Power Internet Leader

Power Internet Leader <<<<<<<<<

Power Internet Leader

Power Internet Leader

Client

elim.net

Class A

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바랍니다.

저작권

이 설명서의 내용은 제품의 기능 향상 등을 이유로 변경될 수 있습니다.

이 설명서에는 제품의 기능 향상으로 인해 실제 제품과 다른 설명이나 그림이 있을 수 있으며, 오자, 인쇄 오류 등이 포함되어 있을 수도 있습니다. 이러한 부분들은 다음 개정판에 개선되어 반영됩니다.

설명서 소개

이 설명서는 엘림넷의 R2SKY 시리즈에 관한 다음과 같은 내용으로 구성되어 있습니다.

◦ 기능과 특징 소개
◦ 각 부분의 명칭과 기능
◦ 랙 설치 방법과 각 포트 연결 방법
◦ 장비 설정 방법
◦ 장비의 설정 정보 및 트래픽 모니터링 방법
◦ 장비와 케이블의 사양
◦ 장비 설치 및 운용 시 주의 사항

제품을 안전하고 효율적으로 사용할 수 있도록 제품을 설치하거나 사용하기 전에 이 설명서의 내용을 주의 깊게 읽고 숙지해주시기 바랍니다. 이 설명서는 엘림넷의 홈페이지 http://www.elim.net에서도 다운로드 하거나 볼 수 있습니다.

연락처

제품 설치 및 사용시 문의 사항이 있으면 아래의 연락처로 연락해주시기 바랍니다.

◦ 주 소 : 서울시 서대문구 충정로 3가 32-11 충정빌딩
◦ 전화번호 : 02 - 3149 - 4999
◦ E-mail : elimtech@elim.net

참고 및 주의 표기

이 설명서에서는 참고 시 도움이 되는 내용과 주의해야 할 사항들을 다음과 같은 표기를 사용하여 별도로 표시합니다.

본 기호는 위험을 끼칠 우려가 있는 사항과 조작에 대하여 주위를 환기시키기 위한 기호입니다. 이 기호가 표시된 부분은 위험 발생을 피하기 위해 주의 깊게 읽고 지시에 따라야 합니다.

경고

표시사항을 위반할 때 심각한 상해나 사망이 발생할 가능성이 있는 경우

주의

표시사항을 위반할 때 경미한 상해나 제품 손상이 발생할 가능성이 있는 경우

참고

본 표시는 보다 편리한 사용을 돕기 위해 사용자에게 참고가 되는 사항이나 유용한 정보를 나타내는 기호입니다.

: 사용설명서를 읽고 난 후, 사용하는 사람이 언제나 볼 수 있는 장소에 필히 보관하십시오.

- 본 설명서의 내용은 만전을 기하여 제작되었지만, 혹 틀린 곳이나 고쳐야 할 내용이 있을 수도 있으니 이점 양해해 주시기 바랍니다. 본 사용설명서에서 사용하는 그림은 예시를 위한 것으로 실제와 다를 수 있습니다.

- 본 제품의 규격 및 외관은 품질 향상을 위하여 사전 통보 없이 변경 될 수 있으며, 엘림넷은 이에 대한 변경 권리를 가집니다.

- 본 설명서의 내용 중 일부 또는 전부를 무단으로 복제하는 것은 금지되어 있습니다.

목 차

설명서의 구성

이 설명서의 각 장은 다음과 같은 내용으로 구성되어 있습니다.

Chapter 1 제품 살펴보기

이 장에서는 엘림넷의 R2SKY 시리즈의 기능에 대해 소개하고, 제품 앞면과 뒷면 각 부분의 이름과 기능에 대해 소개합니다.

Chapter 2 제품 설치하기

이 장에서는 R2SKY 시리즈를 랙에 설치하는 방법과 적절한 케이블을 사용하여 각 포트를 연결하는 방법에 대해 설명합니다.

Chapter 3 웹 콘솔 살펴보기

이 장에서는 웹 콘솔로 로그인하는 방법과 웹 콘솔에 제공하는 기능에 대해 소개합니다.

Chapter 4 제품 설정하기

이 장에서는 웹 콘솔의 ‘CONFIGURATION’메뉴를 사용하여 R2SKY 시리즈를 설정하는 방법에 대해 설명합니다.

