ATA/IDE fixed disk card 설정

8: 시스템 상태 및 로그

VTS는 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, 부트로더 버전 및 VTS의 네트워크 설정 등이 있습니다. 또한 VTS는 system logging 기능을 통해 지정된 수취인에게 email로 로그 데이터를 자동으로 전달하게 설정될 수 있습니다.

8.1 시스템 상태

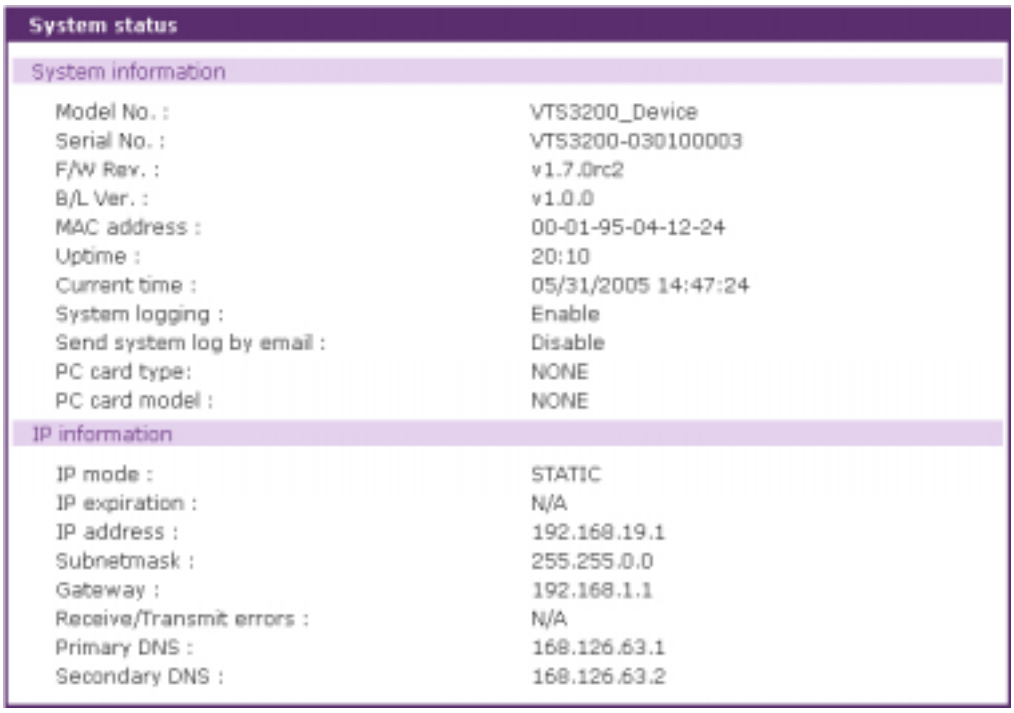


그림 8-1. 시스템 상태 디스플레이

8.2 시스템 로그 설정

VTS는 system logging 기능과 시스템 로그 상태 표시 기능을 제공합니다. 사용자는 system logging 프로세스를 enable 또는 disable 상태가 되도록 할 수 있을 뿐만 아니라, 시스템 로그를 저장하는 위치 및 시스템 로그 버퍼 크기를 선택할 수 있습니다.

Enable/disable system logging
System logging 기능을 사용할 것인지를 설정합니다.

System log storage location

시스템 로그는 **VTS 내부 메모리**, PC 카드 슬롯에 삽입된 **ATA/IDE fixed disk card** 또는 **NFS 서버의 설치 지점**에 저장될 수 있습니다. 시스템 로그 데이터를 저장하는데 내부 메모리를 사용하는 경우, 로그 데이터는 VTS가 꺼질 때 삭제됩니다. 시스템 로그 데이터를 보존하려면, 저장 위치를 ATA/IDE fixed disk card 또는 NFS 서버로 설정하거나 SYSLOG server로 저장을 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 card를 사용하는 경우, 최대 버퍼 크기는 카드 용량에 따라 달라집니다.

로그 데이터를 저장하기 위해 NFS 서버를 사용하는 경우, 최대 버퍼 크기는 무한대입니다. 사용자는 NFS 서버를 설정하여 시스템 로그 기능이 적절히 작동할 수 있도록 해야 합니다.

Automatic backup on mounting

System log storage location이 CF card 또는 NFS 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

VTS는 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.

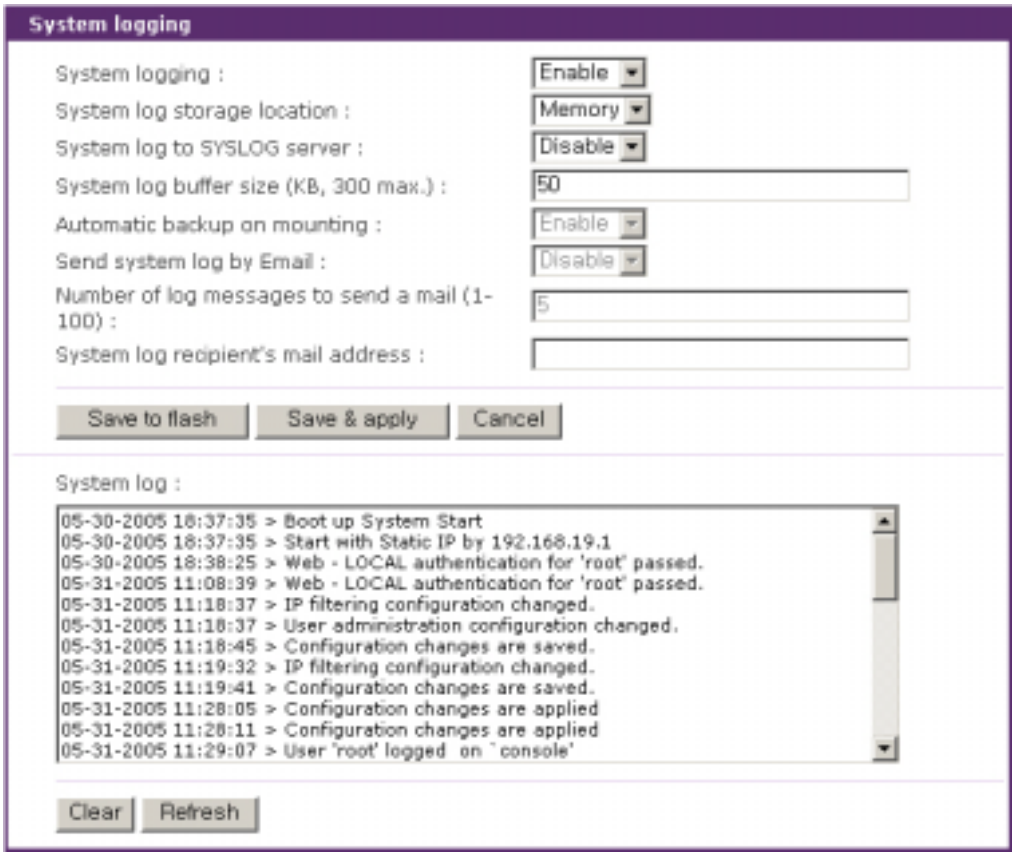


그림 8-2. 시스템 로그 설정 및 보기

8.3 Users logged on list

사용자는 시스템의 현재 및 과거의 사용자 활동을 관찰할 수 있습니다.

그림 8-3. 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 통해 항상 연결되는 것은 아니다.

9: 시스템 관리

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

VTS는 사용자 인증 방법으로 Local 인증 방법 외에 인증 서버를 이용한 방법을 지원합니다. RADIUS, TACAS+, LDAP등과 같은 원격 인증 방법을 설정하면, VTS는 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 VTS의 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 펌웨어를 업그레이드할 수도 있습니다.

9.1 사용자 관리

VTS는 4개의 사용자 그룹으로 사용자들을 관리합니다. VTS 설정 및 시리얼 포트를 접속하기 위한 권한은 사용자 그룹에 따라 다릅니다.

- **User: 일반 포트 사용자 그룹**
  - 시리얼 포트가 시니프 기능이 설정되어 있지 않다면, 이 그룹에 포함되는 Port 접근권한을 가진 모든 사용자는 시리얼 포트에 접속할 수 있습니다.
  - 시리얼 포트가 시니프 기능이 설정되어 있다면, 이 그룹에 속한 Port 또는 Monitor 접근권한을 가진 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.

참고:

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

- *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 설정 메뉴 또는 CLI 에 접속할 수 없습니다.*

- **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 설정 메뉴에 접속할 수 있습니다. 그러나, 이 그룹은 Serial Port, Clustering 및 파워 컨트롤러 아웃렛과 관련된 설정 파라미터만을 변경할 수 있습니다. 그 외의 VTS 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 program 들을 수행할 수 있습니다. 이 그룹은 CLI 를 통해 VTS 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 VTS에서 관리되는 사용자 그룹 및 해당되는 사용자 그룹의 권한을 요약해 놓았습니다.

표 9-1. 사용자 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 **설정** **텍스트 메뉴 접속**	O	O	Δ **	X
port access menu **접속**	O	O	O	O
웹 GUI **접속**	O	O	Δ **	Δ ***
시스템 파라미터 변경	O	O	Δ **	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.

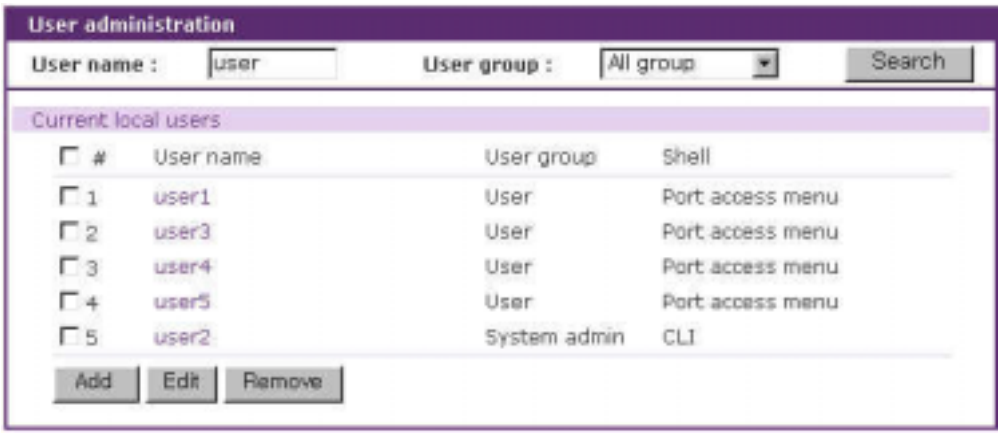


그림 9-1. 사용자 관리

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.

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

참고:

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

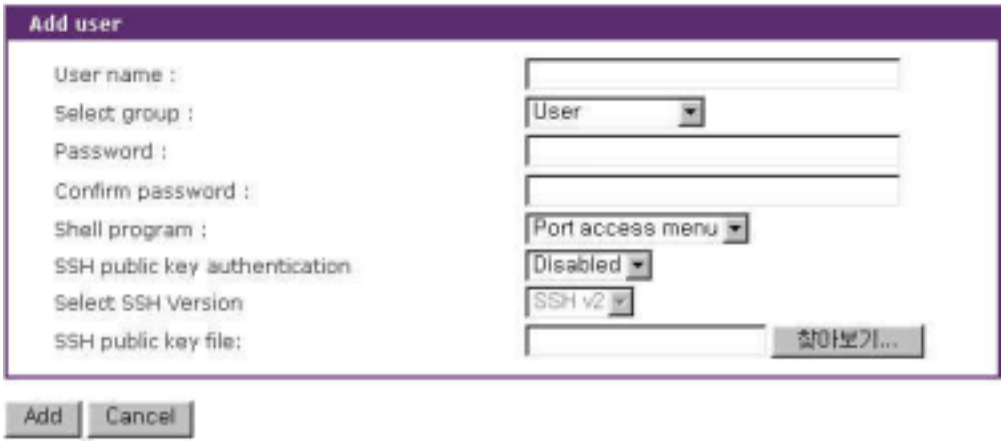


그림 9-2. 사용자 추가하기

사용자를 제거하려면 다음을 수행하십시오.

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

사용자 계정의 파라미터를 변경하려면, 사용자 관리화면에서 사용자 이름을 선택하여 사용자 편집화면을 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.

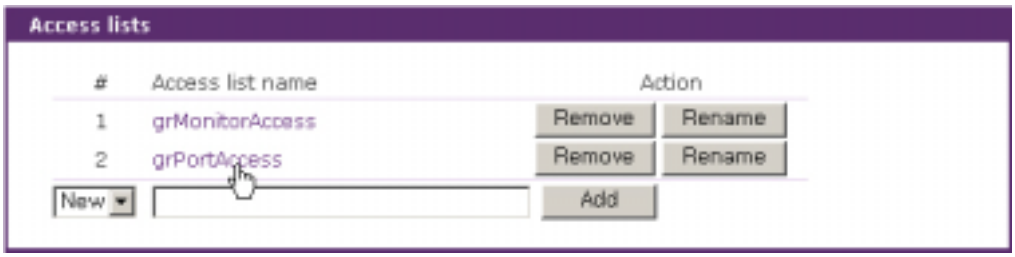


그림 9-3. 액세스 리스트 - 액세스 리스트 관리

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, [Rename] 버튼을 클릭하여 액세스 리스트의 이름을 변경할 수도 있습니다. 액세스 리스트를 제거하거나 이름을 바꾸어도 개별 포트의 User access control에서 사용된 액세스 리스트를 자동으로 제거하거나 이름을 바꾸지 않아 개별포트가 존재하지 않는 액세스 리스트를 참조할 수 있으므로 주의하시기 바랍니다.

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

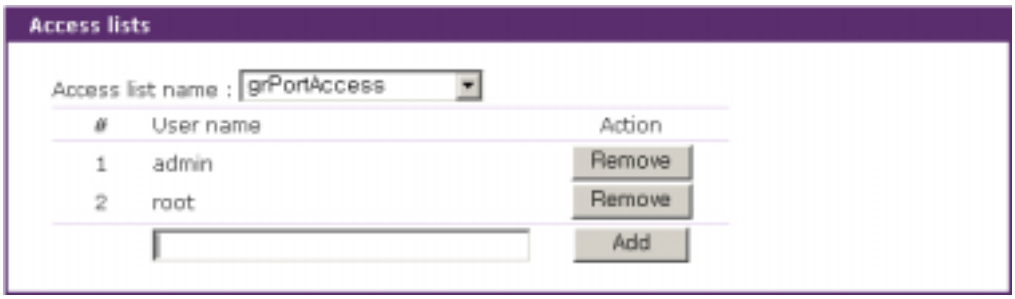


그림 9-4. 액세스 리스트 - 사용자 관리

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.

