Secure Terminal Server

STS 시리즈

사용자 설명서

Version 1.3.3

2005-11-08

저작권

등록 상표

HelloDevice™은 세나테크놀로지의 상표입니다.
Windows®는 Microsoft 사의 등록 상표입니다.
Ethernet®은 XEROX 사의 등록 상표입니다.

사용자 공지

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

Revision history

Revision	Date	Name	Description
V1.0.2	**2003-12-3**	**O.J. Jung**	Initial Release
V1.1.0	**2004-01-12**	**O.J. Jung**	펌웨어 v1.1.0에 따른 수정
V1.1.1	**2004-01-30**	**O.J. Jung**	오자 수정
V1.2.0	**2004-06-11**	**O.J. Jung**	펌웨어 v1.2.0 에 따른 수정
V1.3.0	**2004-10-11**	**O.J. Jung**	펌웨어 v1.3.0 에 따른 수정
V1.3.1	**2004-10-15**	**O.J. Jung**	부록 6 추가
V1.3.2	**2005-05-18**	**O.J. Jung**	부록 7 추가 , PC 카드 리스트 수정, DTR/DSR 동작에 관한 설명 수정
V1.3.3	**2005-11-08**	**Hunn Lee**	온도 및 습도 관련 변경

Contents

1. 서론

1.1. 개요

STS 시리즈는 산업표준 Ethernet 네트워크로 귀하의 시리얼 장비를 관리할 수 있게 해주는 범용 터미널 서버(또는 디바이스 서버)입니다. STS 시리즈는 TCP/IP와 UDP와 같은 오픈 네트워크 프로토콜에 기반을 두고 귀하의 시리얼 장비에 최대한의 유연성을 제공할 것입니다. STS 시리즈의 PPPoE(PPP-over-Ethernet) 연결 특성을 사용하면 DSL기반의 광대역 네트워크를 통해서 RS232 시리얼 장비들을 관리할 수 있습니다.

DHCP, PPPoE, 동적 DNS(DDNS: Dynamic DNS) 등의 풍부한 광대역 네트워크 연결 프로토콜을 이용하면 DSL 또는 케이블 모뎀 연결로 광대역 인터넷을 통해 시리얼 장비를 쉽게 관리할 수 있습니다. STS 시리즈에 내장된 동적 DNS 프로토콜을 사용하면 도메인 이름으로 시리얼 장비에 접속할 수 있습니다.

또한 STS 시리즈는 Telnet, 시리얼 콘솔 포트, 또는 웹 등의 다양한 방법으로 시스템 상태 표시, 펌웨어 업그레이드, 원격 리셋, 시스템 로그 표시를 할 수 있는 완벽한 시스템 관리 기능을 제공합니다.

암호 보호 기능의 지원을 받으면서 Telnet이나 시리얼 콘솔 포트를 이용한 상태 감시, 원격 리셋, 에러 로그 감시, 펌웨어 업그레이드 등의 완벽한 관리 기능으로 STS 시리즈를 쉽게 설정하고 관리할 수 있습니다.

안전한 데이터 교환을 요하는 매우 중요한 애플리케이션을 위해, STS 시리즈는 데이터 암호화를 위한 SSLv2, SSLv3, 그리고 TLSv1을 지원합니다. 추가 기능으로, STS 시리즈에 의도하지 않는 데이터가 전송되어 들어오는 것을 막기 위해 IP 주소 필터링 기능이 제공되어 있습니다.

STS 시리즈가 일반적으로 적용되는 분야는 다음과 같습니다.

- 산업 자동화
- 소매/유통(POS)
- 원격 검침 및 디스플레이
- 빌딩 자동화 및 보안 시스템
- 일반 데이터 수집 애플리케이션
- 의학용 애플리케이션

STS 시리즈는 RS232 시리얼 장비를 통해 관리, 감시, 진단, 그리고 데이터 수집을 할 수 있는 이상적인 원격 관리 기능을 제공합니다.

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

1.2. 패키지 체크 리스트

- STS 시리즈 외장 박스
- 110V 또는 230V 전원 코드
- CAT5 케이블
- 콘솔 케이블 키트
- Quick Start Guide
- Serial/IP Com Port Redirector, HelloDevice Manager 유틸리티 및 사용자 설명서를 포함한 CD-ROM

1.3. 제품 사양

	STS800	STS1600
시리얼 인터페이스	8-포트	16-포트
	시리얼 속도 75bps ~ 230Kbps	
	흐름 제어: 하드웨어 RTS/CTS, 소프트웨어 Xon/Xoff	
	RJ45 커넥터	
	신호: RS232 Rx, Tx, RTS, CTS, DTR, DSR, DCD, GND	
	모뎀 제어: DTR/DSR and RTS/CTS	
Network Interface	RJ45 Ethernet 커넥터를 장착한 10/100 Base Ethernet	
	고정 및 유동 IP 주소 지원	
프로토콜	- ARP, IP/ICMP, TCP, UDP, Telnet, SSH v1 & v2, - SSL v2 & v3, TLS v1 - DNS, Dynamic DNS, HTTP, HTTPS, - SMTP with/without Authentication, pop-before SMTP, - DHCP client, NTP, PPPoE, SNMP v1 & v2	
PCMCIA	다음 PC 카드 지원: ATA 플래쉬 메모리 카드 802.11b 무선 랜 카드 10/100 Base-TX 랜 카드 모뎀 카드	
보안	사용자 ID 및 암호	
	HTTPS	
	보안 터미널 인터페이스: SSH	
	데이터 암호화: SSLv2/v3, TLS v1, 3DES 및 RC4	
	IP 주소 필터링	
	SCP	
Modem emulation	AT 명령어 지원	
관리	시리얼 콘솔 포트, telnet, 웹, HelloDevice Manager	
	운영체제 지원: Windows 98/ME/NT/2000/XP	
	시스템 로깅 오류 로그를 자동으로 email 전달	
	시스템 상태 다양한 시스템 상태 표시 기능	
	펌웨어 telnet, 콘솔 또는 웹 인터페이스를 통한 다운로드 가능 기능	
진단 LED	Power Ready 10/100 Base Link, Act 각 포트 : Serial InUse / Rx/ Tx PC 카드	
환경	작동 온도: 0'C ~ 50'C 보관 온도: –20'C ~ 66'C 습도: 90% Non-condensing	
전원	5VDC, 1.5A @ 5VDC	110 ~ 240VAC
크기 **L x W x H (mm)**	245 x 153 x 30 (mm)	432 x 193 x 44.5
	DIN-rail mount option	19 in. rack mountable
무게 (kg)	1.5	2.8

인증	FCC(A), CE(A), MIC
품질 보증 기간	5-year limited warranty

1.4. 용어 및 약어

이 섹션은 본 매뉴얼에서 일반적으로 사용되는 용어를 정의합니다. 이 용어들은 인터넷과 관련이 있으며 STS 시리즈의 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. STS 시리즈의 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 STS 시리즈를 처음 설치하고 설정하는 방법에 대하여 설명합니다

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

2.1.1. STS800 패널 레이아웃

그림 2-1에 보여지는 것처럼 STS800에는 상태 표시를 위한 세 그룹의 LED 지시 램프가 있습니다 (예: System, Ethernet 그리고 Serial Ports). 좌측에 위치한 처음 세 개의 램프는 전원(Power), 준비 상태(Ready) 그리고 PC 카드 인터페이스(PC Card Interface)를 나타냅니다. 그 다음 세 개의 램프는 Ethernet 100Mbps(Ethernet 100Mbps), 링크(Link), 그리고 활동 상태(Act)입니다. 마지막 램프는 시리얼 포트의 수신(Receive)과 전송(Transmit)을 보여줍니다. 표 2-1에서 각 LED 지시 램프의 기능을 설명합니다. 뒤 패널에는 RJ45 커넥터용 시리얼 포트, Ethernet 포트, STS400 콘솔 포트, 그리고 전원 소켓이 보입니다.

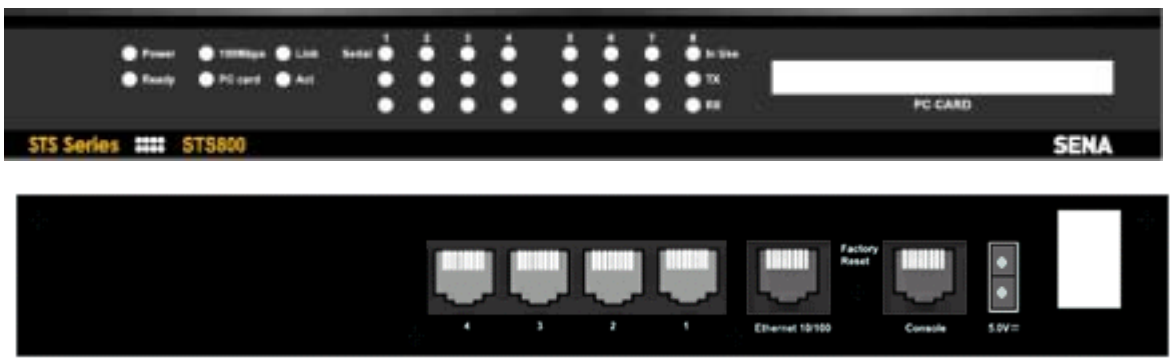


그림 2-1 STS800의 페널 레이아웃

표 2-1 STS 시리즈의 LED 지시 램프

램프		기능
System	**Power**	전원이 공급되면 켜집니다.
	Ready	시스템이 동작할 준비가 되면 켜집니다.
	PC card	PCMCIA 장치가 작동 중이면 켜집니다.
Ethernet	**100Mbps**	100Base-TX 연결이 감지되면 켜집니다.
	LINK	Ethernet 네트워크에 연결되면 켜집니다.
	Act	STS 시리즈 Ethernet 포트를 통해서 패킷이 들어오거나 나가는 것과 같은 활동이 있을 때마다 깜박입니다.
Serial port	**InUse**	시리얼 포트가 사용 중이면 켜집니다
	Rx/Tx	STS 시리즈의 시리얼 포트를 통해서 데이터가 들어오거나 나올 때마다 깜박입니다.

2.1.2. STS1600 Panel Layout

그림 2-2에 보여지는 것처럼 STS1600에는 상태 표시를 위한 세 그룹의 LED 지시 램프가 있습니다 (예: System, Ethernet 그리고 Serial Ports). 좌측에 위치한 처음 세 개의 램프는 전원(Power), 준비 상태(Ready) 그리고 PC 카드 인터페이스(PC Card Interface)를 나타냅니다. 그 다음 세 개의 램프는 Ethernet 100Mbps(Ethernet 100Mbps), 링크(Link), 그리고 활동 상태(Act)입니다. 마지막 램프는 시리얼 포트의 수신(Receive)과 전송(Transmit)을 보여줍니다. 표 2-1에서 각 LED 지시 램프의 기능을 설명합니다.

그림 2-2 STS1600의 패널 레이아웃

2.2. 하드웨어 연결하기

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

- STS 시리즈의 전원 공급 장치를 연결합니다.
- STS 시리즈를 Ethernet 허브 또는 스위치에 연결합니다.
- 해당되는 시리얼 장치에 연결합니다.

2.2.1. 전원에 연결하기

STS 시리즈에 전원 케이블을 연결합니다. 전원이 적절히 공급된 경우 [Power] 표시등이 초록색으로 점등 상태를 유지합니다.

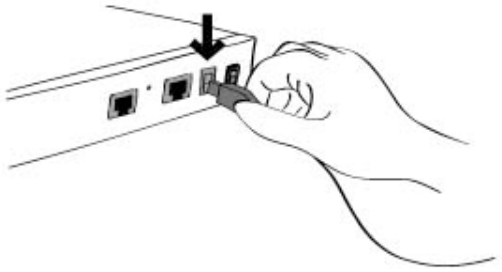


그림 2-3 STS800에 전원 연결하기

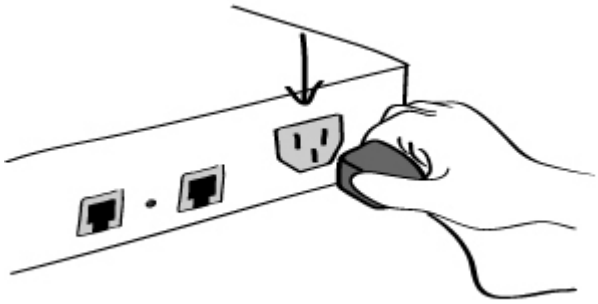


그림 2-4 STS1600에 전원 연결하기

2.2.2. 네트워크에 연결하기

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

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

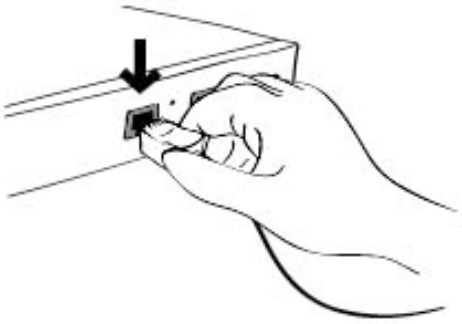


그림 2-5 STS800/1600에 네트워크 케이블 연결하기

2.2.3. 해당 장치에 연결하기

STS 시리즈의 시리얼 포트에 콘솔 케이블을 연결합니다. 사용자가 장치의 콘솔 포트에 연결하려면 장치 자체에서 제공한 콘솔 포트의 유형을 고려할 필요가 있습니다. STS 시리즈케이블 키트 패키지 내의 플러그-인 어댑터들은 사용자 장치에 맞는 케이블 형태를 지원하기 위해 제공됩니다. 자세한 내용은 *부록 1. 연결* 부분을 참조하십시오.

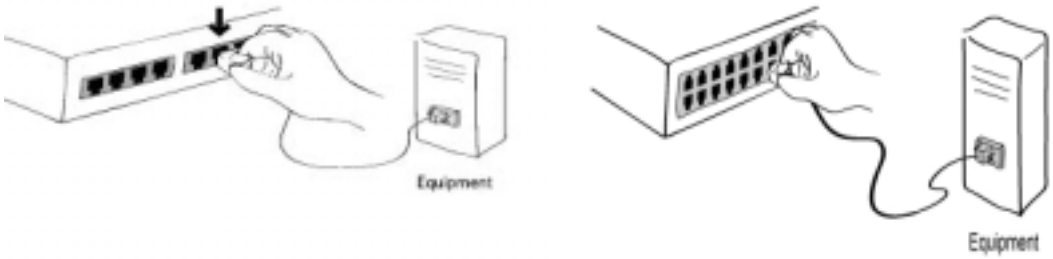


그림 2-6 장비를 STS800(왼쪽) / STS1600(오른쪽)에 연결하기

2.2.4. 시스템 콘솔에 접속하기

STS 시리즈에 접속하는 방법은 여러 가지가 있습니다. 이는, 사용자의 위치가 현지 또는 원격이냐 여부에 따라 달라집니다. 또한, STS 시리즈는 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 STS 시리즈의 시스템 콘솔 포트에 직접 연결할 수 있습니다.

- 원격 콘솔:

텍스트 메뉴 인터페이스를 요구하는 원격 사용자는 터미널 에뮬레이터를 사용해 STS 시리즈의 telnet(TCP 포트 23)에 접속할 수 있습니다.

- 웹:

웹 브라우저를 사용하여 STS 시리즈를 설정하려는 원격 사용자는 Internet Explorer 또는 Netscape Navigator와 같은 웹 브라우저를 사용하여 STS 시리즈에 연결할 수 있습니다.

위의 방법들은 모두 SUPER 시리즈시스템으로의 로그인을 요구합니다.

2.2.5. 시스템 콘솔 사용하기

1) 콘솔/Ethernet 케이블의 한쪽 끝을 STS 시리즈의 콘솔 포트에 연결합니다.

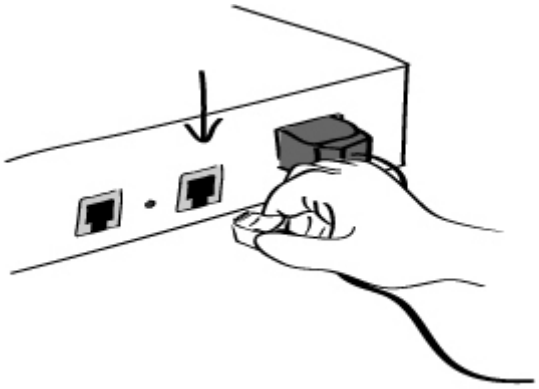


그림 2-7 STS 시리즈에 콘솔 케이블 연결하기

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**
   - **Data bits 8**
   - **Parity None**
   - **Stop bits 1**
   - **No flow control**
5) [ENTER] 키를 누릅니다.
6) 사용자 이름과 비밀 번호를 입력하고 STS 시리즈에 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:~#
```

7) CLI를 이용하여 초기 설정을 할 수 있습니다. CLI에 대한 자세한 내용은 8장 CLI 안내서를 참조하십시오.

8) 기본 인터페이스가 텍스트 메뉴로 설정된 경우에 “ss.edit” 명령어를 실행하면, *그림 2-8* 에 있는 메뉴 화면이 나타납니다.