Chapter 5 트래픽 모니터링하기

이 장에서는 웹 콘솔의 ‘STATISTIC’메뉴를 사용하여 R2SKY 시리즈의 현재 설정 정보와 R2SKY 시리즈를 통해 송수신되는 트래픽 정보를 다양한 형태로 조회하는 방법에 대해 설명합니다.

Chapter 6 방화벽(Firewall) 설정하기

이 장에서는 웹 콘솔의 ‘FIREWALL’메뉴를 사용하여 특정한 서비스의 트래픽을 필터링하는 방법을 살펴봅니다.

Chapter 7 QOS(Quality of Service) 설정하기

이 장에서는 웹 콘솔의 'QOS'메뉴를 사용하여 R2SKY 시리즈에 QOS 기능을 설정하는 방법을 소개합니다.

Chapter 8 DNS 설정하기

Appendix A 제품과 케이블 사양

이 장에서는 R2SKY 시리즈의 제품 사양과 제품 설치 시 사용되는 케이블에 대한 사양이 정리되어 있습니다.

Appendix B 제품 설치 및 사용시 주의 사항

이 장에서는 R2SKY 시리즈를 설치하기 전에 숙지하고 있어야 하는 설치/사용시 주의 사항과 설치 장소가 갖추어야 하는 환경에 대해 설명합니다.

Chapter

1 제품 살펴보기

이 장에서는 엘림넷의 R2SKY 시리즈의 기능에 대해 소개하고, 제품 앞면과 뒷면 각 부분의 이름과 기능에 대해 소개합니다.

1. 제품 살펴보기

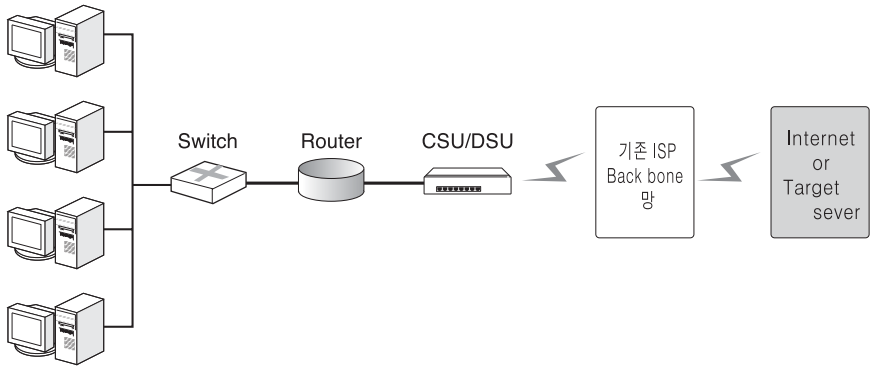
R2SKY 시리즈 소개

엘림넷의 R2SKY 시리즈는 세계 최고 수준의 VPN 장비로 다음과 같은 기능을 지원합니다.

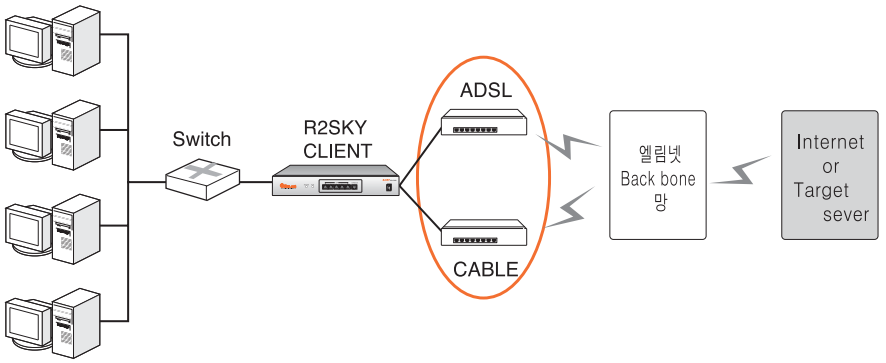
- 패킷의 종류별로 대역폭을 다르게 할당하여 전송 서비스를 최적화 해주는 QoS 기능
- 해커의 공격과 바이러스로부터 네트워크를 안전하게 보호 해주는 Firewall 기능
- 데이터의 크기와 어플리케이션의 종류에 따라 고속으로 전송할 수 있게 해주는 데이터 express 기능
- 내부의 사설 네트워크 주소를 공인 외부 네트워크 주소로 변환해주는 NAT와 DMZ 기능
- IP 주소를 중앙에서 효율적으로 관리할 수 있게 해주는 DHCP 서버와 릴레이 기능
- 장비 구성과 관리 및 각종 트래픽 모니터링을 손쉽게 할 수 있는 웹 인터페이스
- 주기적으로 저장된 데이터를 분석할 수 있도록 도와주는 로그 관리 기능
- VPN 서버의 설정 기능
- 최대 20Mbps의 다운로드 속도와 최대 2Mbps의 업로드 속도 (ADSL 기준)