9.3 패스워드 변경

그림 9-5은 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.

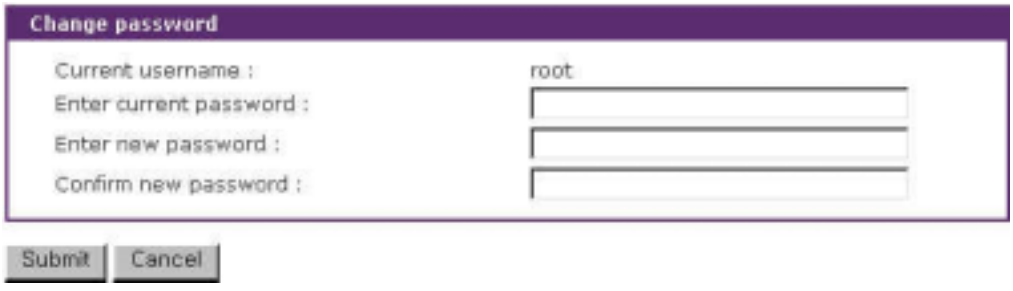


그림 9-5. 패스워드 변경

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.

```
[VTS3200_Device]
================================================================================
 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  ( 1-32 serial port, P passwd, S slave unit
                   R remote port, Q exit )
  ------> P
  Enter new password : *****
  Retype new password : *****
  Password was changed.
```

9.4 장치 이름(Device name) 설정

VTS의 관리를 위해 자체적으로 장비 이름을 설정할 수 있습니다. 그림 9-6는 장치 이름 설정 화면입니다. 사용자가 Device name을 변경하게 되면 VTS의 hostname 이 변경되게 되며 CLI 상의 프롬프트 또한 아래와 같이 해당되는 hostname 으로 변경이 됩니다.

```
root@VTS3200_Device:~#
```

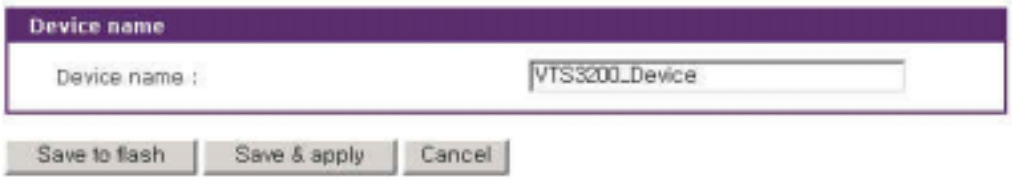


그림 9-6. 장치 이름 설정

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

9.5 날짜 및 시간 설정

VTS는 현재의 날짜 및 시간 정보를 가지고 있습니다. VTS의 시계 및 달력 설정은 내부 배터리 전원에 의해 백업됩니다. 사용자는 그림 9-7에 나타난 바와 같이 현재 날짜 및 시간을 변경할 수 있습니다.

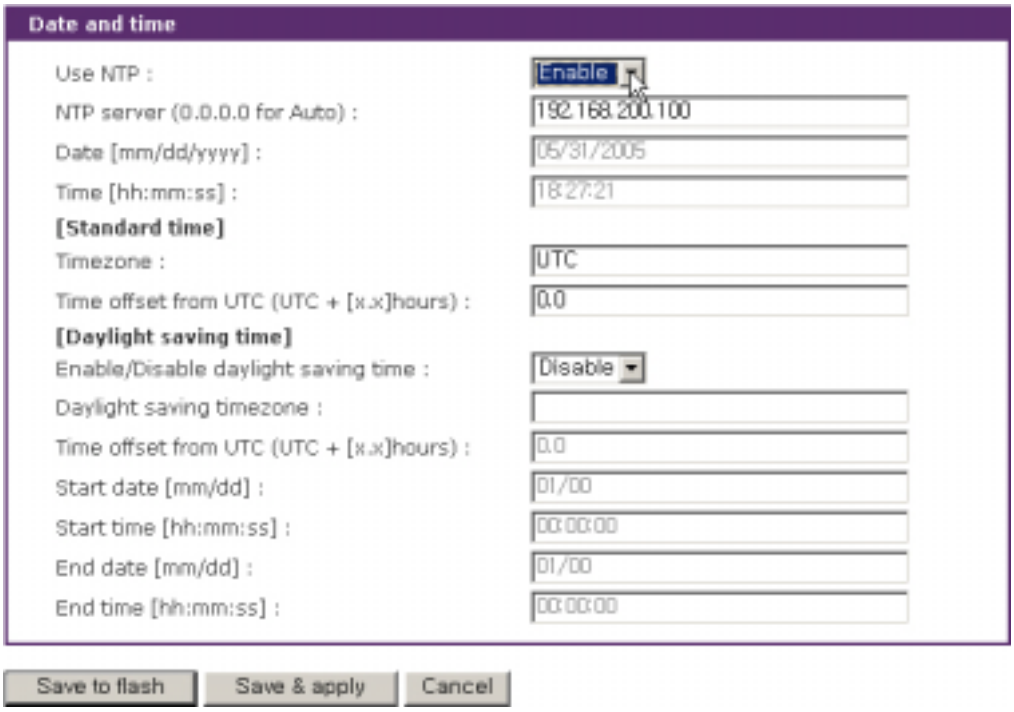


그림 9-7. 날짜 및 시간 설정

날짜 및 시간 설정을 설정하기 위한 방법은 2가지가 있습니다. 첫번째 방법은, NTP 서버를 사용하는 것입니다. NTP 기능이 활성 상태가 되면, VTS가 재부팅될 때마다 NTP 서버로부터 날짜 및 시간 정보를 얻을 수 있습니다. NTP 서버가 0.0.0.0 으로 설정되면, VTS는 기본 NTP 서버를 사용합니다. 이런 경우에, VTS는 인터넷과 연결되어 있어야 합니다. 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. VTS는 이런 파라미터를 이용하여 정확한 시스템 날짜와 시간을 계산합니다.

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. VTS를 공장 출하 상태의 설정 상태로 되돌리기 위해서는 설정 불러오기(Configuration import) 부분의 위치(Location) 파라미터를 [Factory default]로 선택하여 설정을 불러오거나, VTS의 후면 패널의 reset button 을 누르면 됩니다.

VTS가 자동으로 설정을 저장하는 기능을 지원합니다. Automatic backup configuration을 설정하고 적용하면 VTS는 지정된 시간에 지정된 방법으로 설정을 자동으로 저장합니다.

그림 9-8은 설정 관리 화면을 보여줍니다.

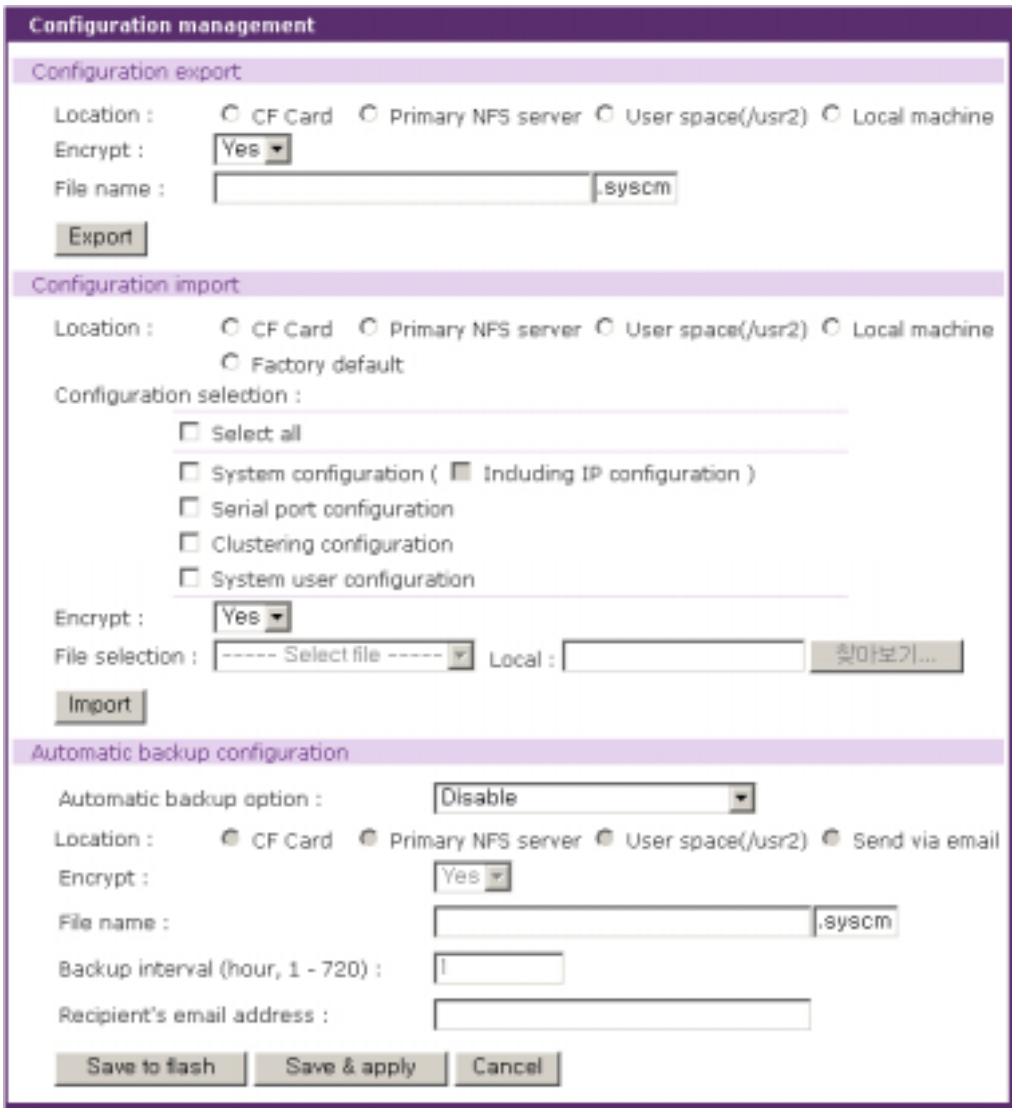


그림 9-8. 설정 관리

설정 저장하기, 설정 불러오기 및 자동 설정 저장을 정상적으로 수행하기 위해서는 다음 파라미터들을 적절히 설정하여야 합니다.

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

VTS를 운영하는 보안 정책을 설정합니다. VTS 서비스에 관련된 보안, 네트워크 보안, 개별 포트의 연결에 대한 보안 및 패스워드 관리를 통한 보안등에 관한 정책을 결정합니다. 시큐리티 프로파일은 다음과 같이 4개 그룹으로 분류됩니다.

1. Services
2. Network security
3. Per port security
4. Password security

9.7.1 Services

VTS에서 지원하는 서비스를 제공할 지 여부를 결정합니다. 그림 9-9는 서비스 시큐리티 프로파일 설정 화면입니다.

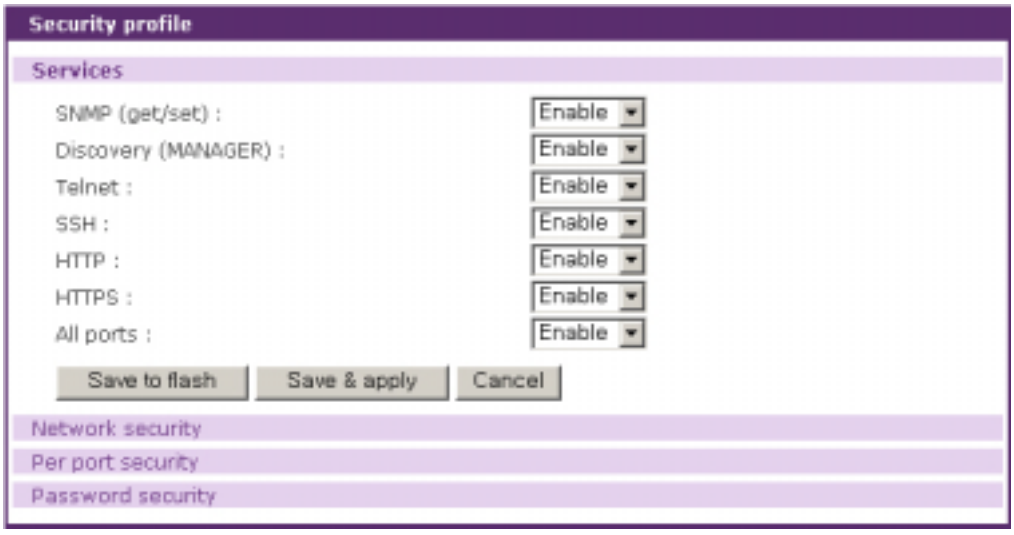


그림 9-9. Security profile - Services

설정 가능한 파라미터는 다음과 같습니다.

SNMP (get/set)

Discovery(MANAGER)

Telnet

SSH

HTTP

HTTPS

All ports

SNMP (get/set)

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

Discovery(MANAGER)

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

Telnet

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

상태	Interface	Option	IP address/Mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	23	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	23	ACCEPT

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

SSH

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

상태	Interface	Option	IP address/Mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	22	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	22	ACCEPT

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

HTTP

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

상태	Interface	Option	IP address/Mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	80	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	80	ACCEPT

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

HTTPS

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

상태	Interface	Option	IP address/Mask	Port	Chain rule
Disable	all	Normal	0.0.0.0/0.0.0.0	443	DROP
Enable	all	Normal	0.0.0.0/0.0.0.0	443	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. 모든 개별 포트의 Port IP Filtering 설정을 다음과 같이 변경하여 지원합니다.

상태	Allowed base host IP	Subnet mask to be applied
Disable	255.255.255.255	255.255.255.255
Enable	0.0.0.0	0.0.0.0

Port IP filtering 설정에 대한 자세한 내용은 ***4.3.8 Port IP Filtering 설정***을 참조하시기 바랍니다.

9.7.2 Network Security

네트워크 보안과 관련된 정책을 설정합니다. 그림 9-10은 네트워크 시큐리티 설정 화면입니다.