```
root@192.168.161.5:~#ss.edit

--------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 08/22/2003 21:52:36     F/W REV.: v1.0.1
 Serial No.: STS800438349-42944        MAC address: 00-01-95-04-19-5a
 IP mode: DHCP                         IP address: 192.168.14.7
--------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
 ----->
```

그림 2-8 메인 메뉴 화면 (STS800)

메인 메뉴 화면의 사용자는 메뉴 번호를 입력하거나 [ENTER] 키를 눌러 STS 시리즈 파라미터 설정에 필요한 메뉴 항목을 선택할 수 있습니다. 하위 메뉴 화면에 있는 사용자는 온라인 설명을 통해 제공된 필수 파라미터를 설정할 수 있습니다. 모든 파라미터는 STS 시리즈의 비휘발성 메모리 공간에 저장되며, 이는 사용자가 *메뉴 5. Save Changes*을 선택하여 저장할 수 있습니다. *메뉴 7. Exit and Apply Changes* 또는 *8. Exit and Reboot* 을 선택한 다음 모든 변경 사항을 설정할 수 있습니다.

2.2.6. 원격 콘솔 사용하기

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

원격 콘솔 기능은 원격 호스트 접속 옵션에서 disable 될 수 있습니다.(자세한 내용은 섹션

3.5의 *IP 필터링* 을 참조하십시오).

The following instructions will assist in setting up the Remote Console functionality:

1) Telnet프로그램 또는 telnet기능(예, TeraTerm-Pro 또는 Hyper Terminal)을 지원하는 프로그램을 실행시킵니다. 목적지 IP 주소 및 port number는 STS 시리즈와 동일해야 합니다. 필요한 경우, port number를 23으로 지정합니다. 사용자 컴퓨터 명령 라인 인터페이스에 다음 명령어를 입력합니다.

   ```
   telnet 192.168.161.5
   ```

   또는 다음 파라미터를 갖는 telnet 프로그램을 실행시킵니다.

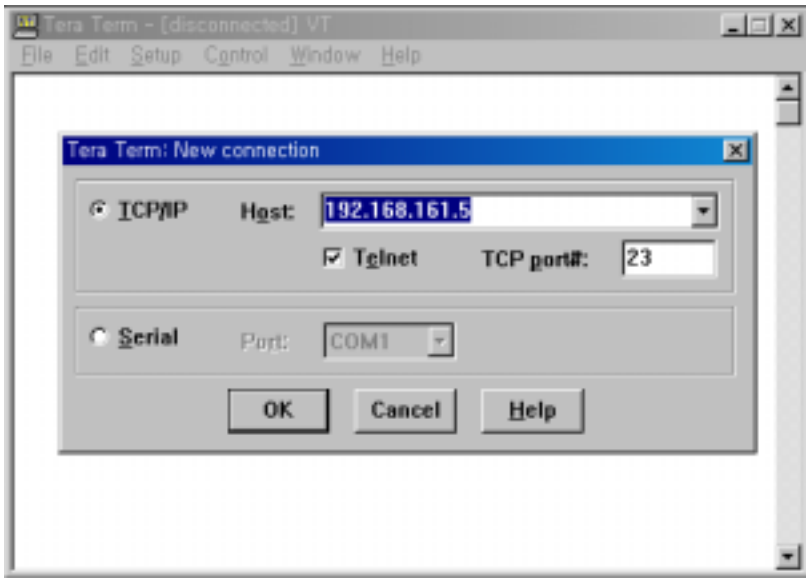


그림 2-9 Telnet 프로그램 설정 예제 (TeraTerm Pro)

2) 사용자는 반드시 STS 시리즈로 로그인해야 하며, 이때 사용자 이름과 암호를 입력합니다. 사용자 이름 및 암호의 디폴트 설정은 시스템 root를 위한 **root** 및 시스템 관리자를 위한 **admin** 두 가지입니다
3) STS 시리즈가 승인한 경우, CLI 프롬프트 또는 텍스트 메뉴 화면이 나타납니다.

2.3. 웹 브라우저 관리 인터페이스에 접속하기

STS 시리즈는 HTTP와 HTTPS(HTTP over SSL) 프로토콜을 모두 지원합니다. 또한 STS 시리즈는 자체 웹 관리 페이지를 제공합니다. STS 시리즈 웹 관리 페이지에 접속하려면, STS 시리즈의

IP주소나 주소 분석이 가능한 호스트 명을 웹 브라우저의 URL/Location 필드에 입력하십시오 . 그러면 사용자는 STS 시리즈의 로그인 화면을 보게 될 것입니다. 사용자는 반드시 올바른 사용자 명과 암호를 사용하여 시스템에 로그인 함으로써 본인임을 인증해야 합니다. 초기 환경 설정은 다음과 같습니다.

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

주의: 사용자께서는 STS 시리즈 웹 관리 페이지에 접속하기 전에 반드시 STS 시리즈의 IP주소(또는 주소 분석 가능 호스트명)와 서브넷 마스크 설정을 검사하시기 바랍니다.

그림 2-10 STS 시리즈 웹 관리의 로그인 화면

그림 2-100 는 STS 시리즈 웹 관리의 로그인 화면입니다. 이 화면에서 사용자는 로그인 후에 이동하고자 하는 페이지를 선택할 수 있습니다. 사용자가 환경 설정 페이지(Configuration page)를 선택하면, 그림 2-18에 보이는 STS 시리즈 웹 관리 인터페이스의 환경설정 홈페이지를 볼 수 있습니다.

*그림 2-111*는 STS 시리즈 웹 관리 인터페이스의 환경설정 홈페이지입니다. 화면의 좌측에 메뉴 바가 제공됩니다. 이 메뉴 바에는 최상위 환경설정 메뉴 그룹이 포함됩니다. 메뉴 바에서 한 항목을 선택하면 각 그룹에서 사용 가능한 모든 하위 메뉴가 트리 형태로 나타납니다. 사용자는 하위 메뉴 항목을 선택해서 해당 항목에 대한 파라미터 설정을 변경할 수 있습니다. 사용자는 모든 페이지에서 변경 사항을 [플래시에 저장(Save to flash)], [저장 및 적용(Save & apply)] 또는 [취소(Cancel)]할 수 있습니다. 사용자는 환경 파라미터값을 변경한 후에 반드시 [플래시에 저장(Save to Flash)]을 선택하여 변경된 파라미터 값을 비휘발성 기억장치에 저장해야 합니다. 모든 변경사항을 적용하기 위해서 사용자는 반드시 [변경사항 적용(Apply Changes)]을 선택해야 합니다. 이 옵션은 메뉴 바의 아래 부분에 있습니다. 사용자가 [변경사항 적용(Apply Changes)]을 선택했을 때에만 새 파라미터 값이 STS 시리즈 환경설정에 적용됩니다. 또한 사용자는 한번에 파라미터를 저장하고 변경사항을 적용하기 위해 [저장 및 적용(Save & Apply)]을 선택할 수 있습니다.

사용자가 새 파라미터 값을 원하지 않는다면 [취소(Cancel)]을 선택해야 합니다. 이렇게 하면 모든 변경사항이 취소되고 이전 값으로 복구됩니다.

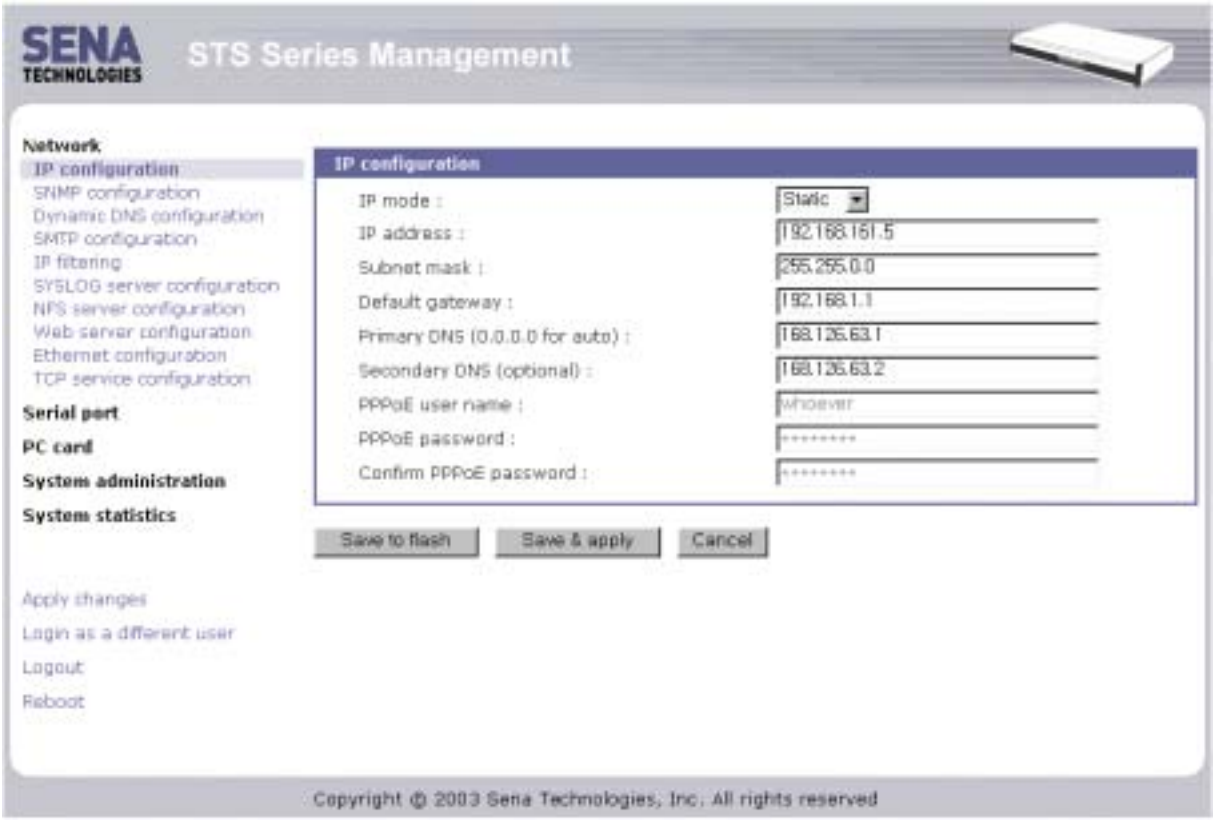


그림 2-11 STS 시리즈 웹 관리 화면

3. 네트워크 설정

3.1. IP 설정

사용자 네트워크 환경에서 STS 시리즈를 사용하려면, 유효한 IP 주소가 필요합니다. IP 주소가 준비되지 않은 경우, 시스템 관리자에게 문의하여 STS 시리즈를 위한 유효한 IP 주소를 할당 받습니다. 네트워크에 STS 시리즈를 연결하려면, 고유 IP 주소가 있어야 한다는 사실을 명심해야 합니다.

STS 시리즈 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)

The STS Series is initially defaulted to **STATIC** mode, with a static IP address of **192.168.161.5**. *표 3-1* shows the configuration parameters for all three IP configurations. *그림 3-1* shows the actual web-based GUI to change the user's IP configuration.

표 3-1 IP 설정 파라미터

Static IP	IP address
	Subnet mask
	Default gateway
	Primary DNS/ Secondary DNS
DHCP	Primary DNS/ Secondary DNS (Optional)
PPPoE	PPPoE Username
	PPPoE Password
	Primary DNS/ Secondary DNS (Optional)

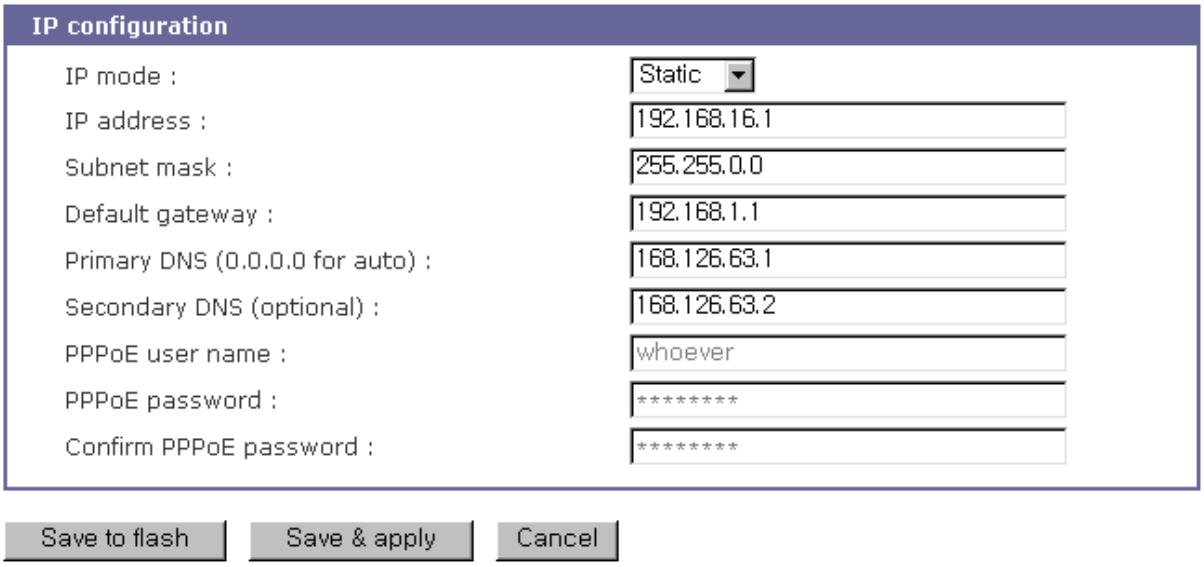


그림 3-1 IP 설정

3.1.1. Static IP 주소 사용하기

사용자가 **static IP** 주소를 사용할 경우, STS 시리즈의 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: STS 시리즈는 시스템이 시작될 때, 설정된 정보에 따라 네트워크를 초기화 합니다.

- **IP address**

Static IP는 고정적이면서 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. STS 시리즈 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 STS 시리즈 시리즈는 패킷이 지정한 TCP/IP 호스트가 로컬 네트워크 영역에 있는지 서브넷 마스크를 통해 확인합니다. 주소가 STS 시리즈와 동일한 네트워크 영역에 있다면, 물리적인 주소(Physical address)를 통해서 직접

연결됩니다. 그렇지 않으면 주어진 기본 게이트웨이를 통해 연결됩니다.

- **Default gateway**

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 STS 시리즈가 기본 게이트웨이 컴퓨터의 IP 주소를 알아야 합니다. 게이트웨이의 IP 주소에 대한 정확한 정보는 네트워크 관리자에게 문의하십시오.

- **Primary and Secondary 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.

STS 시리즈 시리즈의 DNS 기능을 사용하려면 도메인 네임으로 호스트에 접속할 수 있도록 이 DNS 서버의 IP 주소를 설정해야 합니다. STS 시리즈 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 네트워크에서 중앙 관리하고 자동화할 수 있게 하는 통신 프로토콜입니다. DHCP는 네트워크 관리자가 IP 주소를 중심점에서 감독하고 분배하도록 하며 컴퓨터가 다른 네트워크 위치에 플러그인 된 경우 새로운 IP 주소를 자동으로 전송되도록 합니다.

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

DHCP를 사용하도록 설정되었을 경우, STS 시리즈는 시스템이 시작 될때마다, 네트워크 상에 DHCP 요청을 발송합니다. DHCP 서버의 응답에는 IP 주소를 비롯하여 서브넷 마스크, 게이트웨이 주소, DNS 서버 및 “대여” 시간이 포함되어 있습니다. STS 시리즈는 즉시 이런 정보를 자체 메모리에 저장합니다. “대여”가 만료되는 경우, STS 시리즈는 DHCP 서버로부터 ”대여”

시간의 연장을 요청합니다. DHCP 서버가 대여 연장을 승인할 경우, STS 시리즈는 계속해서 현재 IP 주소로 작동할 수 있습니다. DHCP 서버가 대여 연장을 승인하지 않는 경우, STS 시리즈는 DHCP 서버로부터 새로운 IP 주소 요청 절차를 시작합니다.

참고: DHCP 모드에서 DNS 서버를 포함한 모든 네트워크 관련 STS 시리즈 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 STS 시리즈가 작동될 때마다 다른 IP 주소를 수신합니다. DHCP 서버에서 IP 주소를 예약하여 사용자가 새롭게 할당된 STS 시리즈 주소를 항상 인식할 수 있도록 보장해야 합니다. DHCP 네트워크에서 IP 주소를 예약하려면 관리자는 STS 시리즈의 하단 부분에 있는 라벨 스티커에 있는 STS 시리즈의 MAC 주소를 알아야 합니다.

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 STS 시리즈를 사용하려면 사용자는 PPPoE 계정 및 ADSL 모뎀과 같은 PPPoE 접속용 장비가 있어야 합니다. STS 시리즈는 PPPoE 프로토콜을 지원하기 때문에 ADSL 연결을 통해 인터넷 상의 원격 호스트에 접속할 수 있습니다. 사용자는 STS 시리즈에 대한 PPPoE 계정의 사용자 이름 및 암호를 설정해야만 합니다.

시동될 때마다 STS 시리즈는 PPPoE 서버와 PPPoE 연결을 시작합니다. 연결을 시작하는 동안 STS 시리즈는 IP 주소, 게이트웨이, 서브넷 마스크 및 DNS 서버와 같은 인터넷 연결에 필요한 정보를 수신합니다. 연결이 되면 STS 시리즈는 연결을 가능한 한 오래 유지하려 합니다. 연결이 종료되면 STS 시리즈는 새로운 연결을 요청하여 새로운 PPPoE 연결을 시도합니다.

참고: PPPoE 모드에서는 DNS 서버를 포함한 STS 시리즈의 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 Configurations

STS 시리즈는 SNMP v1 및 v2 프로토콜을 지원하는 SNMP(Simple Network Management Protocol) 에이전트 기능을 내장하고 있습니다. NMS 또는 SNMP 브라우저와 같은 네트워크 관리자를 이용하여 STS 시리즈에 접속할 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.

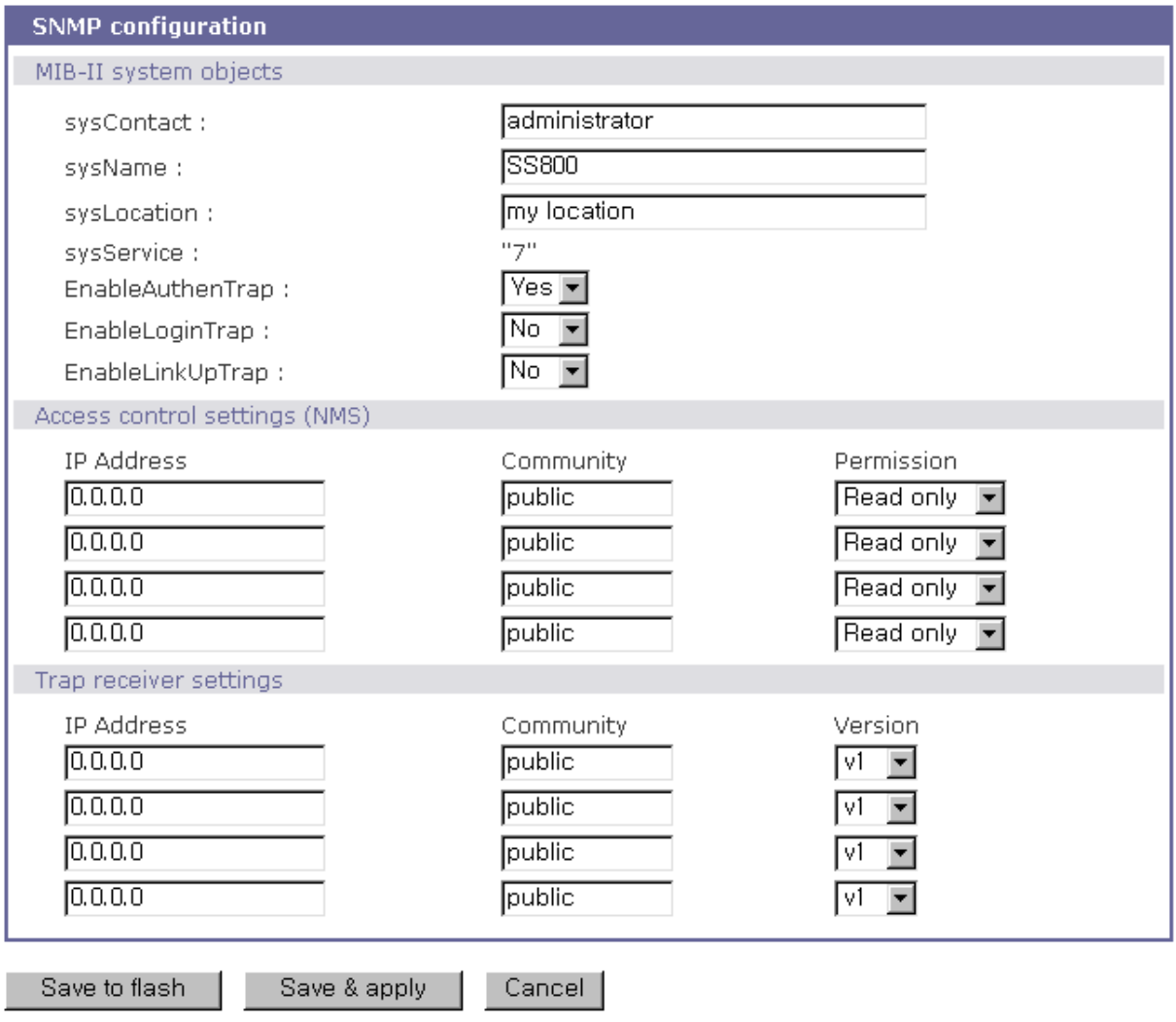


그림 3-2 SNMP 설정

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

MIB-II 시스템 객체 설정을 통해 시스템 연락, 이름, 위치 및 STS 시리즈의 SNMP 에이전트가 사용하는 인증 실패 정보(Authentication-failure traps)를 설정할 수 있습니다. 이러한 설정은 MIB-II sysName, sysContact, sysLocation, sysService 그리고 enableAuthenTrap 객체 식별 정보(OID)가 사용하는 값을 제공해 줍니다.

각 OID의 간단한 설명은 다음과 같습니다.

- sysContact: 관리 시스템(STS 시리즈)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 STS 시리즈는 응용 프로그램(7) 레벨만을 지원합니다.
- 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.
- EnableLinkUpTraps: SNMP 에이전트 프로세스가 Ethernet 연결이 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 STS 시리즈 SNMP 에이전트에 대한 관리자의 접속 허용 여부를 정의하고 있습니다. 이 메뉴 상에 설정된 관리자만이 STS 시리즈 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 STS 시리즈 SNMP 에이전트에 접속할 수 있습니다.

3.2.3. 트랩 수신기 설정(Trap receiver settings)

트랩 수신기는 STS 시리즈 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 STS 시리즈를 관리할 수 있습니다. STS 시리즈가 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 STS 시리즈 SNMP 에이전트의 MIB-II OID를 브라우징 하고 있는 일반적인 SNMP 브라우저 화면을 보여줍니다.

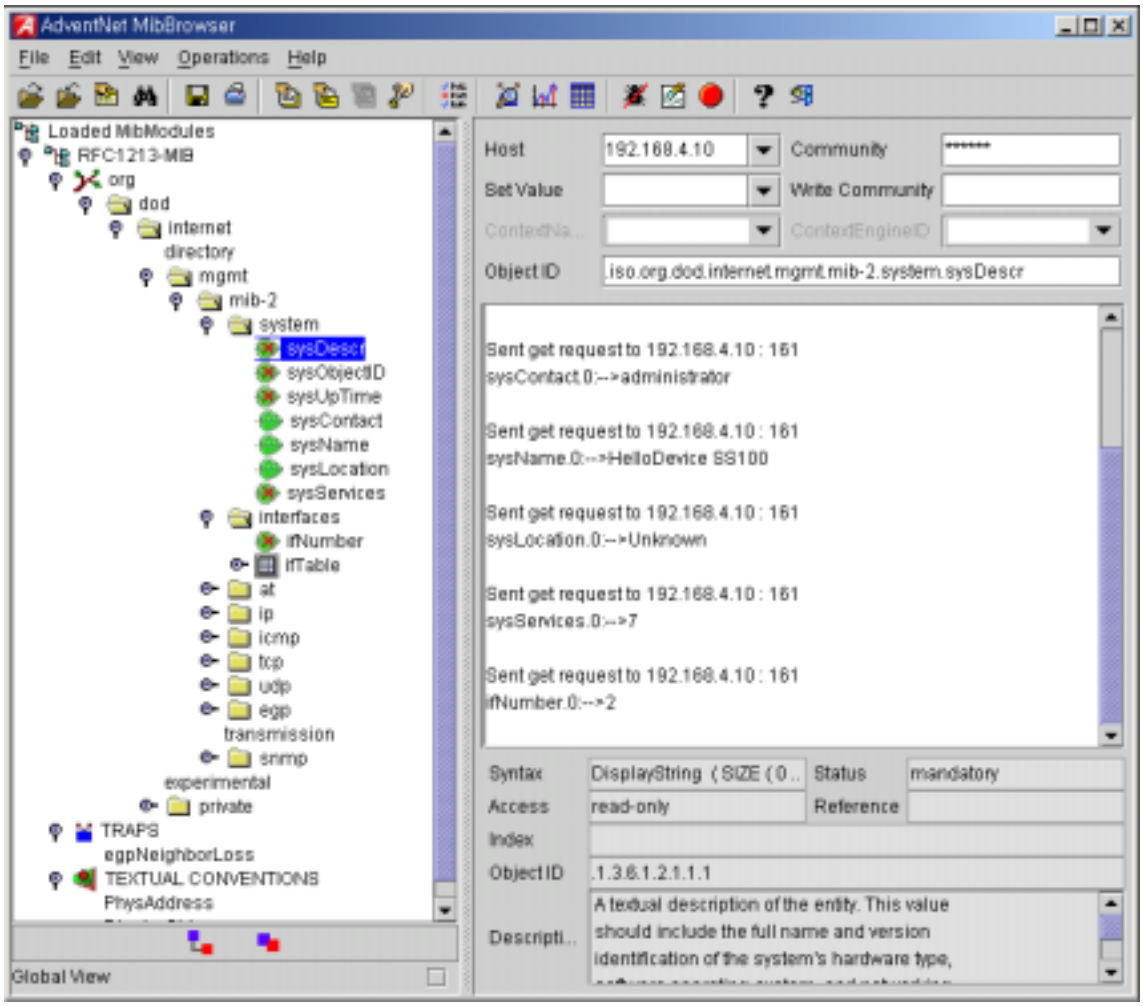


그림 3-3 SNMP 브라우저를 사용한 STS 시리즈 SNMP 에이전트의 MIB-II OID 브라우징 (AdventNet MIB브라우저)

3.3. 동적 DNS(Dynamic DNS) 설정

사용자가 STS 시리즈를 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 서비스이며, 여러 ISP 또는 단체에서 제공합니다. 동적 DNS 서비스를 사용함으로써, 사용자는 IP 주소의 변경에 상관없이 동적 DNS 서버에 등록된 호스트 이름을 통해 STS 시리즈에 접속할 수 있습니다.

일반적으로, STS 시리즈는 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 STS 시리즈에 접속할 수 있습니다

*그림 3-4*는 동적 DNS 설정 웹 인터페이스를 보여줍니다.

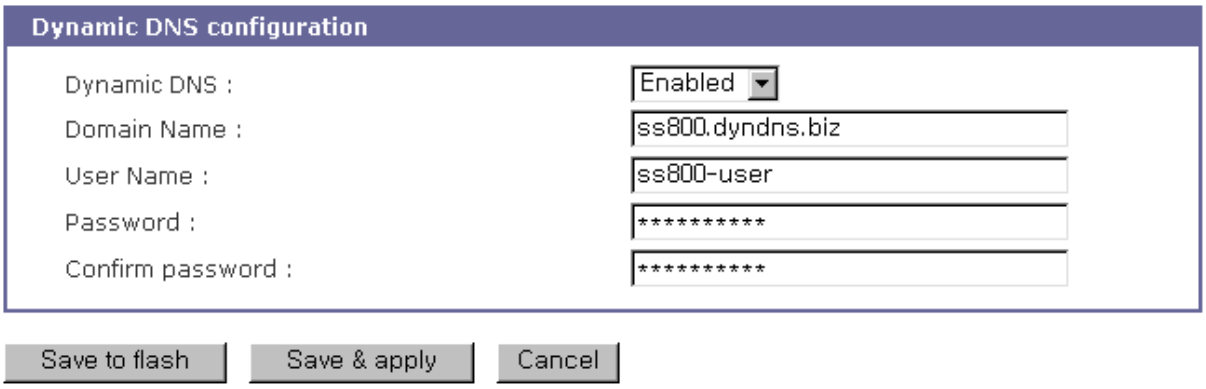


그림 3-4 동적 DNS 설정

3.4. SMTP 설정

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

- 인증이 없는 SMTP
- 인증이 있는 SMTP
- POP-before-SMTP

*그림 3-6.*은 SMTP 모드 선택을 하는 설정 화면입니다.
각 SMTP 설정에서 필요한 파라미터는 다음과 같습니다.

- SMTP server IP address
- SMTP user name
- SMTP user password
- Device mail address

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

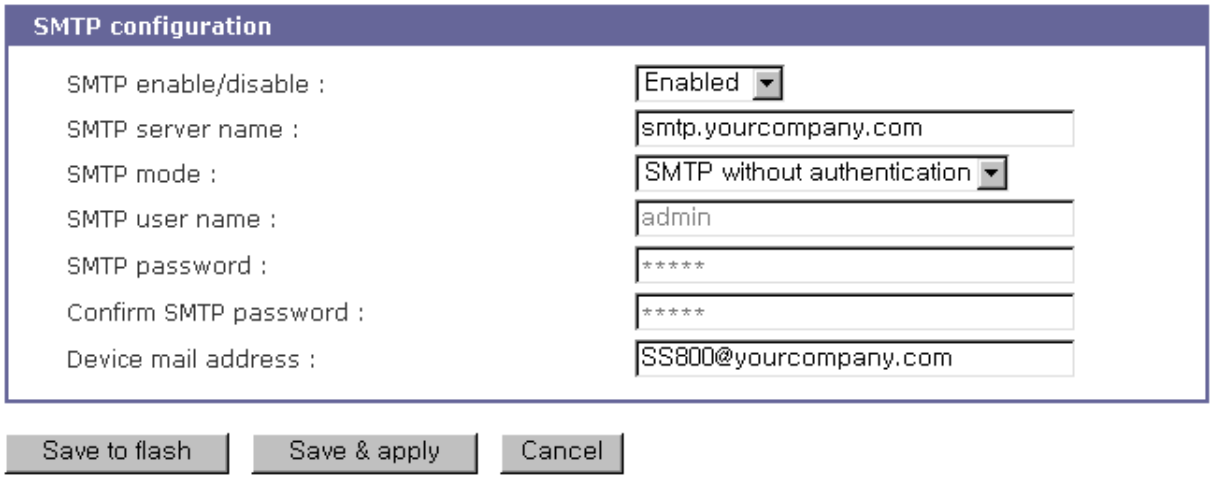


그림 3-5 SMTP 설정

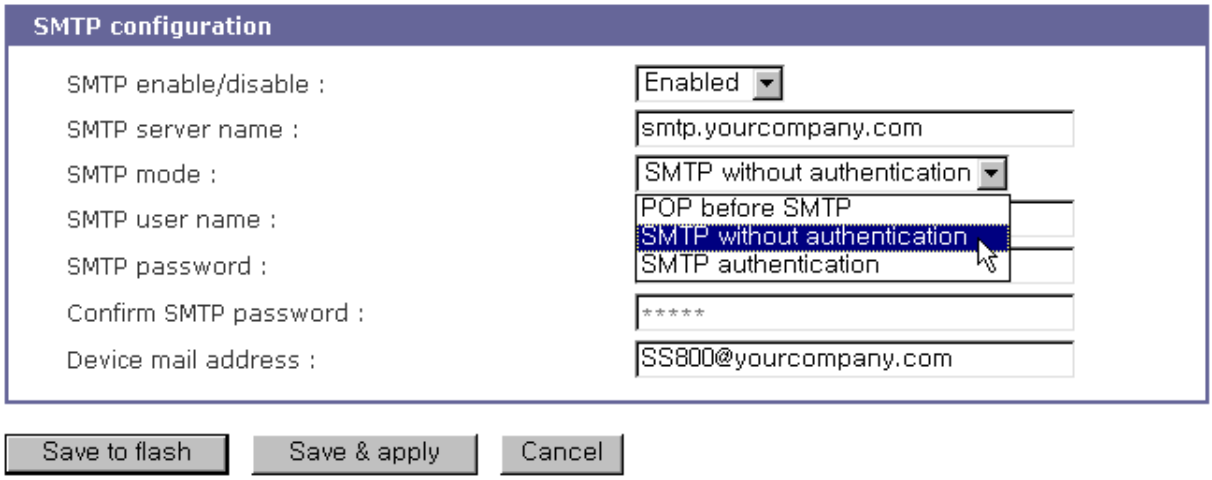


그림 3-6 SMTP 설정에서 SMTP 모드 선택

3.5. IP 필터링

STS 시리즈는 IP 주소 기반 필터링 규칙이나 관리 웹을 이용하여 승인 권한이 없는 호스트가 STS 시리즈에 접근하는 것을 막을 수 있습니다. 사용자는 파라미터의 설정을 수정함으로써 다음과 같은 규칙을 만들 수 있습니다.

- 특정 IP 주소를 가진 호스트만이 STS 시리즈에 접근할 수 있다.
- 특정 서브넷에 있는 호스트만이 STS 시리즈에 접근할 수 있다.
- 모든 호스트가 STS 시리즈에 접근할 수 있다.

Telnet 콘솔, SSH 콘솔 또는 웹 서버에 접근을 제한하기 위해서 IP 필터링 규칙을 접근허용(enabled) 또는 접근제한(disabled)으로 만들 수 있습니다. 공장 출하 시 IP 필터링 규칙은 “접근허용(Enabled)” 상태로 되어 있습니다.

사용자는 STS 시리즈를 설정할 수 있는 호스트나 호스트의 그룹을 만들 수 있습니다. 그러나, 사용자는 반드시 접근이 허용된 IP 주소와 서브넷을 입력해야만 합니다. 원격 호스트상의 모든 사용자는 STS 시리즈에 접근하기 위해서 반드시 입력된 서브넷의 범위 안에 있어야만 합니다.

특정 호스만이 STS 시리즈에 접근하도록 규칙을 변경하려면, 특정 호스트의 IP 주소와 255.255.255.255로 서브넷을 입력해야만 합니다.

모든 호스트가 STS 시리즈에 접근하도록 규칙을 변경하려면, IP 주소와 서브넷을 모두 0.0.0.0으로 설정합니다. 자세한 사항은 표 3-2를 참조하세요. 설정에 대한 원격 호스트의 상태는 “Any(모든 호스트)”로 되어 있습니다.

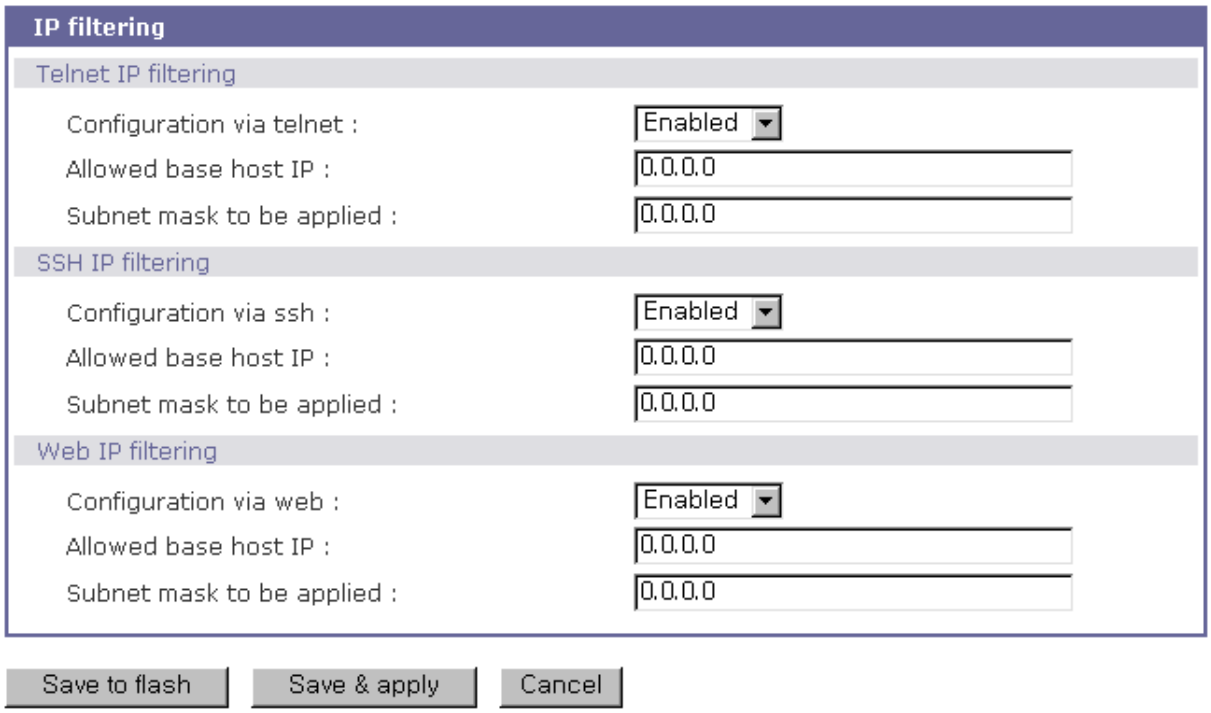


그림 3-7 IP 필터링 설정

표 3-2 허용된 원격 호스트들의 입력예

Allowable Hosts	Input format	
	Base Host IP address	Subnet mask
Any host	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

웹 또한 접근 제한을 위해서 “Enabled”과 ” Disabled”의 IP 필터링 기능을 사용합니다. 제품 출하시 기본값은 “Enabled” 입니다. “접근허용(Enabled)” 상태에서 사용자는 설정하기 위해서 STS 시리즈에 접근하는 특정 웹 호스트(들)를 지정할 수 있습니다.

3.6. SYSLOG 서버 설정

STS 시리즈는 원격 메시지 로깅 서비스, 시스템 및 포트 데이터 로깅을 위한 SYSLOG service를 지원합니다. 원격 SYSLOG service를 사용하려면, 사용자는 SYSLOG 서버의 IP주소와 사용할 facility를 반드시 지정해야 합니다. 그림 3-8은 웹 인터페이스의 SYSLOG server configuration 화면을 보여줍니다.

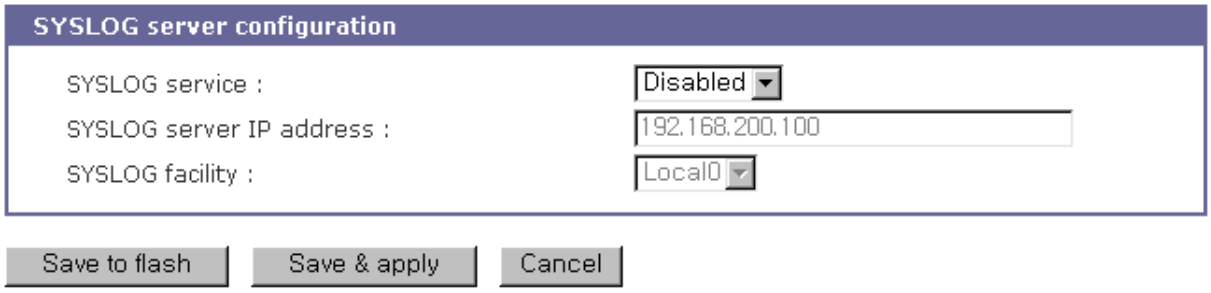


그림 3-8 SYSLOG 서버 설정

로그 메시지를 STS 시리즈로부터 수신하려면 STS 시리즈 설정에서 지정된 SYSLOG 서버는 “remote reception allowed ” 으로 설정되어야 합니다. STS 시리즈 및 SYSLOG 서버 사이에 방화벽이 있는 경우, 사용자는 나가고 들어오는 UDP 패킷이 자유롭게 이동할 수 있는 규칙을 반드시 추가해야 합니다.

STS 시리즈는 local0 에서 local7까지 SYSLOG Facility들을 지원합니다. 사용자는 이러한 Facility들을 사용하여, SYSLOG 메시지의 형태로 STS 시리즈 메시지를 저장할 수 있습니다.

SYSLOG service가 가능한 상태에 있고 SYSLOG 서버 설정이 적절히 설정된 경우에만, 사용자는 STS 시리즈 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 ***4.3.10 포트 로깅*** 및 ***6.2 시스템 로그 설정*** 을 참조하십시오.

3.7. NFS 서버 설정

STS 시리즈는 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.

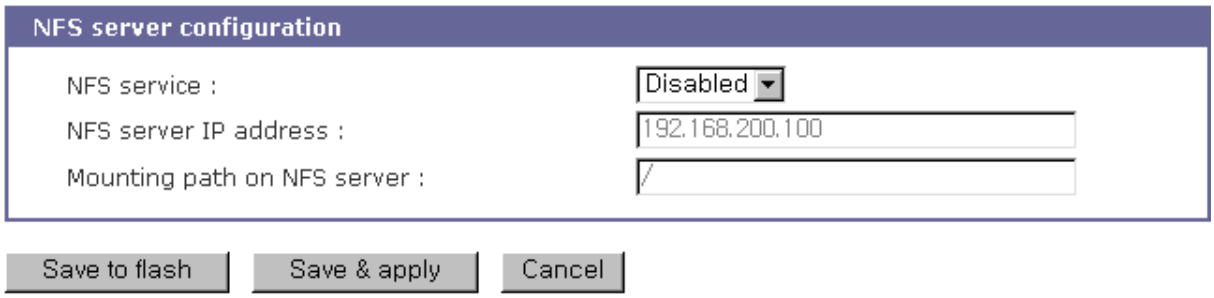


그림 3-9 NFS 서버 설정