1. 제품 살펴보기

VPN 장비를 사용하지 않는 기존의 네트워크에서는 인터넷과 연결하기 위해 다음 그림과 같이 라우터와 CSU 혹은 DSU를 통해 ISP 백본 네트워크와 연결해야 합니다.



엘림넷의 백본 네트워크를 이용하게 되면 아래 그림과 같이 엘림넷의 VPN 장비와 ADSL 라인 혹은 케이블 라인을 통해, 기존 ISP를 거치지 않고서도 인터넷과 연결할 수 있습니다.

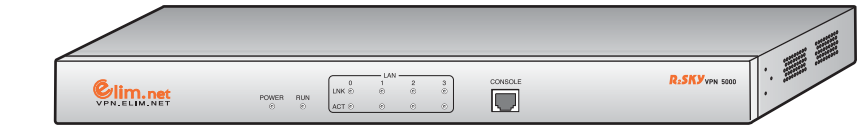


이러한 네트워크 구성은 라우터와 같은 고가의 장비를 필요로 하지 않습니다. 그리고, 값에 비해 낮은 대역폭을 지원하는 CSU나 DSU 대신 저렴한 가격으로 높은 대역폭을 제공하는 ADSL과 케이블 회선을 이용하므로, 비용적인 측면에서 네트워크를 구축하고 운용하는 데 있어 매우 효율적입니다. 뿐만 아니라, 엘림넷의 VPN 장비는 L3 라우터에서나 지원되는 QOS 기능과 Firewall 기능을 제공하기 때문에 높은 대역폭을 보다 더 효과적으로 사용할 수 있고, 내부 네트워크를 안전하게 보호할 수 있습니다.

1. 제품 살펴보기

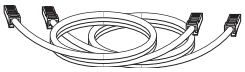
포장 내용물 확인하기

구입한 R2SKY 시리즈의 포장 박스를 열고 박스 속에 다음과 같은 내용물이 들어 있는지 확인합니다. 만약 빠진 물품이나 손상된 물품이 있는 경우에는 구입처로 연락하시면, 새로운 물품을 제공 받을 수 있습니다.

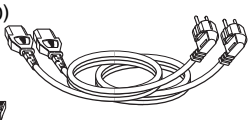


R2SKY 시리즈 본체(R2SKY 5000)

콘솔 케이블(DB9-RJ45) 1개



UTP 케이블(Straight) 2개



AC 전원 케이블 2개

◦ R2SKY 시리즈 본체
◦ 콘솔 케이블(DB9-RJ45) 1개
◦ AC 전원 케이블 2개
◦ UTP 크로스케이블(Straight) 2개

제품을 설치한 후에도 제품의 포장 박스와 쿠션을 버리지 않고 보관해 두도록 합니다. 이 후, 제품을 옮겨야 하는 경우에는 보관해 둔 포장 박스와 쿠션을 사용하여 제품을 포장한 후에 이동하는 것이 좋습니다.

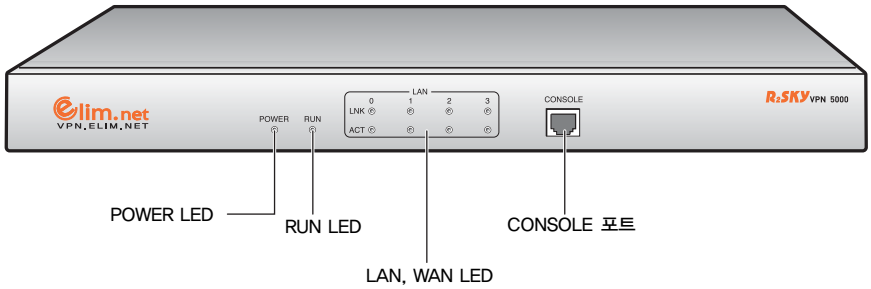
1. 제품 살펴보기

R2SKY 시리즈 살펴보기

이 절에서는 R2SKY 시리즈의 앞면과 뒷면, 옆면의 외관과 각 부분의 명칭 및 기능에 대해 알아봅니다.