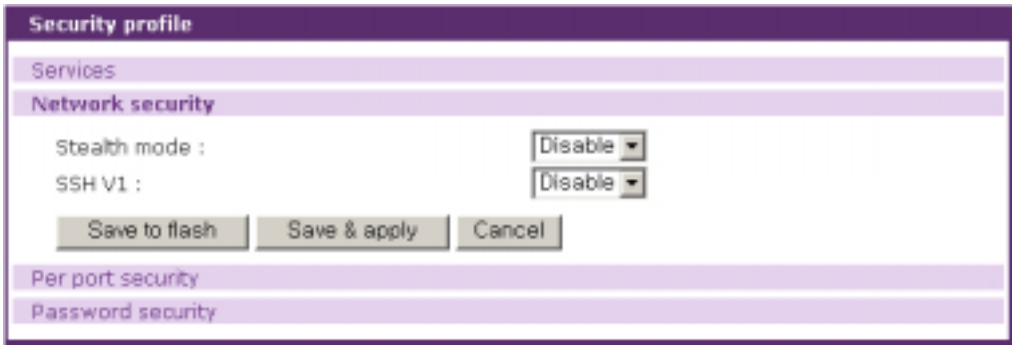


그림 9-10. Security profile – Network security

설정 가능한 파라미터는 다음과 같습니다.

Stealth mode

SSH V1

Stealth mode

Stealth mode가 Enable로 설정되면, 클라이언트가 지원하지 않는 포트로 연결을 시도할 경우 VTS

가 연결 거부하지 않고 응답을 하지 않습니다.

SSH V1
SSH 버전1 프로토콜을 지원할 지 여부를 설정합니다. Disable로 설정할 경우 SSH 버전2만 지원됩니다.

9.7.3 Per Port Security

port access menu, 시리얼 포트 및 원격 포트의 연결할 수 있는 프로토콜을 SSH로 제한할 수 있습니다. 그림 9-11은 개별 포트 시큐리티 설정 화면입니다.

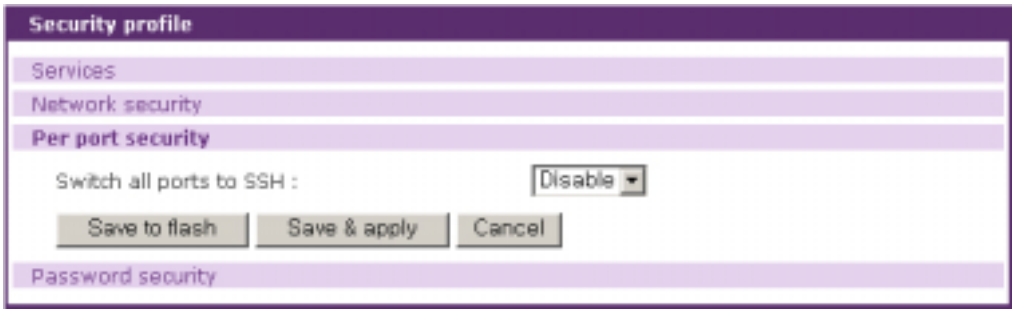


그림 9-11. Security profile – Per port security

설정 가능한 파라미터는 다음과 같습니다.
Swtich all ports to SSH

Switch all ports to SSH
port access menu, 시리얼 포트 및 원격 포트의 연결할 수 있는 프로토콜을 SSH로 제한할 지 여부를 설정합니다. Enable로 설정되면 포트 액세스 메뉴 설정의 **Port access menu protocol** 파마미터와 시리얼 포트 및 원격 포트의 Host mode 설정 중 **Protocol** 파라미터를 SSH를 변경합니다. 자세한 내용은 ***4.2 Port access menu 설정***와 ***4.3.4 Host mode 설정***을 참조하시기 바랍니다.

9.7.4 Password Security

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

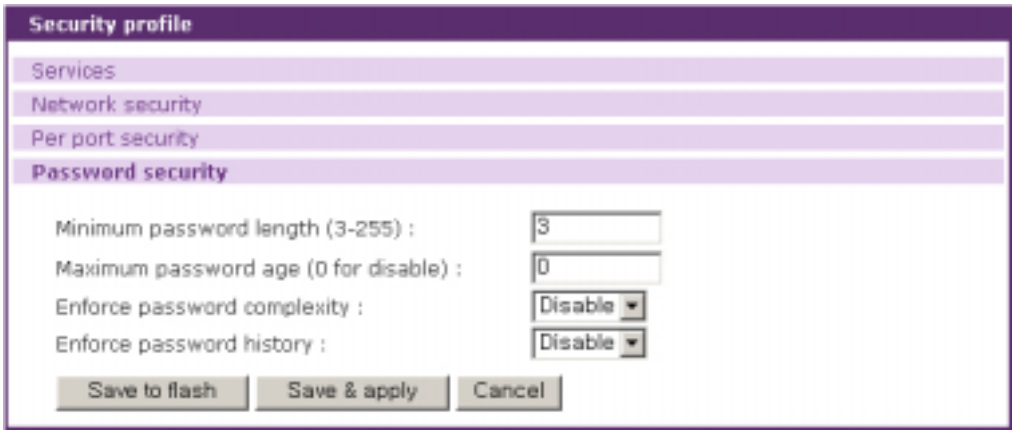


그림 9-12. Security profile – Password security

설정 가능한 파라미터는 다음과 같습니다.

Minimum password length

Maximum password age

Enforce password complexity

Enforce password history

Minimum password length

패스워드 변경시 패스워드 길이의 최소값을 설정합니다.

Maximum password age

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

주의 : *설정에 관계없이 3회 연속해서 로그인 실패하면 관리자가 사용자 계정을 유효하게 조치하기 전까지 사용할 수 없게 됩니다.*

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 패스워드와 같은 패스워드 사용을 제한합니다.

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. VTS는 부팅시 자동으로 Firmware 및 설정을 자동으로 업그레이드하는 기능을 제공합니다. automatic firmware and configuration 부분을 설정하면 VTS는 부팅할 때 Firmware와 설정이 새로운 버전인지 확인한 후 필요하면 새로운 버전으로 업그레이드 합니다. 그림 9-13에 firmware upgrade 웹 인터페이스 화면을 나타내었습니다.

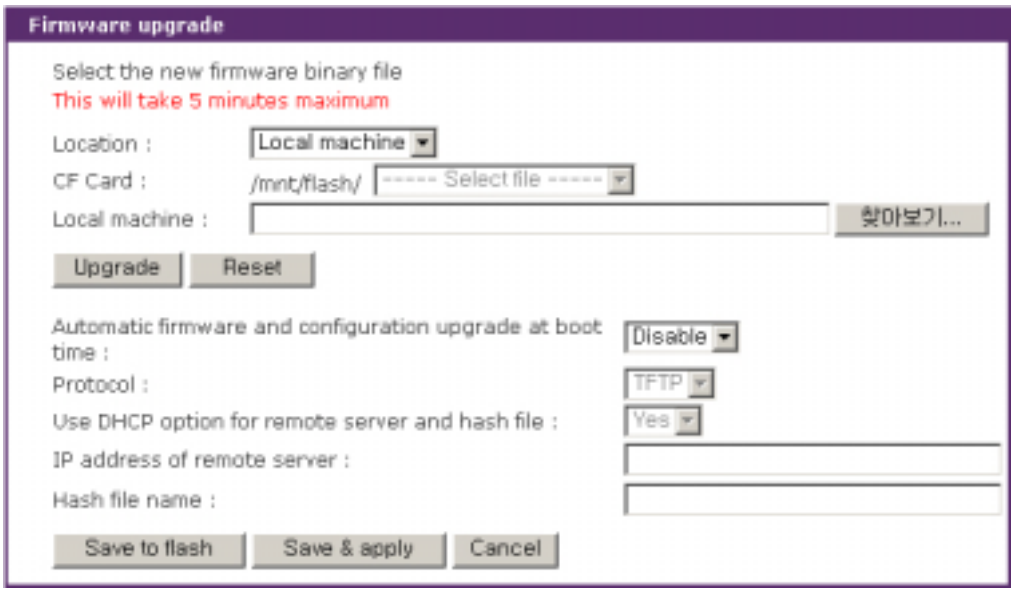


그림 9-13. Firmware upgrade

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.

VTS의 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.

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 card를 통해 업그레이드 하려면 “Location”을 “CF Card”로 선택하고 파일명을 입력하면 됩니다.
5. 업그레이드가 완료되면, 시스템을 재부팅하여 변경 사항을 적용합니다.
6. Firmware upgrade가 실패한 경우, 그림 9-16과 같이 VTS가 오류 메시지를 나타냅니다. 이때는, 업그레이드 전의 Firmware 버전이 유지됩니다.

```
Login : admin
Password : *****

------------------------------------------------------------------------------
Welcome to VTS-3200 configuration page
Current time : 0000/00/00 00:00:00     F/W REV.     :
Serial No.   :                      MAC Address  : 00-01-95-04-1b-2e
IP mode      : DHCP                  IP Address   : 192.168.0.129
------------------------------------------------------------------------------
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 7
------------------------------------------------------------------------------
System Administration
------------------------------------------------------------------------------
Select menu
1. User Administration
2. Access Lists
3. Device name : VTS3200 Device
4. Date and time
5. Configuration management
6. Security Profile
7. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
-----> 7
```

```
--------------------------------------------------------------------------------
 System Administration --> Firmware Upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Firmware Upgrade
 2. Automatic firmware and configuration upgrade at boot time : Disable
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select the location of the firmware
 ( 1 = Local Machine, 2 = CF Card )
 -----> 1

-----------------------------------
 Location : Local Machine
-----------------------------------

 *** Firmware upgrade will RESTART your device. ***
 Do you want to start firmware upgrade ? (y/n) : y
 Preparing for firmware upgrade. Wait a moment...
 Transfer firmware by zmodem using your terminal application.
** B0ff000005b157
```

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

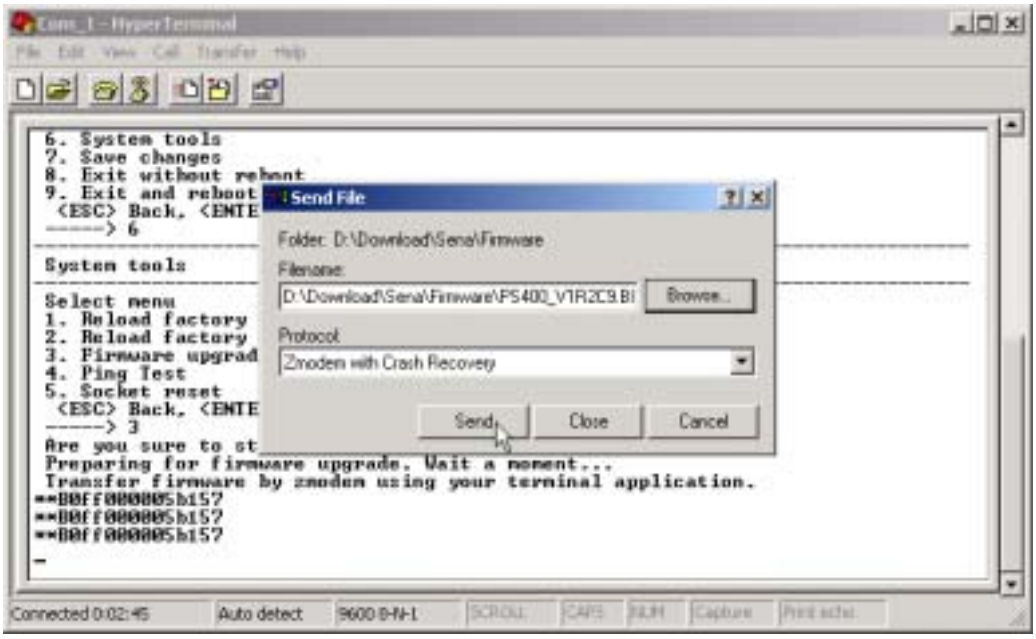


그림 9-15. Zmodem을 이용한 firmware 파일 전송 (Hyper Terminal)

```
-----> 5

 *** Firmware upgrade will RESTART your device. ***
 Do you want to start firmware upgrade ? (y/n) : y
 Preparing for firmware upgrade. Wait a moment...
 Transfer firmware by zmodem using your terminal application.
** B0ff000005b157
** B0ff000005b157
** B0ff000005b157
** B0ff000005b157
Firmware upgrade failed !
 Now reboot ...
```

그림 9-16. firmware upgrade 실패 메시지

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 VTS가 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 VTS의 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
VTS가 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. VTS는 해쉬 파일에 기록된 모델이름, 버전을 대상 VTS의 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> - VTS800, VTS1600, VTS3200등의 VTS의 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.

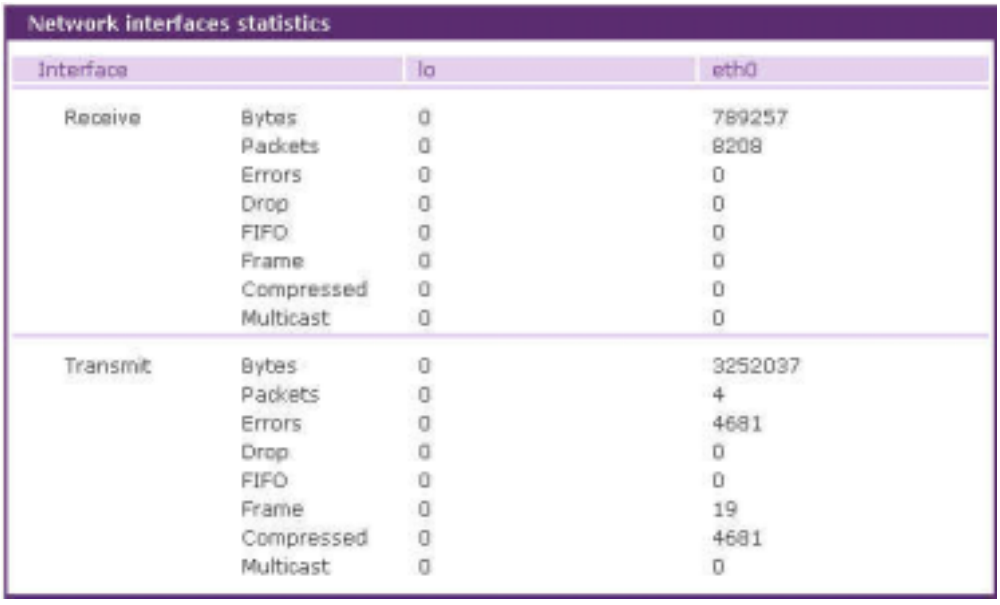
```
1,vts48.img,VTS3200,v1.5.0
2,vts48.syscm,VTS3200,v1.0.0
3,test_hash.tar,FXU,/mnt/flash
3,active_detect.tar.gz,FXZU,/mnt/flash
4,mkdir /tmp/test
```

10: 시스템 통계

VTS 웹 인터페이스는 시스템 통계 화면을 제공합니다. 사용자는 시스템 통계 화면을 참조하여 VTS 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 VTS의 local loop back interface 인 **lo** 및 VTS의 기본 네트워크 인터페이스인 **eth0** 대한 기본 네트워크 인터페이스 사용을 나타냅니다.