STS 시리즈 로그 데이터를 NFS 서버에 저장하려면, STS 시리즈 설정에 지정된 NFS 서버를 “ read and write allowed ” 으로 설정해야 합니다. STS 시리즈 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 경우에만, 사용자는 STS 시리즈의 시스템 로그 또는 포트 데이터 로그로 NFS 서버로 저장할 수 있습니다. 포트/시스템 로그 저장 위치에 대한 자세한 정보는 *4.2.110* ***포트 로깅*** 및 *6.2* ***시스템 로깅*** 섹션을 참조하십시오.

3.8. Ethernet 설정

STS 시리즈는 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, STS 시리즈가 네트워크 환경에서 동작하지 않을 수 있습니다.

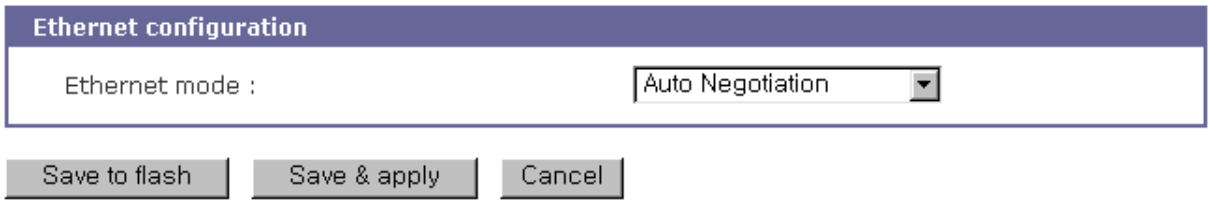


그림 3-10 Ethernet 모드 설정

3.9. Web server configuration

STS 시리즈의 웹 서버는 HTTP 및 HTTPS(HTTP Over SSL) 서비스를 모두 지원합니다. 사용자는 각각 개별적으로 Enabled 또는 Disabled로 설정할 수 있습니다. 그림 3-11은 웹 서버 설정 페이지를 보여줍니다.

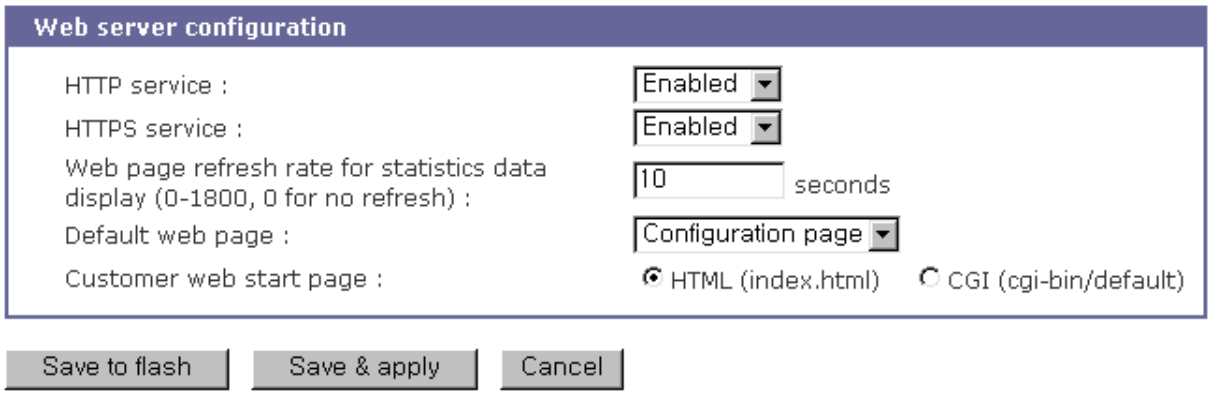


그림 3-11 웹 서버 설정

본 설정 페이지에서 웹 페이지 업데이트 주기(web page refresh rate)는 조정될 수 있습니다. 업데이트 주기는 시리얼 포트 연결 페이지와 네트워크 인터페이스, 시리얼 포트, IP, ICMP, TCP 및 UDP와 같은 시스템 상태 페이지에 적용됩니다. 그 외의 웹 페이지에서는 자동으로 새로고침(Refresh)이 적용 되지 않습니다. 자세한 내용은 섹션 ***7. 시스템 통계***를 참조하십시오..

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

STS 시리즈로 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, STS 시리즈는 데이터가 통신이 없는 상태부터 15 초가 지난 후 5 초 간격으로 3 회 keepalive 패킷을 전송합니다.

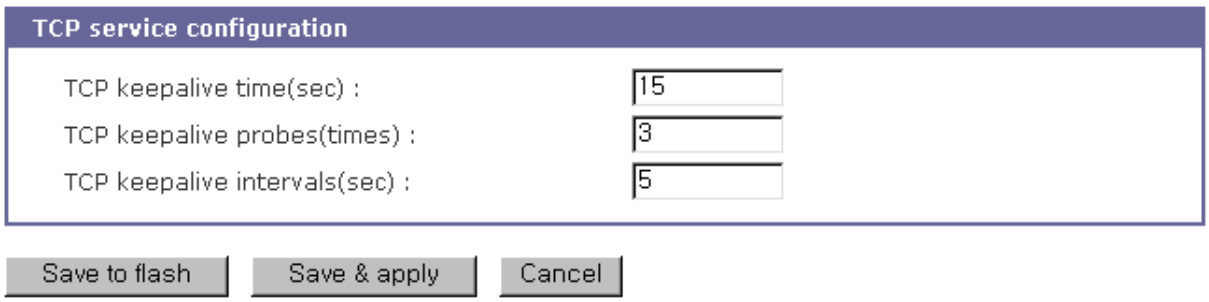


그림 3-12 TCP keep-alive 설정

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.

- **TCP** :
  TCP를 통해서 받은 데이터를 해당하는 시리얼 장치로 내보내고, 시리얼 장치를 통해서 받은 데이터를 TCP를 통해서 내보냅니다. TCP 서버, TCP 클라이언트, TCP 서버 및 클라이언트 모드로 작동될 수 있습니다. 또한 다수의 연결을 통해서 시리얼 장치에 데이터를 보내거나 데이터를 받아오는 것도 가능합니다.
- **UDP** :
  UDP 모드 동작은 UDP 프로토콜에 기반 하였다는 점을 제외하고 TCP 모드 동작과 같습니다.
- **Modem emulation** :
  이 모드는 AT 명령어를 사용하길 원하는 사용자나 기존에 시리얼 장치가 모뎀 AT 명령어를 지원하고 있을 때 선택할 수 있습니다.

port logging 기능으로, 시리얼 포트를 통해 전송되는 데이터를 **MEMORY, SYSLOG server, NFS server** 또는 PC 카드 슬롯을 통해서 **ATA/IDE fixed disk card**에 저장 할 수 있습니다. **port event** 기능으로, 사용자는 포트 별로 키워드 메시지들을 등록할 수 있으며, 이때 STS 시리즈는 시리얼 장치로부터 키워드 메시지들을 받게 되면, 시리얼 장치에 미리 설정되어 있는 메시지를 보내고, email 또는 SNMP trap 을 통해 관리자에게 통보하게 할 수 있습니다. 이를 통해 사용자는 연결된 장치로부터의 메시지를 감시할 수 있습니다.

MEMORY에 저장된 로그 데이터는 STS 시리즈에 전원이 꺼지는 순간 지워지기 때문에, 시리얼 포트 로그 데이터를 보존하기 위해서는 **SYSLOG server, NFS server** 또는 또는 PC 카드 슬롯을 통해서 **ATA/IDE fixed disk card**를 사용하셔야 합니다.

시리얼 포트는 개별적으로 또는 한꺼번에 모두 설정할 수 있습니다. 표 4-1은 시리얼 포트 설정과 관련한 설정 파라미터를 요약하고 있습니다.

표 4-1 시리얼 포트 설정 파라미터

All serial ports setting **Or** **Individual serial port setting #1~#8(1/4)**	Port Enable/Disable		
	Port title		
	Apply all port settings (Individual serial port setting only)		
	Host mode	**TCP**	TCP listening port
			Telnet protocol
			Max allowed connection
			Cyclic connection
			Inactivity timeout (0 for unlimited)
		UDP	UDP listening port
			Max allowed connection
			Accept UDP datagram from unlisted remote host or not
			Send to recent unlisted remote host or not
			Inactivity timeout (0 for unlimited)
		Modem emulation	
	Remote host[1]	Add or Edit a remote host[2] Primary host address Primary host port Secondary host address Secondary host port	
		Remove a remote host	
	Port IP filtering[3]	Allowed host IP	
		Subnet mask to be applied	
	Cryptography[4]	Encryption method None/SSLv2/SSLv3/SSLv3 rollback to v2/ TLSv1/3DES/RC4	
		Cipher suite selection	
		Verify client (server mode only)	
		Verify certificate chain depth	
		Check the certificate CN	
	Serial Port Parameters	Type	
		Baud rate	
		Data bits	
		Parity	
		Stop bits	
		Flow control	
		DTR behavior	
		DSR behavior	
		Inter-character timeout (ms)	
	Modem	Enable/Disable modem	
		Modem init-string	
		DCD behavior	
	Port logging	Enable/Disable Port logging	
		Port log storage location	
		Port log buffer size	
		Display port log	
	Port event handling	Enable/Disable port event handling	
		Notification interval	
		Email notification	Enable/Disable Email notification
			Title of Email
			Recipient's Email address

[1] TCP/UDP mode only.
[2] A secondary remote host is available for connection-fail backup in TCP mode
[3] TCP/UDP mode only.
[4] TCP mode only

		SNMP notification	Enable/Disable SNMP notification
			Title of SNMP trap
			SNMP trap receiver's IP address
			SNMP trap community
			SNMP trap version
		Add/Edit a keyword Keyword string Email notification SNMP trap notification Port command	
		Remove a keyword	
All serial ports setting **Or** **Individual serial port setting #1~#8(1/4)**	Port Enable/Disable		
	Port title		
	Apply all port settings (Individual serial port setting only)		
	Host mode	**TCP**	TCP listening port
			Telnet protocol
			Max allowed connection
			Cyclic connection
			Inactivity timeout (0 for unlimited)
		UDP	UDP listening port
			Max allowed connection
			Accept UDP datagram from unlisted remote host or not
			Send to recent unlisted remote host or not
			Inactivity timeout (0 for unlimited)
		Modem emulation	
	Remote host[5]	Add or Edit a remote host[6] Primary host address Primary host port Secondary host address Secondary host port	
		Remove a remote host	
	Port IP filtering[7]	Allowed host IP	
		Subnet mask to be applied	
	Cryptography[8]	Encryption method None/SSLv2/SSLv3/SSLv3 rollback to v2/ TLSv1/3DES/RC4	
		Cipher suite selection	
		Verify client (server mode only)	
		Verify certificate chain depth	
		Check the certificate CN	
		Filter application arguments	
	Serial Port Parameters	Type	
		Baud rate	
		Data bits	
		Parity	
		Stop bits	
		Flow control	
		DTR behavior	
		DSR behavior	
		Inter-character timeout (ms)	
	Modem	Enable/Disable modem	
		Modem init-string	

[5] TCP/UDP 모드만 該當
[6] TCP 모드에서 secondary remote host 는 연결 실패시에 백업을 위해서 유용합니다.
[7] TCP/UDP 모드만 該當
[8] TCP 모드만 該當

		DCD behavior	
	Port logging	Enable/Disable Port logging	
		Port log storage location	
		Port log buffer size	
		Display port log	
	Port event handling	Enable/Disable port event handling	
		Notification interval	
		Email notification	Enable/Disable Email notification
			Title of Email
			Recipient's Email address
		SNMP notification	Enable/Disable SNMP notification
			Title of SNMP trap
			SNMP trap receiver's IP address
			SNMP trap community
			SNMP trap version
		Add/Edit a keyword Keyword string Email notification SNMP trap notification Port command	
		Remove a keyword	

그림 4-1은 웹-기반 시리얼 포트 설정 화면을 보여줍니다. 시리얼 포트 설정 처음 화면은 각 포트들의 정보를 요약하여 보여줍니다. 사용자는 이 페이지에서 호스트 모드, 암호화 옵션, 로컬 포트 넘버에 대한 정보를 볼 수 있습니다. 다음은 호스트 모드의 용어가 의미하는 것을 설명한 것입니다.

Host mode	Description		
	Mode[9]	Encryption[10]	Telnet[11]
TCP	TCP	Disabled	Disabled
TCPs	TCP	Enabled	Disabled
TEL	TCP	Disabled	Enabled
TELs	TCP	Enabled	Enabled
UDP	UDP	*[12]	*
Modem Emulation	Modem Emulation	*	*

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

[9] 섹션 4.2.4 호스트 모드 환결 설정 참조.
[10] 섹션 4.2.7 암호화 구성 참조.
[11] 섹션 4.2.4.1 TCP 모드 참조
[12] 지원 하지 않음.

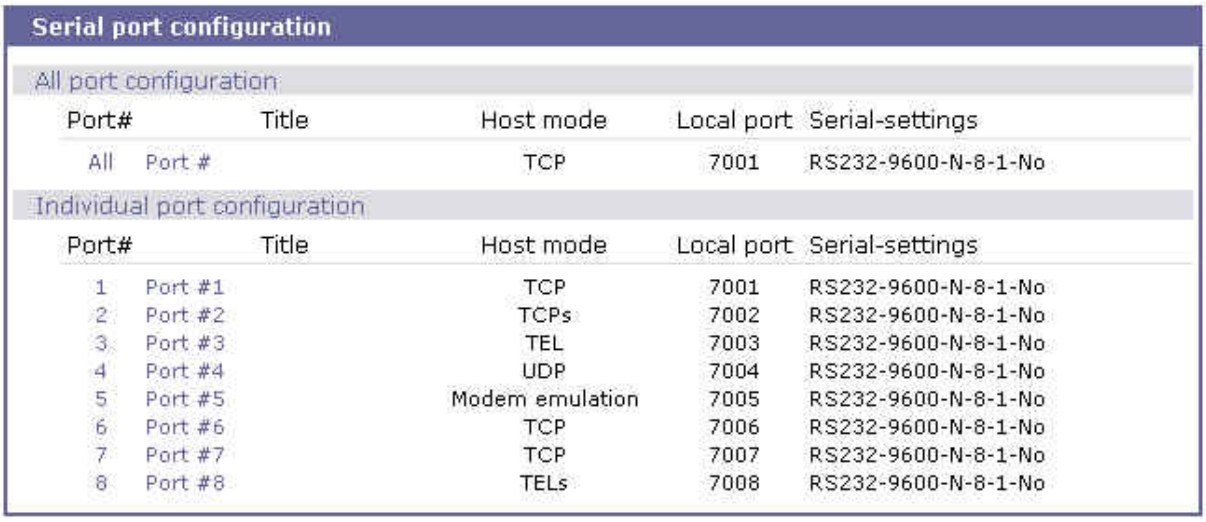


그림 4-1 시리얼 포트 설정 메인 화면

4.2. 개별 포트 설정

STS 시리즈의 시리얼 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
5. Remote host: A*vailable only when the host mode is set to TCP or UDP mode*
6. Port IP filtering: A*vailable only when the host mode is set to TCP or UDP mode*
7. Cryptography: A*vailable only when the host mode is set to TCP mode and Modem Emulation mode*
8. Serial port parameters
9. Modem configuration
10. Port logging
11. Port event handling: A*vailable only when the port-logging feature of the port is enabled*

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

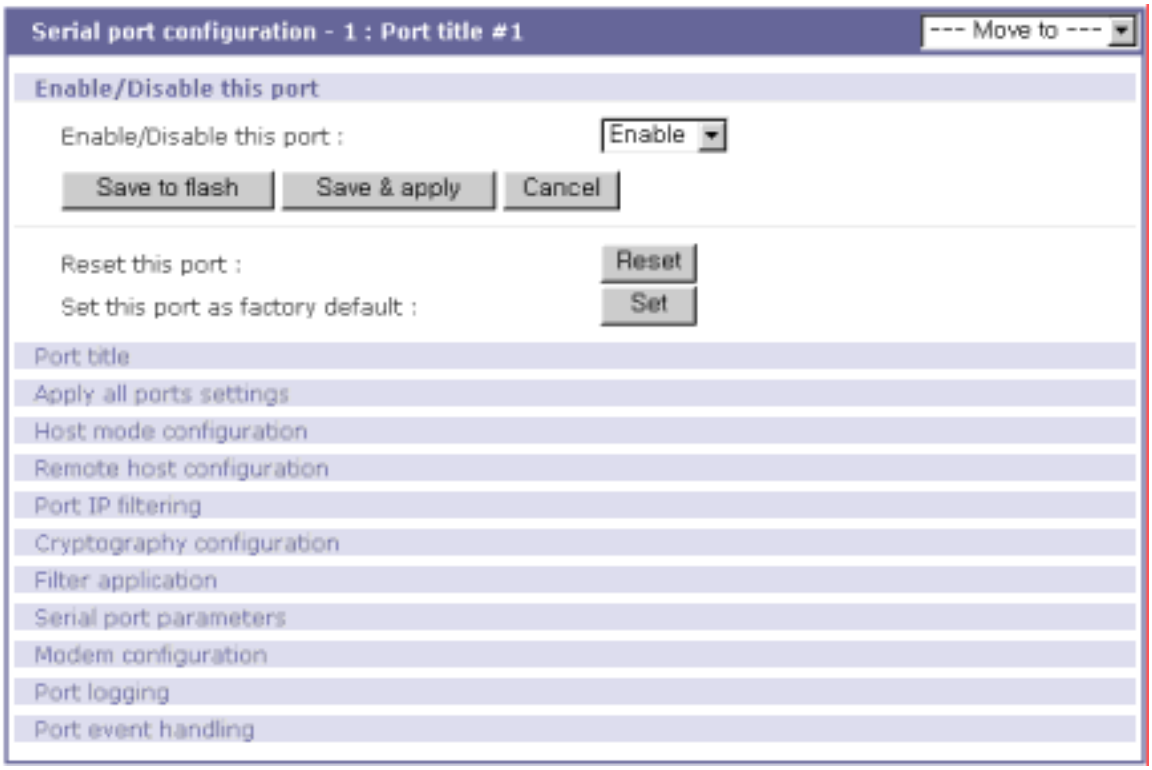


그림 4-2 Serial port enable/disable

4.2.1. Port Enable/Disable

각 시리얼 포트는 enable 또는 disable 될 수 있습니다. 만약 시리얼 포트가 disable 상태가 되면 사용자는 해당 시리얼 포트로 접속할 수 없습니다. 그림 4-2는 시리얼 포트 enable/disable 화면을 보여줍니다.

각 stuck된 시리얼 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.

4.2.2. Port Title

사용자는 각각의 포트에 연결된 장치에 대한 설명을 입력할 수 있습니다. 여기에 장치의 유형, 협력 업체 또는 위치 정보 등을 입력하여, 각 포트의 식별을 위해서 사용할 수 있습니다.

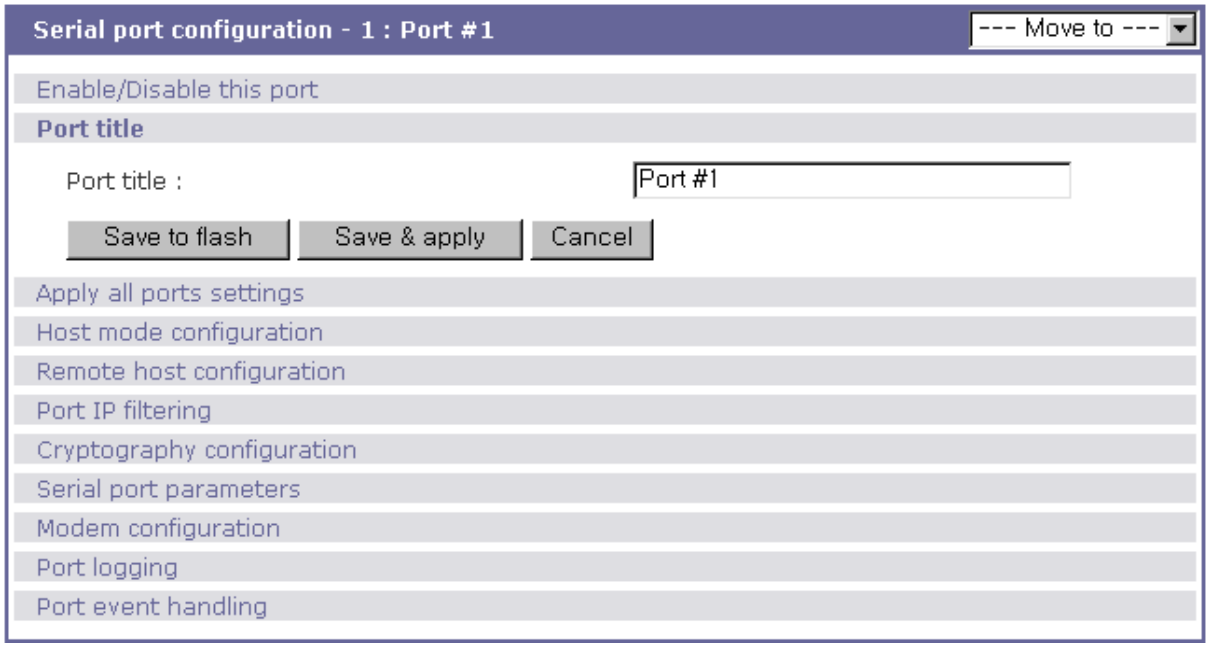


그림 4-3 Port title configuration

4.2.3. Apply All Port Settings

사용자가 all ports settings 을 수행하여 모든 포트의 설정을 한꺼번에 수행하다가, 변경해서는 안 되는 기존 포트 설정 값들을 초기화하는 것을 막기 위해, STS 시리즈는 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 4-4는 **apply all ports settings** 설정 화면을 보여줍니다.

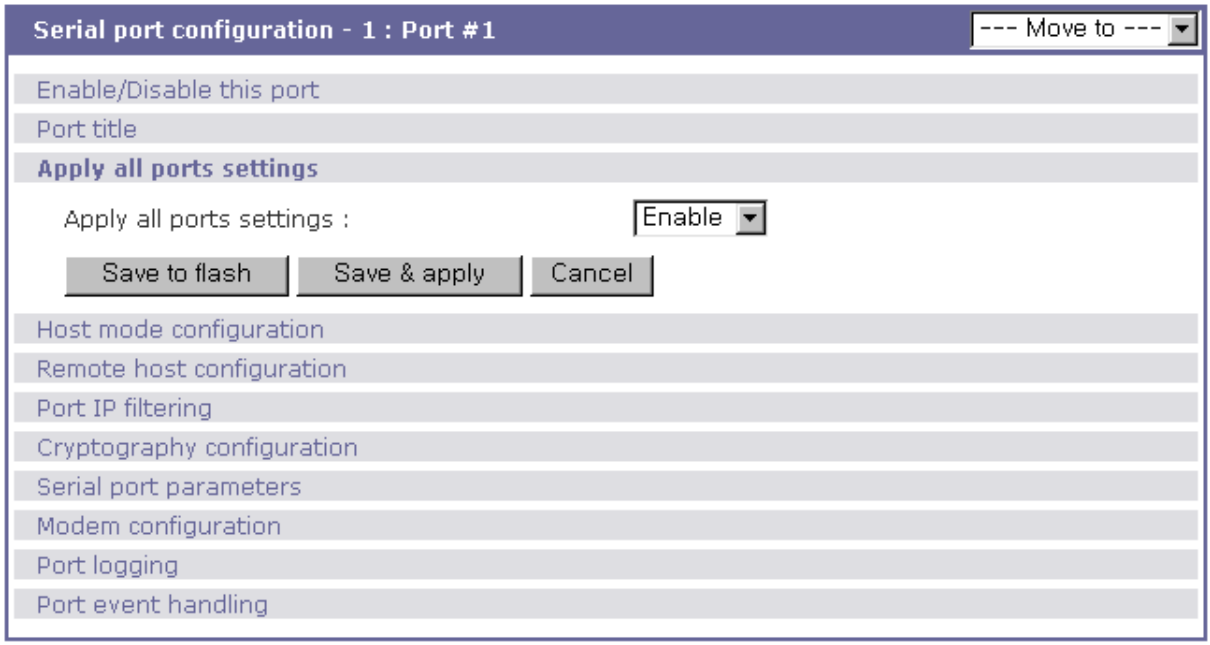


그림 4-4 Apply all port setting configuration.

4.2.4. 호스트 모드 환경설정

STS 시리즈의 작동 모드를 "호스트 모드"라 합니다. 호스트 모드에는 **TCP 모드**, **UDP 모드, 모뎀 에뮬레이션 모드** 세 가지가 있습니다.

TCP 모드

TCP를 통해서 들어온 데이터를 시리얼 포트로 내보내고, 시리얼포트로 들어온 데이터를 TCP로 내보냅니다. TCP 연결은 설정된 TCP 로컬 포트 넘버로 STS 시리즈로 들어오는 연결과 STS 시리즈에 설정된 원격 호스트로 나가는 연결을 모두 사용할 수 있습니다. 또한 다수의 TCP 연결을 이용해서 시리얼 포트로 데이터를 보내고 받을 수도 있습니다.

UDP 모드

UDP 모드 동작은 UDP 프로토콜을 활용한다는 점을 제외하면 TCP 모드의 동작과 비슷합니다.

모뎀 에뮬레이션 모드

시리얼 장치가 이미 모뎀 AT 명령을 지원하거나 사용자가 AT 명령을 사용해서 세션을 제어하고자 할 때 이 모드를 선택합니다. TCP 세션만 지원됩니다.

*그림 4-5*는 호스트 모드 환경설정의 처음 화면입니다.

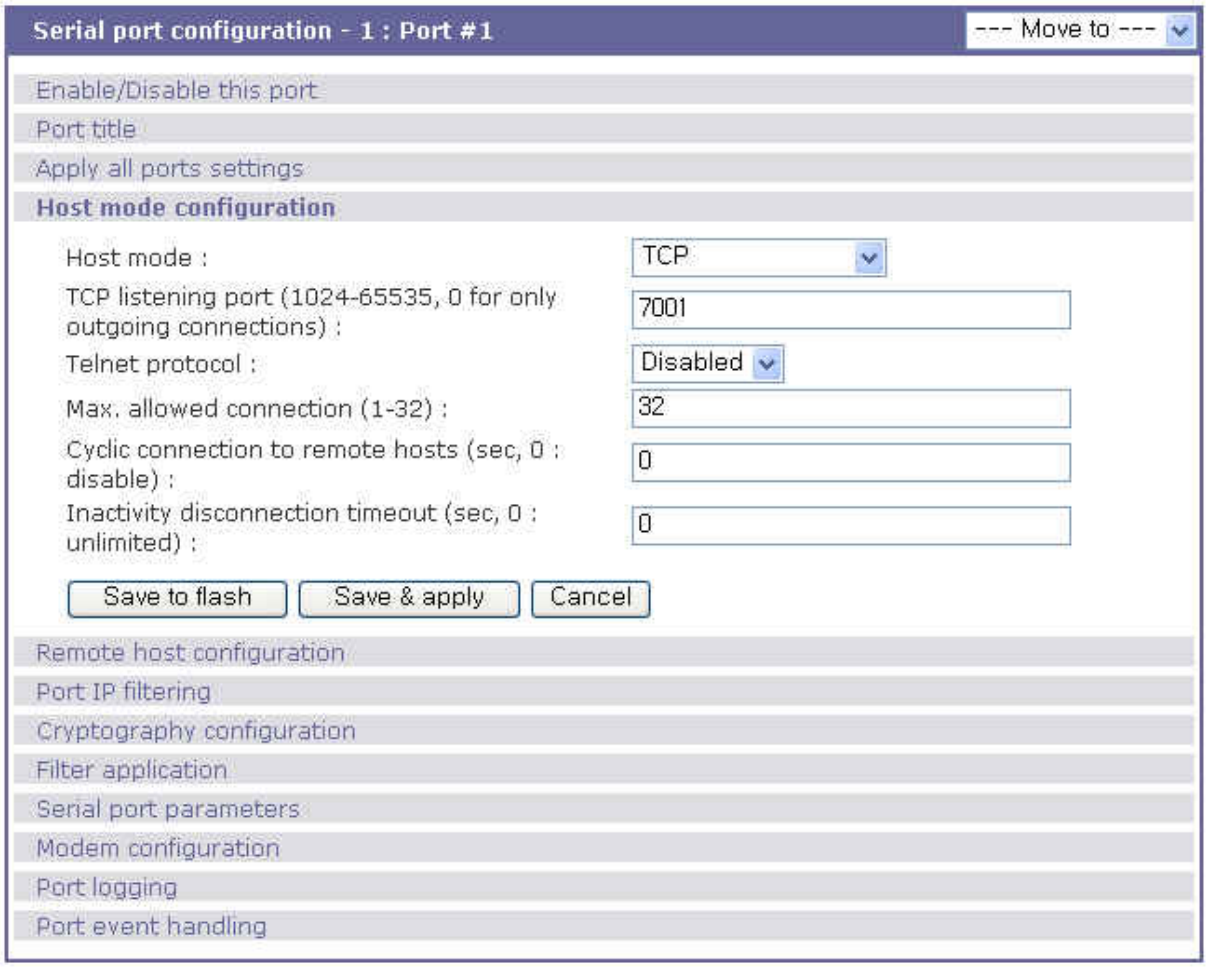


그림 4-5 호스트 모드 환경설정

4.2.4.1. TCP 모드

TCP 모드를 더 쉽게 이해하기 위해서 단순화된 상태전이도(State Transition Diagram)를 사용하는 경우가 많습니다. 그리고 이 다이어그램에 대한 사용자의 이해를 돕기 위해서 STS 시리즈의 상태를 다음과 같이 간략하게 설명하였습니다.

- [듣기(Listen)]

"등록된 원격 호스트 중 어디에선가 연결 요청이 오기를 기다리고 있음"을 나타냅니다. TCP모드로 설정되었을 때 디폴트 시작 모드입니다.

- [닫힘(Closed)]

"연결이 없는 상태"를 뜻합니다. 원격 호스트와 STS 시리즈간의 데이터 전송이 완료되면, 원격 호스트 또는 STS 시리즈 중 하나가 보낸 연결해제 요청의 결과 이 상태로 바뀌게 됩니다. 그 후 상태는 자동으로 [듣기(Listen)]모드로 전환됩니다.

- [싱크-받음(Sync-Received)]

원격 호스트 중 하나가 연결 요청을 보냈다면 [듣기(Listen)] 상태에서 [싱크-받음(Sync-

Received)]로 바뀝니다. STS 시리즈가 요청을 받아들이면, [수립(Established)] 상태로 바뀝니다.

- [싱크-보냄(Sync-Sent)]

STS 시리즈가 연결 요청을 원격 호스트에 보냈다면 [닫힘(Closed)] 상태에서 [싱크-보냄(Sync-Sent)]로 바뀝니다. 이 상태는 원격 호스트가 연결 요청을 받아들일 때까지 유지됩니다.

- [수립(Established)]

"연결이 수립됨(open connection)"을 나타냅니다. 원격 호스트 또는 STS 시리즈 중의 하나가 다른 쪽의 연결 요청을 받아들이면 연결이 되고 [수립(Established)] 상태로 바뀝니다.

- [데이터(Data)]

[수립(Established)] 상태일 때 한 호스트의 데이터는 다른 호스트로 전송될 것입니다. TCP 세션 동작을 보다 쉽게 이해하기 위해서, 이렇게 실제 데이터 전송이 이루어지는 상태를 [데이터(Data)] 라고 부릅니다. 실제로, [데이터(Data)] 모드는 RFC 793 [TCP: Transmission Control Protocol]에서 설명되는 것처럼 [수립(Established)] 상태의 일부분입니다. 연결의 데이터 전송 단계에서는 이 상태가 일반적입니다.

STS 시리즈는 상황에 따라 TCP 서버나 클라이언트로 동작합니다. STS 시리즈는 시리얼 포트 또는 TCP 포트로부터 데이터를 전송하므로 대부분의 애플리케이션에 대해 일반적인 모드가 됩니다. 디폴트 TCP 상태는 TCP 서버 모드와 똑같은 [듣기(Listen)]입니다.

1) 전형적인 상태 전이

[듣기(Listen)] --> [싱크-받음(Sync-Received)] --> [수립(Established)] --> [데이터(Data)] --> [닫힘(Closed)] --> [듣기(Listen)]
Or
[듣기(Listen)] --> [싱크-받음(Sync-Sent)] --> [수립(Established)] --> [데이터(Data)] --> [닫힘(Closed)] --> [듣기(Listen)]

초기 상태는 [듣기(Listen)]입니다. 시리얼 포트로부터 들어오는 데이터가 있으면 TCP 클라이언트로서 원격 호스트에 접속을 하고 TCP포트를 통해서 데이터를 전송합니다. 들어오겠다는 연결 요청을 원격 서버로부터 받으면 TCP서버로서 연결을 수락한 후 시리얼 포트를 통해 데이터를 전송합니다. 이런 식으로, 사용자는 항상 STS 시리즈가 특정 원격 호스트에 접속이 되어 있다고 가정할 수 있습니다.

2) 동작

시리얼 데이터 전송