R2SKY 5000

앞면



■ POWER LED

장비의 앞면 왼쪽에 있는 POWER LED는 장비의 전원 공급 상태를 나타냅니다. 장비에 전원이 정상적으로 공급되면 초록색 불이 켜집니다.

■ RUN LED

POWER LED의 오른쪽에 있는 RUN LED는 R2SKY 5000에 있는 플래시 메모리의 액세스 여부를 표시합니다. 플래시 메모리가 액세스되지 않는 동안 RUN LED는 꺼져 있고, 플래시 메모리에서 데이터가 읽혀지거나 혹은 플래시 메모리에 데이터가 기록되는 동안 RUN LED가 깜박입니다.

제품이 초기화되는 동안 플래시 메모리의 설정 정보가 계속 읽혀지기 때문에 초기화가 시작될 때부터 끝날 때까지 RUN LED가 계속해서 깜박입니다. RUN LED가 더 이상 깜박이지 않고 꺼지면 초기화가 끝난 것을 알 수 있습니다.

1. 제품 살펴보기

■ LAN LED

LAN LED는 장비 뒷면에 있는 4(5)개의 Ethernet 포트의 상태를 나타내는 LED로, 각 포트 별로 LINK LED와 ACT LED, 2개의 LED가 포트의 상태를 표시해줍니다. LAN LED는 포트의 상태에 따라 다음과 같이 동작합니다.

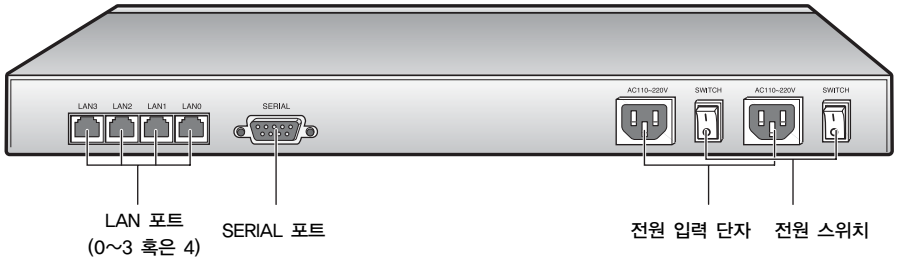
LED	LED의 상태	의 미
LINK	켜짐(파란색)	포트가 동작 중이고, 상대 장비와 연결되어 있는 상태입니다.
	꺼짐	포트가 동작 중이지 않거나(disable 상태) 장비와 연결되어 있지 않은 상태입니다.
ACT	켜짐(파란색)	포트를 통해 데이터가 송수신되는 중입니다.
	꺼짐	포트를 통해 송수신되는 데이터가 없는 상태입니다.

■ CONSOLE 포트

CONSOLE 포트는 R2SKY 5000의 관리 작업을 수행할 수 있는 콘솔 터미널을 연결할 때 사용하는 포트로 RJ-45 타입의 커넥터입니다. CONSOLE 포트와 콘솔 터미널을 연결할 때에는 제품과 함께 제공된 콘솔 케이블을 사용하면 됩니다. 콘솔 터미널은 터미널 에뮬레이터 프로그램이 설치된 PC나 웍스테이션, 혹은 VT-100 터미널을 사용하면 됩니다. CONSOLE 포트에 콘솔 터미널을 연결하는 방법은 다음 장의 내용을 참고합니다.

1. 제품 살펴보기

뒷면



■ LAN 포트(0 ~ 3 혹은 4)

R2SKY 5000의 뒷면에는 LAN0 ~ LAN3(4)의 4(5)개의 RJ-45 포트가 있습니다. LAN0 포트는 관리용 PC와 연결하여 장비를 설정하고 모니터링 작업을 할 수 있습니다. 혹은 LAN의 여러 PC가 장비를 통해 외부 WAN에 접속할 수 있도록 LAN 허브나 스위치와 연결할 수도 있습니다.