Network interfaces statistics

Interface		lo	eth0
Receive	Bytes	0	789257
	Packets	0	8208
	Errors	0	0
	Drop	0	0
	FIFO	0	0
	Frame	0	0
	Compressed	0	0
	Multicast	0	0
Transmit	Bytes	0	3252037
	Packets	0	4
	Errors	0	4681
	Drop	0	0
	FIFO	0	0
	Frame	0	19
	Compressed	0	4681
	Multicast	0	0

그림 10-1. 네트워크 인터페이스 상태

10.2 시리얼 포트 통계

시리얼 포트 통계는 32개의 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

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

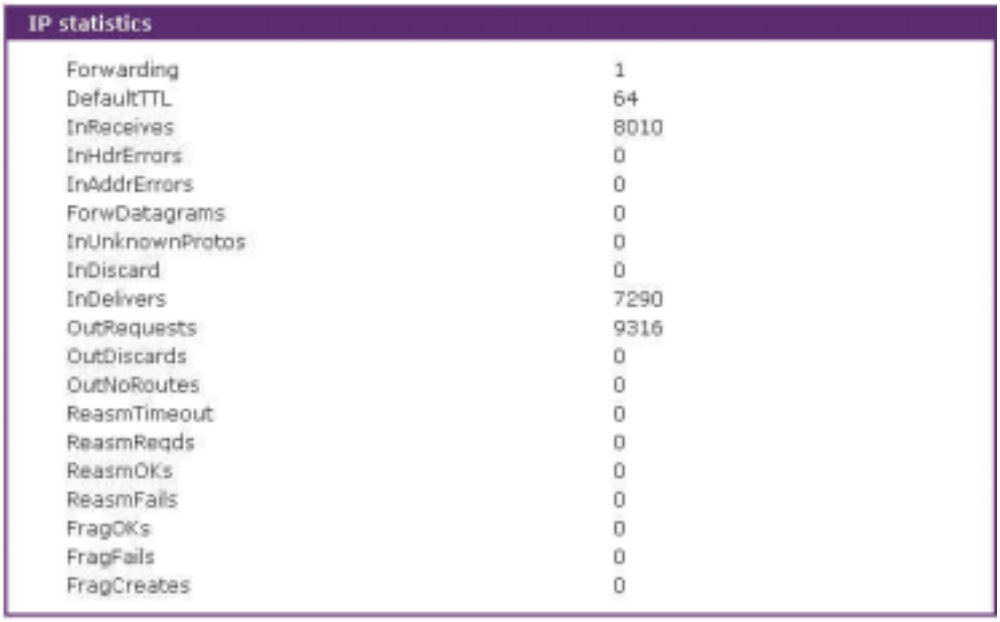


그림 10-3. IP 상태

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

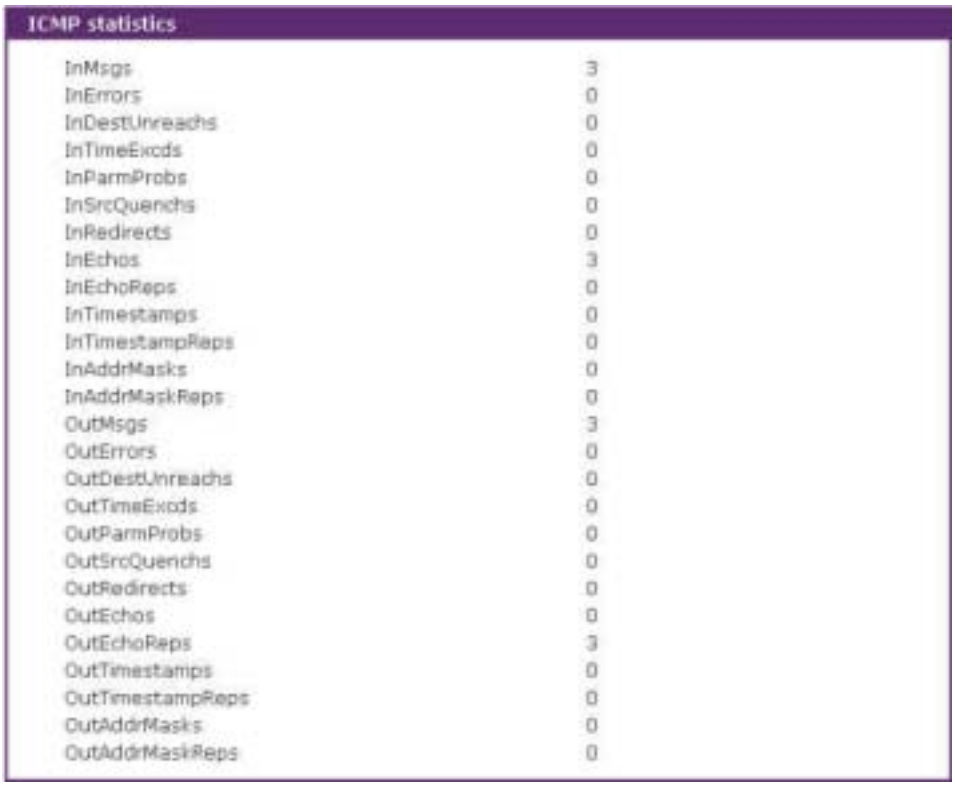


그림 10-4. ICMP 상태

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

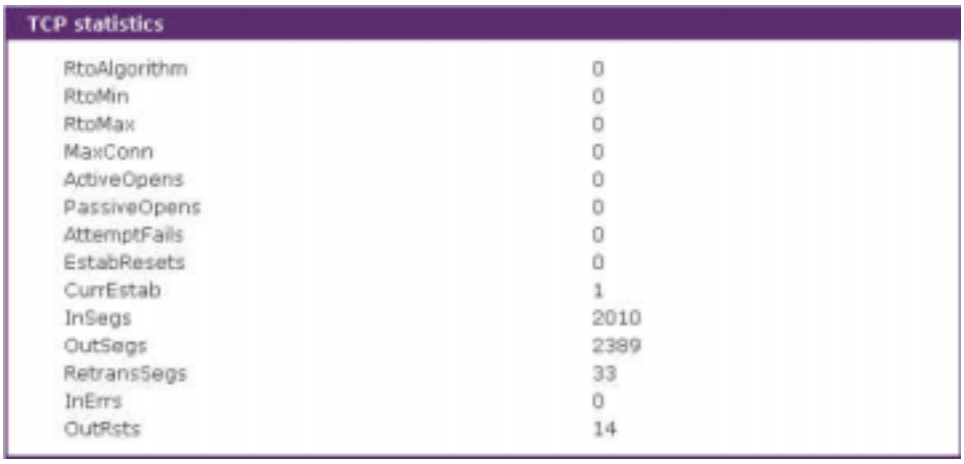


그림 10-5. TCP 상태

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 VTS의 Linux 콘솔 커맨드라인 인터페이스(CLI)에 접속 할 수 있습니다. CLI 에서 인증된 사용자는 표준 Linux 명령을 통하여 VTS 상태를 감시하고, 설정을 편집하고 변경 사항을 적용하고, 사용자 정의 script를 실행하며 원격 호스트로부터 파일을 다운로드 받을 수도 있습니다.
VTS는 내부 플래시 메모리에서 읽고/쓸 수 있도록 /usr2 에 1024 KB의 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 컨솔 연결을 제한하려면 /etc/pam.d/login 파일에 있는 아래 줄의 주석 문자를 제거하십시오.

```
auth       requisite  pam_securetty.so
```

root 사용자의 SSH 원격/시리얼 컨솔 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, rc.user 파일에 아래의 내용을 추가한 후 시스템을 재부팅 하여 변경 내용을 반영해야 합니다.

```
echo 57600 > /var/run/mgetty.console
```

여기서, 57600은 모뎀과 콘솔포트의 보레이트입니다.

11.2. 플래시 구성

VTS 내부 플래시는 아래의 표와 같이 구성됩니다. 사용자는 Mtdblock5 에 자유롭게 접속할 수 있는데, 이는 /usr2 에 마운트되어 있습니다. 사용자는 /etc, /var 및 /temp 파일에 접근할 수 있습니다. 재부팅한 후 이런 파일에 단순히 접근하는 것은 VTS에 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 가 올바르게 동작하지 않을 수 있습니다. 최악의 경우, VTS가 작동하지 않을 수도 있습니다.

블록	유형	마운트 지점	크기(KB)
Mtdblock0	Bootloader	none	128
Mtdblock1	Kernel	none	768
Mtdblock2	CRAMFS (읽기 전용)	/	6080
Mtdblock3	램 디스크 이미지(4MB)	/etc, /var, /tmp	64
Mtdblock4	EXT2 (R/W)	/cnf (정상적으로 마운트됨)	64
Mtdblock5	JFFS2 (R/W)	/usr2	1024
Mtdblock6	Reserved	none	64
합계			8192

Note : CLI에서 mount 또는 dd 명령어를 사용하여 각각의 mtdblock에 접근하지 마십시오. VTS가 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 VTS의 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 root 계정으로 로그인합니다.

Telnet/SSH 콘솔:

1) telnet VTS_ip_address or
2) ssh root@VTS_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 설정 편집하기

11.5.1 설정 파일 저장/로드 동작:

1) VTS는 부팅 시, /cnf/cnf.tar.gz 파일을 /tmp/cnf/ 에 압축을 풀어 저장하고 /cnf/ 디렉토리를 unmount 합니다.
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, VTS는 /cnf 를 다시 mount하고 /tmp/cnf/ 에 있는 변경된 파일들을 /cnf/cnf.tar.gz 로 다시 압축합니다.

11.5.2 CLI에서 설정 변경 방법:

CLI에서 VTS의 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 C. VTS 설정 파일*** 을 참조하세요)
2) saveconf 유틸리티를 사용해 설정 파일을 플래쉬 메모리에 저장합니다.
3) applyconf 유틸리티를 사용해 모든 변경 사항을 시스템에 적용합니다.

```
root@192.168.0.117:~# configmenu
```

```
or

root@192.168.0.117:~# cd /tmp/cnf
root@192.168.0.117:/tmp/cnf# vi redirect.cnf
root@192.168.0.117:/tmp/cnf# saveconf
root@192.168.0.117:/tmp/cnf# applyconf
```

11.6. 사용자 Script 실행하기

Shell script /usr2/rc.user 는 VTS가 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@192.168.0.117:~# cd /usr2
root@192.168.0.117:/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(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 컨솔에 연결하기

사용자는 시리얼 포트에 연결된 모뎀을 통해 시리얼 컨솔에 접근할 수 있습니다. /usr2/rc.user에 다음과 같은 스키립트를 추가한 후 재부팅하여 스크립트가 자동 실행되도록하면 됩니다.

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

여기서 9600은 시리얼 포트와 모뎀의 보레이트입니다.

US Robotics 모뎀등과 같이 일부 모뎀에서는 다음의 스크립트를 추가해야 합니다.

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

11.9. 예제

11.9.1 장치의 telnet disable 하기

VTS 장치는, 원격 콘솔 포트(SSH 용 TCP 포트 22 또는 telnet용 TCP 포트 23)들을 개별적으로 비활성화 하는 기능을 지원하지는 않습니다.

현재, 사용자는, 웹/Telnet/SSH 를 통한 VTS 설정 메뉴에서, 모든 원격 콘솔을 비활성 또는 활성 상태가 되도록 할 수 있습니다.

사용자는 사용자용 script rc.user 를 수정함으로써, 단지 하나의 원격 콘솔(telnet 또는 SSH)만을 비활성 상태가 되도록 할 수 있습니다. 수행하는 방법은 다음과 같이 2가지의 예제가 있습니다.

예제 1. inetd.conf 파일을 수정합니다.

1 단계 /etc/inetd.conf (telnet 서비스를 comment out 또는 삭제)을 수정합니다.

2 단계 inetd.conf 를 /usr2/inetd.conf 로 복사합니다.

3 단계 /usr2/rc.user script 를 다음과 같이 편집합니다.

```
#!/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
# Add shell command to execute from here
```

```
cp -a /usr2/inetd.conf /etc/inetd.conf
ps -ef
while killall inetd 2>/dev/null;
do sleep 1;
ps -ef
done
/usr/sbin/inetd
ps -ef

exit 0
```

이렇게 하면, 사용자는 매번 시스템을 부팅할 때마다 telnet 서비스가 비활성 상태가 되도록 동작시킬 수 있습니다.

예제 2. iptables rule 실행

1 단계 다음과 같이 /usr2/rc.user script를 수정합니다.

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#!/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

# if user wants to disable telnet service from all host
iptables -A INPUT -p tcp -s --dport 23 -j DROP

# if user wants to enable telnet service only from specific hosts(192.168.0.0 ~
192.168.0.255)
#iptables -A INPUT -p tcp -s ! 192.168.0.1/255.255.255.0 --dport 23 -j DROP

exit 0
```

사용자는 시스템을 부팅할 때마다 telnet 서비스를 disable 상태가 되도록 할 수 있습니다. 사용자가 Factory Reset 기능을 이용하여, VTS를 원래 설정치 대로 복원하면, /usr2/rc.user script 파일의 이름은 /usr2/rc.user.old# 파일로 저장되며 원래의 rc.user 파일이 복구됩니다.

11.9.2 CLI 로그인에 대한 RADIUS 인증 하기

VTS 장치의 CLI는 Linux-PAM (Pluggable Authentication Modules for Linux)을 지원합니다. 이 기능 을 통해 사용자는 CLI 로그인을 위한 RADIUS 인증 기능을 추가할 수 있습니다. 로그인 작업에서 원격 인증 후 사용자에게 적절한 쉘 프로그램을 할당하기 위해서, Radius 서버에 등록된 이름과 같은 이름의 사용자가 VTS에도 등록되어 있어야 한다는 것을 주의하십시오.

예제 1. Serial/Telnet console

1 단계 사용자 계정을 RADIUS 서버(192.168.0.135)에 추가합니다.

2 단계 사용자 계정을 VTS 장치에 추가합니다.

3 단계 /usr2/ 디렉토리에 RADIUS 서버의 IP 주소, Secret 및 timeout 값을 포함하는 server 파일을 생성합니다.

vi /usr2/server

```
192.168.0.135 testing123 10
```

4 단계 /usr2/ 디렉토리에 사용자가 장치로 로그인할 수 있는지를 결정하는 PAM 설정 파일인 login 파일을 생성합니다.

vi /usr2/login

Radius 인증

```
auth          required        pam_securetty.so
auth          required        pam_radius_auth.so
account       required        pam_unix.so
password      required        pam_unix.so
session       required        pam_unix.so
```

Radius and Local 인증

(우선 Radius 인증을 거친 후 성공하면 Local 인증을 거침. 사용자는 패스워드를 두 번 입력해야 함.)