STS 시리즈의 시리얼 포트를 통해 시리얼 디바이스가 데이터를 보내면, 데이터는 STS 시리즈의 시리얼 포트 버퍼에 쌓이게 됩니다. 버퍼가 가득차거나 일정 시간동안 데이터 전송이 일어나지 않으면 STS 시리즈는 등록된 원격 호스트와 연결합니다. 이때 이 정해진 시간을 "비활동 타임아웃(Inactivity timeout)"이라고 합니다 (비활동 타임아웃에 관한 자세한

설명은 *4.4절 옵션(Options)*을 참조하시기 바랍니다). TCP 세션이 연결되지 않고 STS 시리즈가 원결 호스트와 연결이 되면, 시리얼 포트 버퍼에 쌓인 데이터는 원격 호스트에게 전송 됩니다. 그렇지 않다면, 버퍼에 저장된 모든 데이터는 삭제됩니다.

세션 연결해제

원격 호스트에서 연결해제 요청을 보내거나 일정한 시간 동안 시리얼 포트에서 데이터 전송이 일어나지 않으면 세션 연결이 해제됩니다. 이때 이 정해진 시간을 "비활동 타임아웃(Inactivity timeout)"이라고 합니다. (비활동 타임아웃에 관한 자세한 설명은 *4.4절 옵션(Options)*을 참조하시기 바랍니다). 시리얼 포트 버퍼에 남아있던 모든 데이터는 연결이 해제될 때 삭제됩니다.

원격 호스트로부터의 연결

모든 들어오는 TCP 연결 요구는 TCP client 모드에서 거부됩니다.

3) 파라미터

TCP 리스닝 포트

이것은 원격 호스트가 TCP세션을 연결하고 데이터를 송수신할 수 있는 TCP 포트 번호입니다. TCP 리스닝 포트를 제외한 포트에 대해 들어오는 연결 요청은 거부될 것입니다. STS 시리즈는 1024부터 66635까지 포트 번호를 제한하며 만약 0으로 설정이 되면 나가는 연결(outgoing connection)만이 허용됩니다. (TCP 서버 모드)

텔넷 프로토콜

TCP모드에서, STS 시리즈는 텔넷 COM 포트 제어 옵션(RFC2217 호환)을 지원하므로 사용자는 전송 속도(baud rate), 데이터 비트 그리고 흐름 제어 옵션과 같은 시리얼 파라미터를 사용자측의 RFC2217호환 텔넷 클라이언트 프로그램으로 제어할 수 있습니다. (시리얼 파라미터에 관한 더 상세한 정보는 *4.2.9절 시리얼 포트 파라미터* 를 참조하시기 바랍니다.)

대개 이 옵션은 RFC2217호환 COM 포트 리다이렉터와 함께 사용되어 사용자는 본인의 시리얼 포트 애플리케이션 프로그램을 사용하여 STS 시리즈의 시리얼 포트 파라미터를 제어할 수 있습니다.

이를 위하여, Tactical Software로부터 Serial/IP 가 제공됩니다. COM 포트 리다이렉터 사용에 관해 더 상세한 정보를 보려면 Serial/IP의 문서를 참조하시기 바랍니다. (더 상세한 정보를 원하시면 *부록 6 Serial/IP와 함께 STS 시리즈사용하기* 절을 참조하시기 바랍니다)

허용되는 연결의 최대값

STS 시리즈는 외부 호스트로부터 시리얼 포트로의 다중 접속을 최대 32개까지 지원합니다. 그러나 원격 호스트 리스트 환경설정(remote host list configuration)에 의해 이미 원격 호스트 접속이 있다면, 연결 가능 숫자는 (허용되는 연결의 최대값 – 이미 연결된 원격 호스트의 수)로 감소합니다. 예를 들어 사용자가 허용할 수 있는 연결의 최대값을 32로 설정하고, 원격 호스트 리스트에서 설정된 값에 따라 STS 시리즈에서 원격 호스트로 3개의 연결이 있다면,

외부 호스트로부터 시리얼 포트에 접속할 수 있는 연결의 최대값은 29(=32 – 3)이 될 것입니다. 원격 호스트 리스트 환경설정에 관한 더 자세한 정보를 보려면 *4.2.5 원격 호스트 환경 설정* 을 참조하시기 바랍니다.

주기적 연결

주기적 연결(Cyclic Connection) 기능을 사용하도록 설정되었다면 STS 시리즈는 해당 시리얼 포트에 연결된 장치로부터 들어오는 시리얼 데이터가 없더라도, 일정 시간마다 사용자 정의 원격 호스트에 접속합니다. 원격 호스트에 시리얼 장치로 보낼 데이터가 있다면, 연결이 수립된 후 STS 시리즈의 시리얼 포트를 통해서 시리얼 장치로 전송할 수 있습니다. 만약 STS 시리즈가 방화벽 내부에 있어서, 원격 호스트에서 STS 시리즈로 연결 할 수 없다면, 이 기능을 이용해서 STS 시리즈가 원격 호스트로 연결하게 할수 있습니다. 사용자는 STS 시리즈가 원격 호스트에 접속할 때마다 원격 호스트가 시리얼 명령을 보내도록 함으로써 주기적으로 시리얼 장치를 감시할 수 있습니다. 그림 4-6은 TCP 모드에서 세션 동작의 상태전이도를 보여줍니다.

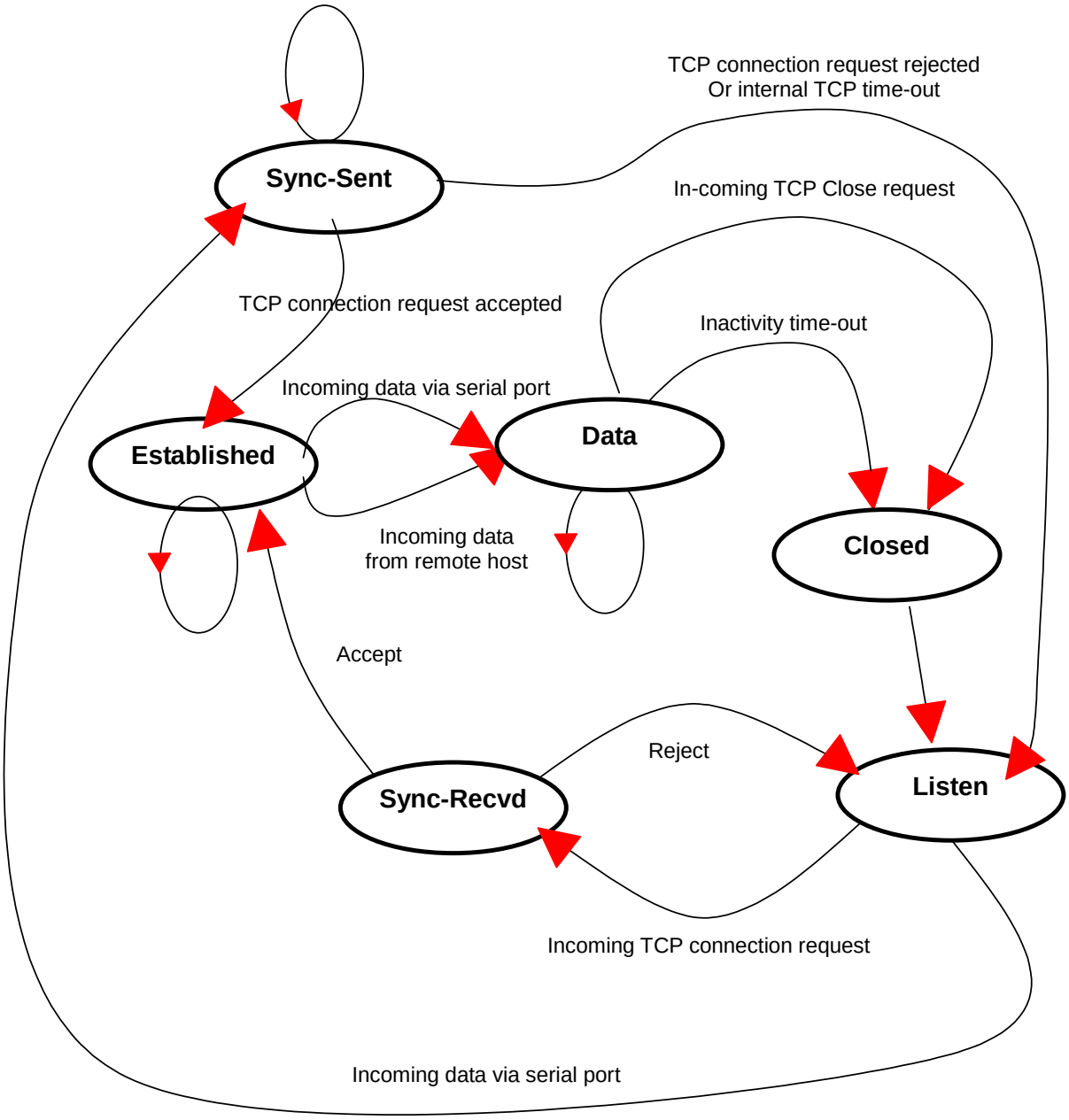


그림 4-6 TCP모드의 상태전이도

비활동 타임아웃(Inactivity Timeout)

비활동 타임아웃(Inactivity Timeout) 기능을 사용하도록 설정했을 때, 비활동 타임아웃 환경설정에서 정해진 값 동안 데이터 전송이 일어나지 않으면 원격 호스트와 STS 시리즈사이의 연결은 자동으로 끊어집니다.

4.2.4.2. UDP 모드

UDP모드 동작은 UDP모드에 기반을 두고 있고 단 하나의 사전 정의된 원격 호스트만이 STS 시리즈와 통신할 수 있다는 것만 제외하면 TCP모드와 비슷합니다. UDP는 비연결 프로토콜이기

때문에 사용자는 주기적 연결을 구성할 필요가 없습니다.

1) 동작

원격 호스트가 UDP 데이터그램을 STS 시리즈의 UDP 로컬 포트 중의 하나에 보내면, 먼저 STS 시리즈는 이 데이터그램이 원격 호스트 환경설정에서 설정된 호스트 중의 하나에서 온 것인지 확인합니다. 해당 원격 호스트가 원격 호스트 환경설정에서 구성된 호스트 중의 하나라면, STS 시리즈는 시리얼 포트를 통해서 데이터를 전송합니다. 그렇지 않다면 STS 시리즈는 들어오는 UDP 데이터그램을 폐기합니다. 그러나 사용자는 '리스트에 없는 원격 호스트로부터 온 UDP datagram을 받기(Accept UDP datagram from unlisted remote host)' 파라미터를 '예(Yes)'로 설정하여 원격 호스트 환경설정에 상관없이 모든 들어오는 UDP 데이터그램을 STS 시리즈가 받도록 만들 수 있습니다. 시리얼 포트로부터 들어오는 데이터가 있으면, STS 시리즈는 이 데이터를 원격 호스트 환경설정에 정의된 원격 호스트로 전송합니다. 만약 목록에 없는 최근 원격 호스트로 전송하기(*Send to recent unlisted remote host)'* 기능이 '예(Yes)'로 설정되어 있다면, 최근에(비활동 타임아웃만큼의 시간이 경과되지 않은) STS 시리즈에 데이터를 보낸 원격 호스트로도 데이터를 전송합니다.

2) 파라미터

UDP 수신 포트

TCP 리스닝 포트와 같은 개념입니다. 자세한 사항은 4.2.4.1절의 ***TCP 모드 파라미터***를 참조하십시오.

허용되는 연결의 최대값

개념은 TCP통신과 같습니다. 자세한 사항은 4.2.4.1절의 ***TCP 모드 파라미터***를 참조하십시오.

목록에 없는 원격 호스트로부터 UDP 데이터그램 받기

'리스트에 없는 원격 호스트로부터 온 UDP datagram을 받기(*Accept UDP datagram from unlisted remote host)'* 기능이 '아니오(No)'로 설정되면, STS 시리즈는 원격 호스트 환경설정에서 구성된 원격호스트로부터 들어오는 UDP 데이터그램만을 받습니다. 반대로 '리스트에 없는 원격 호스트로부터 온 UDP datagram을 받기*(Accept UDP datagram from unlisted remote host)'* 기능이 '예(Yes)'로 설정되면, STS 시리즈는 원격 호스트 환경설정에 상관없이 모든 들어오는 UDP 데이터그램을 받게 됩니다.

목록에 없는 최근 원격 호스트로 전송하기

'목록에 없는 최근 원격 호스트로 전송하기(*Send to recent unlisted remote host)'* 기능이 '예(Yes)'로 설정되면, STS 시리즈는 최근에 STS 시리즈에 접속한 원격 호스트로 데이터를 전송합니다. 목록에 없는 최근 원격 호스트란 STS 시리즈의 해당 시리얼 포트로 데이터를 전송했지만 원격 호스트 환경설정에서 구성되지 않은 원격 호스트를 말합니다. 물론 STS 시리즈는 원격 호스트 환경설정에서 구성된 호스트에도 데이터를 전송합니다. '목록에 없는

최근 원격 호스트로 전송하기(*Send to recent unlisted remote host)'* 기능이 '아니오(No)'로 설정되면 STS 시리즈는 원격 호스트 환경설정에 구성된 호스트에만 데이터를 보냅니다. STS 시리즈는 비활동 타임아웃(Inactivity Timeout) 동안 목록에 없는 최근의 원격 호스트를 유지합니다.

비활동 타임아웃

UDP 모드에서, 목록에 없는 최근의 원격 호스트를 유지하기 위해 비활동 타임아웃을 사용합니다. 비활동 타임아웃 동안 목록에 없는 원격 호스트와 STS 시리즈의 시리얼 포트 사이에 데이터 전송이 없으면, STS 시리즈는 시리얼 포트로부터 목록에 없는 최근의 원격 호스트로 다시 데이터를 보내지 않을 것입니다. 즉, UDP 모드에서 비활동 타임아웃이란 STS 시리즈가 목록에 없는 최근의 원격 호스트를 유지하기 위해 관리하는 시간입니다. UDP 모드에서 사용자가 비활동 타임아웃을 0으로 설정하면, STS 시리즈는 시리얼 포트로부터 목록에 없는 원격 호스트로 어떤 데이터도 보내지 않을 것입니다.

4.2.4.3. 모뎀 에뮬레이션 모드

모델 에뮬레이션 모드에서, 시리얼 포트 프로세스는 마치 시리얼 장치에 부착된 모뎀이 것처럼 동작합니다. 시리얼 포트 프로세스는 마치 모뎀에서 하는 것처럼, AT 모뎀 명령을 받고 명령에 따라 응답합니다. 또한 모뎀 신호를 정확하게 처리합니다. 모뎀 에뮬레이션 모드는 다음과 같은 경우에 유용합니다.

- 이미 사용자의 시리얼 장치에 부착된 모뎀이 있을 경우.

사용자 시리얼 장치에 전화선 연결용 모뎀이 이미 있다면, 이를 단순히 Ethernet 연결용 STS 시리즈로 교체할 수 있습니다. 사용자가 해야 할 일은 ATA/ATDT 명령의 파라미터로 전화번호 대신 IP주소(또는 도메인 명)를 사용하는 것입니다.

- 복수의 원격 호스트로 시리얼 데이터를 보낼 필요가 있을 경우.

시리얼 장치에서 복수의 호스트로 데이터를 보내야 한다면 모뎀 에뮬레이션 모드가 필요합니다. 예를 들어 시리얼 장치의 첫 번째 데이터는 첫 번째 데이터 획득 서버로, 두 번째 데이터는 두 번째 서버로 보낼 수 있습니다. 사용자 장치가 해야 할 일은 장치에서 ATD(T) XXX 명령을 보낼 때마다 IP 주소(또는 도메인 명)을 바꾸는 것입니다.

STS 시리즈의 모뎀 에뮬레이션 모드를 사용하여, 사용자는 시리얼 디바이스를 Ethernet 네트워크에 쉽게 연결할 수 있으며, 이는 전화선 모뎀을 사용하는 것보다 저렴합니다. 표 *4-2*는 STS 시리즈에서 지원하는 요약된 AT 명령어 표입니다. 그림 4-7에서는 Ethernet 네트워크에 연결하기 위해 ATDA 명령을 사용했을 때의 시리얼 포트 명령 흐름의 전형적인 예를 보여줍니다.

표 4-2 STS 시리즈에서 지원되는 AT 명령어

명령	**내부 동작**	**응답** [13] **(verbose code)**
+++	명령 입력 모드로 복귀	없음
ATD(T) [원격 IP 또는 도메인 명]:[원격 포트] [CR][LF]	TCP 모드를 TCP 클라이언트 모드로 설정한 후, 명시된 원격 호스트로 접속을 시도합니다. 예) atdt192.168.1.9:1002: IP 주소 192.168.1.9, 포트 1002로 연결합니다. 예) atdt 명시된 파라미터를 사용하여 원격 호스트로 접속합니다.	성공하면, CONNECT [CR][LF] 연결에 실패하면, NO CARRIER [CR][LF] 다른 에러가 발생하면, ERROR [CR][LF]
AT 또는 ATZ [CR][LF]	TCP 소켓과 시리얼 포트를 초기화합니다.	성공하면, OK [CR][LF] 실패하면, ERROR [CR][LF]
ATA/ [CR][LF]	마지막 명령을 반복합니다.	
ATA [로컬 포트 번호] [CR][LF]	TCP 모드를 TCP 서버 모드로 설정한 후, TCP 상태를 [듣기(Listen)]로 설정합니다. -. 명령 파라미터, 로컬 포트 번호가 명시되지 않으면, 대신 TCP 세션 파라미터, 로컬 포트가 사용됩니다.	
ATEn [CR][LF]	E, E0: 에코 설정을 해제합니다. E1: 에코를 설정합니다.	성공하면, OK [CR][LF] 실패하면, ERROR [CR][LF]
ATHn [CR][LF]	H, H0, H1: 현재 TCP 연결을 해제합니다. 모든 데이터가 삭제됩니다.	
ATOn [CR][LF]	O, O0: 데이터 모드로 전환합니다.	
ATQn [CR][LF]	Q, Q0: 응답을 표시합니다. (디폴트) Q1: 응답을 표시하지 않습니다.	
ATVn [CR][LF]	V, V0: 응답 = <numeric code> [CR][LF] V1 (디폴트): 응답 = <verbose code> [CR][LF]	
AT&Dn [CR][LF]	D, D0: DTR(PC) 신호를 무시합니다. D2(디폴트): TCP 세션 연결을 해제합니다.	
AT&Fn [CR][LF]	F, F0, F1: 디폴트 모뎀 설정값을 복구합니다.	
AT&Kn [CR][LF]	K, K0: 흐름 제어가 없습니다. K3: RTS/CTS 흐름 제어 (디폴트) K4: Xon/Xoff (지원될 때)	
AT&Sn [CR][LF]	S, S0: DSR(PC)는 언제나 높습니다. S1: DSR(PC)가 TCP 연결을 보여줍니다.	
ATIn [CR][LF]	I, I0 : “Sena Technologies, Inc.”를 표시합니다. I3 : 모델 번호를 표시합니다. 다른 경우 : “OK”를 표시합니다.	<=
AT\Tn [CR][LF]	비활동 타이머를 n분으로 설정합니다. \T, \T0: 비활동 타이머를 사용하지 않습니다. (디폴트)	OK [CR][LF]

[13] 에코 모드가 설정되면, 먼저 명령이 반환됩니다. 그리고 나서 해당하는 응답이 나옵니다. 에코 모드를 설정하지 않으면, 응답만이 보내집니다.

ATBn, ATCn, ATLn, ATMn, ATNn, ATP, ATT, ATYn, AT%Cn, AT%En, AT&Bn, AT&Gn, AT&In, AT&Qn, AT&V, AT}Mn, AT\An, AT\Bn, AT\Nn	없음	OK [CR][LF]
ATS?, ATSn=x, AT&Cn, AT&Wn, AT&Zn=x	없음	ERROR [CR][LF]
ATFn [CR][LF]	없음	n이 1이면 OK [CR][LF] 다른 경우라면, ERROR [CR][LF]
ATWn, ATXn	없음	n이 0이라면 OK [CR][LF] 다른 경우라면 ERROR [CR][LF]

표 4-3 AT 명령어 응답 코드

버보스 코드(Verbose Code) (“ATV1” 명령이 실행된 후)	**숫자 코드(Numeric Code)** (“ATV0” 명령이 실행된 후)	**설명**
OK	0	명령이 실행됨
CONNECT	1	모뎀이 회선에 연결됨
RING	2	링 신호가 감지됨
NO CARRIER	3	모뎀이 캐리어 신호를 잃음
ERROR	4	적합하지 않은 명령

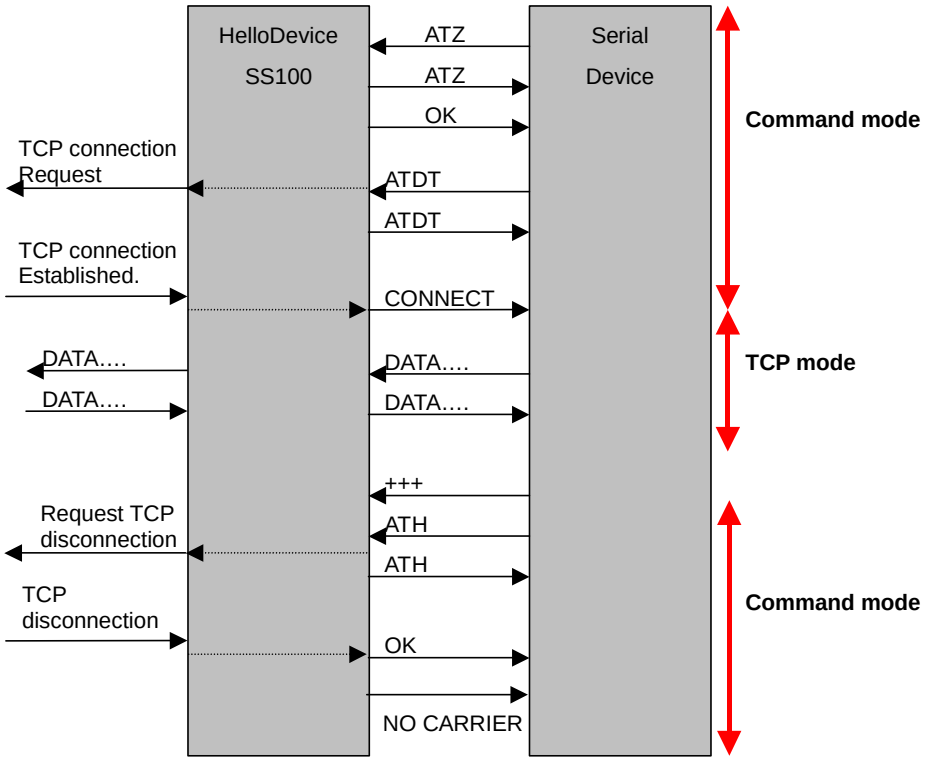


그림 4-7 모뎀 에뮬레이션 모드의 명령/데이터 흐름의 전형적인 예

4.2.5. 원격 호스트 환경설정

*원격 호스트 환경설정(Remote Host Configuration)*이란 STS 시리즈의 시리얼 포트로부터 데이터 전송이 있을 때 STS 시리즈의 시리얼 포트로부터 데이터를 수신할 호스트의 목록을 말합니다.

TCP 모드에서, STS 시리즈가 1차 원격 호스트에 접속하지 못할 때를 대비하여 시리얼 포트로부터 데이터를 수신할 2차 원격 호스트를 설정할 수도 있습니다. 그러나 1차 원격 호스트로 연결이 이루어진다면, STS 시리즈는 1차 원격 호스트로의 연결이 실패할 때까지는 2차 원격 호스트로 데이터를 보내지 않습니다. 그리고 1차 원격 호스트로 설정할 수 있는 숫자는 최대 16개로 제한되어 있습니다.

UDP 모드에서는 STS 시리즈가 1차 원격 호스트의 상태를 검사할 방법이 없으므로 사용자는 1차 원격 호스트만 설정할 수 있습니다. 따라서 2차 원격 호스트는 의미가 없습니다.

*그림 4-8*은 웹 사용자 인터페이스에서 원격 호스트 환경설정을 보여줍니다. (TCP 모드)

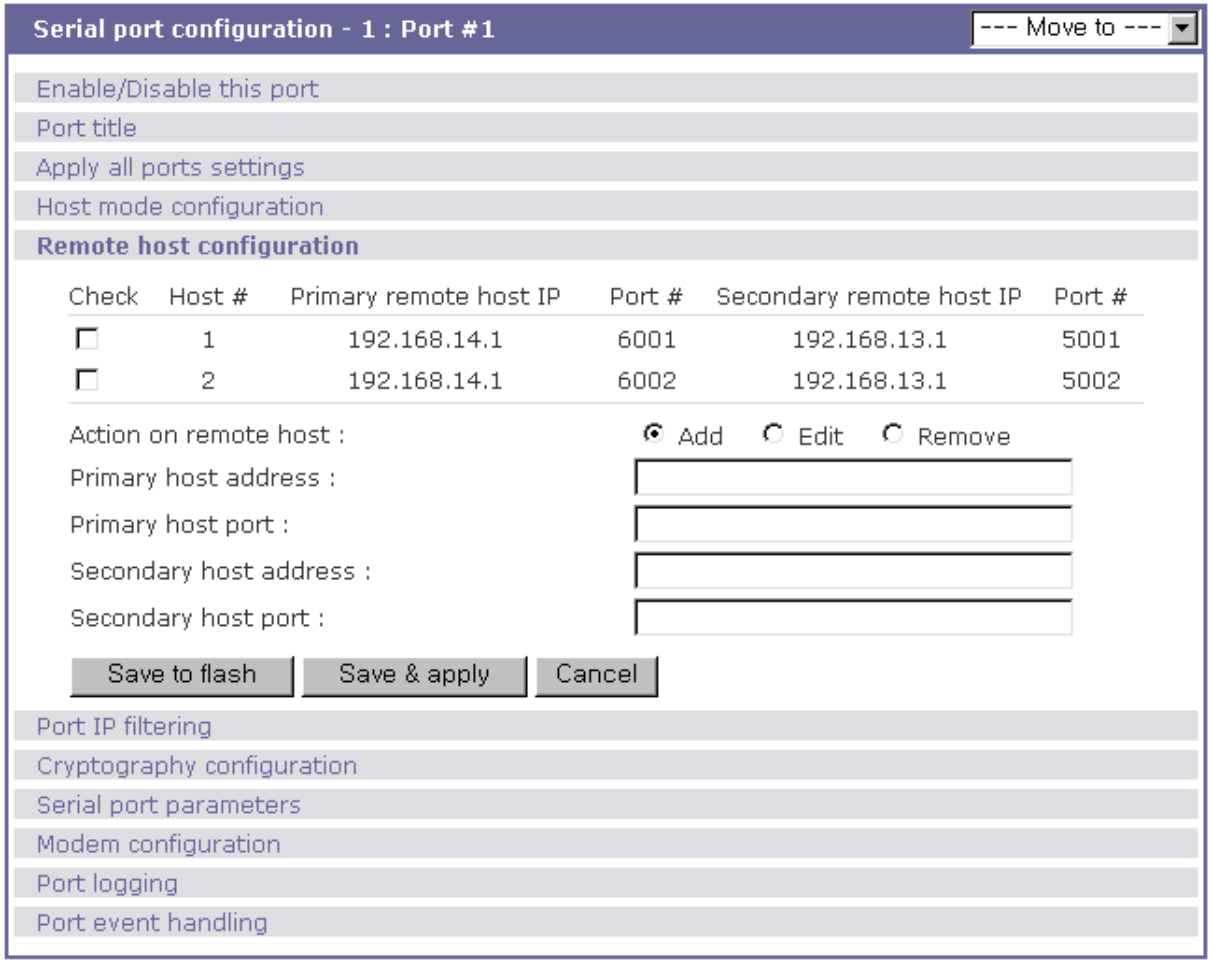


그림 4-8 원격 호스트 환경 설정

4.2.6. Port IP filtering 설정

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

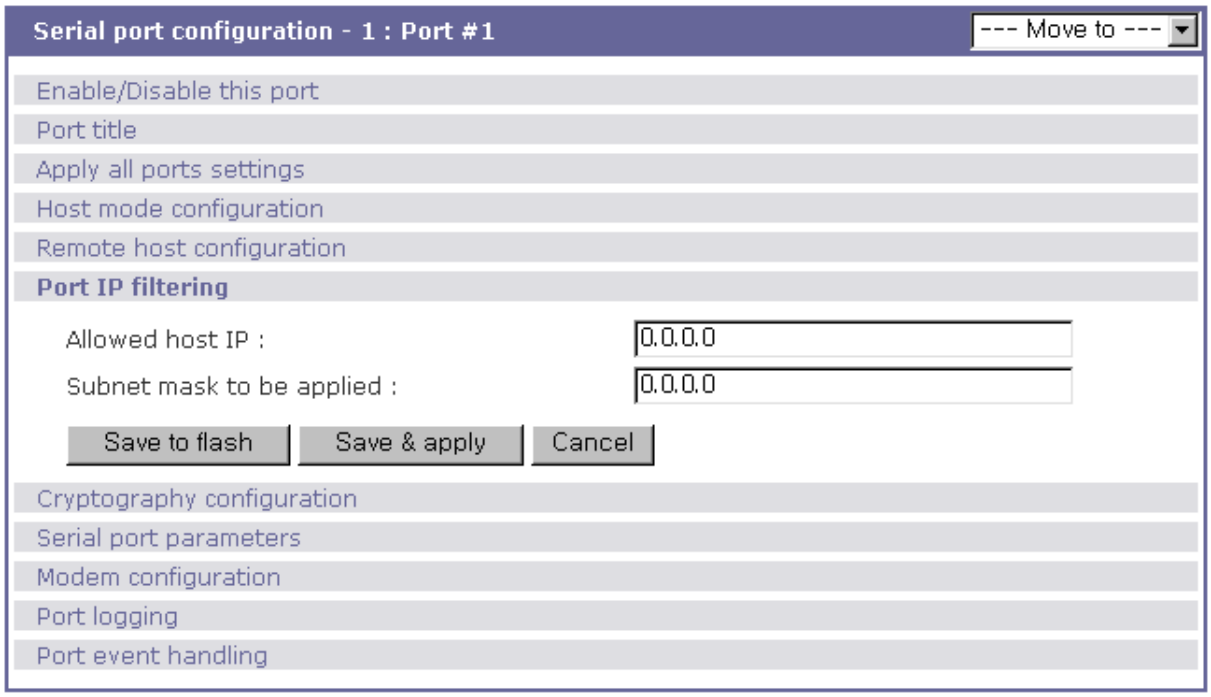


그림 4-9 Port IP filtering for serial ports

4.2.7. 암호화 구성

STS 시리즈는 모뎀 에뮬레이션 모드(UDP 모드 아님)를 포함한 TCP 모드에서만 암호화된 세션을 지원합니다.

4.2.7.1. Secure Sockets Layer(SSL) 및 Transport Layer Security(TLS) 암호화 기법

By setting the cryptography method as one of SSLv2, SSLv3, SSLv3 rollback to v2 or TLSv1, the STS 시리즈가 암호화된 세션에서 SSL/TLS 암호화 기법을 지원하는 다른 장치들과 통신할 수 있습니다.

SSL은 Netscape에 의해서 클라이언트와 서버간에 사용하기 위해서 개발되었습니다. SSL 레이어는 모든 운송 프로토콜보다 상위에 있고 HTTP와 같은 애플리케이션 프로토콜에서 구동 될 수 있습니다. SSL은 안전성, 빠른 속도, 그리고 다른 웹 프로토콜로의 적용가능성을 목표로 하고 있습니다. SSL은 네트워크에 걸쳐서 통신하는 애플리케이션에 데이터 보안을 제공합니다. SSL은 애플리케이션 프로토콜과 TCP/IP 사이에 있는 전송 레이어 보안 프로토콜입니다.

TLS은 SSL의 업데이트된 버전입니다. 이 프로토콜은 Internet Engineering Task Force (IETF)의

원조에 의해서 개발된 Internet RFC내에서 지정됩니다. TLS은 SSL이 진화된 형태이고 클라이언트 또는 서버 둘 중 하나가 새로운 프로토콜을 지원하지 않는 경우, SSL로 내려가는 방법을 지정합니다. 따라서 TLS로 이행하는 것은 상대적으로 어렵지 않은 일입니다.

SSL/TLS 세션을 시작하려면 서버와 클라이언트 사이에 SSL 핸드쉐이크라고 불리는 메시지 교환이 필요합니다. SSL/TLS 프로토콜은 공중 키(public-key)와 대칭 키(symmetric key) 암호화의 조합을 사용합니다. 대칭 키(symmetric key) 암호화는 공중 키(public-key) 암호화와 비교해서 훨씬 빠릅니다. 하지만 공중 키 암호화가 인증 방법 면에서는 좀더 좋습니다. 핸드쉐이크는 서버가 공중 키를 사용해서 자신을 클라이언트에서 인증하고 서버와 클라이언트가 함께 다음 세션에서 사용될 빠른 암호화, 암호 해독 그리고 방해 탐지 등에 사용될 대칭 키를 생성하는 것을 허용해 줍니다. 관련된 핸드쉐이크의 상세 사항은 다음과 같이 요약될 수 있습니다. :

1. 클라이언트가 서버에 클라이언트의 SSL/TLS 버전 번호, 사이퍼(cipher) 설정, 무작위로 생성된 데이터, 그리고 서버가 SSL/TLS을 사용하는 클라이언트와 통신하는 데에 필요한 다른 정보를 보냅니다.
2. 서버가 클라이언트에 서버의 SSL/TLS 버전 번호, 사이퍼(cipher) 설정, 무작위로 생성된 데이터, 그리고 클라이언트가 SSL/TLS을 통해서 서버와 통신하는 데에 필요한 다른 정보를 보냅니다. 서버 또한 자신의 인증서를 보내고 해당 클라이언트가 클라이언트 인증이 필요한 서버 자원을 요청한다면 클라이언트의 인증서를 요청합니다.
3. 클라이언트는 서버를 인증하기 위해서 서버가 보낸 일부 정보를 이용합니다. 해당 서버가 인증될 수 없다면 사용자에게 문제점을 경고해주고 암호화되고 인증된 연결이 만들어 질 수 없다는 것을 알립니다. 서버가 성공적으로 인증되면 클라이언트는 다음 단계를 진행합니다.
4. 클라이언트는 현재까지 핸드쉐이크에서 생성된 모든 데이터를 사용해서 해당 세션을 위해서 premaster secret을 만들고 이것을 서버의 공중 키(단계 2에서 보내진 서버의 인증서에서 얻어진)를 사용해서 암호화하며 이 암호화된 premaster secret을 서버로 보냅니다. 이때에 사용된 사이퍼(chipher)에 따라서 클라이언트와 서버가 협력할 수 있습니다. SSL/TLS는 바로 이 “공유된" 마스터 시크릿의 생성 여부에 따라 달라집니다
5. 서버가 클라이언트 인증을 요구하는 경우(핸드쉐이크의 옵션 단계)에는 해당 클라이언트가 이 핸드쉐이크에만 있고 클라이언트와 서버 양자에 알려진 데이터를 사인합니다. 이 경우에 클라이언트는 사인된 데이터와 클라이언트의 인증서를 암호화된 premaster secret와 함께 서버로 보냅니다.
6. 서버가 클라이언트 인증을 요구하는 경우, 해당 서버는 클라언트를 인증하려고 시도합니다. 해당 클라이언트가 인증될 수 없으면 그 세션은 종료됩니다. 클라이언트가 성공적으로 인증되면 서버는 자신의 사설 키(private key)를 사용해서 premaster secret를 해독하고 일련의 단계(클라이언트 또한 같은 premaster secret에서 시작해서 실행하는)들을 실행해서 마스터 시크릿(master secret)을 생성합니다.