LAN1 ~ LAN3(4) 포트는 외부 WAN과 연결하는 포트입니다. ADSL 회선을 사용하는 경우에는 ADSL 모뎀과, 케이블 회선을 사용하는 경우에는 케이블 모뎀과 직접 연결합니다.

LAN 포트를 연결할 때 사용하는 케이블은 양쪽 커넥터가 RJ-45 커넥터로 된 straight 타입의 twisted pair category-3, 4, 5 케이블입니다. 단, LAN0 포트가 관리용 PC와 연결하는 경우에는 cross 타입의 twisted pair 케이블을 사용해야 합니다. Straight와 cross 타입의 핀 연결은 부록 A의 내용을 참고합니다.

■ 전원 스위치

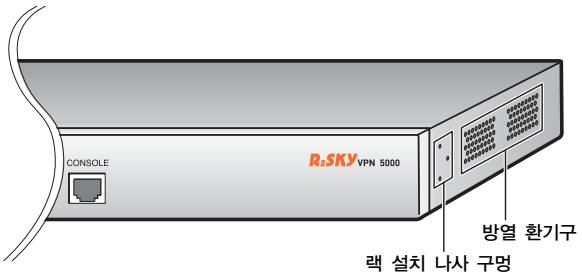
전원 스위치는 장비의 전원을 켜고 끄는 스위치입니다. 전원을 켤 때에는 I 방향으로, 끌 때에는 O 방향을 누릅니다.

■ 전원 입력 단자

R2SKY 5000에는 2개의 전원 입력 단자가 있습니다. 제품과 함께 제공된 2개의 원 케이블을 사용하여 각각 다른 전원 소스로 연결하면 전원을 이중화하여 보다 안전하게 전원을 공급할 수 있습니다. 전원을 이중화하면 전원 부하가 나눠질 뿐만 아니라, 하나의 전원 소스에서 문제가 발생한 경우 나머지 전원 소스를 통해 스위치에 전원을 공급할 수 있게 되어 안전합니다.

1. 제품 살펴보기

옆면



■ 랙 설치 나사 구멍

R2SKY 5000은 19인치 랙에 설치하여 사용할 수 있습니다. 장비의 양쪽 옆면에 3개씩 있는 나사 구멍은 장비를 19인치 랙에 설치하기 위해 브라켓을 장착하는 부분입니다. 장비의 양쪽 옆면에 브라켓을 장착한 후 19인치 랙에 설치하는 방법은 다음 장에 설명되어 있습니다.

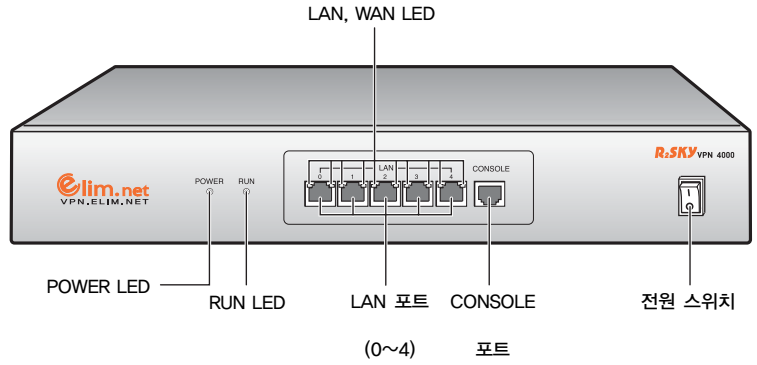
■ 방열 환기구

방열 환기구는 R2SKY 5000이 동작하면서 발생되는 열이 밖으로 빠져 나오고, 외부의 찬 공기가 공급되는 부분입니다. 장비를 사용할 때 이 부분이 막혀 있으면 내부의 더운 공기와 외부의 찬 공기가 제대로 순환되지 못해서 제품이 과열될 수 있으므로 주의합니다.

1. 제품 살펴보기

R2SKY 4000

앞면



■ POWER LED

장비의 앞면 왼쪽에 있는 POWER LED는 장비의 전원 공급 상태를 나타냅니다. 장비에 전원이 정상적으로 공급되면 초록색 불이 켜집니다.