```
auth          required        pam_securetty.so
auth          required        pam_radius_auth.so
auth          required        pam_unix_auth.so
account       required        pam_unix.so
password      required        pam_unix.so
session       required        pam_unix.so
```

Radius or Local 인증

(우선 Radius 인증을 거친 후 실패하면 Local 인증을 거침.)

```
auth          required        pam_securetty.so
auth          sufficient      pam_radius_auth.so
auth          required        pam_unix_auth.so
account       required        pam_unix.so
password      required        pam_unix.so
session       required        pam_unix.so
```

Radius down – Local 인증

(우선 Radius 인증을 거친 후 Radius 서버가 다운됐을 경우에만 Local 인증을 거침.)

```
auth required       pam_securetty.so
auth [success=done new_authtok_reqd=done authinfo_unavail=ignore default=die] pam_radius_auth.so
auth [success=done new_authtok_reqd=done authinfo_unavail=ignore default=die] pam_unix_auth.so
account      required       pam_unix.so
password     required       pam_unix.so
session      required       pam_unix.so
```

5 단계 root 로그인을 허용하는 securetty 를 다음과 같이 생성합니다.

```
# vi /usr2/securetty
```

```
console
ttyS0
pts/0
```

6 단계 server, login과 securetty 파일을 상응하는 디렉토리로 다음과 같이 복사합니다.

```
# cp /usr2/server /etc/raddb
# cp /usr2/login /etc/pam.d
# cp /usr2/securetty /etc/securetty
```

7 단계 시스템을 재부팅할 때마다 적용될 수 있도록 위의 변경 내용을 반영하여 다음과 같이 /usr2/rc.user script를 편집합니다.

```
#!/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

# Add shell command to execute from here
cp –f /usr2/server /etc/raddb/
cp –f /usr2/login /etc/pam.d/
cp –f /usr2/securetty /etc/

exit 0
```

이렇게 수정하면 사용자는 현재 telnet 클라이언트를 통해 CLI에 로그인하기 위해 RADIUS 인증 방법을 사용할 수 있습니다.

RADIUS 인증을 성공적으로 동작시키려면, 사용자는 반드시 위에서 설명한 단계를 완전히 수행해야 합니다. 오류가 발생하는 경우, 사용자는 Factory default reset을 통해 시스템을 원래 값으로 재설정할 필요가 있습니다.

다중의 root 접근을 허용하려면 pts logins를 securetty 파일에 다음과 같이 추가해야 합니다.

```
console
ttyS0
pts/0
pts/1
...
pts/9
```

사용자가 VTS를 공장 출하시의 기본값으로 Reset 하는 경우, /usr2/rc.user script 파일은 /usr2/rc.user.old# 파일로 저장되며, 원래의 rc.user 파일이 복구됩니다.

예제 2. SSH console

1 단계 사용자 계정을 RADIUS 서버(192.168.0.135)에 추가합니다.

2 단계 사용자 계정을 VTS 장치에 추가합니다.

3 단계 /usr2/ 디렉토리에 RADIUS 서버의 IP 주소, Secret 및 timeout 값을 포함하는 server 파일을 생성합니다.

vi /usr2/server

```
192.168.0.135 testing123 10
```

4 단계 /usr2/ 디렉토리에, 사용자가 장비에 로그인하는 것이 허락되었는지를 검사하기 위한 PAM ssh 설정 파일인 sshd 파일을 생성합니다.

vi /usr2/sshd

Radius 인증

```
auth         required       pam_radius_auth.so
auth         required       pam_nologin.so
session      required       pam_unix.so
```

Radius and Local 인증

(우선 Radius 인증을 거친 후 성공하면 Local 인증을 거침. 사용자는 패스워드를 두 번 입력해야 함.)

```
auth         required       pam_radius_auth.so
auth         required       pam_unix_auth.so
session      required       pam_unix.so
```

Radius or Local 인증

(우선 Radius 인증을 거친 후 실패하면 Local 인증을 거침.)

```
auth         sufficient     pam_radius_auth.so
auth         required       pam_unix_auth.so
session      required       pam_unix.so
```

Radius down – Local 인증

(우선 Radius 인증을 거친 후 Radius 서버가 다운됐을 경우에만 Local 인증을 거침.)

```
auth [success=done new_authtok_reqd=done authinfo_unavail=ignore default=die] pam_radius_auth.so
     retry=2
auth [success=done new_authtok_reqd=done authinfo_unavail=ignore default=die] pam_unix_auth.so
session     required       pam_unix.so
```

5 단계 sshd_config 파일에서 UsePAM는 yes로 PasswordAuthentication는 no로 변경하십시오.

cp /etc/ssh/sshd_config /usr2/

vi /usr2/sshd_config

```
...
PasswordAuthentication no
```

```
...
UsePAM yes
```

6 단계 수정된 설정으로 SSHD를 실행하기 위해 inetd.conf을 다음과 같이 수정하십시오.

```
# cp /etc/inetd.conf /usr2/
# vi /usr2/inetd.conf
```

```
...
ssh   stream  tcp   nowait  root  /usr/sbin/tcpd sshd –i -f /usr2/sshd_config
...
```

7 단계 server, sshd와 inetd.conf 파일을 상응하는 디렉토리로 다음과 같이 복사합니다.

```
# cp /usr2/server /etc/raddb/
# cp /usr2/sshd /etc/pam.d/
# cp /usr2/inetd.conf /etc/
```

8 단계 변경된 설정을 적용하기 위해 inetd 프로세스를 재기동하십시오.

```
# killall inetd
# /usr/sbin/inetd
```

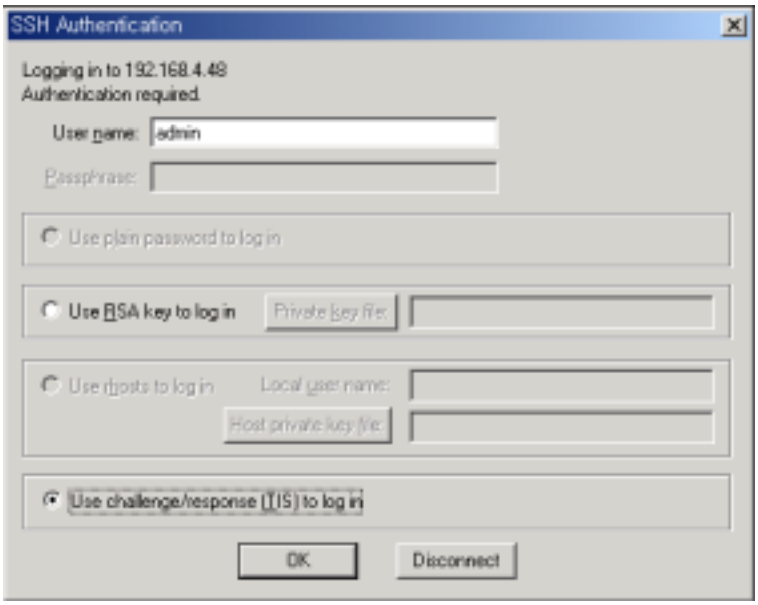
이렇게 수정하면 사용자는 현재 SSH 클라이언트를 통해 CLI에 로그인하기 위해 RADIUS 인증 방법을 사용할 수 있습니다.

9 단계 시스템을 재부팅할 때마다 적용될 수 있도록 위의 변경 내용을 반영하여 다음과 같이 /usr2/rc.user script를 편집합니다.

```
#!/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

# Add shell command to execute from here
cp –f /usr2/server /etc/raddb/
cp –f /usr2/sshd /etc/pam.d/
cp –f /usr2/inetd.conf /etc/

while killall inetd 2>/dev/null;
do sleep 1;
done

/usr/sbin/inetd

exit 0
```

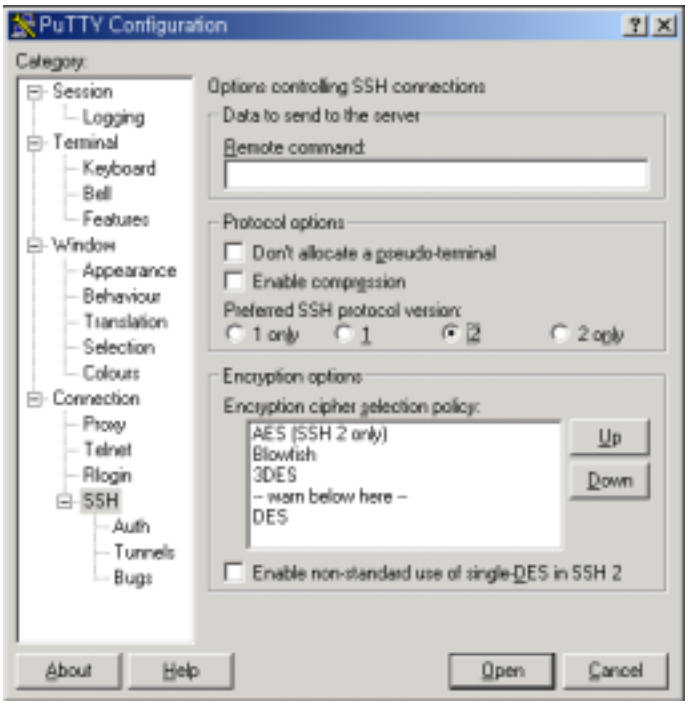
10 단계 SSH 클라이언트 프로그램을 아래와 같이 설정합니다.

TeraTerm Pro SSH 클라이언트 - Use challenge/response(TIS) to login을 선택합니다.

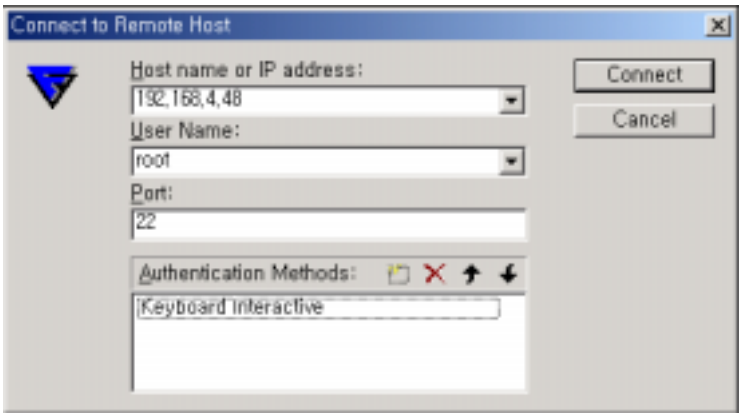


주의 : *Radius Down – Local 인증의 경우에는 TermTerm Pro를 사용할 수 없습니다.*

Putty SSH 클라이언트 - Preferred SSH protocol version을 2로 선택합니다



F-secure SSH 클라이언트 - Authentication Method에 “Keyboard interactive”를 추가합니다.



11.9.3 CLI 로그인에 대한 TACACS+ 인증 하기

VTS 장치의 CLI는 Linux-PAM (Pluggable Authentication Modules for Linux)을 지원합니다. 이 기능 을 통해 사용자는 CLI 로그인을 위한 TACACS+ 인증 기능을 추가할 수 있습니다. 로그인 작업에서 원격 인증 후 사용자에게 적절한 쉘 프로그램을 할당하기 위해서, TACACS+ 서버에 등록된 이름과 같은 이름의 사용자가 VTS에도 등록되어 있어야 한다는 것을 주의하십시오.

예제 1. Serial/Telnet console

1 단계 사용자 계정을 TACACS+ 서버(192.168.0.135)에 추가합니다. 그리고 TACACS+ 서버를 기동합니다.(`# /usr/local/sbin/tac_plus -C /etc/tac_plus.cfg -d 4088`)

2 단계 사용자 계정을 VTS 장치에 추가합니다.

3 단계 /usr2/ 디렉토리에 사용자가 장치로 로그인할 수 있는지를 결정하는 PAM 설정 파일인 login 파일을 생성합니다.

```
# vi /usr2/login
```

TACACS+ 인증

```
auth          required       pam_securetty.so
auth          required       pam_tacplus.so encrypt service=ppp protocol=lcp
server= 192.168.0.135 secret=vts123
#account       required       pam_unix.so
#password       required       pam_unix.so
#session       required       pam_unix.so
```

TACACS+ and Local 인증

(우선 TACACS+ 인증을 거친 후 성공하면 Local 인증을 거침. 사용자는 패스워드를 두 번 입력해야 함.)

```
auth         required       pam_securetty.so
auth         required    pam_tacplus.so encrypt service=ppp protocol=lcp server=
192.168.0.135 secret=vts123
auth         required    pam_unix_auth.so
```

```
account      required       pam_unix.so
password     required       pam_unix.so
session      required       pam_unix.so
```

TACACS+ or Local 인증

(우선 TACACS+ 인증을 거친 후 실패하면 Local 인증을 거침.)

```
auth         required       pam_securetty.so
auth         sufficient     pam_tacplus.so encrypt service=ppp protocol=lcp
server= 192.168.0.135 secret=vts123
auth         required       pam_unix_auth.so
account      required       pam_unix.so
password     required       pam_unix.so
session      required       pam_unix.so
```

4 단계 root 로그인을 허용하는 securetty 를 다음과 같이 생성합니다.

```
# vi /usr2/securetty
```

```
console
ttyS0
pts/0
```

5 단계 login과 securetty 파일을 상응하는 디렉토리로 다음과 같이 복사합니다.

```
# cp /usr2/login /etc/pam.d
# cp /usr2/securetty /etc/securetty
```

6 단계 시스템을 재부팅할 때마다 적용될 수 있도록 위의 변경 내용을 반영하여 다음과 같이 /usr2/rc.user script를 편집합니다.