7. 클라이언트와 서버는 이 마스터 시크릿을 사용해서 SSL/TLS 세션 동안에 교환된 정보를 암호화/암호 해독하는 데에 사용되는 대칭 키인 세션 키(session key)를 생성합니다. 또한 클라이언트와 서버는 이 마스터 시크릿을 사용해서 SSL/TLS 연결을 통해 송수신한 시간 중에 변경된 데이터의 무결성(integrity)을 검증합니다.
8. 클라이언트는 클라이언트로부터의 메시지는 앞으로 이 세션 키를 사용해서 암호화 될 것이라고 알려주는 메시지를 서버로 보냅니다. 또한 클라이언트는 핸드쉐이크의 클라이언트 부분은 종료되었다는 것을 알려주는 독립된 암호 메시지를 보냅니다.
9. 서버는 서버로부터의 메시지는 앞으로 이 세션 키를 사용해서 암호화 될 것이라고 알려주는 메시지를 서버로 보냅니다. 또한 서버는 핸드쉐이크의 서버 부분은 종료되었다는 것을 알려주는 독립된 암호 메시지를 보냅니다.
10. SSL/TLS 핸드쉐이크가 완료되었고 이제 SSL/TLS 세션이 시작되었습니다. 클라이언트와 서버는 이 세션 키를 사용해서 서로간에 송수신한 데이터를 암호화하고 암호 해독하며 이 데이터의 무결성을 검증합니다

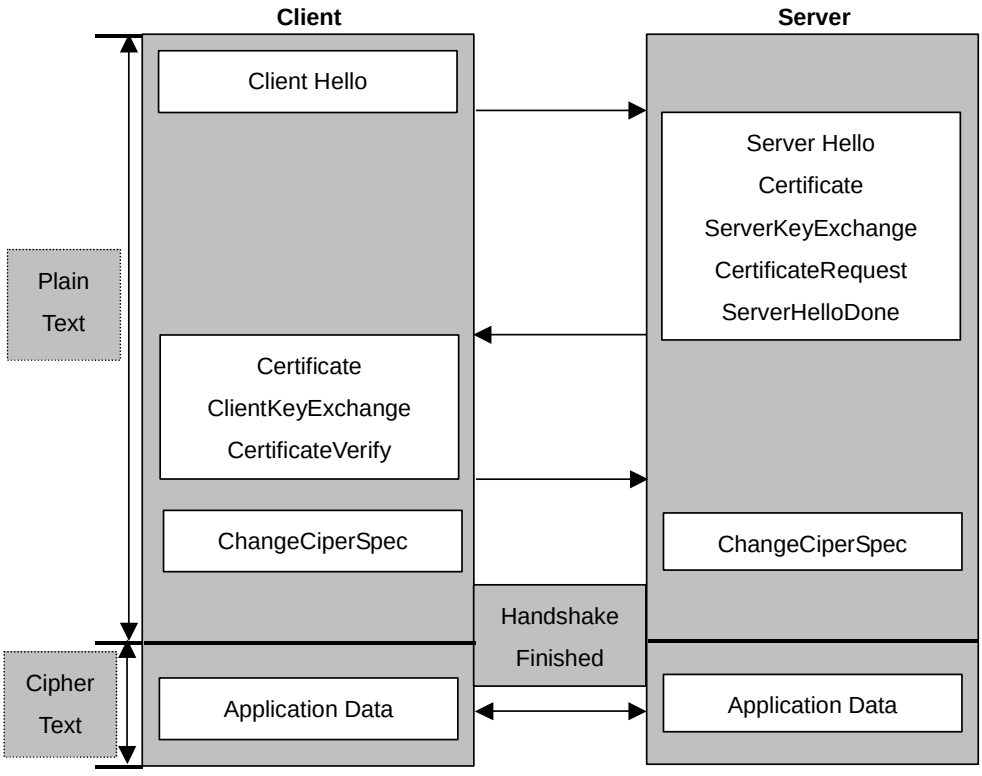


그림 4-10 일반적인 SSL/TLS 핸드쉐이크 프로세스

STS 시리즈는 TCP 모드 상태에 따라 SSL/TLS 서버 또는 클라이언트로써 작동할 수 있습니다. SSL/TLS과의 TCP 연결이 원격 호스트에서 먼저 시작된다면, STS 시리즈는 SSL 핸드쉐이크 동안에 SSL/TLS 서버로써 작동합니다. 반대로, SSL/TLS과의 TCP 연결이 STS 시리즈의 시리얼 포트에서 에서 먼저 시작된다면 STS 시리즈는 SSL 핸드쉐이크 동안에 SSL/TLS 클라이언트로써 작동합니다.

사용자가 SSL/TLS 암호 기법을 사용할 때, 사용자는 다음과 같은 파라미터들을 구성할 수 있습니다.

- **사이퍼 슈트(Cipher suites) 활성화/비활성화**

  Cipher suites는 SSL/TLS 연결 보안에 사용되는 비대칭(asymmetric), 대칭(symmetric) 그리고 해쉬(hash) 알고리즘을 지정하는 데에 사용되는 객체입니다. 비대칭 알고리즘은 서버 또는 클라이언트(옵션)의 서버 아이덴티티(identity)의 검증과 비밀 키 정보를 안전하게 교환하는 데에 사용됩니다. 대칭 알고리즘은 SSL/TLS 연결을 통해서 전송된 대량의 데이터를 암호화 하는 데에 사용됩니다. 해쉬 알고리즘은 전송된 데이터가 전송 도중 변경되는 것을 방지하는데 사용됩니다. 대칭과 비대칭 알고리즘에 사용된 키의 길이도 지정되어야 합니다.

  클라이언트가 서버로 SSL/TLS 연결할 때에 사용 가능하고 사용하려 하는 cipher suite의 목록을 보냅니다. 서버는 이 목록을 자체 지원되는 cipher suite와 비교해서 이 목록 중에 서버가 사용할 수 있고 사용하려 하는 첫 번째 cipher suite를 선택합니다. 클라이언트와 서버는 이제 이 cipher suite를 사용해서 연결을 보안합니다

  cipher suite의 선택은 주어진 환경과 보안 요구사항에 따라 달라집니다. RSA에 기반을 둔 cipher suite들이 가장 많이 사용되며 속도 면에서도 어느 정도의 잇점이 있습니다.

  STS 시리즈는 다양한 cipher suite를 지원하고 사용자는 해당하는 cipher suite를 활성화 또는 비활성화 함으로써 각 cipher suite를 선택할 수 있습니다.

- **클라이언트 검증 (서버 모드 전용)**

  사용자가 *클라이언트 검증* 옵션에 “예”라고 하면, STS 시리즈는 SSL 핸드쉐이크 프로세스 (단계 2)중 클라이언트의 인증서를 요구합니다. 반대로 사용자가 *클라이언트 검증* 옵션에 “아니오”라고 하면, STS 시리즈는 SSL 핸드쉐이크 프로세스 (단계 2)중 클라이언트의 인증서를 요구하지 않습니다.

- **인증서 체인 뎁스(certificate chain depth) 검증**

  인증서 체인은 해당 체인의 인증서가 뒤에 오는 인증서에 의해서 사인되는 것으로, 인증서들의 체인입니다. 이 인증서 체인의 목적은 자체(또는 동등(peer)) 인증서에서 신뢰할 수 있는 CA 인증서까지 신뢰할 수 있는 체인을 만드는 것입니다. CA는 동등(peer) 인증서에 사인함으로써 아이덴티티를 보증합니다. 만약 사용자가 해당 CA를 신뢰한다면, 즉 사용자의 루트 인증서 디렉토리에 해당 인증서의 사본이 있다면, 이것은 사용자가 사인된 동등 인증서 또한 신뢰할 수 있다는 것을 의미합니다. STS 시리즈에서 사용자는 인증서 체인 뎁스의 수를 제한해서 STS 시리즈가 인증서 체인에서 신뢰받는 CA 인증서를 찾아서 무한 검색하지 않도록 해주어야 합니다.

- **인증서 CN 점검**

  사용자가 *인증서 CN 점검* 옵션에 “예”를 선택하면, STS 시리즈는 해당 호스트 이름이 인증서의 CN(일반 이름)과 일치하는지를 점검합니다. 만일 이 둘이 일치하지 않으면 STS

시리즈는 원격 호스트로의 연결 요청을 종료합니다. 반대로 사용자가 *인증서 CN 점검* 옵션에 “아니오”를 선택하면, STS 시리즈는 해당 호스트 이름이 인증서의 CN(일반 이름)과 일치하는지를 점검하지 않습니다.

STS 시리즈는 SSL/TLS로써 작동할 때에만 CN(일반 이름)을 점검합니다.

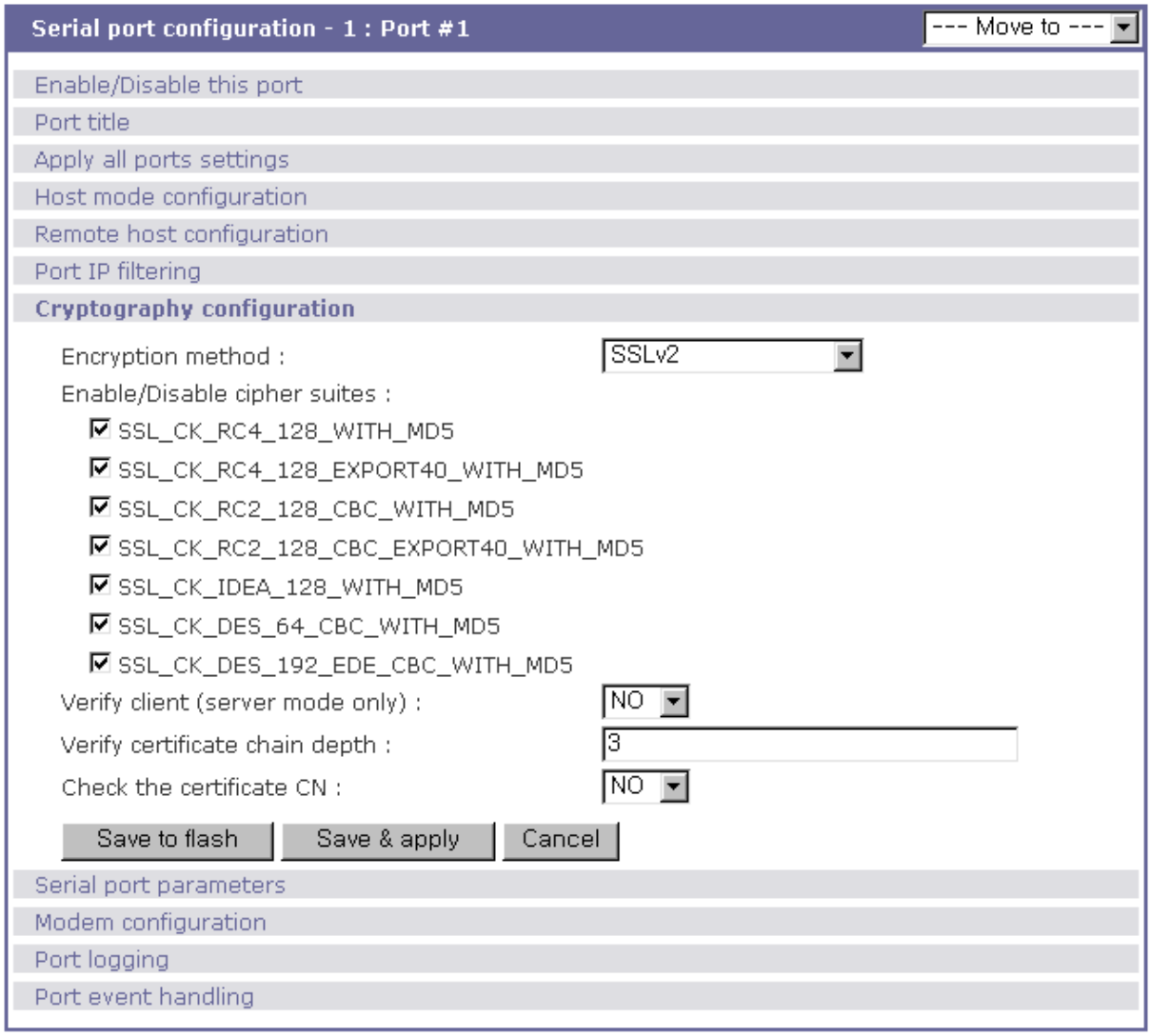


그림 4-11 암호화 구성

4.2.7.2. 3DES 암호화 기법

암호화 기법을 *3DES*로 설정하면 STS 시리즈는 3DES(168 bits) 암호화된 세션에서 다른 STS 시리즈장치 또는 HelloDevice STS 시리즈와 통신할 수 있습니다.

그림 4.12 3DES 패킷의 레코드 포맷을 보여주고 있습니다. 여기에서 각 필드의 의미는 다음과 같습니다.

길이	데이터	패딩(채우기)

그림 4-12 3DES 패킷의 레코드 포맷

- **길이**
  길이는 8-bits 숫자입니다. 이 길이는 내용(데이터 및 패딩)의 길이를 의미합니다. 3DES 는 64 비트 블록 치퍼(cipher) 알고리즘이고 여기에서의 길이는 8(64/8) 배수로 이루어 집니다.

- **패딩(Padding)**
  패딩은 표준 블록 치퍼(cipher)입니다. 패드 값은 패딩(1~8)에서의 전체 패드 바이트입니다.

STS 시리즈의 3DES 알고리즘에서 암호화된 데이터 패킷 생성에 사용된 키와 초기 벡터는 키 블록에서 유도됩니다. 그리고 키 블록은 사용자 구성 키 열을 사용해서 생성됩니다. *그림 4-13* 은 키 유도 과정을 보여주고 있습니다.

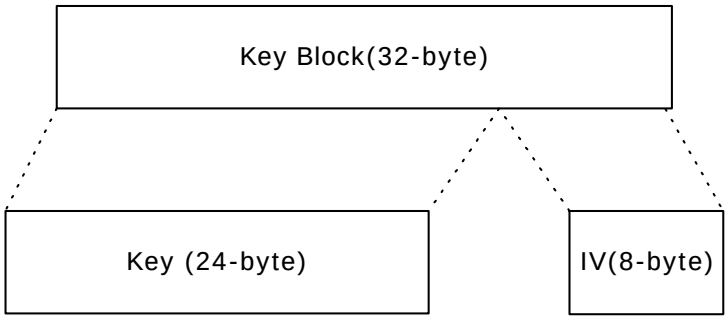


그림 4-13 키 유도

키 블록은 다음과 같이 정의됩니다:

Key_Block = MD5(KEY_STRING) + MD5(MD5(KEY_STRING)+KEY_STRING)
= (16 bytes) + (16 bytes)

Key = 키 블록의 처음 24bytes

IV(Initial Vector) = 키 블록의 마지막 Bytes

4.2.7.3. RC4 암호화 기법

암호화 기법을 RC4로 설정하면 STS 시리즈는 RC4 암호화된 세션에서 STS 시리즈장치와 통신할 수 있습니다. RC4 암호 모드에서 STS 시리즈는 사용자 구성 키 열을 사용해서 모든 TCP 스트림을 암호화하고 해독합니다. RC4 기법은 사용하면 헤더 또는 패딩을 사용하지 않습니다. RC4 기법이 3DES 기법보다 속도가 빠릅니다.

4.2.8. Serial port parameters

4.2.9. 시리얼 포트 파라미터

시리얼 포트에 시리얼 장치를 연결하려면 해당 STS 시리즈의 시리얼 포트의 파라미터를 연결된 시리얼 장치에 맞게 설정해야 합니다. 사용자가 설정할 수 있는 파라미터는 UART 형식, 전송속도(baud rate), 데이터 비트, 패리티, 스톱 비트, 흐름제어, DTR/DSR 신호를 이용한 옵션 그리고 문자간(inter-character) 타임아웃 등입니다.

먼저 STS 시리즈와 해당 시리얼 장치는 시리얼 통신 형식이 RS232로 일치해야 합니다. 시리얼 통신의 핀 구성과 배선도에 대한 자세한 사항은 부록1의 연결 섹션을 참조하십시오.

- **시리얼 전송속도(Baud rate)**
  STS 시리즈에서 사용할 수 있는 시리얼 전송속도는 다음과 같습니다:
  75, 150, 200, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 그리고 230400
  초기 설정된 기본값은 9600입니다.

- **데이터 비트(Data bits)**
  데이터 비트는 7 bits 또는 8 bits입니다. 초기 설정된 기본값은 8 bits입니다.

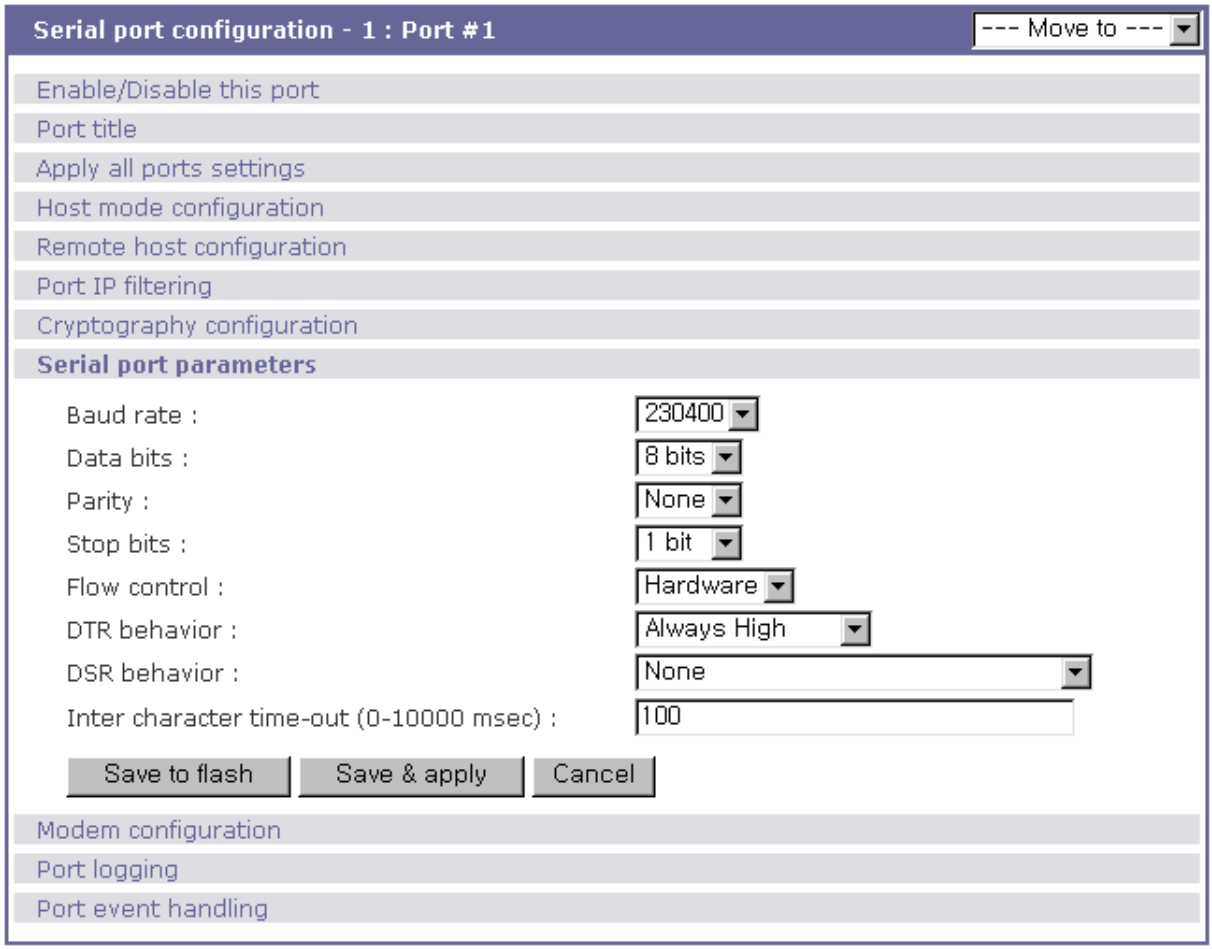


그림 4-14 UART 설정

- **패리티(Parity)**

  패리티는 **none, even** 또는 **odd**입니다. 초기 설정된 기본 값은 none입니다

- **스톱 비트(Stop bits)**

  스톱 비트는 1 bit 또는 2 bit입니다. 초기 설정된 기본 값은 1 bit입니다.

- **흐름 제어(Flow control)**

  초기 설정된 기본 값은 *None*입니다. STS 시리즈는 XON/XOFF를 사용하는 소프트웨어 통신 제어와 RTS/CTS를 사용하는 하드웨어 흐름 제어를 지원합니다.

  소프트웨어 흐름 제어 방식은 특수문자(XON/XOFF(0x11/0x13))를 두 개의 연결된 장치들 간에 전송해서 데이터 통신 흐름을 제어합니다. 하드웨어 흐름 제어 방식에서는 두 개의 연결된 장치들 사이에서 신호를 주고 받음으로써 데이터 통신 흐름을 제어합니다.

참고:

RS232 모드만이 흐름 제어 방식을 지원합니다. RS422 모드와 RS485 모드는 어떠한 종류의 소프트웨어 또는 하드웨어 흐름 제어도 지원하지 않습니다.

- **DTR/DSR 동작**

DTR/DSR 핀의 용도는 시리얼 포트 신호를 사용해서 TCP 연결 상태를 제어하거나 모뎀 신호 제어를 에뮬레이트 하는 데에 있습니다. DTR은 쓰기전용(write-only) 출력 신호인 반면에 DSR는 읽기전용(read-only) 입력 신호입니다.

DTR 출력 동작은 다음 세 개의 형식 중 하나의 형식으로 설정될 수 있습니다.

Always high

항상 높은 상태를 유지합니다.

Always low

항상 낮은 상태를 유지합니다.

High when open

TCP 연결상태에서만 높은 상태를 유지합니다.

DSR 입력 동작은 다음 두 개의 동작 중 하나로 설정될 수 있습니다.

None

DSR신호가 변하더라도 아무 동작도 하지 않습니다

Allow TCP connection only by high

DSR 신호가 낮은 상태에서 높은 상태로 변화할 때, TCP가 연결됩니다. 또한 DSR 신호가 높은 상태일 때만, 원격 호스트로부터의 TCP 연결을 허용하고 UDP로 받은 데이터를 받습니다. DSR 신호가 높은 상태에서 낮은 상태로 변화할 때, 모든 TCP 연결이 끊어집니다.

modem emulation 모드에서 DSR이 낮은 상태로 변화하면 현재 DSR 입력 동작의 옵션에 상관없이 원격 호스트와의 연결이 끊어집니다.

참고:

DTR/DSR 동작 메뉴는 모뎀이 활성화인 상태에서는 나타나지 않습니다.

- **문자간(Inter-character) 타임아웃**

이 파라미터는 연속되는 시리얼 데이터를 TCP/UDP 패킷으로 나누기 위해 사용됩니다. STS 시리즈는 시리얼 데이터를 받을 때, 문자간 타임아웃만큼의 시간동안 연속된 데이터를 기다립니다. 그 시간 안에 데이터가 들어오지 않으면 데이터가 종결된 것으로 간주하고, 하나의 TCP/UDP 패킷으로 묶어서 전송합니다. 만약 문자간 타임아웃이상의 시간 차 없이 시리얼 데이터가 1024 bytes이상 계속되면 1024bytes를 하나의 패킷으로 TCP/UDP로 전송하게 됩니다. 문자간 타임아웃이 '0'으로 설정되면 STS 시리즈는 다음 데이터를 기다리지않고 가능한 빨리 데이터를 전송합니다.

최적 문자간 타임아웃은 사용자의 애플리케이션에 따라 달라집니다. 하지만 최소한 지정된 전송속도에서의 문자 하나의 전송시간보다는 커야 합니다. 예를 들면 시리얼 포트가 1200 bps, 8 데이터 비트, 1 스톱 비트 및 패리티 없음(no parity)으로 설정되었을 경우, 하나의 문자를 전송하는데에 필요한 전체 bit의 수는 10bit이고 하나의 문자를 전송하는 데에 필요한 시간은 10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms입니다. 따라서 사용자는 문자간 타임아웃을 8.3ms보다 크게 설정해야 합니다. 8.3ms이하로 설정값은, 0으로 설정한 것과 같이 작동합니다. 문자간 타임아웃의 단위는 천분의 일초(ms)입니다.

4.2.10. 모뎀 구성

STS 시리즈는 시리얼 포트로의 직접 모뎀 연결을 지원합니다. 사용자가 시리얼 포트에 모뎀을 연결하려 할 때에는 모뎀 구성 페이지에서 DCD 동작과 모뎀 init-string을 구성하여야만 합니다. STS 시리즈는 호스트 모드가 *TCP 모드*로 설정 되었을 경우에만 모뎀 연결을 지원합니다.

- **모뎀 활성화/비활성화**
  STS 시리즈의 시리얼 포트에 모뎀을 직접 연결할 경우 사용합니다. STS 시리즈는 DTR/DSR/DCD 신호를 모뎀이 연결되어 있는 것으로 가정하고 제어합니다.

- **모뎀 init-string**
  사용자는 *Modem init-string* 파라미터에서 모뎀 초기화 명령어(initialization string)을 자신의 모뎀에 맞추어서 설정할 수 있습니다. *Enable/Disable modem* 파라미터를 활성(Enabled)로 설정함으로써 시리얼 포트가 모뎀 모드로 설정되었을 때에는 STS 시리즈는 DTR 신호가 낮은 상태에서 높은 상태로 변화하거나 시리얼 포트 구성에 관련된 파라미터가 변경 될 때마다 모뎀 초기화 명령어를 해당 시리얼 포트로 보냅니다.

- **DCD 동작**
  DCD 동작이 높은 상태 일때에만 'TCP 연결 허용(Allow TCP connection only by HIGH)'으로 설정되면, STS 시리즈는 시리얼 포트의 DCD 상태가 높은 상태일때에만 원격 호스트로부터의 연결을 허용합니다. 사용자가 시리얼 포트를 다이얼인 모뎀모드(dial-in modem mode)로만 사용하려 할 때에 유용한 기능입니다. 이 경우에 이미 연결된 모뎀이 없다면 STS 시리즈는 TCP측 연결을 허용하지 않습니다.

- **자동 해제 모뎀 연결**
  자동 해제 모뎀 연결이 Enable로 설정되면 모든 TCP 연결이 닫혔을 때 STS 시리즈는 모뎀 연결을 닫습니다. 자동 해제 모뎀 연결이 Disable로 설정되면 모든 TCP 연결이 닫혔어도 STS 시리즈는 모뎀 연결을 닫지 않습니다. 이 기능의 설정에 상관없이 모뎀 연결이 끊어지면 실제 전화 연결이 끊어진다는 것을 주의하십시오. 즉, 이 옵션은 STS 시리즈를 이용하여 모

든 TCP 연결이 닫혔을 때 모뎀의 연결을 끊을 수 있습니다.

사용자가 dial-out 기능을 사용하려면, 먼저 모뎀에 dial out 명령어를 보내기 위해서 시리얼 포트에 연결된 모뎀에 접속할 수 있어야 하기 때문에 사용자는 DCD 동작 상태를 *None*으로 설정해야만 합니다.

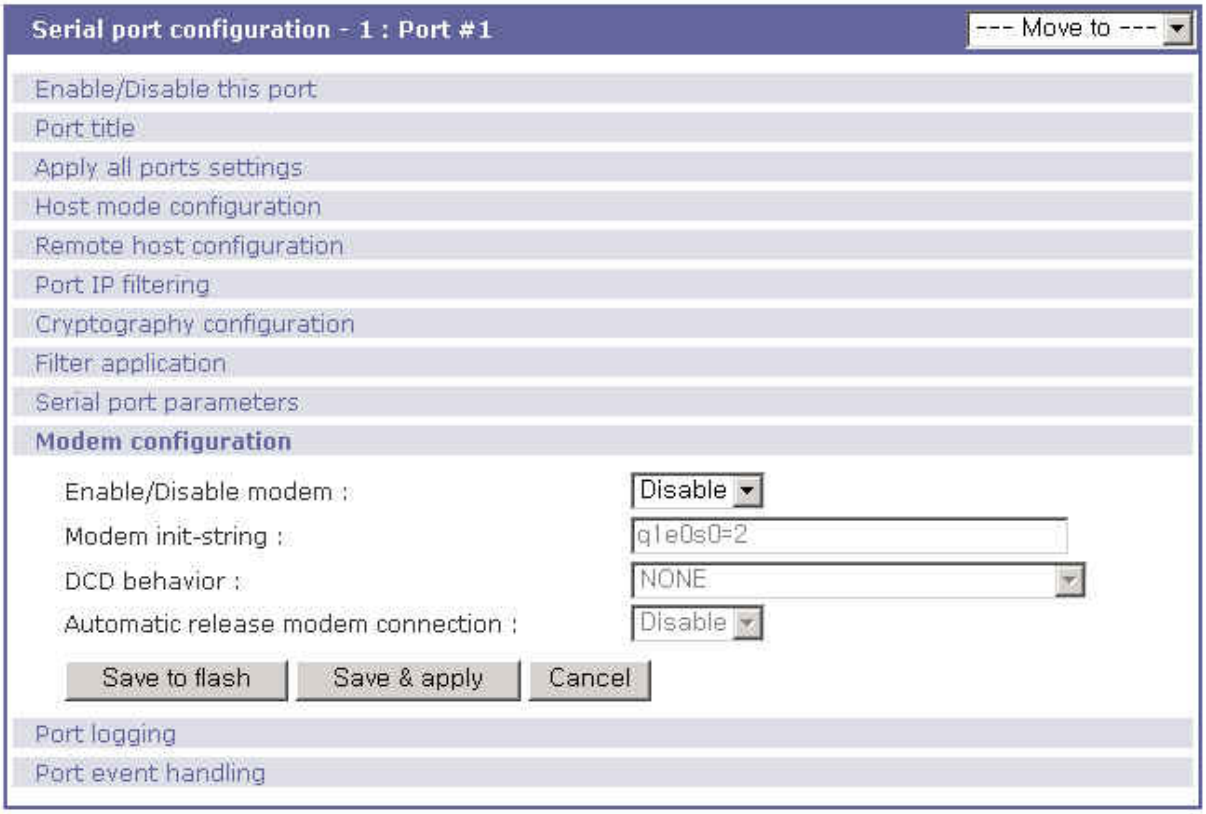


그림 4-15 모뎀 구성

4.2.11. 포트 로깅(Port Logging)

포트 로깅 기능을 사용하면 시리얼 포트를 통해서 보내진 데이터는 MEMORY, ATA/IDE 고정 디스크 카드, SYSLOG 서버 또는 NFS 서버의 장착 위치 등에 저장됩니다.

- **포트 로깅 활성화/비활성화(Enable/disable)**
  이 파라미터는 포트 로깅의 활성화 또는 비활성화를 정의합니다. 초기 설정은 [비활성화(disabled)]입니다.

- **Port log storage location**
  포트 로그 데이터는 STS 시리즈내부 메모리, ATA/IDE 고정 디스크 카드(PCMCIA 슬롯 대용), NFS 서버의 장착 위치 또는 SYSLOG 서버에 저장할 수 있습니다. 내부 메모리를 사용해서 포트 로그 데이터를 저장하는 경우에는 STS 시리즈가 꺼질 때에 이 포트 로그 데이터도 소

멸됩니다. 시리얼 포트 로그 데이터를 보조하려면 저장 위치를 ATA/IDE 고정 디스크 카드, SYSLOG 서버 또는 NFS 서버로 잡으십시오. 이렇게 하려면 사용자가 사전에 해당 매체를 구성해야 합니다. 이 매체가 적절하게 설정되지 않으면 사용자는 인터페이스에서 저장 위치를 선택할 수 없습니다.

- **포트 로그 버퍼의 크기**

  이 파라미터는 로그될 포트 로그 데이터의 최대량을 정의합니다. 내부 메모리를 사용해서 로그 데이터를 저장할 때에는 포트 버퍼의 전체 크기가 3200 Kbytes를 넘을 수 없습니다.(각 시리얼 포트의 모든 포트 버퍼들의 크기의 합이 3200 Kbytes 이하여야만 합니다.) 초기 설정 값은 4 Kbytes입니다.

  ATA/IDE 고정 디스크 카드를 사용해서 로그 데이터를 저장할 때 포트 버퍼의 최대 크기는 해당 카드의 용량에 따라 달라집니다.

  NFS 서버를 사용해서 로그 데이터를 저장할 때에는 포트 버퍼의 최대 크기는 제한되지 않습니다. 사용자가 해당 포트 로깅 시스템에 맞추어서 NFS 서버를 구성해야 합니다.

  SYSLOG 서버를 사용해서 로그 데이터를 저장할 때에는 사용자가 포트 로그 버퍼의 크기를 설정할 수 없습니다.

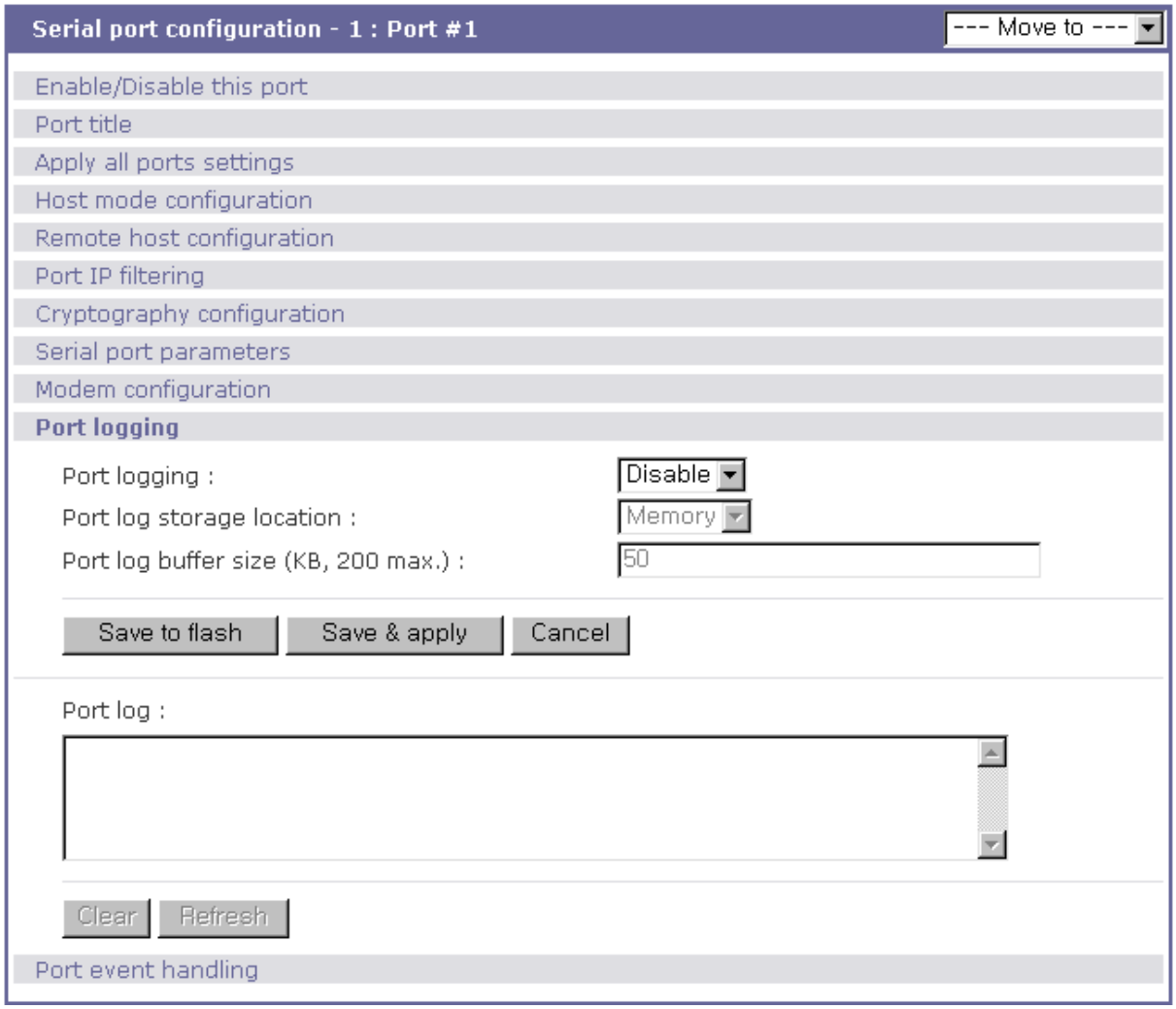


그림 4-16 Port logging configuration

4.2.12. Port event handling configurations

STS 시리즈는 사용자가 포트 이벤트 핸들링 구성을 통해서 시리얼 포트로 연결된 시리얼 장치에서 데이터를 모니터링거나 데이터에 반응할 수 있는 수단을 제공합니다. 이름 그대로 사용자는 email/SNMP 알림(notification) 또는 포트 이벤트 핸들링 구성을 통해서 시리얼 포트로 직접 보내진 명령을 트리거할 각 시리얼 포트용 키워드를 정의할 수 있습니다. 또한 이 기능은 사용자가 연결된 장치를 통해서 데이터를 모니터링하거나 사전 정의된 키워드가 탐지 되었을 때에 연결된 장치를 직접 관리/제어 할 수 있게 해줍니다. 또한 STS 시리즈와 해당 시리얼 장치간의 연결 상태 그리고 STS 시리즈와 원격 호스트간의 TCP 연결 상태를 포트 키워드 사용법과 같은 방법으로 관리하고 모니터링 할 수 있습니다.

각각의 이벤트에 대한 독립된 반응이 구성될 수 있습니다. 여기에서 반응(reaction)은 email 전송, SNMP 트랩 전송, 명령 전송 또는 모든 반응들의 조합이 될 수 있습니다.

- **포트 이벤트 핸들링**

  사용자가 *포트 이벤트 핸들링* 기능을 이용하려면, *포트 이벤트 핸들링을* 활성화(enable)해야 합니다. 이것은 글로벌 파라미터이기 때문에 이 기능이 비활성화(disable)되면 해당 STS 시리즈포트 이벤트에 관한 한 어떠한 일도 하지 않습니다.

- **알림 간격(Notification interval)**

  STS 시리즈는 알림 간격마다 알림 email 또는 SNMP 트랩을 보냅니다. 키워드가 발견될 때마다 email 또는 SNMP 트랩을 보내게 되면, 과도하게 많은 email과 SNMP 트랩이 발생할 가능 성이 있으므로, STS 시리즈는 알림 간격의 시간동안 이벤트를 모아서, 한번에 알려줍니다. 이 파라미터의 값이 너무 작으면 시스템 자원을 많이 쓰게 됩니다. 사용자가 받아 들일 수 있는 가장 큰 값을 설정해야 시스템 자원 사용을 최소화 할 수 있습니다.

- **Email 알림(Email notification)**

  STS 시리즈의 Email 알림 기능을 활성화 또는 비활성화 하는 기능입니다. STS 시리즈 Email 알림을 보낼 때 이것은 SMTP 서버 구성에서 구성된 SMTP 서버를 사용합니다. SMTP 서버가 정확하게 구성되지 않았거나 비활성화 되어 있다면 Email 기능 역시 비활성화 됩니다. SMTP 서버 구성 및 자세한 설명은 3.4 *SMTP* 을 참조하십시오.

- **Email 제목**

  이 파라미터는 사전 정의된 키워드가 탐지 되었을 때 STS 시리즈에 의해서 보내질 Email의 제목을 설정합니다.

- **수신자의 Email 주소**

  이 파라미터는 사전 정의된 키워드가 탐지되었을 때 알림 메일을 받을 수신자를 설정합니다.

- **SNMP 알림**

  이 파라미터는 STS 시리즈의 SNMP 알림 기능을 활성화 또는 비활성화 합니다.

- **SNMP 트랩의 제목**

  이 파라미터는 사전 정의된 키워드가 탐지되었을 때 STS 시리즈에 의해서 보내질 SNMP 트랩의 제목을 설정합니다.