■ RUN LED

POWER LED의 오른쪽에 있는 RUN LED는 R2SKY 4000에 있는 플래시 메모리의 액세스 여부를 표시합니다. 플래시 메모리가 액세스되지 않는 동안 RUN LED는 꺼져 있고, 플래시 메모리에서 데이터가 읽혀지거나 혹은 플래시 메모리에 데이터가 기록되는 동안 RUN LED가 깜박입니다.

제품이 초기화되는 동안 플래시 메모리의 설정 정보가 계속 읽혀지기 때문에 초기화가 시작될 때부터 끝날 때까지 RUN LED가 계속해서 깜박입니다. RUN LED가 더 이상 깜박이지 않고 꺼지면 초기화가 끝난 것을 알 수 있습니다.

1. 제품 살펴보기

■ LAN 포트(0 ~ 4)

R2SKY 4000의 앞면에는 LAN0 ~ LAN4의 5개의 RJ-45 포트가 있습니다. LAN0 포트는 관리용 PC와 연결하여 장비를 설정하고 모니터링 작업을 할 수 있습니다. 혹은 LAN의 여러 PC가 장비를 통해 외부 WAN에 접속할 수 있도록 LAN 허브나 스위치와 연결할 수도 있습니다.

LAN1 ~ LAN4 포트는 외부 WAN과 연결하는 포트입니다. ADSL 회선을 사용하는 경우에는 ADSL 모뎀과, 케이블 회선을 사용하는 경우에는 케이블 모뎀과 직접 연결합니다.

LAN 포트를 연결할 때 사용하는 케이블은 양쪽 커넥터가 RJ-45 커넥터로 된 straight 타입의 twisted pair category-3, 4, 5 케이블입니다. 단, LAN0 포트가 관리용 PC와 연결하는 경우에는 cross 타입의 twisted pair 케이블을 사용해야 합니다. Twisted pair 케이블의 사양과 straight, cross 타입의 핀 연결은 부록 A의 내용을 참고합니다.

■ LAN LED

각 LAN 포트의 양쪽 위에는 LAN 포트의 상태를 나타내는 LINK LED와 ACT LED, 2개의 LED가 있습니다. 이 LED들은 각 LAN 포트의 상태에 따라 다음과 같이 동작합니다.

LED	LED의 상태	의 미
LINK	켜짐(초록색)	포트가 동작 중이고, 상대 장비와 연결되어 있는 상태입니다.
	꺼짐	포트가 동작 중이지 않거나(disable 상태) 장비와 연결되어 있지 않은 상태입니다.
ACT	켜짐 (주황색)	포트를 통해 데이터가 송수신되는 중입니다.
	꺼짐	포트를 통해 송수신되는 데이터가 없는 상태입니다.

1. 제품 살펴보기

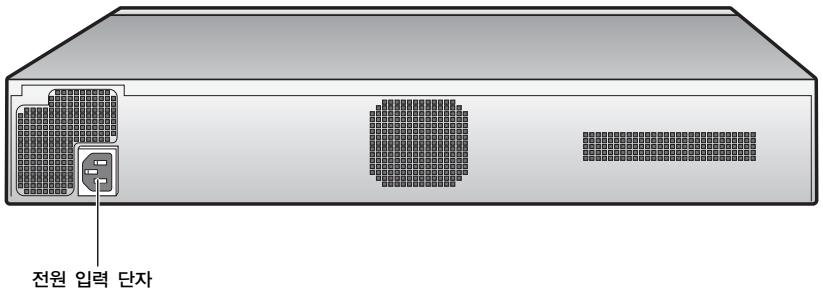
■ CONSOLE 포트

R2SKY 4000에 있는 CONSOLE 포트는 R2SKY VPN 5000과 달리 RJ-11 타입의 커넥터입니다. 커넥터의 모양은 다르지만, 관리 작업을 수행할 수 있는 콘솔 터미널을 연결하는 용도는 같습니다. CONSOLE 포트와 콘솔 터미널을 연결할 때에는 제품과 함께 제공된 콘솔 케이블을 사용하면 됩니다. 콘솔 터미널은 터미널 에뮬레이터 프로그램이 설치된 PC나 웍스테이션, 혹은 VT-100 터미널을 사용하면 됩니다. CONSOLE 포트에 콘솔 터미널을 연결하는 방법은 다음 장의 내용을 참고합니다.