```
#!/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

# Add shell command to execute from here
cp –f /usr2/login /etc/pam.d/
cp –f /usr2/securetty /etc/

exit 0
```

이렇게 수정하면 사용자는 현재 telnet 클라이언트를 통해 CLI에 로그인하기 위해 TACACS+ 인증 방법을 사용할 수 있습니다.

TACACS+ 인증을 성공적으로 동작시키려면, 사용자는 반드시 위에서 설명한 단계를 완전히 수행해야 합니다. 오류가 발생하는 경우, 사용자는 Factory default reset을 통해 시스템을 원래 값으로 재설정할 필요가 있습니다.

다중의 root 접근을 허용하려면 pts logins를 securetty 파일에 다음과 같이 추가해야 합니다.

```
console
ttyS0
pts/0
pts/1
...
pts/9
```

사용자가 VTS를 공장 출하시의 기본값으로 Reset 하는 경우, /usr2/rc.user script 파일은 /usr2/rc.user.old# 파일로 저장되며, 원래의 rc.user 파일이 복구됩니다.

예제 2. SSH console

1 단계 사용자 계정을 TACACS+ 서버(192.168.0.135)에 추가합니다.

2 단계 사용자 계정을 VTS 장치에 추가합니다.

3 단계 /usr2/ 디렉토리에, 사용자가 장비에 로그인하는 것이 허락되었는지를 검사하기 위한 PAM ssh 설정 파일인 sshd 파일을 생성합니다.

vi /usr2/sshd

TACACS+ 인증

```
auth          required       pam_tacplus.so encrypt server=192.168.0.135
secret=vts123
auth          required       pam_nologin.so
session        required       pam_unix.so
```

TACACS+ and Local 인증

(우선 TACACS+ 인증을 거친 후 성공하면 Local 인증을 거침. 사용자는 패스워드를 두 번 입력해야 함.)

```
auth         required   pam_tacplus.so encrypt server=192.168.0.135
secret=vts123
auth         required       pam_unix_auth.so
session      required       pam_unix.so
```

TACACS+ or Local 인증

(우선 TACACS+ 인증을 거친 후 실패하면 Local 인증을 거침.)

```
auth         sufficient pam_radius_auth.so
auth         required       pam_unix_auth.so
session      required       pam_unix.so
```

4 단계 sshd_config 파일에서 UsePAM는 yes로 PasswordAuthentication는 no로 변경하십시오.

cp /etc/ssh/sshd_config /usr2/

vi /usr2/sshd_config

```
...
PasswordAuthentication no
...
UsePAM yes
```

5 단계 sshd 와 sshd_config 파일을 상응하는 디렉토리로 다음과 같이 복사합니다.

```
# cp /usr2/sshd /etc/pam.d/
# cp /usr2/sshd_config /etc/ssh/
```

6 단계 시스템을 재부팅할 때마다 적용될 수 있도록 위의 변경 내용을 반영하여 다음과 같이 /usr2/rc.user script를 편집합니다.

```
#!/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

# Add shell command to execute from here
cp –f /usr2/sshd /etc/pam.d/
cp –f /usr2/sshd_config /etc/ssh/

exit 0
```

이렇게 수정하면 사용자는 현재 SSH 클라이언트를 통해 CLI에 로그인하기 위해 TACACS+ 인증 방법을 사용할 수 있습니다.

7 단계 SSH 클라이언트 프로그램을 **11.9.2 CLI 로그인에 대한 RADIUS 인증하기** 중 **예제 2. SSH console**의 10단계와 같이 설정합니다.

부록 A: 연결

A.1 Ethernet Pin out

VTS는 AT&T 258 규격을 준수한 커넥터인 표준 Ethernet 커넥터를 사용합니다. 표 A-1은 핀 할당 및 전선 색상을 보여줍니다.

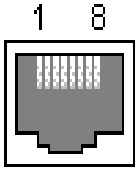


그림 A-1. RJ45 커넥터의 핀 배치

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

VTS는 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: VTS가 지원하는 PC 카드

VTS 시리즈는 다음의 PC 카드를 지원합니다.

표 B-1. 네트워크 카드

제조 업체	모델 이름	VTS 프로브 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
Corega	FetherII PCC-TXD	corega K.K. corega FEtherII PCC-TXD	10/100 Mbps LAN card
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 프로브 모델 이름	규격
Cisco Systems	AIR-PCM340/Aironet 340/350	Cisco Systems 340/350 Series Wireless LAN Adapter	11 Mbps 무선 LAN 어댑터
Cisco Systems	AIR-PCM350/Aironet 350	Cisco Systems 350 Series Wireless LAN Adapter	11 Mbps 무선 LAN 어댑터
Lucent Technologies	PC24E-H-FC/Orinoco Silver	Lucent Technologies WaveLAN/IEEE Version 01.01	11 Mbps 무선 LAN 어댑터
Agere Systems (Lucent Technologies)	Orinoco Classic Gold (PC24E-H-FC/Orinoco Gold)	Lucent Technologies WaveLAN/IEEE Version 01.01	11 Mbps 무선 LAN 어댑터
Buffalo	AirStation (WLI-PCM-L11GP)	MELCO WLI-PCM-L11 Version 01.01	11 Mbps 무선 LAN 어댑터

표 B-3. ATA/IDE Fixed Disk Card

제조 업체	모델 이름	VTS 프로브 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. 시리얼 모뎀 카드

제조 업체	모델 이름	VTS 프로브 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
TDK	TDK DH6400	TDK DH6400 1.0	64Kbps
NTT DoCoMo	Mobile Card Triplex N	NTT DoCoMo Mobile Card Triplex N	64Kbps

부록 C: VTS 설정 파일

C.1 System.cnf

```
#
# system.cnf
#
#   system configuration which exist only one place on this file.
#

# kind of IP configuration mode
# 1 - static ip , 2 - dhcp , 3 - pppoe
ipmode = 1

# system ip addres
ipaddr = 192.168.161.5

# system subnet mask
subnet = 255.255.0.0

# system gateway
gateway = 192.168.1.1

# dns configuration
# 'p_dns' is a primary dns ip address and 's_dns' is a secondary dns ip address
# if you want to set dns authmatically in case of dhcp or pppoe,
# you can set 'bmanual_dns' to 0.
p_dns = 168.126.63.1
s_dns = 168.126.63.2
bmanual_dns = 1

# pppoe configuration
# 'ppp_usr' is pppoe account name and 'ppp_pwd" is a password for that account
ppp_usr = whoever
ppp_pwd = pppoepwd

# Email logging configuration
# if you want to send log via E-mail, set 'emaillog' to 1
# 'emaillog_num' trigger sending email.
# The number of logs are greater than 'emaillog_num", then send it.
emaillog = 0
emaillog_num = 5

# SMTP configuration
# 'smtpsvr' is a SMTP server .
# 'sysmailaddr' is a sender address.
# 'recvmailaddr' is a receiver address.
# 'smtp_mode' means a SMTP server authentication mode.
#  1 - smtp w/o authentication , 2 - pop before smtp , 3 - smtp w/
authentication
# If 'smtp_mode" is 2 or 3, you need SMTP account information.
# 'smtp_user' is a SMTP account name and 'smtp_pwd" is a password.
smtpsvr = smtp.yourcompany.com
sysmailaddr = vts1600@yourcompany.com
recvmailaddr = admin@yourcompany.com
smtp_mode = 1
smtp_user = admin
smtp_pwd = admin

# 'device_name' mean a unit name assigned. A unit name will be a identifier
```

```
among PS products.
device_name = VTS Device

# IP filtering configuration
# By setting 'btelnet' to 1, you can use remote console.
# Similarly by setting 'bweb' to 1, you can use remote console.
# 0 means that protect any access.
# 'enable_ip', 'enable_netmask' pair is a source rule specification for remote
console filtering.
# 'enable_webip', 'enable_webnetmask' pair is for web filtering.
btelnet = 1
bweb = 1
enable_ip = 0.0.0.0
enable_netmask = 0.0.0.0
enable_webip = 0.0.0.0
enable_webnetmask = 0.0.0.0

# dynamic DNS(DDNS) configuration
# dynamic dns can be enabled by setting 'bdyndns' to 1. 0 for disable.
# 'dyn_dn' is a domain name for your DDNS.
# 'dyn_user' is a account name for DDNS and 'dyn_pwd" is a password for it.
bdyndns = 0
dyn_dn = vts1600.dyndns.biz
dyn_user = vts1600-user
dyn_pwd = vts1600-pwd

# NTP configuration
# 'ntp_enable' set to 1 for using NTP or set to 0.
# 'ntp_serverip' is the IP address of NTP server and 'ntp_offset' is a your
offset from UTC.
# If you don't know any NTP server IP, then set 'ntp_auto_conf' to 1.
ntp_enable = 0
ntp_auto_conf = 1
ntp_offset = 0.0
ntp_serverip = 192.168.200.100

# Log configuration
# system logging is enabled by 'log_enable' to 1.
# 'logbuf_size' is a variable for representing log buffer size by KB.
# 'log_stoloc' is a location to save log.
#  1 = memory 2 = CF card 3 = NFS 4 = SYSLOGD
# If you choose log location to SYSLOGD, 'logbuf_size' you've set will loose his
role - limiting log file size.
log_enable = 1
logbuf_size = 4
log_stoloc = 1

# Port access menu(PAM) configuration
# Enable or disable port access menu by setting 'master_enb' 1 or 0.
# 'master_port' is a listening port for PAM.
# 'master_proto' means a protocol .
#  1 = Telnet , 2 = SSH , 3 = RawTCP
# To set inactivity time-out, set 'master_inactivity'. A unit is second.
# 'master_localip' means a assigned ip for PAM.
# 'master_authmethod' means a authentication method for PAM.
#    0 = None
#    1 = radius   2 = local   3 = radius/local   4 = local/radius
#    5 = TACACS+  6 = TACACS+/local   7 = local/TACACS+
#    8 = LDAP     9 = LDAP/local     10 = local/LDAP
# If your authenticatio method is not None or Local, then you have to specify
other parameters
# 'master_p_radius_auth' and 'master_s_radius_auth' is a authentication server
ip address.
# One is a primary server and the other is secondary one.
# 'master_p_radius_acct' and 'master_s_radius_acct' is for accounting server.
# Accounting server parameters isn't needed in case of LDAP.
# 'master_radius_secret' is a shared secret only for RADIUS and TACACS+.
```

```
# In RADIUS case, you have two more parameters, 'master_radius_timeout' and
'master_radius_retries'.
# One is for the timeout and the other is for the count of retries.
# 'master_ldap_search_base' parameter - ldap base string - is ONLY FOR LDAP.
master_enb = 1
master_port = 7000
master_proto = 1
master_inactivity = 100
master_localip = 192.168.1.100
master_authmethod = 2
master_radius_timeout = 10
master_radius_retries = 3
master_ldap_search_base = "dn=yourcomapy,dn=com"

# syslog configuration
# You can run or kill syslogd by setting 'bsyslog_service' to 1 or 0.
# 'syslog_ip' is a IP addresss of a remote syslog server.
# 'syslog_2ndip' is a IP address of a secondary syslogd server which will get
the same logs.
# 'syslog_facility' specify what type of program is logging. 0 ~ 7 for LOCAL0 to
LOCAL7
bsyslog_service = 0
syslog_ip = 192.168.200.100
syslog_facility = 0

# NFS configuration
# You can mount or unmount NFS by setting 'bnfs_service'  to 1 or 0.
# 'nfs_ip' is a NFS server IP addresss and 'nfs_path' is a mount path.
bnfs_service = 0
nfs_ip = 192.168.200.100
nfs_path = /

# WEB configuration
# If you want to support HTTP, then set 'bweb_http' to 1. If not, set tot 0.
# 'bweb_https' is for HTTPS.
# 'web_refresh_rate' is for refresh the changing page when you see the system
status page.
bweb_http = 1
bweb_https = 1
web_refresh_rate = 10

# TCP configuration
# 'keepalive_time' is a time before keep alive takes place.
# 'keepalive_probes' is the number of allowed keep alive probes.
# 'keepalive_intvl' is a time interval between keep alive probes.
keepalive_time = 15
keepalive_probes = 3
keepalive_intvl = 5

# Ethernet configuration
# 'ethernet_mode' is a ethernet mode.
# 0 = Auto Negotiation,  1 = 100BaseT Half Duplex, 2 = 100BaseT Full Duplex,
# 3 = 10BaseT Half Duplex, 4 = 10BaseT Full Duplex
ethernet_mode = 0

# PCMCIA configuration
# 'pcmcia_card_type' shows a pcmcia card type.
# 0 for empty , -1 for unsupported card, 1 for CF card, 2 for Network card,
# 3 for Wireless Network card, 4 for Serial Modem card
pcmcia_card_type = 0

# PCMCIA ipconfiguration
# same with system ip configuration
pcmcia_ipmode = 2
pcmcia_ip = 192.168.1.254
pcmcia_subnet = 255.255.255.0
pcmcia_gateway = 192.168.1.1
```

```
pcmcia_ppp_usr = whoever
pcmcia_ppp_pwd = pppoepwd
pcmcia_bmanual_dns = 0

# In case of serial modem card, 'pcmcia_modem_initstr' means a modem init string.
pcmcia_modem_initstr = q1e0s0=2

# Wireless network card configuration
# To enable or disable Wired Equivalent Privacy(WEP), set 'pcmcia_wep_enb' to 1
or 0.
# 'pcmcia_web_mode' is a WEP mdoe. 1 for encrypted, 2 for shared
# 'pcmcia_wep_length' is a length for WEP. 1 for 40 bits, 2 for 128 bits
# 'pcmcia_wep_key_str' is a key string for WEP.
pcmcia_wep_enb = 0
pcmcia_wep_mode = 1
pcmcia_wep_length = 1

# 'pcmcia_cf_conf_max' is a maximum size to use in case of CF card.
pcmcia_cf_conf_max = 0
```

C.2 Redirect.cnf

```
#
# redirect.cnf
#
#   Port configuration except port access menu place on this file.
#   Basically keys followed by 'port' key are data for those port.
#   Port number is zero-by-index and the maximum value for port is used as all
port configuration
#   Data followed by all port are default values and will NOT be applied.