- **SNMP 트랩 수신기 IP(SNMP trap receiver IP)**

  이 파라미터는 사전 정의된 키워드가 탐지 되었을 때 SNMP 트랩 알림을 수신하는 SNMP 트랩 수신기의 IP 주소를 설정합니다.

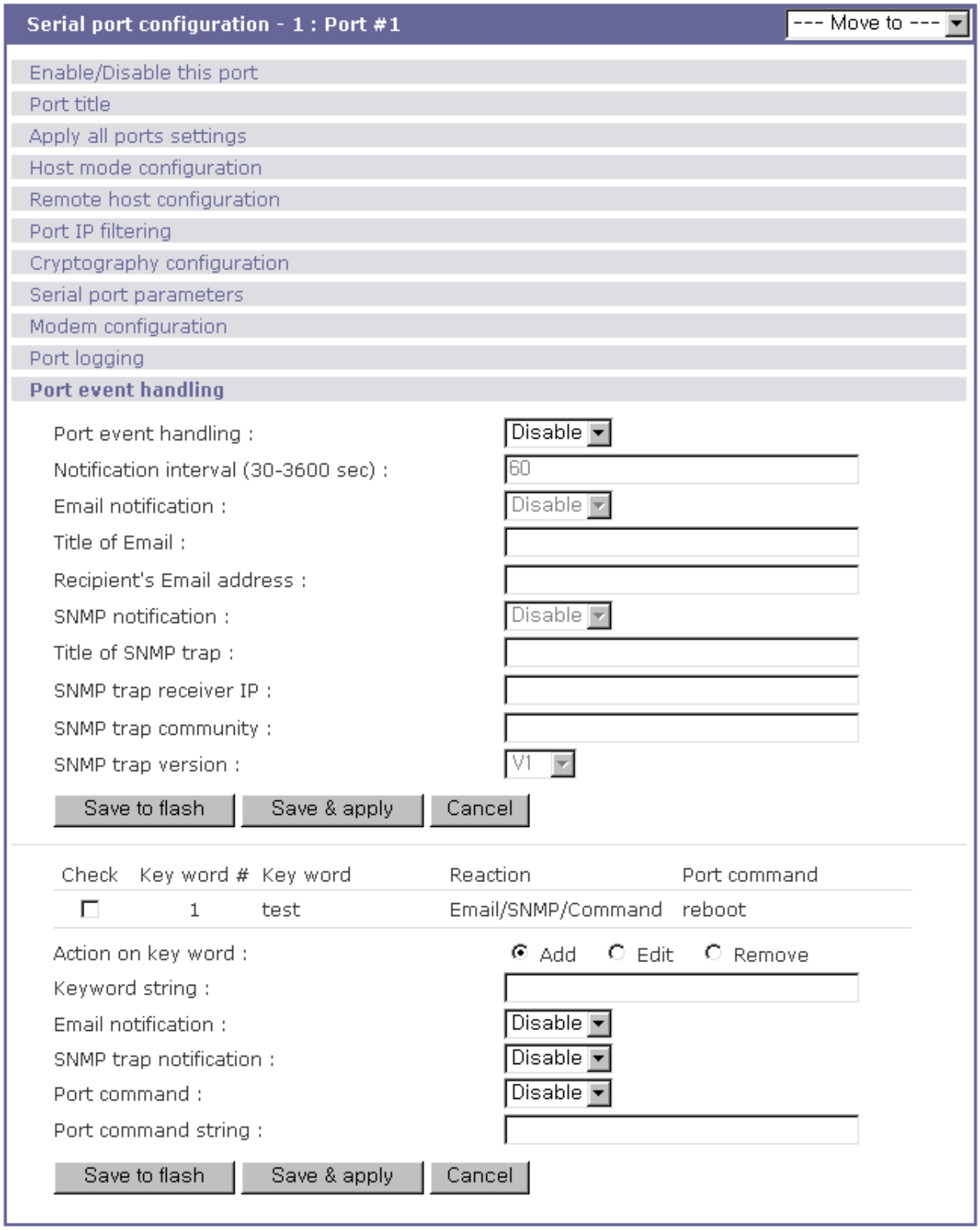


그림 4-17 포트 이벤트 핸들링 구성

- **SNMP 트랩 커뮤니티(SNMP trap community)**
  이 파라미터는 사전 정의된 키워드가 탐지 되었을 때 SNMP 트랩 메시지에 포함된 커뮤니티를 설정합니다.

- **SNMP 트랩 버전(SNMP trap version)**
  이 파라미터는 사전 정의된 키워드가 탐지 되었을 때 보내질 SNMP 트랩의 버전을 설정합니다.

[상태 이벤트 편집]

- **장치 연결/분리**
  시리얼 장치 연결 또는 분리의 이벤트에서 취해야 할 우선 동작의 체크 박스를 체크합니다.

- **TCP 연결/분리**
  원격 호스트로부터 TCP 연결 또는 분리의 이벤트에서 취해야 할 우선 동작의 체크 박스를 체크합니다.

[키워드 목록 편집]

- **키워드 동작**
  사용자는 선택된 키워드에 대한 동작으로 “추가” 또는 “제거”를 선택할 수 있습니다.

- **키워드 열(Keyword string)**
  사용자는 설정하고자 하는 키워드로 어떤 단어든 사용할 수 있습니다.

- **Email 알림**
  사용자가 선택된 키워드로 Email 알림 작동을 활성화 또는 비활성화 할 수 있습니다.

- **SNMP 트랩 알림(SNMP trap notification)**
  사용자가 선택된 키워드로 SNMP 트랩 알림 작동을 활성화 또는 비활성화 할 수 있습니다.

- **Port 명령**
  사용자가 선택된 키워드로 포트 명령 작동을 활성화 또는 비활성화 할 수 있습니다.

- **Port 명령어(Port command string)**
  STS 시리즈는 사전 정의된 키워드가 탐지 되었을 때 시리얼 포트로 연결된 장치로 직접 반응을 지원합니다. 사용자는 이 메뉴에서 시리얼 포트로 보내질 명령을 지정할 수 있습니다.

4.3. 모든 포트 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
4. Remote host configuration
5. Port IP filtering
6. Cryptography configuration (*Only valid and visible if host mode set to TCP or Modem Emulation mode*)
7. Serial port parameters
8. Modem configuration (*Only valid and visible if host mode set to TCP mode*)
9. Port logging
10. Port event handling

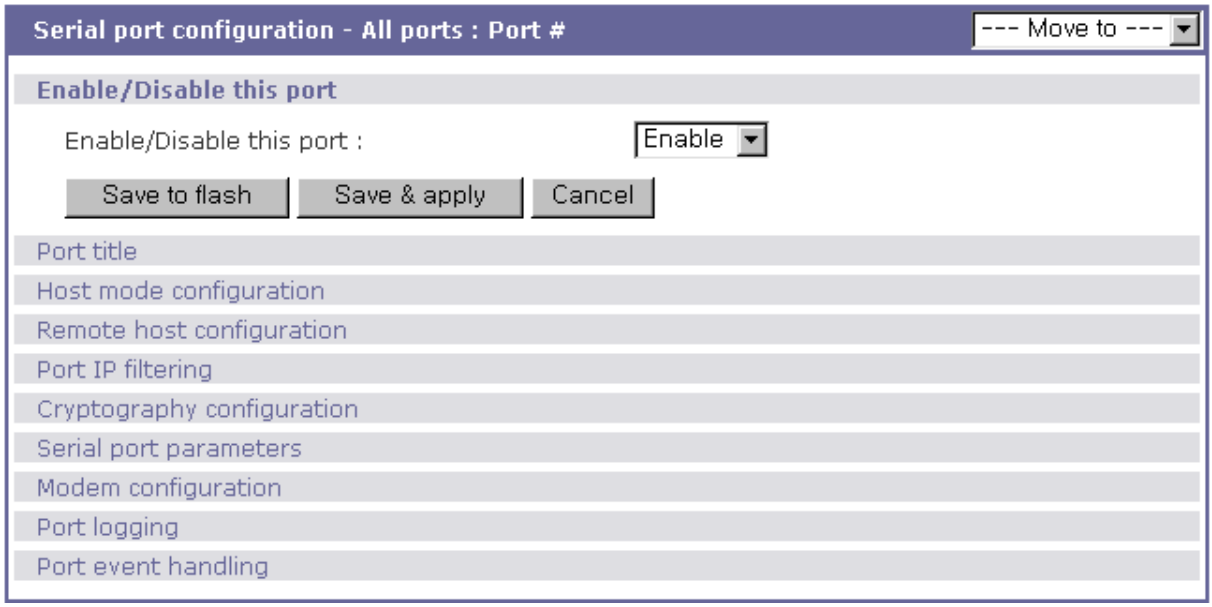


그림 4-18 모든 포트 설정

- **Port enable/disable**

  이 파라미터는 포트의 기능 사용여부를 설정합니다.

- **Port title**

  이 파라미터가 특정 단어로 설정된 경우, 각 시리얼 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.

- **Host mode**

  호스트 모드가 TCP 또는 UDP 모드로 설정되는 경우, 각 시리얼 포트는 듣기(listening) 포트 넘버가 다음과 같이 자동으로 할당됩니다.

  (listening port number + serial port number - 1)

  각 시리얼 포트의 다른 파라미터들은 “all port configuration”와 같은 value set으로 설정됩니다.

- **Remote host configuration, Port IP filtering, Cryptography configuration, Serial port parameters, Modem configuration, Port logging, Port event handling**

  상기 그룹들의 파라미터를 위해, “all port configuration” 의 values set은 모든 시리얼 포트에서 동일하게 설정됩니다.

5. PC 카드 설정

STS 시리즈는 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 STS 시리즈에 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 STS 시리즈에 망외 (out-of-band) 접속을 할 수도 있습니다.

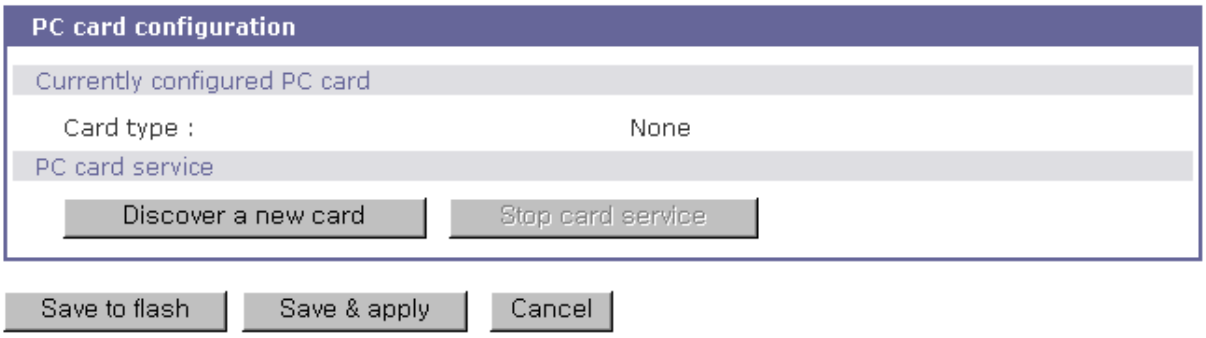


그림 5-1 초기 PC 카드 설정 메뉴 화면

PC 카드 슬롯을 사용하기 위해 사용자는 다음의 단계를 수행해야 합니다.

단계 1. PC 카드 슬롯에 PC 카드를 삽입합니다.

단계 2. Select PC 카드 설정 메뉴에서 

을 선택합니다.

단계 3. STS 시리즈는 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 the configuration settings by selecting 

을 선택하여 설정 상태를 저장합니다.

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

STS 시리즈가 PC 카드를 발견하는데 실패하면, 다음 오류 메시지가 나타납니다.

그림 5-2 확인 실패 에러 메시지

STS 시리즈가 지원하는 PC 카드의 리스트를 보길 원하시면 *부록 B. 지원되는 PC 카드*를 참조하십시요.

PC 카드의 작동을 멈추거나 제품에서 제거하려면, 사용자는 다음과 같은 절차를 거쳐야 합니다.

Step 1. [(**Ban- show the actual button)** Stop card service]를 선택하십시오.

Step 2. [**Save to flash**]를 선택하여 변경된 설정 내용을 저장하십시오..

Step 3. 메뉴에서 [Apply changes]를 선택하여 변경 내용을 적용시키십시오.

Step 4. PC 카드 슬롯에서 PC 카드를 제거 하십시오.

주의: 위와 같은 절차를 거치지 않고 슬롯에서 PC 카드를 제거하면 시스템 오작동의 원인이 될 수 있습니다.

5.1. 랜 카드 설정

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

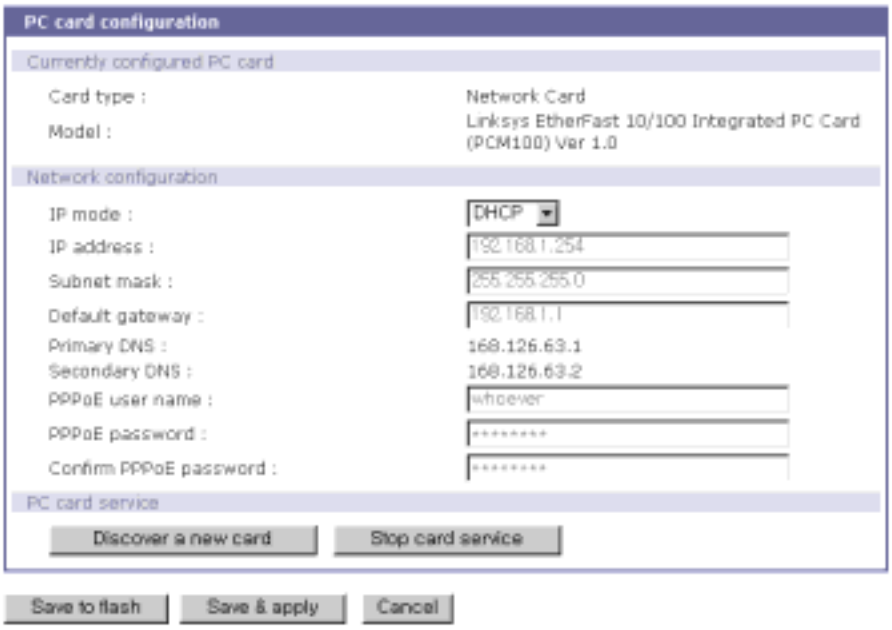


그림 5-3 PC LAN 카드 설정

사용자는 반드시 PC 랜 카드를 설정할 때 PC 랜 카드를 선택하고 primary 및 secondary DNS 서버를 설정해야 합니다. 모든 다른 설정의 단계들은 섹션 *3.1 IP 설정에* 자세히 설명되어 있습니다.

STS 시리즈가 지원하는 랜 PC 카드 리스트를 보려면 *부록 B. STS 시리즈가 지원하는 PC 카드*를 참조하십시오.

5.2. 무선 LAN 카드 설정

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

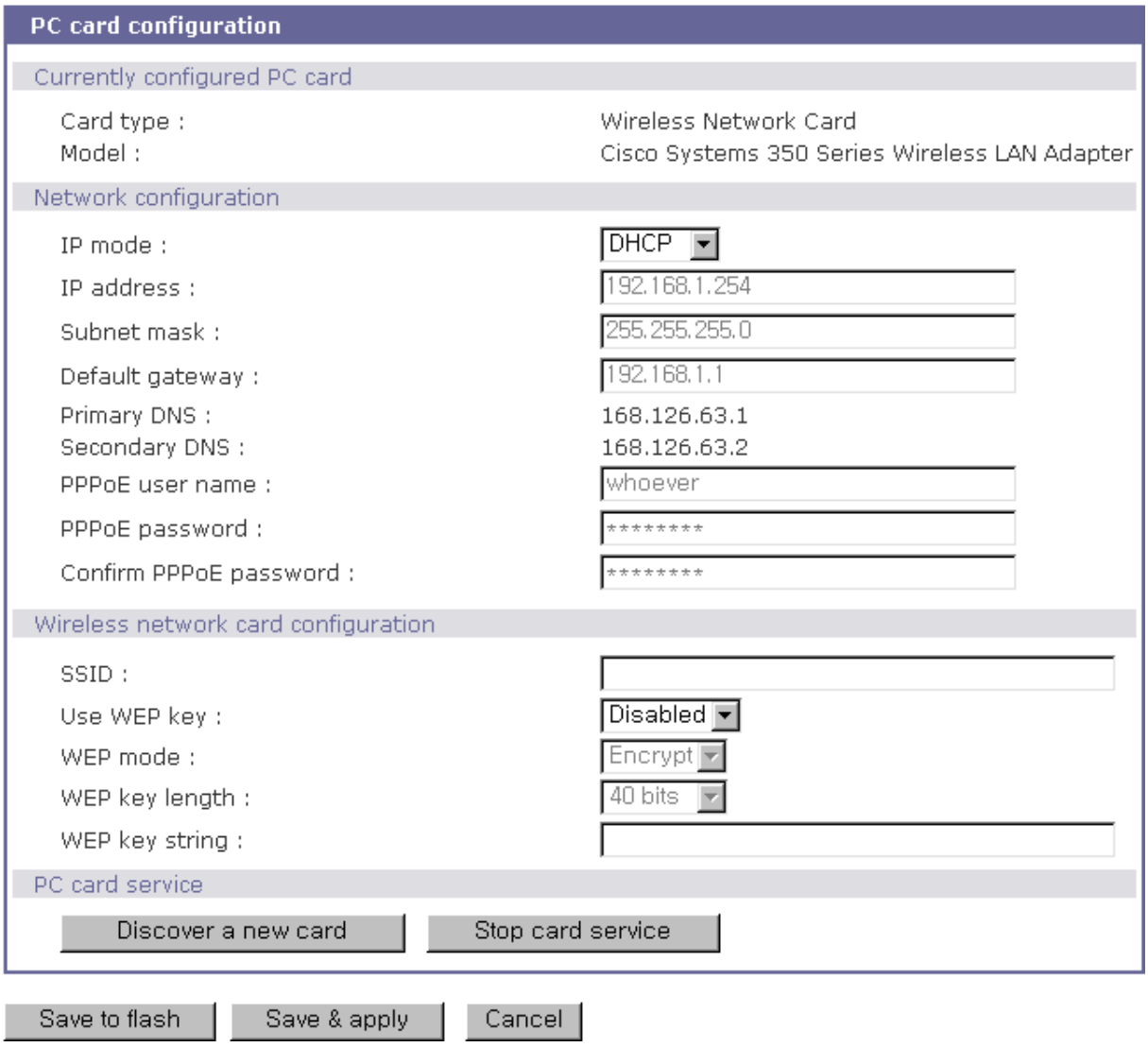


그림 5-4 무선 LAN 카드 설정

사용자는 반드시 PC 랜 카드를 설정할 때 무선 랜 카드를 선택하고 primary 및 secondary DNS 서버를 설정해야 합니다. 모든 다른 설정의 단계들은 섹션 *3.1 IP 설정에* 자세히 설명되어

있습니다.

STS 시리즈는 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

STS 시리즈가 지원하는 무선 랜 PC 카드 리스트를 보려면 *부록 B. STS 시리즈가 지원하는 PC 카드*를 참조하십시오.

5.3. 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. STS 시리즈가 지원하는 PC 카드 목록을 보려면 *부록 B. STS 시리즈가 지원하는 PC 카드*를 참조하십시오.

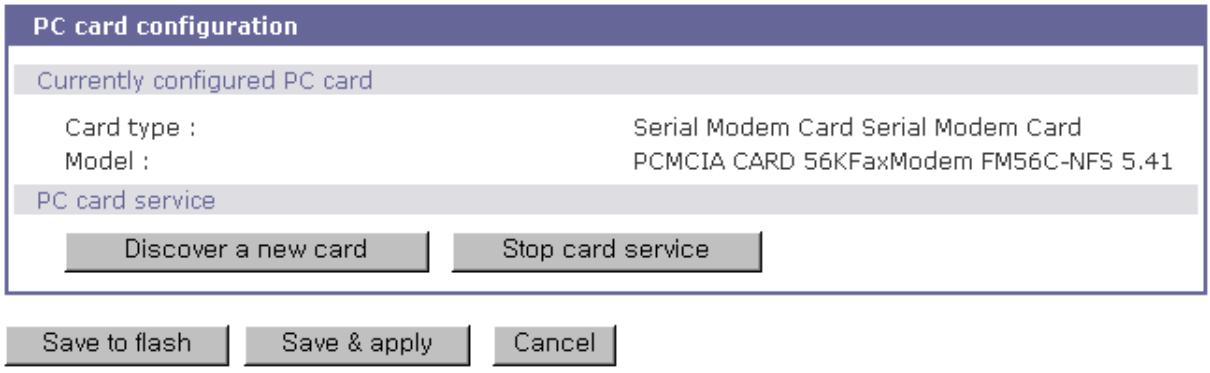


그림 5-5 PC serial modem 카드 설정

5.4. ATA/IDE Fixed Disk Card Configuration

사용자는 시스템 및 시리얼 포트 로그를 저장하기 위해 PC ATA/IDE fixed disk card를 사용하는데 필요한 전체 데이터 크기를 반드시 설정해야 합니다. STS 시리즈는 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. STS 시리즈는 디스크 카드의 **EXT2** 및 **VFAT** 파일 시스템을 지원합니다.

사용자는 STS 시리즈의 시스템 설정을 export 및 import 함으로써, STS 시리즈 설정 파일을 저장 또는 복구할 수 있습니다.

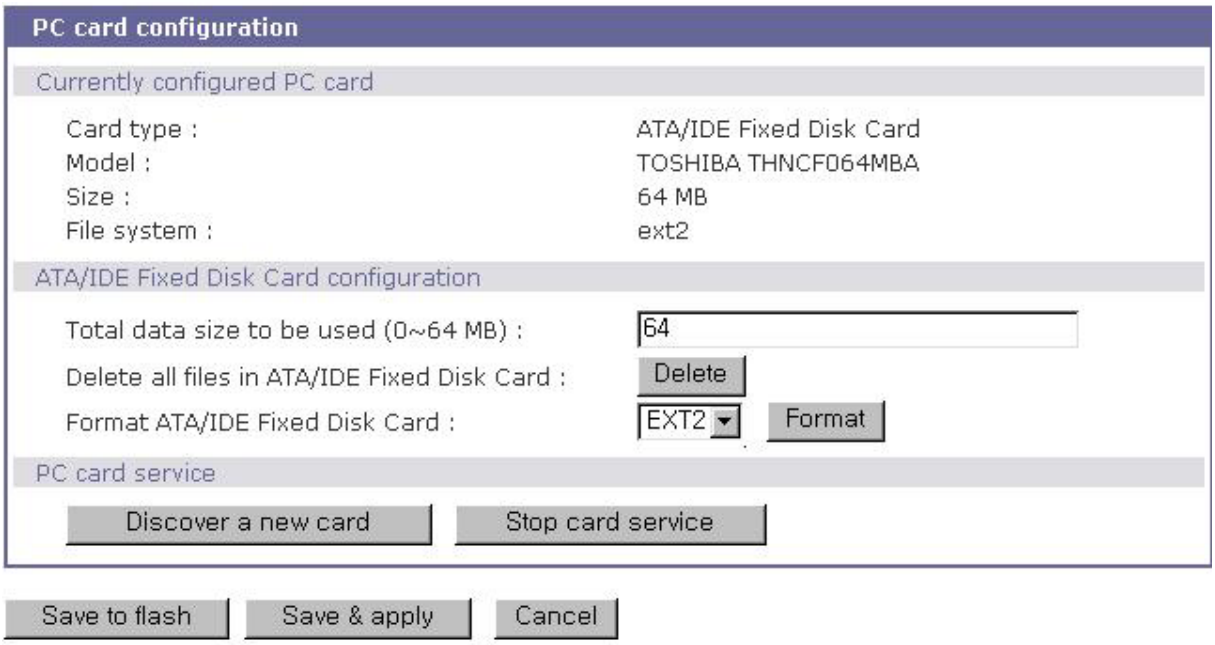


그림 5-6 PC ATA/IDE fixed disk card 설정

6. System Administration

STS 시리즈는 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 및 STS 시리즈의 네트워크 설정 등이 있습니다. 또한 STS 시리즈는 system logging 기능을 통해 지정된 수취인에게 email로 로그 데이터를 자동으로 전달하게 설정될 수 있습니다.

사용자는 STS 시리즈의 장치 이름, 날짜와 시간, 공장 출하시 기본값으로 재지정할 수도 있습니다. 또한 사용자는 웹 인터페이스, 원격 콘솔 및 시리얼 콘솔을 사용하여 STS 시리즈 펌웨어를 업그레이드할 수도 있습니다.

6.1. 시스템 상태

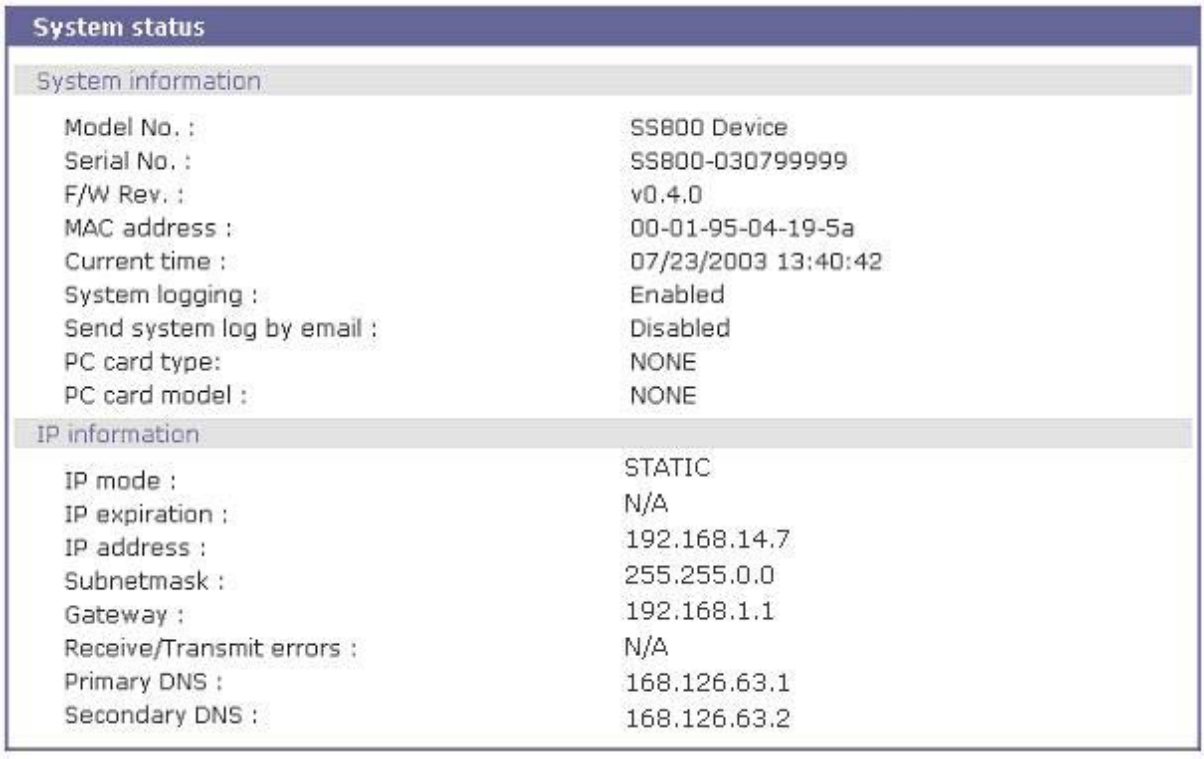


그림 6-1 시스템 상태 디스플레이

6.2. 시스템 로그 설정

STS 시리즈는 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.

- **System log storage location**

  시스템 로그는 **STS 시리즈 내부 메모리**, PC 카드 슬롯에 삽입된 **ATA/IDE fixed disk card**, **NFS 서버의 설치 지점** 또는 **SYSLOG 서버**에 저장할 수 있습니다. 시스템 로그 데이터를 저장하는데 내부 메모리를 사용하는 경우, 로그 데이터는 STS 시리즈가 꺼질 때 삭제됩니다. 시스템 로그 데이터를 보존하려면, 저장 위치를 ATA/IDE fixed disk card, SYSLOG 서버 또는 NFS 서버로 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 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.

  로그 데이터를 저장하기 위해 SYSLOG 서버 로그를 사용하는 경우, 사용자는 버퍼 크기를 설정할 필요가 없습니다.

  STS 시리즈는 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 6-2는 설정 및 시스템 로그 보기 화면을 보여줍니다.

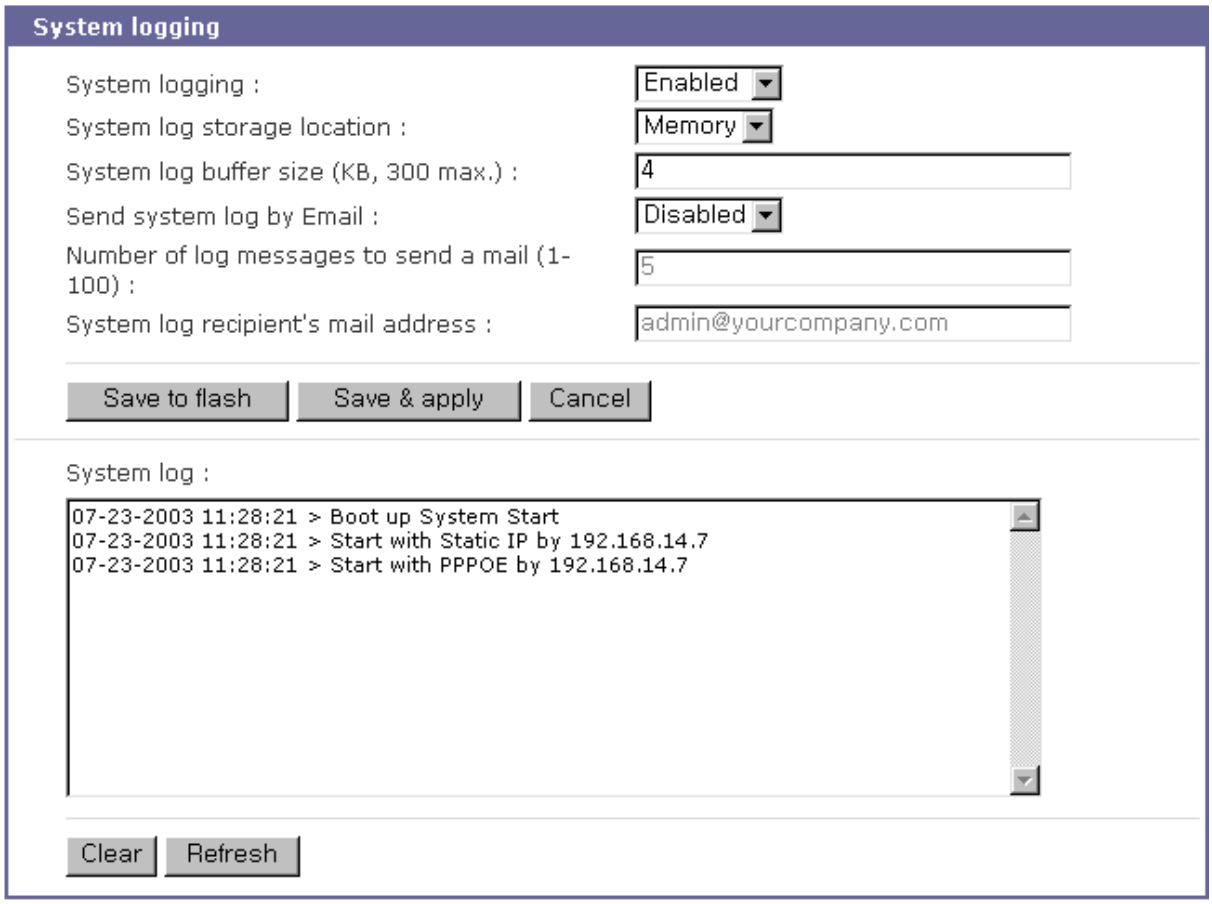


그림 6-2 시스템 로그 설정 및 보기

6.3. 사용자 로그온 목록

사용자는 시스템의 현재 및 과거의 사용자 활동을 확인할 수 있습니다.

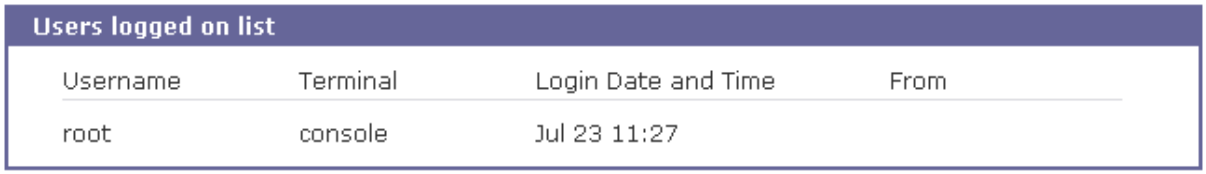


그림 6-3 사용자 로그온 목록

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)

주의:
웹을 통해 접속하는 사용자는 목록에 나타나지 않습니다. HTTP/HTTPS 프로토콜을 통해 항상 연결되는 것은 아니다.

6.4. 패스워드 변경

그림 6-4는 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.

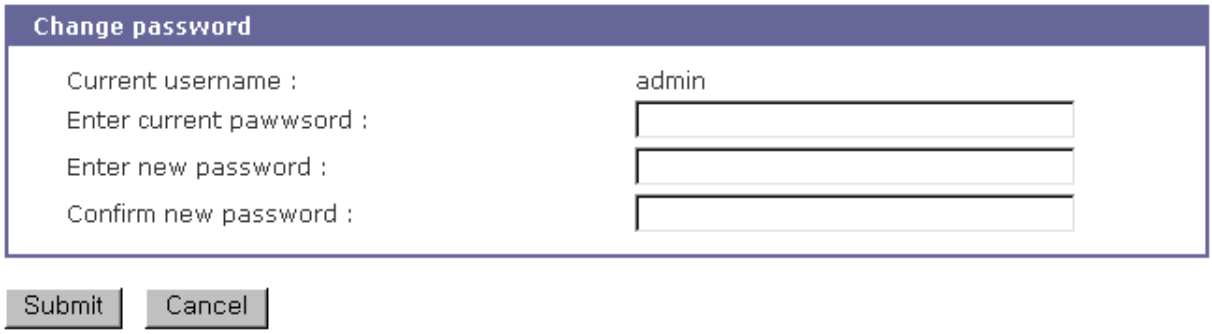


그림 6-4 패스워드 변경

6.5. Device Name Configuration

STS 시리즈의 관리를 위해 자체적으로 장비 이름을 설정할 수 있습니다. 그림 6-5는 장치 이름 설정 화면입니다. 사용자가 Device name을 변경하게 되면 STS 시리즈의 hostname 이 변경되게 되며 CLI 상의 프롬프트 또한 아래와 같이 해당되는 hostname 으로 변경이 됩니다.

그림 6-5 장치 이름 설정

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

6.6. Date and Time Settings

STS 시리즈는 현재 날짜 및 시간 정보를 관리합니다. STS 시리즈의 시계 및 달력 설정은 내부 전지 전원에 의해 유지됩니다. 그림 6-6과 같이 사용자는 현재 날짜 및 시간을 변경할 수 있습니다.

날짜 및 시간 설정에는 두 가지 방법이 있습니다. 첫 번째는 NTP서버를 사용하여 날짜 및 시간 설정을 유지하는 것입니다. NTP 기능을 사용하도록 설정하면, STS 시리즈는 시스템을 재시작할 때마다 NTP서버에서 날짜 및 시간 정보를 가져옵니다. NTP 서버를 0.0.0.0로 설정하면, STS 시리즈는 디폴트 NTP 서버를 사용합니다. 이 경우에 STS 시리즈는 네트워크를 통해서 인터넷에 연결되어 있어야 합니다. 사용자는 거주지역에 따라 국제 조정 시간(UTC: Universal Time Coordinated)과의 시간 오프셋을 설정해야 합니다. 두 번째 방법은 NTP 서버를 사용하지 않고 날짜와 시간을 수동으로 설정하는 것입니다. 이 방법을 사용하면 내부 전지를 이용하여 날짜와 시간 정보를 유지할 수 있습니다.

또한 사용자가 시스템의 날짜 및 시간을 정확하게 설정하기 위해서는 시간대(timezone)와 UTC와의 시간 오프셋 설정이 필요할 수도 있습니다. 사용자가 서머타임을 사용한다면, 서머타임 시간대, UTC와의 시간 오프셋, 시작 날짜 및 시간, 종료 날짜 및 시간과 같은 서머타임과 관련된 속성을 설정할 필요가 있습니다. 이를 통해 STS 시리즈는 정확한 시스템 시간을 계산할 수 있습니다.

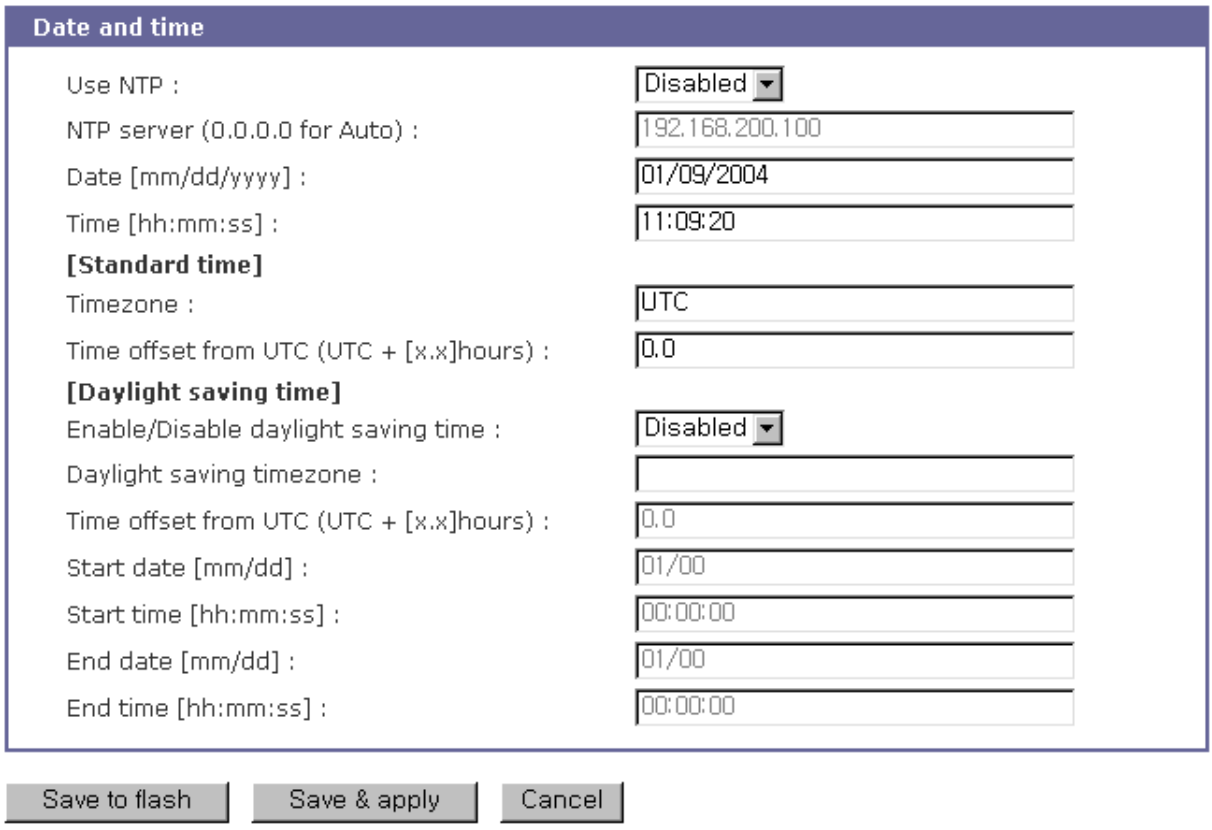


그림 6-6 날짜와 시간 구성

6.7. 설정 관리

사용자는 현재 설정 정보를 CF 카드, NFS 서버, 사용자 공간(user space) 또는 로컬 머신 같은 위치에 파일로 보낼(Export) 수 있고, CF 카드, NFS 서버, 사용자 공간 또는 로컬 머신에서 설정 정보를 들여와(Import) 현재 설정 정보로 만들 수도 있습니다.

사용자는 들여오기(Import)를 할 때 위치 속성에서 "Factory default"를 선택하거나 STS 시리즈의 뒤 패널의 공장 출하 기본 설정 스위치를 눌러 언제라도 초기 기본 설정을 복구할 수 있습니다. *그림 6-7*에서 설정 관리 화면을 보여줍니다. 설정 정보를 보내기(Export)하거나 들여오기(Import)하려면 다음 파라미터들을 적절하게 설정해야 합니다.

설정정보 보내기(Configuration export)

위치(Location) : 보내기(Export)할 위치.

암호화(Encrypt) : Yes 또는 No.

파일명(File name)

설정정보 들여오기(Configuration import)

위치(Location) : 들여오기(Import)할 위치. **Factory default**를 선택하면 초기 기본 설정을 복구할 수 있습니다.

설정정보 선택(Configuration selection) : 어떤 종류의 설정정보를 들여오기(Import)할 지를 결정합니다.

암호화(Encrypt) : Yes 또는 No. 들여오기(Import)할 위치가 **Factory default**이면 아무 영향을 주지 않습니다.

파일 선택(File selection) : CF 카드, NFS 서버, 그리고 사용자 공간 중의 선택된 위치에서 암호화 옵션을 만족하는 보내기(Export)된 파일의 목록을 보여줍니다.

로컬(Local) : 위치가 로컬 머신일 때 로컬 머신에서 보내기(Export)된 파일을 찾는 것을 도와줍니다.

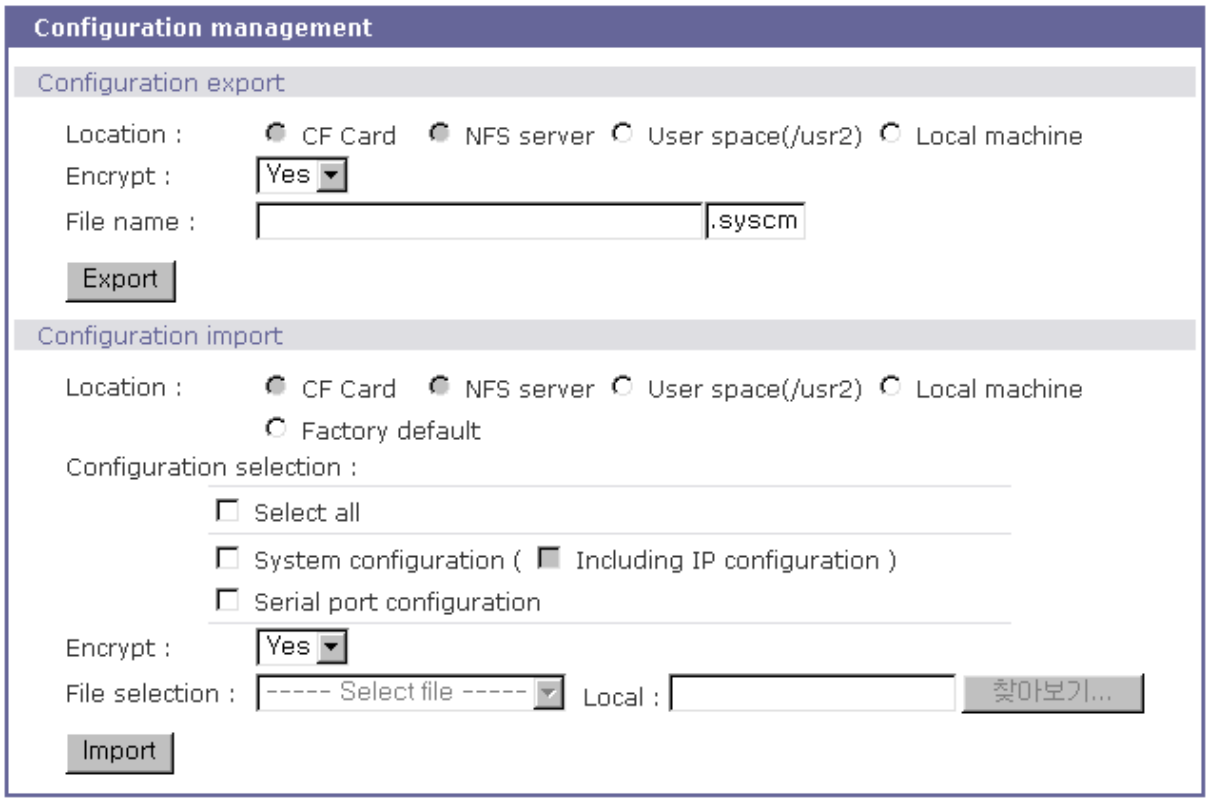


그림 6-7 설정 관리

현재 설정정보를 보내기(Export)하려면 다음 절차를 따릅니다.

1. 보내기(Export)할 위치를 선택합니다.
2. 암호화 옵션을 선택합니다.
3. 파일명을 입력합니다.
4. [Export] 버튼을 클릭합니다.

보내기(Export)된 설정정보를 들여오기(Import)하려면 다음 절차를 따릅니다.

1. 들여오기(Import)할 위치를 선택합니다.
2. 들여오기(Import)할 설정정보를 선택합니다.
3. 암호화 옵션을 선택합니다.
4. 들여오기(Import) 위치가 로컬 머신도 아니고 **Factory default**도 아니라면 파일 선택 리스트 박스에서 들여오기(Import)할 파일을 선택합니다.
5. 들여오기(Import) 위치가 로컬 머신이라면 찾아보기(browse) 버튼을 클릭하여 들여오기(Import)할 파일을 선택합니다.
6. [Import] 버튼을 클릭합니다.

6.8. 펌웨어 업그레이드

펌웨어 업그레이드는 시리얼 콘솔, 원격 콘솔 또는 웹 인터페이스를 통해 가능합니다. 최신 업그레이드는 http://www.sena.com/support/downloads/ Sena 웹사이트에서 이용할 수 있습니다. *그림 6-8*은 펌웨어 업그레이드 웹 인터페이스를 보여줍니다.

웹을 통해 펌웨어를 업그레이드하려면 다음의 절차를 따릅니다.

1. 찾아보기 버튼을 클릭하여 최신 펌웨어 바이너리를 선택합니다.
2. 선택된 버전으로 업그레이드 합니다.
3. 업그레이드를 마친 후 변경사항을 적용하기 위해서 시스템이 재시작될 것입니다.

그림 6-8 펌웨어 업그레이드

펌웨어를 업그레이드할 때 원격 콘솔 또는 시리얼 콘솔을 사용하기 위해서는 TELENT/SSH 또는 터미널 에뮬레이션 프로그램이 Z모뎀 전송 프로토콜을 지원해야만 합니다. 펌웨어 업그레이드 후에는 이전의 환경설정은 IP 설정 설정을 제외하고 초기 기본 설정으로 리셋될 것입니다.

원격 콘솔을 이용하여 펌웨어를 업그레이드 하기 위해서는 다음의 절차를 따릅니다.

1. 최신 펌웨어를 구합니다.
2. TELENT/SSH 또는 시리얼 콘솔 포트를 사용하여 터미널 에뮬레이션 프로그램을 연결합니다.
   (시리얼 콘솔 포트를 이용할 경우 상당히 오래 걸리므로, Telnet 또는 SSH를 사용하기를 권장합니다.)
3. 그림 6-9에 보이는 것처럼 펌웨어 업그레이드 메뉴를 선택합니다.
4. 온라인 지시사항을 따르고 그림 6-10에 보이는 것처럼 Z모뎀 프로토콜을 사용하여 펌웨어 바이너리 파일을 전송합니다.
5. 업그레이드가 끝나면 변경 사항을 적용하기 위해 시스템이 재시작될 것입니다.
6. 펌웨어 업그레이드를 실패하면, STS 시리즈는 그림 6-11처럼 에러 메시지를 표시할 것입니다. 또한 STS 시리즈는 현재 펌웨어 버전을 유지하게 됩니다.

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

--------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 07/23/2003 15:04:07    F/W REV.:    v1.0.0
 Serial No.:   STS800438349-42944     MAC address: 00-01-95-04-19-5a
 IP mode:     Static IP            IP address:  192.168.14.7
--------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
---> 4
--------------------------------------------------------------------------------
 System administration
--------------------------------------------------------------------------------
 Select menu:
  1. System status
  2. System logging
  3. Device name: STS800 Device
  4. Date and time
  5. Change password
  6. User file upload
  7. Reload factory default settings
  8. Reload factory default settings except IP settings
  9. Firmware upgrade
  <ESC> Back, <Enter> Refresh
--->9
Do you want to upgrade firmware? (y/n): y
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157
```