■ 전원 스위치

R2SKY 4000에는 전원 스위치가 장비의 앞면에 있습니다. 전원을 켤 때에는 전원 스위치를 I 방향으로, 끌 때에는 O 방향을 3~5초간 누르면 됩니다.

뒷면

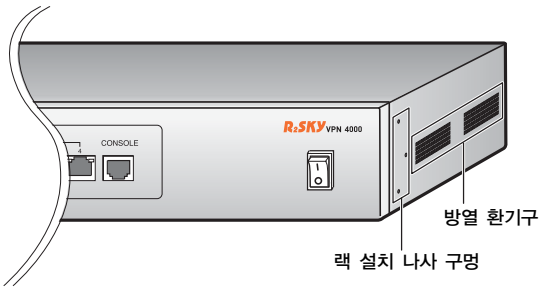


■ 전원 입력 단자

R2SKY 4000의 뒷면에는 하나의 전원 입력 단자가 있습니다. 제품과 함께 제공된 전원 케이블을 사용하여 접지된 전원 소스에 연결하도록 합니다.

1. 제품 살펴보기

옆면



■ 랙 설치 나사 구멍

R2SKY 4000은 19인치 랙에 설치하여 사용할 수 있습니다. 장비의 양쪽 옆면에 3개씩 있는 나사 구멍은 장비를 19인치 랙에 설치하기 위해 브라켓을 장착하는 부분입니다. 장비의 양쪽 옆면에 브라켓을 장착한 후 19인치 랙에 설치하는 방법은 다음 장에 설명되어 있습니다.

■ 방열 환기구

방열 환기구는 R2SKY 4000이 동작하면서 발생되는 열이 밖으로 빠져 나오고, 외부의 찬 공기가 공급되는 부분입니다. 장비를 사용할 때 이 부분이 막혀 있으면 내부의 더운 공기와 외부의 찬 공기가 제대로 순환되지 못해서 제품이 과열될 수 있으므로 주의합니다.

Chapter

2 제품 설치하기

이 장에서는 R2SKY 시리즈 중 R2SKY 5000을 예로 들어 장비를 랙에 설치하는 방법과 적절한 케이블을 사용하여 각 포트를 장비와 연결하는 방법에 대해 설명합니다.

2. 제품 설치하기

설치과정

주의

R2SKY 시리즈를 설치하기 전에 다음과 같은 사항을 반드시 확인하도록 합니다.

- 제품을 설치하는 장소가 이 설명서의 부록 B에 제시된 환경 조건을 만족하는지 점검합니다.
- 장비의 뒷면에 있는 전원 스위치를 끕니다.
- 포트에 연결되어 있는 케이블과 전원 입력 단자에 연결되어 있는 전원 케이블까지 모두 빼냅니다.

다음은 R2SKY 시리즈를 설치하는 과정을 순서대로 정리한 것입니다. 각 과정을 수행하는 방법은 다음 절에서 차례로 설명합니다.

1. 19인치 랙에 설치하기 (옵션 사항, 일부 R2SKY 제품은 랙에 장착할 수 없습니다.) R2SKY 시리즈는 19인치 랙에 장착하여 사용할 수 있도록 설계되어 있습니다. 19인치 랙에 장착하기 위해서는 장비의 양쪽 옆면에 브라켓을 먼저 부착해야 합니다.

2. WAN 연결하기
   적절한 타입의 UTP 크로스케이블을 이용하여 R2SKY 시리즈의 LAN1 ~ LAN3(LAN4) 포트를 WAN(모뎀이나 허브 등)과 연결합니다. 이때 해당 포트의 LINK LED에 불이 켜지면 정상적으로 연결된 상태입니다. 만약, LINK LED에 불이 켜지지 않으면 Cross 타입의 twisted pair 케이블을 사용하여 연결한 후 다시 확인하도록 합니다.