# 'port' key notify the port data follow.
# If you want to activate the port, set 'benable' to 1. If not, set to 0.
# If you set 'bmanset' to 1, you don't want to change the port data by changing
all port configuration.
# If you want to change the port data by changing all port configuration, set to
0.
port = 0
benable = 0
bmanset = 0
port = 1
benable = 0
bmanset = 0
port = 2
benable = 0
bmanset = 0
port = 3
benable = 0
bmanset = 0
port = 4
benable = 0
bmanset = 0
port = 5
benable = 0
bmanset = 0
benable = 0
port = 6
bmanset = 0
benable = 0
port = 7
```

```
bmanset = 0
benable = 0
port = 8
benable = 0
bmanset = 0
port = 9
benable = 0
bmanset = 0
port = 10
benable = 0
bmanset = 0
port = 11
benable = 0
bmanset = 0
port = 12
benable = 0
bmanset = 0
port = 13
benable = 0
bmanset = 0
port = 14
benable = 0
bmanset = 0
port = 15
benable = 0
bmanset = 0

# As refered, maximum port (in case 16 port machine ,16) represents the defaults
values for
# all port configuration.
port = 16
benable = 0
bmanset = 0

# Serial parameter configuration
# 'uarttype' is for UART type. But PS only support RS232.
# So set 'uarttype' to 0 and DO NOT CHANGE.
# 'baudrate' is for baudrate. From 1200 to 230400 is available.
# 'stopbits' is for stop bits. 1 for 1 bit, 2 for 2 bits
# 'databits' is for data bits. 7 for 7 bits, 8 for 8 bits.
# 'parity' is for parity. 0 for none, 1 for even , 2 for odd parity.
# 'flowcontrol" is for flow contorl. 0 for none, 1 for XON/XOFF, 2 for hardware
flow control
# 'dtropt' is for dtr option.
#  1 = Always HIGH, 2 = Always LOW, 3 = High when open
# 'interchartimeout' is for inter-character timeout. It works ONLY FOR RAWTCP
mode.
uarttype = 0
baudrate = 9600
stopbits = 1
databits = 8
parity = 0
flowcontrol = 0
dtropt = 0
interchartimeout = 100

# Host mode configuration
# 'protocol' means a host mode.
#  0 = Terminal Server, 1 = Console Server, 2 = Dial-in modem, 3 = Dial-In
Termimal Server
protocol = 1
# In Terminal Server mode, 'destip' and 'destport' is destination IP and port to
connect.
destip = 0.0.0.0
destport = 0
# In Console Server mode, 'localip' is a assigned IP to the port and 'localport'
is a listenning port.
```

```
local_ip = 0.0.0.0
localport = 0
# 'inactivitytimeout' is a inactivity timeout in seconds.
inactivitytimeout = 100
# 'run_proto' is a ethernet protocol for this port. This key is useless for
Dial-In modem mode.
#  1 = Telnet , 2 = SSH , 3 = RawTCP
run_proto = 1
# 'ssh_break_string' is a string for send a break in case of Console server mode
and 'run_proto' is SSH.
ssh_break_string = ~break

# IP filtering configuration
# 'allow_ip', 'allow_netmask' pair is a source rule specification for serial
port access filtering.
allow_ip = 0.0.0.0
allow_netmask = 0.0.0.0

# 'porttitle' is a port title.
porttitle = Port Title

# Email notification configuration
# Enable of disable e-mail notification by setting 'en_enable' to 1 or 0.
# 'en_minsnddelay' is a minimum delay of sending email notification.
# A unit is second and minimum value is 5.
# 'en_msgtitle' is a message title of email.
# 'en_mailto' is reciever addresss.
# 'en_keywords' is a keyword to monitor. 'en_keyword' key can occur serveral
times.
# But the maximum number of keywords is 30.
en_enable = 0
en_minsnddelay = 5
en_msgtitle = Email Alarm Notification
en_mailto = admin@yourcompany.com

# Port buffering configuration
# Enable of disable port buffering by setting 'pb_enable' to 1 or 0.
# 'pb_size' is a maximum port buffering size. Maximum value are different by
location.
# 'pb_loc' is a location to store port buffer data.
#  1 = memory 2 = CF card 3 = NFS 4 = SYSLOGD
pb_enable = 0
pb_size = 4
pb_loc = 1

# In Dial-In Modem or Dial-in Terminal Server mode, you can set modem initstring
by setting 'modem_initstr'.
modem_initstr = q1e0s0=2

# Authentication configuration
# 'authmethod' means a authentication method for port log-in.
#    0 = None
#    1 = radius   2 = local   3 = radius/local   4 = local/radius
#    5 = TACACS+  6 = TACACS+/local   7 = local/TACACS+
#    8 = LDAP     9 = LDAP/local     10 = local/LDAP
# If your authenticatio method is not None nor Local, then you have to specify
other parameters
# 'p_radius_auth' and 's_radius_auth' is a authentication server ip address.
# One is a primary server and the other is secondary one.
# 'p_radius_acct' and 's_radius_acct' is for accounting server.
# Accounting server parameters isn't needed in case of LDAP.
# 'radius_secret' is a shared secret only for RADIUS and TACACS+.
# In RADIUS case, you have two more parameters, 'radius_timeout' and
'radius_retries'.
# One is for the timeout and the other is for the count of retries.
# 'ldap_search_base' parameter - ldap base string - is ONLY FOR LDAP.
authmethod = 2
```

```
radius_timeout = 10
radius_retries = 3
ldap_search_base = "dn=yourcomapy,dn=com"

# 'user_ctrl_mode' is user access control mode.
#  0 = disable, 1 = restriction , 2 = permission
#  'restricted_user_list' is a string shows a restricted user list
#  'permitted_user_list' is a string shows a permitted user list
#  in user list string, user IDs must be seperated by comma(,).
user_ctrl_mode = 0

# 'sniff_mode' is a sniffing mode option.
#   0 = disable, 1 = input , 2 = output , 3 = Both
# 'sniff_user_list' is a sniff user list. Like above user list, user name should
be seperated by comma.
sniff_mode = 0
```

부록 D: 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 D-1은 잘 알려진 포트 번호 중의 일부를 보여줍니다. 자세한 내용은 IANA 웹사이트를 방문하시기 바랍니다.
http://www.iana.org/assignments/port-numbers

표 D-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 E: Bootloader 메뉴 프로그램 안내

E.1 개요

Bootloader 메뉴는 비상 시, 복구 옵션으로 BOOTP/TFTP를 사용하여 VTS를 복구하고 시스템 하드웨어를 진단하는 방법을 제공합니다. VTS 장치에 전원이 공급된 후 3초 이내에 사용자가 <ESC> 키를 누르면, bootloader 메뉴 프로그램을 입력할 수 있습니다. 이 메뉴 프로그램으로부터, 사용자는 다양한 시스템 파라미터를 설정할 수 있고, 하드웨어 시스템 테스트 및 firmware 업그레이드를 수행할 수 있습니다.

E.2 메인 메뉴

Bootloader 메뉴 프로그램에 들어가면, 사용자는 다음과 같이 페이지를 볼 수 있습니다.

```
Bootloader 0.3.0 (Feb 14 2003 - 10:49:27)

CPU     :  XPC855xxZPnnD4 (50 MHz)
DRAM    :  64 MB
FLASH   :   8 MB
PC CARD  :  No card
EEPROM   :  A Type exist
Ethernet :  AUTO-NEGOTIATION
Autoboot Start:  0
-------------------------------------------------------------------------------
 Welcome to Boot Loader Configuration page
-------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Feb 14 2003 - 11:00:26 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v0.6.11]
 4. Exit and boot from flash
 5. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 E-1. Bootloader 메인 프로그램의 메인 메뉴 페이지

E.3 RTC 설정 메뉴

RTC 설정 메뉴를 사용함으로써, 사용자는 VTS의 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 E-2. Bootloader 메뉴 프로그램 내의 RTC 설정

E.4 하드웨어 테스트 메뉴

사용자는 하드웨어 테스트 메뉴를 사용하여 하드웨어 구성 요소들을 테스트할 수 있습니다. 다음과 같은 3가지의 하드웨어 테스트 모드가 있습니다.

- 1회
- 루핑(자동 테스트에서 외부 테스트 없이 수행함)
- 루핑(자동 테스트에서 외부 테스트를 사용해 수행함)

사용자가 **1회**를 선택하는 경우, 자동 테스트 또는 각 구성 요소 테스트가 한 번만 수행됩니다. 이 모드에서, 원격 호스트(서버 IP 주소)의 ping 테스트와 UART 테스트가 한 번 씩 수행됩니다. 사용자가 루핑(자동 테스트에서 외부 테스트 없이 수행함)을 선택하는 경우, 사용자가 <ctrl-c>

키를 누르기 전까지 자동 테스트가 반복적으로 수행됩니다. 이 모드에서, 원격 호스트(서버 IP 주소)의 ping 테스트와 UART 테스트가 수행되지 않습니다

사용자가 루핑(자동 테스트에서 외부 테스트를 사용해 수행함)을 선택하는 경우, 사용자가 <ctrl-c> 키를 누르기 전까지 자동 테스트가 반복적으로 수행됩니다. 그리고, 원격 호스트(서버 IP 주소)의 ping 테스트와 UART 테스트가 반복적으로 수행됩니다.

참고:

Ethernet 및 UART에서 테스트를 적절히 수행하려면, 사용자는 VTS의 Ethernet 포트에 Ethernet 케이블을 반드시 연결하고 루프백 커넥터를 VTS의 모든 시리얼 포트에 연결해야 합니다. 또한, 유효한 IP 주소를 갖는 원격 호스트가 반드시 있어야 합니다. 기본 서버의 IP 주소는 192.168.0.128 이며 이는 [Firmware Upgrade] 메뉴를 사용하여 변경할 수 있습니다. 그렇지 않으면, 테스트를 적절히 수행할 수 없습니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <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. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <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. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <ESC> Back, <ENTER> Refresh
 ----->0

--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 E-3. Bootloader 메뉴 프로그램 내의 하드웨어 테스트 메뉴

사용자가 [Auto test]을 선택한 경우, 모든 하드웨어 구성 요소에 대한 테스트가 자동으로 수행됩니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <ESC> Back, <ENTER> Refresh
 ----->1

*******  Hardware auto-detect and auto-test *******
[DRAM]
DRAM Test in progress ---------------------------------------[65536KB]
DRAM Test ---------------------------------------------------[SUCCESS]

[FLASH]
Flash Test Status--------------------------------------------[  100 %]
Flash Test ---------------------------------------------------[SUCCESS]

[FAN]
Fan Status ---------------------------------------------------[7020 RPM]
```

```
[LED]
SERIAL READY LED ON/OFF-------------------------------------3 time(s)

[EEPROM]
EEPROM   :  A Type exist
EEPROM Test ------------------------------------------------ [SUCCESS]

[UART]
<--Internal loop 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 # 4 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]
<--External loop 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 # 4 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]

[PCMCIA]
 5V CARD
 5.0V card found: Lucent Technologies WaveLAN/IEEE Version 01.01
          Network Adapter Card

[Ethernet]
Ethernet chip test-----------------------------------------[SUCCESS]
PING 192.168.0.135 from 192.168.161.5 : 64 bytes of ethernet packet.
64 bytes from 192.168.0.135 : seq=0 ttl=255 timestamp=11172879 (ms)
64 bytes from 192.168.0.135 : seq=1 ttl=255 timestamp=11173874 (ms)
64 bytes from 192.168.0.135 : seq=2 ttl=255 timestamp=11174875 (ms)
64 bytes from 192.168.0.135 : seq=3 ttl=255 timestamp=11175876 (ms)

      *******  Hardware auto-detect and auto-test  SUMMARY *******
1. DRAM Test  ----------------------------------------------[SUCCESS]
2. FLASH Test ----------------------------------------------[SUCCESS]
3. FAN Test   ----------------------------------------------[SUCCESS]
4. EEPROM Test---------------------------------------------[SUCCESS]
5. 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

6.PC CARD Test Summary
 5V CARD
 5.0V card found: Lucent Technologies WaveLAN/IEEE Version 01.01
          Network Adapter Card
7. PING Test  ----------------------------------------------[SUCCESS]

PRESS any key to continue!!
```

그림 E-4. Bootloader 메뉴 프로그램 내의 하드웨어 테스트 화면

각 하드웨어 구성 요소 테스트를 위해, 사용자는 <ESC> 키를 눌러 테스트를 건너뛸 수 있습니다.

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. FAN test
 5. LED test
 6. EEPROM test
 7. UART test
 8. PC card test
 9. Ethernet test
  <ESC> Back, <ENTER> Refresh
 -----> 1

          *******  Hardware auto-detect and auto-test *******
[DRAM]
DRAM Test in progress ----------------------------------------[  640KB]
DRAM Test ----------------------------------------------------[SKIPPED]

[FLASH]
Flash Test Status---------------------------------------------[   2 %]
FLASH Test ---------------------------------------------------[SKIPPED]
```

그림 E-5. ESC 키를 사용하여 특정 테스트 건너뛰기

루핑 모드를 갖는 자동 테스트가 수행되는 동안 문제가 발생하는 경우, 테스트가 정지되며 시리얼 InUse LED는 하드웨어 테스트가 실패했다는 알리기 위해 깜빡입니다. 이 경우, 사용자는 <ctrl-c> 키를 눌러 메뉴 페이지로 돌아가야만 합니다.

E.5 Firmware upgrade 메뉴

Firmware upgrade 메뉴를 사용함으로써 사용자는 장치의 firmware를 업그레이드할 수 있습니다. firmware를 업그레이드하기 전, 사용자는 메인 메뉴 페이지의 메뉴 항목 3을 선택하여 현재 firmware 버전을 확인할 수 있습니다. firmware upgrade 메뉴 프로그램은 원격 firmware 다운로드를 위해 BOOTP 및 TFTP 2개의 프로토콜을 지원합니다. DHCP 환경을 위한 기본 프로토콜은 BOOTP입니다. 사용자가 TFTP를 선택한 경우, 사용자는 적절한 장치의 IP 주소를 설정해야 합니다. 장치의 기본 IP 주소는 192.168.161.5.입니다.