그림 6-9 원격 또는 시리얼 콘솔을 사용한 펌웨어 업그레이드

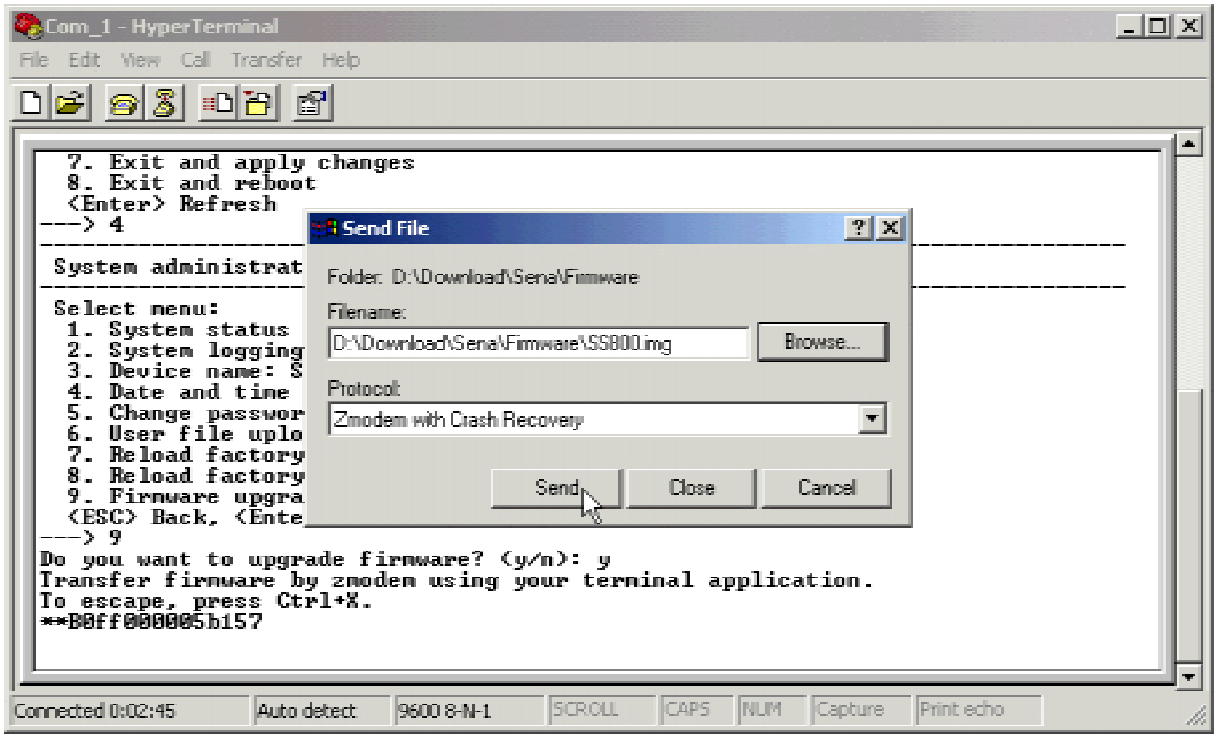


그림 6-10 Z모뎀 (HyperTerminal)을 이용한 바이너리 파일 전송)

```
--->9
Do you want to upgrade firmware? (y/n): y
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157
**B0ff000005b157
**B0ff000005b157
**B0ff000005b157
Firmware upgrade failed !
 Now reboot ...
```

그림 6-11 펌웨어 업그레이드 실패 메시지

6.9. 사용자 파일 업로드하기

사용자는 자신의 파일을 STS 시리즈에 업로드할 수 있습니다. 그러나 파일 업로드 기능은 콘솔 메뉴에서만 지원됩니다. 파일 업로드 메뉴는 그림 6-12에서 보여지듯이 콘솔 메뉴의 *"4. System administration --> 6. User file upload"*에 위치해 있습니다.

사용자가 콘솔 메뉴를 사용해서 STS 시리즈에 파일을 업로드하기 위해서는, 반드시 Z모뎀 전송 프로토콜을 지원하는 TELNET/SSH 또는 터미널 에뮬레이션 프로그램을 사용해야 합니다. 업로드 절차는 다음과 같이 콘솔 메뉴를 사용해서 펌웨어를 업그레이드하는 과정과 비슷합니다.

1. 업로드할 사용자 파일을 준비합니다.

2. TELNET/SSH 또는 시리얼 콘솔 포트를 사용해서 터미널 에뮬레이션 프로그램에 접속합니다.
   (시리얼 콘솔 포트를 이용할 경우 상당히 오래 걸리므로, Telnet 또는 SSH를 사용하기를 권장합니다.)
3. *그림 6-12*와 같이 사용자 파일 업로드 메뉴에서 선택을 합니다.
4. 그림 6-10에 보이는 것처럼 온라인 지시사항 따라 Z모뎀 프로토콜을 사용해서 사용자 파일을 전송합니다.
5. 일단 업로드가 완료되면 시스템은 그림 6-12와 같이 성공 메시지를 표시할 것입니다.
6. 업로드를 실패하면 STS 시리즈는 그림 6-13같이 에러 메시지를 표시할 것입니다.

주의

사용자 파일 업로드는 오직 사용자 공간 (/usr2) 디렉토리에서만 허용됩니다. STS 시리즈내부의 파일 시스템에 관한 더 많은 정보를 보려면, *8.2 플래시 파티션* 절을 참조하시기 바랍니다.

```
--------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 08/14/2003 11:56:13     F/W REV.    : v1.0.0
 Serial No.  : STS800438349-42944      MAC address: 00-01-95-04-d3-03
 IP mode     : DHCP                    IP address : 192.168.222.206
--------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
---> 4
--------------------------------------------------------------------------------
 System administration
--------------------------------------------------------------------------------
 Select menu:
  1. System status
  2. System logging
  3. Device name: STS800 Device
  4. Date and time
  5. Change password
  6. User file upload
  7. Reload factory default settings
  8. Reload factory default settings except IP settings
  9. Firmware upgrade
  <ESC> Back, <Enter> Refresh
---> 6
 Do you want to upload a file to user space? (y/n): y
 Enter a filename: test.txt
 The file will be saved as /usr2/test.txt.
 Transfer a file by zmodem using your terminal application.
 To escape, press Ctrl+X.
**B01ff000005b157

Uploading a file is completed.
```

그림 6-12 사용자 파일 업로드 메뉴와 성공 메시지

```
Do you want to upload a file to user space? (y/n): y
 Enter a filename: test.txt
 The file will be saved as /usr2/test.txt.
 Transfer a file by zmodem using your terminal application.
 To escape, press Ctrl+X.
**B01ff000005b157

Uploading a file failed.
```

그림 6-13 사용자 파일 업로드 실패 메시지

7. 시스템 통계

STS 시리즈 웹 인터페이스는 시스템 통계 화면을 제공합니다. 사용자는 시스템 통계 화면을 참조하여 STS 시리즈 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 설정 요소들에 대한 사용 통계를 나타냅니다.

7.1. 네트워크 인터페이스(Network Interfaces) 통계

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

Network interfaces statistics

Interface		lo	eth0
Receive	Bytes	680	7448861
	Packets	8	8057
	Errors	0	0
	Drop	0	0
	FIFO	0	0
	Frame	0	0
	Compressed	0	0
	Multicast	0	0
Transmit	Bytes	680	766794
	Packets	8	3991
	Errors	0	0
	Drop	0	0
	FIFO	0	0
	Frame	0	330
	Compressed	0	0
	Multicast	0	0

그림 7-1 네트워크 인터페이스 통계

7.2. 시리얼 포트 통계

시리얼 포트 통계는 32개의 시리얼 포트의 사용 통계, Baud rate 설정 및 각 포트의 핀 상태를 나타냅니다. (: On : Off)

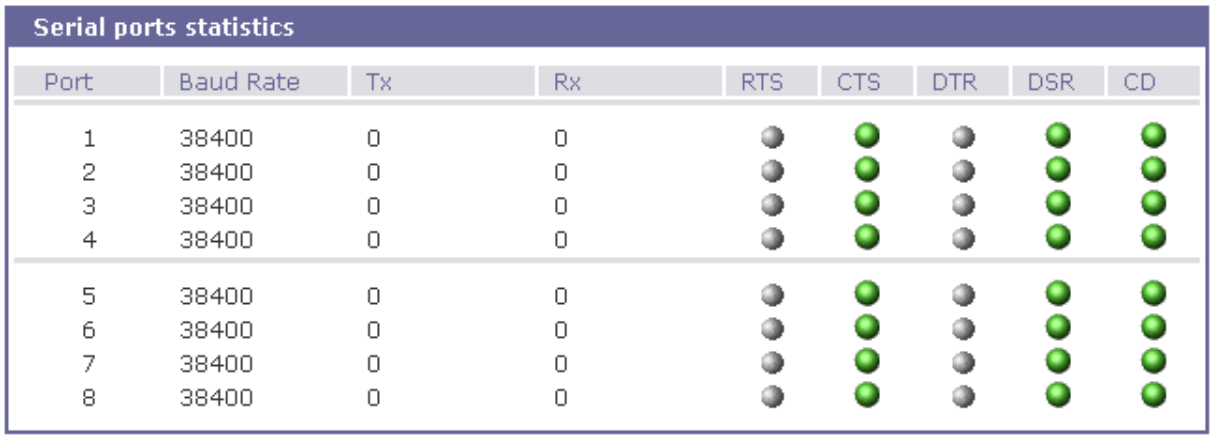


그림 7-2 시리얼 포트 상태

7.3. 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(잘못된 체크섬(checksum),맞지 않는 버전 넘버, 기타 포맷 에러, TTL 초과 등)

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 데이터그램의 수

FragFails :

fragmentation 실패한 데이터그램의 수

FragCreates :

생성된 fragment 수

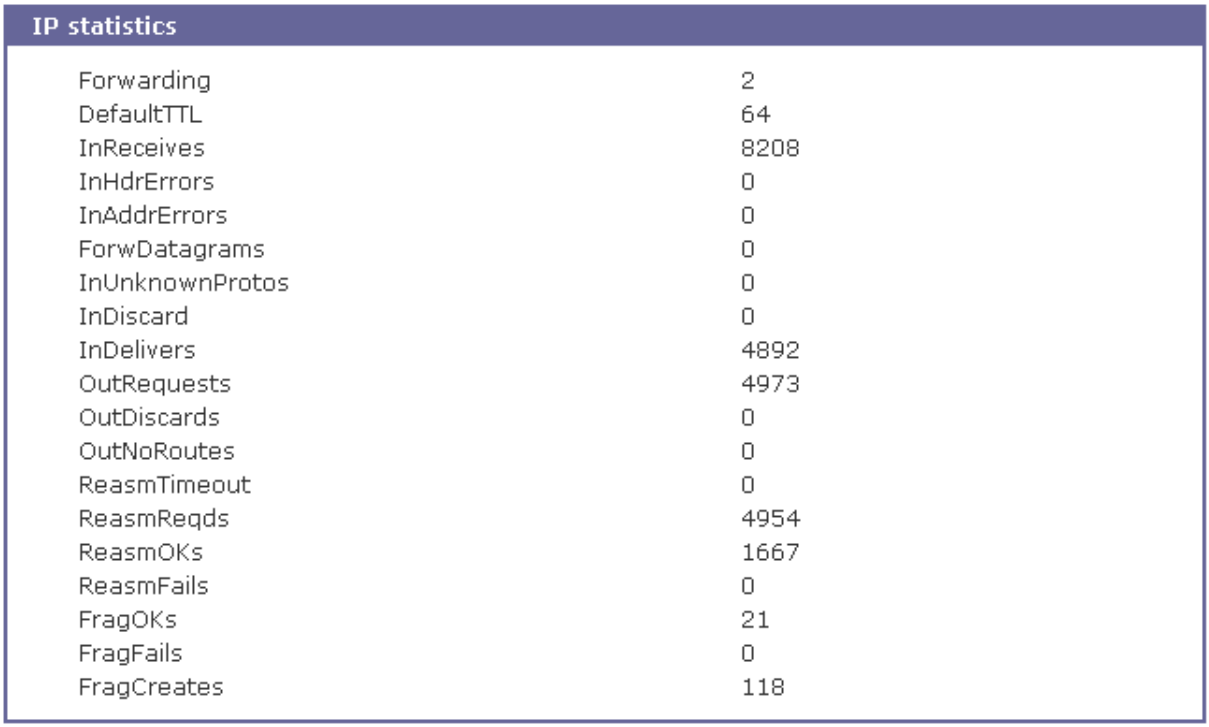


그림 7-3 IP 통계

7.4. 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 메시지 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 :

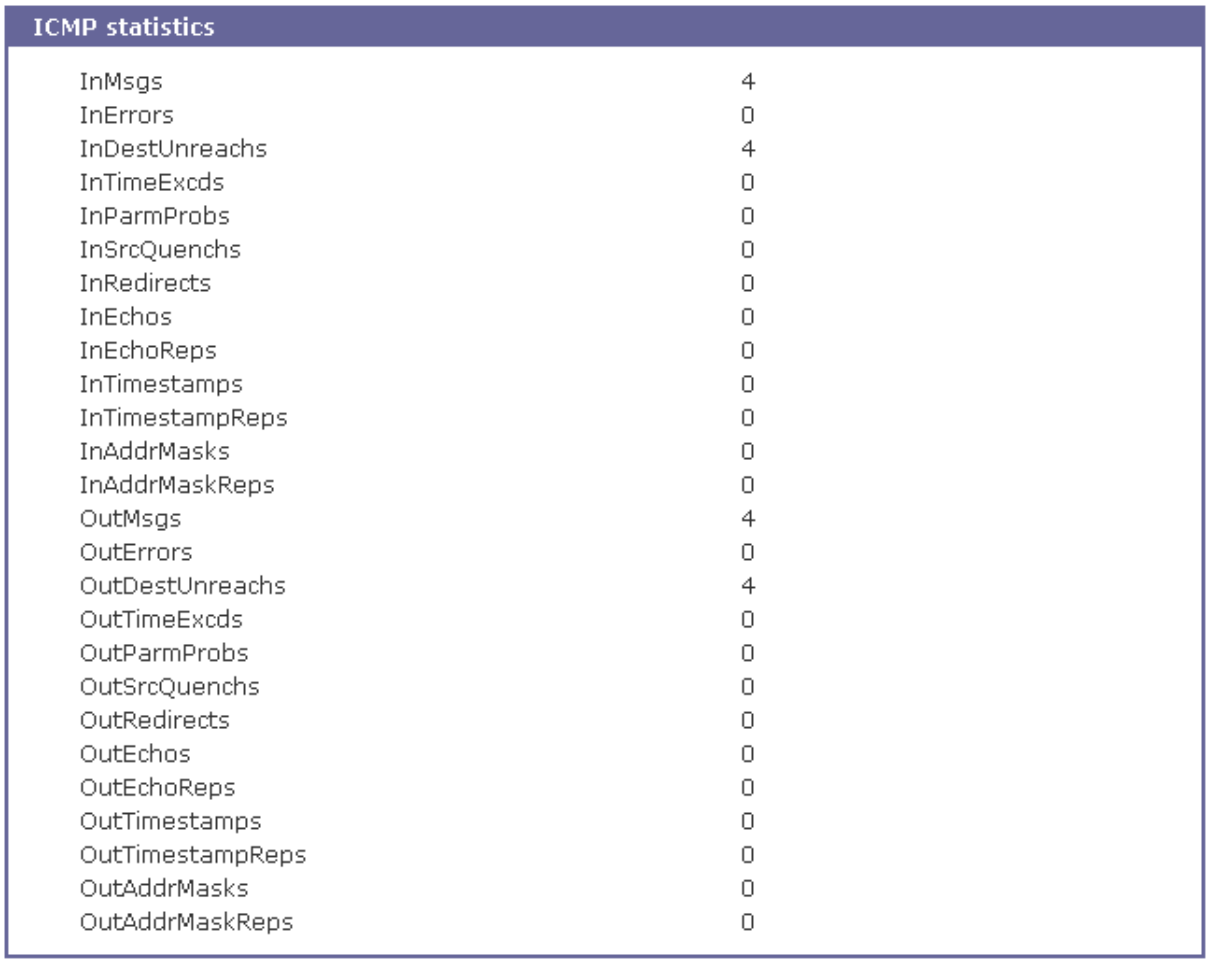
수신 또는 전송된 time-stamp 응답의 수

InAddrMasks, OutAddrMasks :

수신 또는 전송된 주소 마스크의 수

InAddrMaskReps, OutAddrMaskReps :

수신 또는 전송된 주소 마스크 응답의 수



ICMP statistics	
InMsgs	4
InErrors	0
InDestUnreachs	4
InTimeExcds	0
InParmProbs	0
InSrcQuenchs	0
InRedirects	0
InEchos	0
InEchoReps	0
InTimestamps	0
InTimestampReps	0
InAddrMasks	0
InAddrMaskReps	0
OutMsgs	4
OutErrors	0
OutDestUnreachs	4
OutTimeExcds	0
OutParmProbs	0
OutSrcQuenchs	0
OutRedirects	0
OutEchos	0
OutEchoReps	0
OutTimestamps	0
OutTimestampReps	0
OutAddrMasks	0
OutAddrMaskReps	0

그림 7-4 ICMP 통계

7.5. 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 부록 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

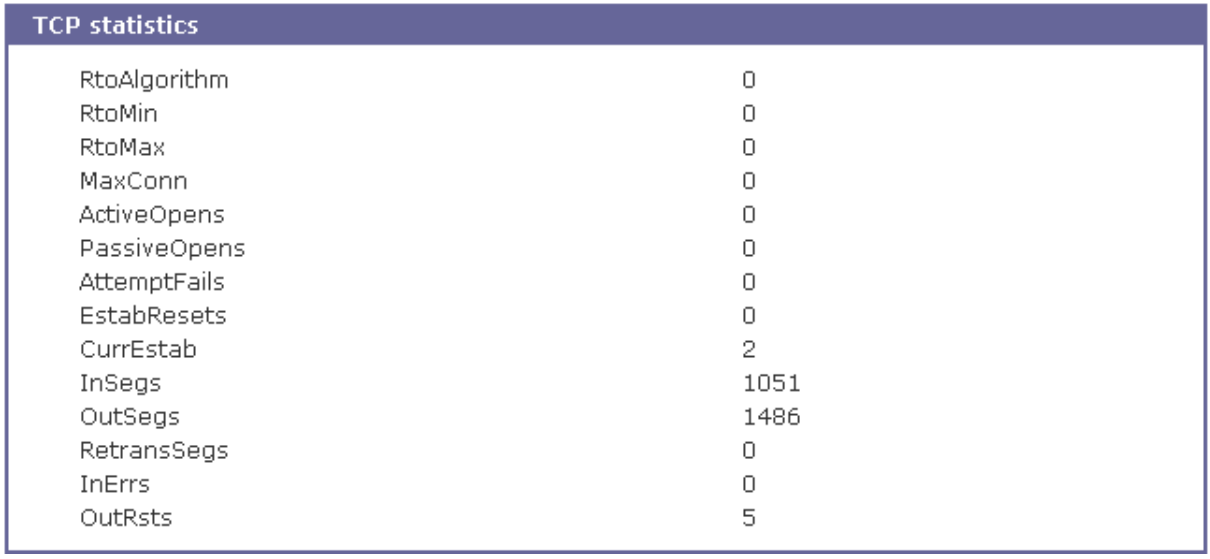


그림 7-5 TCP 통계

7.6. UDP 통계

UDP 통계 화면은 UDP 프로토콜을 사용하는 패킷 또는 연결에 관한 통계 정보를 제공합니다. 아래에 각 파라미터의 정의 및 설명이 나와 있습니다.

InDatagrams :

수신된 데이터그램의 수

NoPorts :

지정된 포트가 유효하지 않아 폐기 처분된 수신 데이터그램의 수

InErrors :

수신된 오류 데이터그램의 수

OutDatagrams :

전송된 데이터그램의 수

그림 7-6 UDP 통계

8. CLI 안내서

8.1. 서론

root 또는 **System admin** 은 시스템 콘솔 또는 Telnet/SSH 원격 콘솔을 통해 STS 시리즈의 Linux 콘솔 커맨드라인 인터페이스(CLI)에 접속 할 수 있습니다. CLI 에서 인증된 사용자는 표준 Linux 명령을 통하여 STS 시리즈 상태를 감시하고, 설정을 편집하고 변경 사항을 적용하고, 사용자 정의 script를 실행하며 원격 호스트와 STS 시리즈 사이에서 파일을 전송할 수 있습니다.

STS 시리즈는 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 admin은 CLI에 접속 할 수 없습니다. 콘솔 설정 메뉴나 웹을 통해서만 접속할 수 있습니다.

8.2. 플래시 구성

STS 시리즈 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 STS 시리즈에 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 STS 시리즈 가 올바르게 동작하지 않을 수 있습니다. 최악의 경우, STS 시리즈가 작동하지 않을 수도 있습니다.

Block	Type	Mount point	Size (KB)
Mtdblock0	Bootloader	None	128
Mtdblock1	Kernel	None	768
Mtdblock2	CRAMFS (Read only)	/	6080
Mtdblock3	Ram disk image (4MB)	/etc, /var, /tmp	64
Mtdblock4	EXT2 (R/W)	/cnf (normally unmounted)	64
Mtdblock5	JFFS2 (R/W)	/usr2	1024
Mtdblock6	Reserved	None	64
Total			8192

8.3. 지원되는 Linux 유틸리티

8.3.1. Shell 및 shell utilities:

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

8.3.2. File 및 disk utils:

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

8.3.3. 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, who

8.3.4. 네트워크 유틸리티:

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

8.4. root 또는 system admin으로 CLI 접속하기

시리얼 콘솔:

1) PC의 시리얼 포트와 STS 시리즈의 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) STS 시리즈 root 계정이나 admin 계정으로 로그인합니다.

Telnet 콘솔:

1) telnet *STS 시리즈_ip_address*

8.5. 예제

8.5.1. 장치의 telnet disable 하기

STS 시리즈 장치는, 원격 콘솔 포트(SSH 용 TCP 포트 22 또는 telnet용 TCP 포트 23)들을 개별적으로 비활성화 하는 기능을 지원하지는 않습니다. 사용자는 웹/Telnet/SSH 를 통한 STS 시리즈 설정 메뉴를 통해서는 모든 원격 콘솔을 비활성 또는 활성 상태가 되도록 할 수만 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.

Example1. '`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` script를 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 script`를 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, STS 시리즈를 원래 설정치 대로 복원하면, /usr2/rc.user script 파일의 이름은 /usr2/rc.user.old# 파일로 저장되며 원래의 rc.user 파일이 복구됩니다.

8.5.2. 주기적인 프로그램 실행

사용자는 crontab을 이용하여 주기적으로 특정 프로그램을 실행할 수 있습니다. crontab을 이용하여 주기적 작업을 가능하게 하려면 다음의 단계들을 완료해주시기 바랍니다.

단계 1 /usr2 디렉토리에 crontab 파일을 생성합니다. 다음의 샘플 crontab 파일은 /tmp 디렉토리 밑에 current-date 파일을 생성하고 그 내용을 2분마다 갱신합니다.

```
SHELL=/bin/bash
# Sample crontab job
# Run every two minutes
* * * * * echo `date` > /tmp/current_date
```

단계 2 다음의 명령을 이용해서 crontab 파일을 등록합니다.

```
root@STS800_Device:/usr2# crontab samplecrontab_file
```

단계 3 시스템을 매번 재시작할 때에도 cron 작업을 영구적으로 만들려면 다음과 같이 rc.user 스크립트를 사용하면 됩니다.

```
#!/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
crontab /usr/samplecrontab_file

exit 0
```

STS에서는 –e 옵션(에디터를 사용하여 현재 crontab을 편집)이 지원되지 않는다는 것을 주의하시기 바랍니다. 따라서 사용자는 반드시 vi 에디터를 사용하여 crontab 파일의 내용을 변경해야 합니다.

crontab 파일의 포맷에 관한 자세한 정보는 리눅스 crontab 매뉴얼을 참조하십시오. (man 5 crontab).

부록 1. 연결

A 1.1 Ethernet Pin outs

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

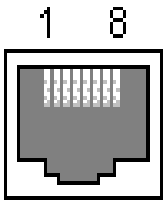


그림 A-1 RJ45 커넥터의 핀 배치

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 1.2 콘솔 및 시리얼 포트 Pin out

STS 시리즈는 콘솔 및 시리얼 포트 용 RJ45 커넥터를 사용합니다. 시리얼 포트용 RJ45 커넥터의 핀 지정은 표 A-3에 요약되어 있습니다. 각 핀에는 시리얼 통신 설정에 따른 기능이 있습니다.

표 A-1 콘솔 및 시리얼 포트용 RJ45 커넥터 핀 할당

Pin	**RS232** (console and serial ports)
1	CTS
2	DSR
3	RxD
4	GND
5	DCD
6	TxD
7	DTR
8	RTS

A 1.3 Ethernet 결선도

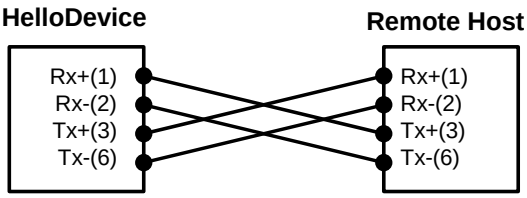


그림 A-2 Ethernet direct connection using crossover Ethernet cable

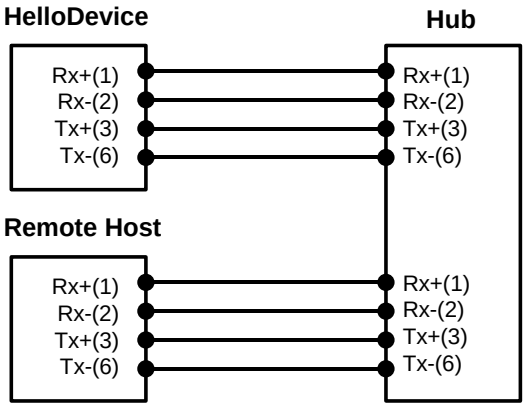


그림 A-3 Ethernet connection using straight through Ethernet cable

A 1.4 RS232 시리얼 배선도

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

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

부록 2. STS 시리즈가 지원하는 PC 카드

STS 시리즈 시리즈는 다음의 PC 카드를 지원합니다.

표 A-2 네트워크 카드

Manufacturer	Model/Name	STS probed Model name	Specification
3COM	3CXE589ET-AP	3Com Megahertz 589E TP/BNC LAN PC Card	10 Mbps LAN card
Linksys	Linksys EtherFast 10/100 Integrated PC Card (PCM100)	Linksys EtherFast 10/100 Integrated PC Card (PCM100) Ver 1.0	10/100 Mbps LAN card
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 A-3 무선 네트워크 카드

Manufacturer	Model/Name	STS probed Model name	Specification
Cisco Systems	AIR-PCM340/Aironet 340	Cisco Systems 340 Series Wireless LAN Adapter	11 Mbps Wireless LAN Adapter
Lucent Technologies	PC24E-H-FC/Orinoco Silver	Lucent Technologies WaveLAN/IEEE Version 01.01	11 Mbps Wireless LAN Adapter
Lucent Technologies	PC24E-H-FC/Orinoco Gold	Lucent Technologies WaveLAN/IEEE Version 01.01	11 Mbps Wireless LAN Adapter
Agere Systems (Lucent Technologies)	Orinoco Classic Gold (PC24E-H-FC/Orinoco Gold)	Lucent Technologies WaveLAN/IEEE Version 01.01	11 Mbps Wireless LAN Adapter
Buffalo	AirStation (WLI-PCM-L11GP)	MELCO WLI-PCM-L11 Version 01.01	11 Mbps Wireless LAN Adapter

표 A-4 ATA/IDE Fixed 디스크 카드

Manufacturer	Model/Name	STS probed Model name	Specification
Advantech	CompactFlash	CF 48M	48 MB Storage card
SanDisk	SDP series	SunDisk SDP 5/3 0.6	64 MB Storage card
SanDisk	SDP series	SanDisk SDP 5/3 0.6	256 MB Storage card
Kingston	CompactFlash Storage Card	TOSHIBA THNCF064MAA	64 MB Storage card
Viking	CompactFlash	TOSHIBA THNCF064MBA	64 MB Storage card

표 A-5 시리얼 모뎀 카드

Manufacturer	Model/Name	STS probed Model name	Specification
Billionton Systems Inc.	FM56C series	PCMCIA CARD 56KFaxModem FM56C-NFS 5.41	Ambient (Intel) V.90 FAX/MODEM PC Card
Viking	PC Card Modem 56K	Viking V.90 K56flex 021 A	MODEM PC Card
KINGMAX	KIT PCMCIA 56K Fax/Modem Card	CIRRUS LOGIC 56K MODEM CL-MD56XX 5.41	V.90 FAX/MODEM PC Card
TDK	TDK DH6400	TDK DH6400 1.0	64Kbps
NTT DoCoMo	Mobile Card Triplex N	NTT DoCoMo Mobile Card Triplex N	64Kbps

부록 3. STS 시리즈 설정 파일

A 3.1 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

# 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.
bsmtp = 0
smtpsvr = smtp.yourcompany.com
sysmailaddr = STS800@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 = STS800 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 = ss800.dyndns.biz
dyn_user = ss800-user
dyn_pwd = ss800-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

# 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
```

A 3.2 Redirect.cnf

```
#
# redirect.cnf
#
#   Port configuration is placed on this file.
#   Basically keys followed by 'port' key are data for those port.
#   Port number is zero base 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

# As refered, maximum port (in case 8 port machine ,8) represents the
# defaults values for all port configuration.
port = 8
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 control. 0 for none, 1 for XON/XOFF,
#                                    2 for hardware flow control
# 'dtropt' is for DTR pin option.
#  1 = Always HIGH, 2 = Always LOW, 3 = High when open
# 'dsropt' is for DSR pin option.
#  0 = None, 1 = Allow TCP connection only by HIGH 2 = open/close TCP connection
# '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
dsropt = 0
interchartimeout = 100

# Host mode configuration
# 'hostmode' means a host mode.
#  0 = TCP mode, 1 = UDP mode, 2 = Mode emulation
hostmode = 0
# In TCP mode, 'localport' is a listening port.
localport = 0
# 'max_connection' is a maximum allowed number of remote host
```

```
max_connection = 32
# 'remotehost' is a remote host list
#                   (Primary IP address:port Secondary IP address:port)
remotehost = 192.168.0.135:7000 192.168.0.135:7001
# 'cyclictime ' is a cyclic connection time in seconds
cyclictime = 10
# 'inactivitytimeout' is a inactivity timeout in seconds.
inactivitytimeout = 100

# Cryptography Options
# 'encryptionmode' is encryption mode
# 0 = None, 1 = SSLv2, 2 = SSLv3, 3 = SSLV3 rollback v2, 4 = TLSv1
# 'encryptionkey' is encryption key file name
# 'key_password' is password for encryption key file
# 'cipher_suite' represents a combination of cipher suite.
# 'verify_client' is Verify client(server mode only) option
#  0 = No, 1 = Yes
# 'verify_chain_depth' is a number of chain depth to be searched
# 'verify_cn' is Compare the certificate CN and hostname option
#  0 = No, 1 = Yes
encryptionmode = 2
encryptionkey =
key_password = testing
cipher_suite = 524287
verify_client = 1
verify_chain_depth = 3
verify_cn = 1


# In UDP mode,
# 'accept_unlisted' is Accept UDP datagram from unlisted remote host option
# 0 = No, 1 = Yes
# 'send_to_unlisted' Send to recent unlisted remote host option
# 0 = No, 1 = Yes
accept_unlisted = 1
send_to_unlisted = 1

# 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

# Mode configuration option
# 'modem_mode' is modem mode option
# 0 =Disable, 1 =Enable
# 'modem_initstr' is a modem initialization string
# 'modem_dcd_option' is modem DCD pin option
# 0 = None, 1 = Allow TCP connection only by HIGH
modem_mode = 0
modem_initstr =
modem_dcd_option = 0

# Event notification configuration
# Enable of disable Event notification by setting 'event_enable' to 1 or 0.
# 'notification_interval' is interval of event notification.
# 'bmail_handle' is a Enable/Disable E-mail notification option
# 0 = Disable, 1 = Enable
# 'mail_title' is a title of email notification.
# 'mail_address' is a mail recipient’s address
# 'bsnmp_handle' is a Enable/Disable SNMP notification option
# 0 = Disable, 1 = Enable
# 'snmp_title' is a title of SNMP trap notification.
# 'snmp_trap_receiver_ip' is a IP address of SNMP Trap receiver
```

```
# 'snmp_trap_receiver_community' is community of SNMP Trap
# 'snmp_trap_receiver_version' is SNMP trap version
# 0 = v1, 1 = v2c
event_enable = 1
notification_interval = 0
bmail_handle = 1
mail_title = jungoj@sena.com
mail_address = jung@sss.com
bsnmp_handle = 1
snmp_title = khfgj
snmp_trap_receiver_ip = 192.168.0.8
snmp_trap_receiver_community = public
snmp_trap_receiver_version = 0

# Event Keyword option
# 'keyword_index' is a index of keyword event
# 'keyword_str' is a event keyword
# 'snmp_enable' is a SNMP notification option for keyword
# 0 = Disable, 1 = Enable
# 'mail_enable' is a email notification option for keyword
# 0 = Disable, 1 = Enable
# 'command_enable' is a port command option for keyword
# 0 = Disable, 1 = Enable
# 'port_command' is a port command string for keyword
keyword_index = 0
keyword_str = test
snmp_enable = 1
mail_enable = 1
command_enable = 1
port_command = fghfgh

# 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
```

부록 4. 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 A-6 Well-known port numbers

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 5. Guide to the Bootloader 메뉴 프로그램 안내서

A 5.1 개요

Bootloader 메뉴는 비상 시, 복구 옵션으로 BOOTP/TFTP를 사용하여 STS 시리즈를 복구하고 시스템 하드웨어를 진단하는 방법을 제공합니다. STS 시리즈 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.

A 5.2 메인 메뉴

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

```
Bootloader 1.1.0 (May 23 2003 - 22:48:25)

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 : v1.0.0]
 4. Exit and boot from flash
 5. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 A-4 Bootloader 메인 프로그램의 메인 메뉴 페이지

A 5.3 RTC 설정 메뉴

RTC 설정 메뉴를 사용함으로써, 사용자는 STS 시리즈의 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 A-5 Bootloader 메뉴 프로그램 내의 RTC 설정

A 5.4 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.

주의:

Ethernet 및 UART에서 테스트를 적절히 수행하려면, 사용자는 STS 시리즈의 Ethernet 포트에 Ethernet 케이블을 반드시 연결하고 루프백 커넥터를 STS 시리즈의 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. Ethernet test
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 A-6 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. 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 # 7 test in progressing(Read/Write)----------[SUCCESS]
Port # 8 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 # 7 test in progressing(Read/Write)----------[SUCCESS]
                       (RTS/CTS)-------------[SUCCESS]
                       (DTR/DSR)-------------[SUCCESS]
Port # 8 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

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 A-7 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. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. 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 A-8 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.

A 5.5 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 [sts800.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 [sts800.bin]
```

```
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 A-9 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 [sts800.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 'sts800.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 [sts800.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

그림 A-10 firmware upgrade 프로세스

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

.

부록 6. Serial/IP로 STS 시리즈 사용하기

A 6.1 STS 시리즈와 Serial/IP의 옵션 비교

표 A-7 STS 시리즈 vs. Serial/IP 옵션 호환성 행렬 테이블

Serial Port Configuration of STS Series			**Serial/IP Configuration**		
Host mode Configuration		Cryptography Configuration	Credentials	Connection Protocol	Security
Host mode	Telnet Protocol	Encryption Method			
TCP	Disabled	None	No login required	Raw TCP connection	Disable
TCP	Enabled	None	No login required	Telnet	Disable
TCP	Disabled	“SSLv2” or “SSLv3 rollback to v2”	No login required	Raw TCP connection	Negotiate SSLv3/TSLv1
TCP	Disabled	“SSLv3” or “SSLv3 rollback to v2”	No login required	Raw TCP connection	SSLv3
TCP	Disabled	“TLSv1” or “SSLv3 rollback to v2”	No login required	Raw TCP connection	TSLv1
TCP	Enabled	“SSLv2” or “SSLv3 rollback to v2”	No login required	Telnet	Negotiate SSLv3/TSLv1
TCP	Enabled	“SSLv3” or “SSLv3 rollback to v2”	No login required	Telnet	SSLv3
TCP	Enabled	“TLSv1” or “SSLv3 rollback to v2”	No login required	Telnet	TSLv1

STS 시리즈에 “SSLv3 rollback to v2” 옵션은 Serial/IP에 “Negotiate SSLv3/TSLv1”과 같은 것입니다. “SSLv3”로 STS 시리즈의 암호화 메소드가 설정되었다면, Serial/IP는 “Negotiate SSLv3/TSLv1”

옵션으로는 STS 시리즈와 연결될 수 없습니다.

A 6.2 연결 예제 - Telnet 및 SSLv3 encryption

단계 1. 다음과 같이 1번 시리얼 포트를 호스트 모드로 설정합니다.

Host mode = TCP,

TCP listening port = 7001,

Telnet protocol = Enabled

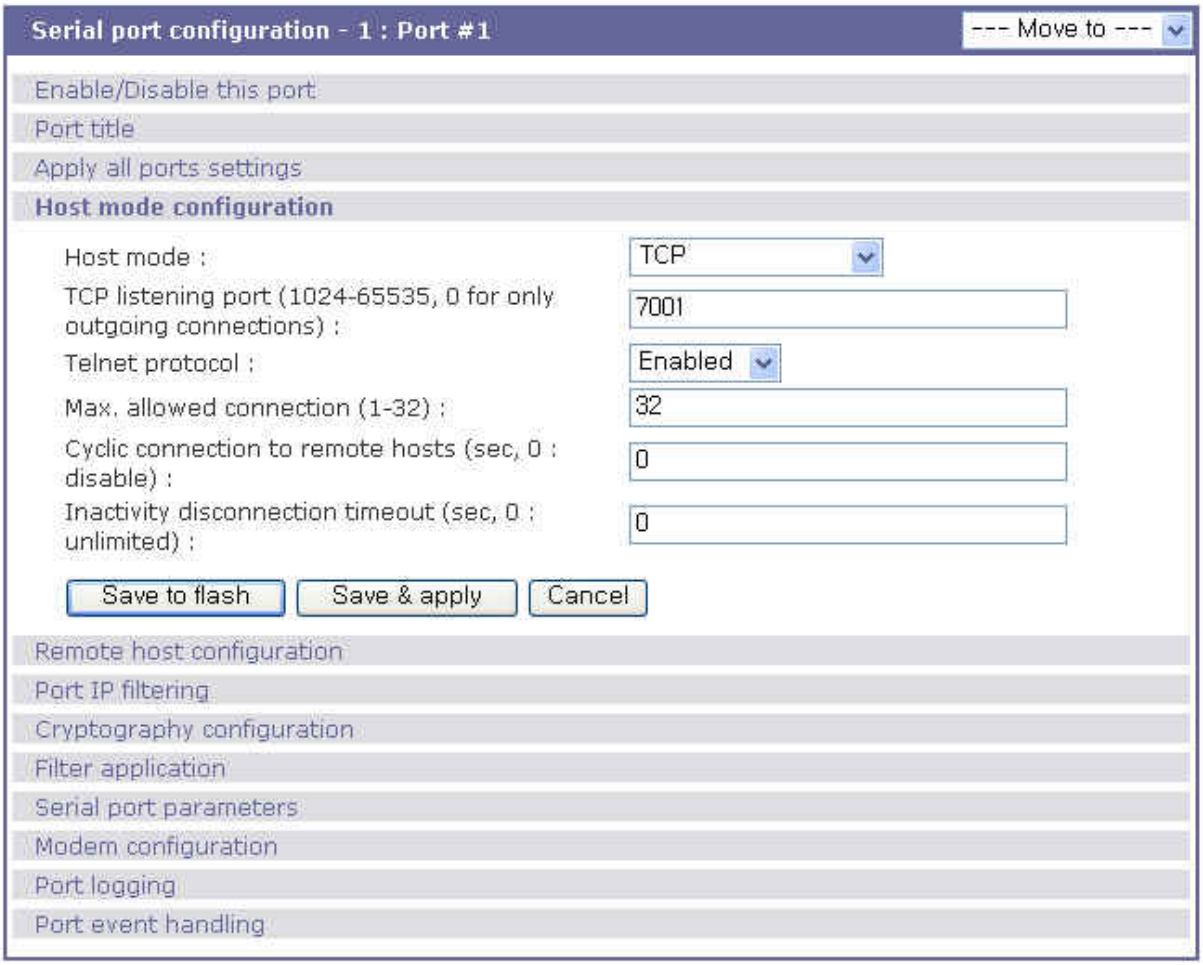


그림 A-11 호스트 모드 설정

단계 2. 다음과 같이 1번 시리얼 포트를 암호화 기능 설정(Cryptography configuration) 합니다.

Encryption method = SSLv3

나머지 옵션은 고장 출하시의 기본 값으로 놔두십시오.

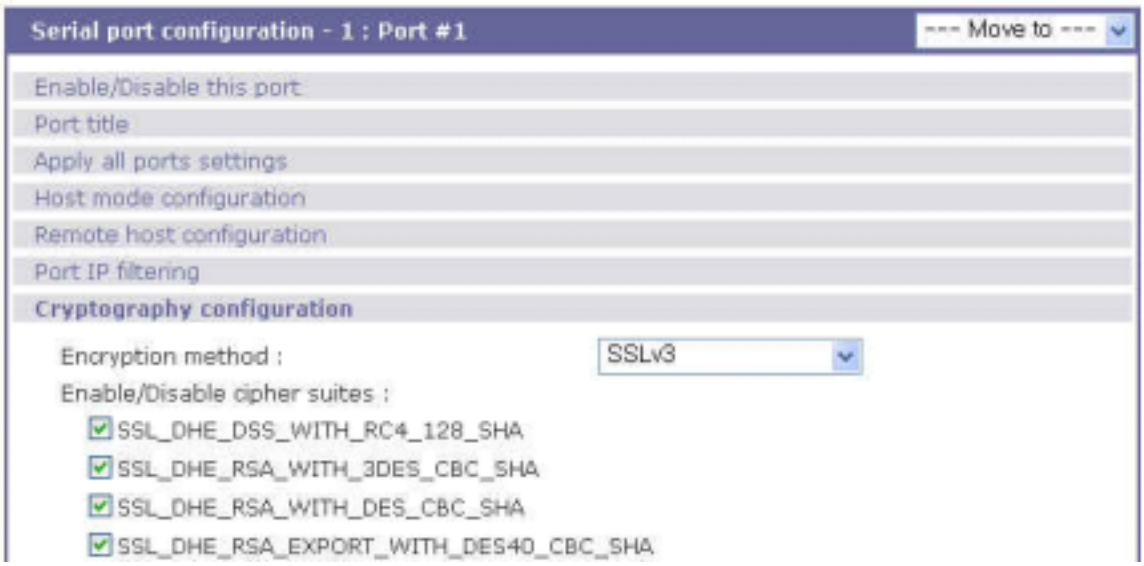


그림 A-12 암호기법 설정(Cryptography configuration)

단계 3. Open Serial/IP Control Panel을 열고, STS 시리즈의 1번 시리얼 포트와 통신하길 원하는 COM 포트를 "Select Ports" 버튼을 눌러 선택합니다.

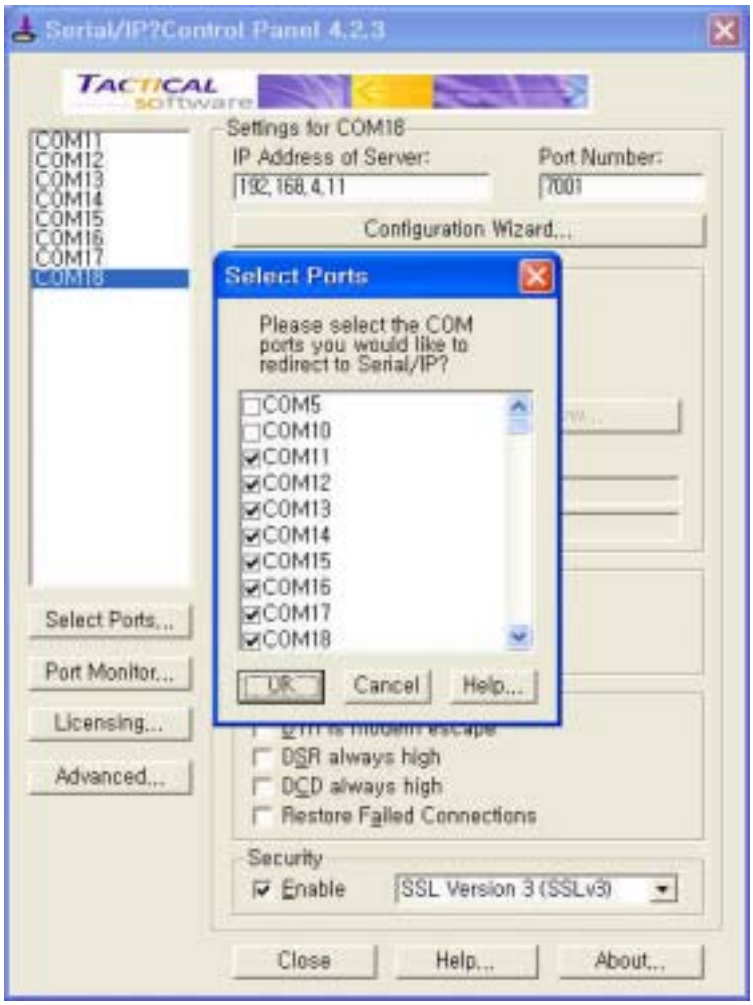


그림 A-13 Serial/IP Control Panel에서 포트들을 선택

단계 4. Enter 서버의 IP 주소(ISuper 시리즈 IP 주소)와 포트 넘버(1번 시리얼 포트의 포트 넘버)를 정확하게 입력하고 다음과 같이 다른 파라미터들을 선택합니다.

Credentials = No Login Required,

Connection Protocol = Telnet,

Security = SSL Version 3 (SSLv3)

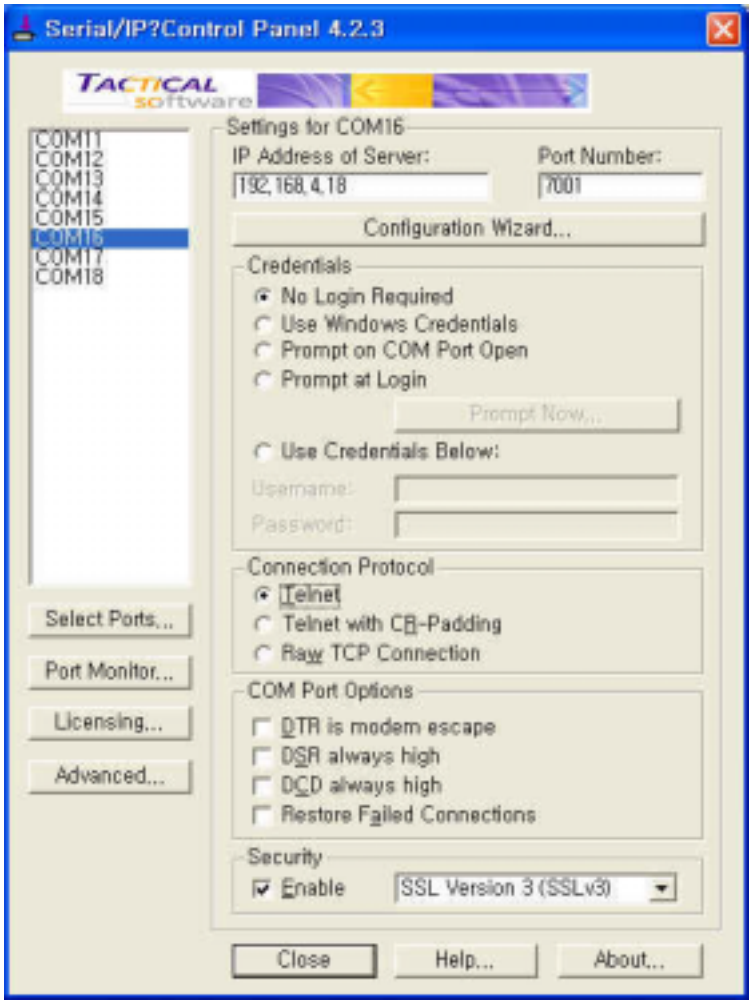


그림 A-14 Serial/IP Control Panel에서 파라미터 설정

단계 5. 터미널 에뮬레이션 프로그램을 열고 상응하는 COM 포트를 선택합니다. 그러면, 사용자는 마치 자신의 PC에 있는 COM 포트에서 터미널 에뮬레이션 프로그램을 사용하듯이 STS 시리즈의 시리얼 포트를 사용할 수 있습니다

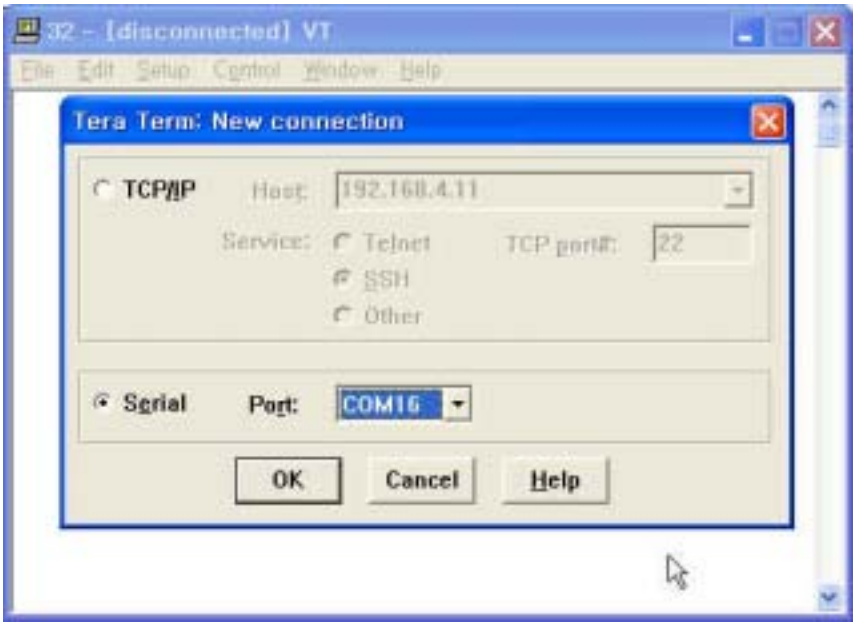


그림 A-15 Serial/IP로 STS series의 시리얼 포트에 연결하기

단계 6. 사용자는 Serial/IP의 Serial/IP Port Monitor이나 Trace window로 연결 상태를 모니터하거나 추적할 수 있습니다.

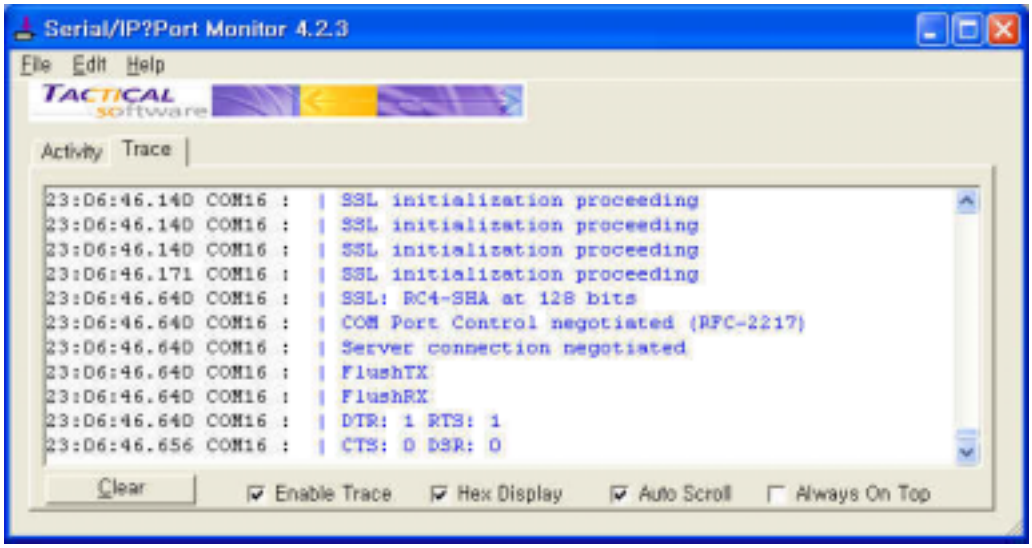


그림 A-16 Serial/IP Trace Window

부록 7. SSL 인증서 만들기

A 7.1 OpenSSL 패키지 설치

Step 1. Download the latest OpenSSL package. (http://www.openssl.org)

Step 2. Install the OpenSSL package.

<For Windows user>

Download OpenSSL for Windows binary file and run it.

(http://www.slproweb.com/products/Win32OpenSSL.html)

<For Linux user>

Download OpenSSL source code and compile it.

```
# cd /work/
# tar –xvzf openssl-0.9.7d.tar.gz
# cd openssl-0.9.7d
# ./config
# make
# make test
# make install
```

A 7.2 root CA (for Self-signed) 만들기

Step 1. Editing openssl configuration file.

Default configuration file location is as follows,

< Windows >

C:\Program Files\OpenSSL\bin

< Linux >

/usr/share/ssl/openssl.cnf

Modify [req_distinguished_name] section as follows,

```
countryName             = Country Name (2 letter code)
countryName_default     = KR
countryName_min         = 2
countryName_max         = 2

stateOrProvinceName     = State or Province Name (full name)
#stateOrProvinceName_default    = Some-State

localityName        = Locality Name(eg, city)
localityName_default        = Seoul
```

```
0.organizationName      = Organization Name (eg, company)
0.organizationName_default  = Sena Technologies Inc.

# we can do this but it is not needed normally :-)
#1.organizationName     = Second Organization Name (eg, company)
#1.organizationName_default = World Wide Web Pty Ltd

organizationalUnitName      = Organizational Unit Name (eg, section)
#organizationalUnitName_default =

commonName          = Common Name (eg, your name or your server\'s hostname)
commonName_default      = Sena Technologies
commonName_max          = 64

emailAddress        = Email Address
emailAddress_max    = 40
```

Modify [req_attributes] section as follows,

```
     challengePassword_min =0
     challengePassword_max =0
```

Step 2. Making self-signed Root CA(Certificate Authority)

< Windows >

cd /work/openssl-0.9.7d/

< Linux >

cd /work/openssl-0.9.7d/

mkdir CA

cd CA

sh /usr/local/ssl/misc/CA.sh –newca

```
CA certificate filename (or enter to create)
   ;(Press Enter to use default value)
Making CA certificate ...
; openssl is called here as follow from CA.sh
; openssl req -new -x509 -keyout ./demoCA/private/./cakey.pem \
;  -out ./demoCA/./cacert.pem -days 365
Using configuration from /usr/local/ssl/lib/ssleay.cnf
Generating a 1024 bit RSA private key
........++++++
.....................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:   ; CA Password (Enter password and remember this)
Verifying password - Enter PEM pass phrase:  ; CA Password
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----  ; CA's Information
Country Name (2 letter code) [AU]: KR
State or Province Name (full name) [Some-State](Enter)
Locality Name (eg, city) []:Seoul
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Sena Technologies
Organizational Unit Name (eg, section) [](Enter)
Common Name (eg, YOUR name) []:Sena Technologies
```

```
Email Address []:(Enter)
#
```

2-3. Check whether CA key file(demoCA/private/cakey.pem) and CA certificate (demoCA/cacert.pem) is generated

ls demoCA/

```
cacert.pem certs   crl index.txt      newcerts
private    serial
```

ls demoCA/private

```
cakey.pem
```

A 7.3 인증 요청서(certificate request) 만들기

To make new certificates, you should make a certificate request first.

cd /work/openssl-0.9.7c/CA

Run following commands,

openssl genrsa -out key.pem 1024

openssl req -new -key key.pem -out req.pem

(It is assumed that you are using sample configuration file - “openssl.conf.sena”)

```
Using configuration from /usr/share/ssl/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]: (Enter)
State or Province Name (full name) [Minnesota]: (Enter)
Locality Name (eg, city) [Minneapolis]: (Enter)
Organization Name (eg, company) [Digi International]: (Enter)
Organizational Unit Name (eg, section) []:(Enter)
Common Name (eg, your name or your server's hostname) []:Sena VTS
Email Address []:(Enter)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:(Press Enter – Do not enter any other characters)
An optional company name []:(Press Enter – Do not enter any other characters)
```

A 7.4 인증 요청서(certificate request)에 서명 하기

4-1. Signing a certificate request

cd /work/openssl-0.9.7c/CA

cp req.pem newreq.pem

sh /usr/local/ssl/misc/CA.sh -sign

```
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase: CA Password (Enter CA password in step 2-2)
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName         :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'Minnesota'
localityName        :PRINTABLE:'Minneapolis'
organizationName     :PRINTABLE:'Digi International'
commonName          :PRINTABLE:'Digi PortServer CM'
Certificate is to be certified until Oct  6 09:39:59 2013 GMT (3653 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 1 (0x1)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
International
      Validity
         Not Before: Oct  6 09:39:59 2003 GMT
         Not After : Oct  6 09:39:59 2013 GMT
      Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
PortServer CM
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
....
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

4-2. Check whether signed certificate(newcert.pem) is generated.

ls

```
  demoCA       key.pem     newcert.pem      newreq.pem     req.pem
```

A 7.5 STS 용 인증서 만들기

5-1. Removing headings in newcert.pem file

cd /work/openssl-0.9.7c/CA

cp newcert.pem server.pem

vi server.pem

```
Certificate:
```

```
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=KR, ST=, L=Seoul, O=Sena Technologies Inc., CN= Sena
Technologies
       Validity
          Not Before: Oct  6 09:39:59 2003 GMT
          Not After : Oct  6 09:39:59 2013 GMT
       Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
PortServer CM
       Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (1024 bit)
....
== Removing above lines ===
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
```

5-2. Concatenating key.pem file to server.pem

cat key.pem >> server.pem