Firmware upgrade 의 경우, [Server's IP address]로 설정된 서버에 반드시 [Firmware File Name]로 설정된 firmware 파일이 반드시 존재해야 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. Firmware File Name [vts3200.bin]
 5. 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. Firmware File Name [vts3200.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 E-6. Bootloader 메뉴 프로그램 내의 firmware upgrade 메뉴

사용자가 [Start firmware upgrade]를 선택하는 경우, 확인 메시지가 화면에 나타납니다. 사용자가 'y' 를 입력하면, Firmware upgrade 프로세스가 시작합니다. 이러한 프로세스는 완료될 때까지 멈추지 않습니다.

```
--------------------------------------------------------------------------------
 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. Firmware File Name [vts3200.bin]
 5. Start firmware upgrade
 -----> 5
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)?y
BOOTP broadcast 1
ARP broadcast 1
TFTP from server 192.168.0.128; our IP address is 192.168.161.5
Filename 'vts3200.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. Firmware File Name [vts3200.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 E-7. firmware upgrade 프로세스

firmware upgrade 프로세스가 완료되면, 프로그램은 성공 메시지와 함께 메뉴를 다시 나타냅니다.

부록 F: 암호화된 NFS 기능 안내

F.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. VTS에서 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.

F.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 받는다.

Step 2. "nfserver.exe" 프로그램을 실행시키고 이때 나타나는 지시에 따른다.

Step 3. Omni-NFS server 설치를 완료한 후에, “시작 -> 프로그램 -> Omni-NFS Server V4.” 에서 NFS server를 선택 한다.

Step 4. XLink NFS Server 창에서, Action 메뉴 밑의 New Entry 를 선택한다.

Step 5. NFS Server Export 창의 Browse 버튼을 선택하여 NFS로 mount 될 폴더를 선택한다.

주의 *: 1. 사용자는 export 될 폴더의 "Exported Alias" 를 기억하고 있어야 합니다. 이것은 VTS 에서 NFS server 상의 mounting path로 사용 됩니다.*

2. 일반적으로 Linux는 NTFS 파일 시스템을 인식하지 못합니다.
VTS 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

F.3 OpenSSH 패키지의 설치

VTS상의 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 받는다.
Step 2. "setupssh361-20030512.exe" 를 실행 시킨다.
Step 3. command prompt(Dos 창)을 실행 시켜고 OpenSSH 가 설치된 디렉토리로 이동한다,(Program Files\OpenSSH 가 기본 설정입니다,)
Step 4. bin 디렉토리로 이동한다.
Step 5. mkgroup 프로그램을 이용하여 group permissions 파일을 만든다.

```
C:\Program Files\OpenSSH\bin> mkgroup -l >> ..\etc\group
```

Step 6. mkpasswd 프로그램을 이용하여 passwd 파일에 인증된 사용자를 추가 한다. 이 경우 Windows 상의 모든 사용자를 추가 하려면 '-u username' 옵션을 사용하지 말아야 한다.

```
C:\Program Files\OpenSSH\bin> mkpasswd -l >> ..\etc\passwd
```

Step 7. OpenSSH server 를 실행 한다..

```
C:\Program Files\OpenSSH\bin> net start opensshd
```

Step 8. “ pause.exe ” 프로그램을 "Program Files\OpenSSH\bin" directory 에 복사한다.

주의 *: 1. "pause.exe" 프로그램은 세나테크놀로지에서 만든 VTS용 응용프로그램입니다.*
2. 이 프로그램은 server와 client 간의 Encrypted TCP 연결을 유지하는 역할을 합니다,
3. 이 프로그램은 VTS 제품과 같이 제공되는 CD ROM 안에 수록되어 있습니다. 만일 이 프로그램이 없을 경우에는 세나 기술 지원으로 문의 하시기 바랍니다.

F.4 VTS 에서 Encrypted NFS 기능의 설정

NFS server 와 OpenSSH 의 설치를 완료하면 사용자는 VTS의 설정 메뉴 상에서 Encrypted NFS 기능을 설정할 수 있습니다. 설정 절차는 다음과 같습니다.

Step 1. VTS의 Web UI 에 로그인 한다.
Step 2. NFS server configuration 페이지로 이동한다.
Step 3. 각 변수들을 다음과 같이 설정 한다.
NFS service : Enabled
Primary NFS server IP address : *Encrypted NFS server 의 IP address를 적는다.*
Mounting path on primary NFS server : *"Exported Alias" 적는다.*
Primary NFS timeout (sec, 5-3600) : *원하는 임의의 값을 적는다.* (*5sec 가 기본값*)
Enable/Disable encrypted primary NFS server : Enabled
Encrypted primary NFS server user : *Encrypted NFS server 의 사용자 이름을 적는다.*
Encrypted primary NFS server password : *해당 사용자의 password를 적는다.*
Confirm primary NFS server password : *해당 사용자의 password를 다시 적는다.*
Step 4. Save & apply. 를 선택한다.
Step 5. system log 나 port log 의 location을 NFS server로 설정 한다.
Step 6. 테스트한다.

Encrypted NFS를 테스트하려면, 사용자는 LanExplorer나 EtherReal과 같은 이더넷 패킷 캡쳐 프로그램을 사용할 수 있어야 합니다. 일반적인 NFS의 경우에는, 단순한 텍스트 형태에서는 VTS와 NFS 서버간의 모든 전송 데이터를 캡쳐할 수 있습니다. 그러나, Encrypted NFS의 경우에는, 사용자는 CM과 NFS 서버간의 모든 전송 데이터를 캡쳐할 수는 있지만, 암호화된 모든 전송 데이터를 복호화(Decode)할 수는 없습니다.

부록 G: SNMP를 이용한 VTS 관리

G.1 개요

관리자는 NMS(네트워크 관리 시스템) 또는 SNMP 브라우저를 사용하는 SNMP 프로토콜을 통해 VTS를 관리할 수 있습니다. VTS가 NMS 또는 SNMP 브라우저가 실행되고 있는 호스트에 접속을 허용하려면 NMS 또는 SNMP 브라우저를 사용하기 전에, 액세스 제어 설정을 적절히 설정해야 합니다. 그림G-1은 VTS SNMP 에이전트의 MIB-II OID를 브라우징 하고 있는 일반적인 SNMP 브라우저 화면 쇼트를 보여줍니다.

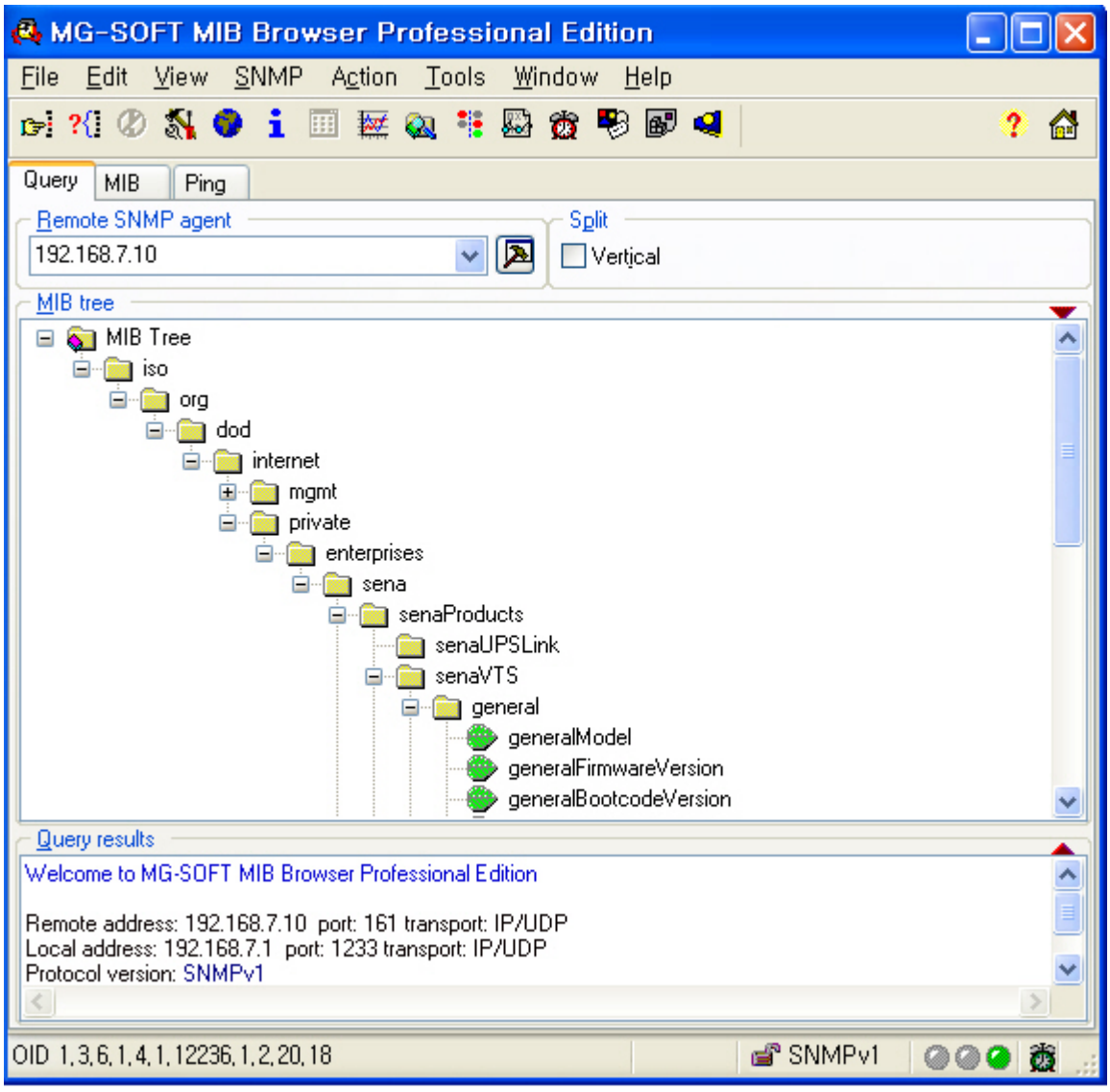


그림 G-1. SNMP 브라우저

G.2 정보 조회

관리자는 SNMP 프로토콜의 Get / Get-Next를 사용하여 VTS의 정보를 조회할 수 있다.

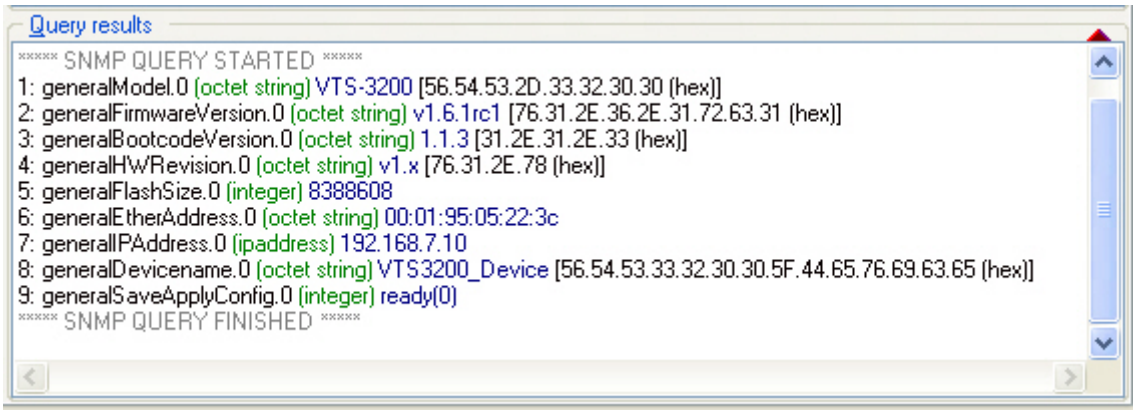


그림 G-2. SNMP를 이용한 정보 조회

G.3 정보 변경

관리자는 SNMP 프로토콜의 Set을 사용하여 VTS의 정보를 변경할 수 있다.

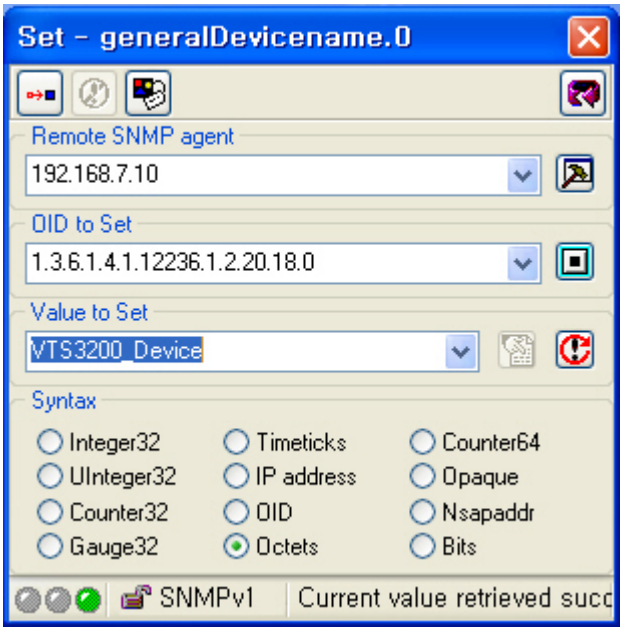


그림 G-3. SNMP를 이용한 정보 변경

G.4 주의사항

- 변경된 정보는 임시로 저장 하기 때문에 정보의 보존을 위해 generalSaveApplyConfig를 save 혹은 saveApply로 변경해야 한다.

- 포트에 처음으로 키워드를 추가할 때는 default-keyword에서 addRow하고 portIndex를 변경하여 사용한다.

- 키워드가 있는 포트에 다른 키워드를 추가할 때는 해당 포트의 키워드에서 addRow하여 추가한다.

- 다른 port에서 addRow한 후에 portIndex를 변경하면 같은 포트에 같은 인덱스를 갖는 키워드가 2개 생성되기 때문에 추가되지 않는다.

- portsResetFactoryDefault와 같이 excute 하는 정보를 MIB-Browser에서 셋팅하는 경우에는 한번에 하나씩 해야 한다.

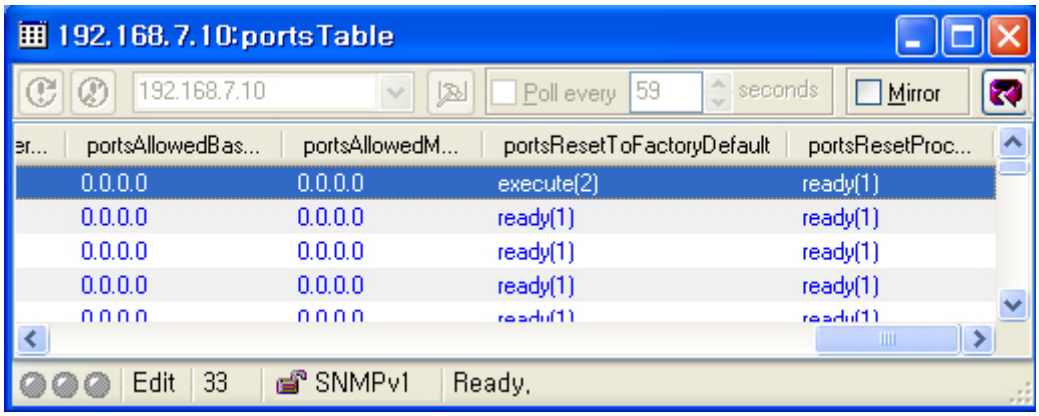


그림 G-4. excute 설정