3. LAN 연결하기
   적절한 타입의 UTP 크로스케이블을 사용하여 R2SKY 시리즈의 LAN0 포트를 허브나 스위치에 연결합니다. 허브나 스위치의 업링크(Uplink) 포트와 연결하는 경우에는 Cross 타입의 twisted pair 케이블을 사용하도록 합니다.

4. 관리용 PC 연결하기 (옵션 사항)
   LAN0 포트에 관리용 PC를 직접 연결하는 경우에는 cross 타입의 twisted pair 케이블을 사용하여 R2SKY 시리즈의 LAN0 포트를 관리용 PC에 연결합니다.

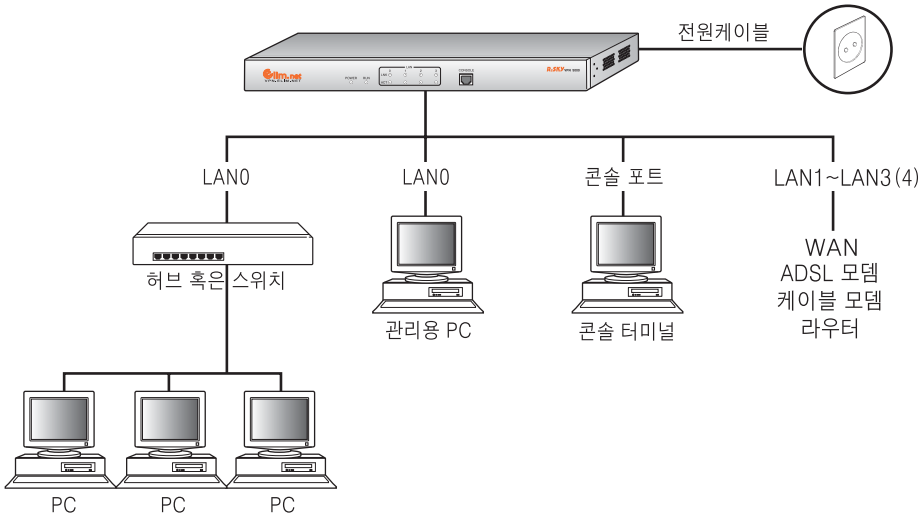
2. 제품 설치하기

5. 콘솔 터미널 연결하기 (옵션 사항)
   콘솔 케이블을 사용하여 R2SKY 시리즈의 CONSOLE 포트를 콘솔 터미널과 연결합니다.

6. 전원 연결하기
   R2SKY 시리즈의 설치와 케이블 연결이 끝나면 근처에 있는 전원을 연결합니다.

연결도

다음은 R2SKY 시리즈를 WAN, LAN, 콘솔 터미널, 관리용 PC, 전원과 모두 연결한 그림입니다.



2. 제품 설치하기

랙에 설치하기

R2SKY 시리즈는 테이블과 같이 평평한 곳에 두고 사용하거나 혹은 19인치 랙에 설치하여 사용할 수 있습니다. R2SKY 시리즈는 양쪽 옆면에 있는 냉각 팬을 통해 차가운 공기가 내부로 유입되고 더워진 공기가 밖으로 빠져 나가게 됩니다. 장비를 테이블에 두고 사용하는 경우에는 장비의 이러한 공기 순환을 방해하는 물건이 없는지 반드시 확인하도록 합니다.

R2SKY 시리즈를 19인치 랙에 장착하여 사용하는 경우에는 다음과 같은 방법으로 장착할 수 있습니다. 일부 R2SKY제품(R2SKY 2000 등)을 제외한 R2SKY 시리즈는 모든 종류의 19인치 표준 랙에 장착할 수 있도록 설계되어 있습니다.

필요한 도구

R2SKY 시리즈를 19인치 랙에 장착할 때 다음과 같은 도구가 필요하므로, 미리 준비하도록 합니다.

◦ 십자 드라이버
◦ 정전기 방지용 스트랩
◦ 브라켓 2개
◦ 브라켓 설치용 나사 6개
◦ 랙 설치용 나사 4개

랙에 장착하기

주의

R2SKY 시리즈를 랙에 설치할 때, 랙으로 인해 발생할 수 있는 위험을 방지하기 위해 다음과 같은 주의 사항을 꼭 지키도록 합니다.

◦ 랙이 비어 있는 경우에는 반드시 랙의 맨 아래쪽에 스위치를 장착합니다.
◦ 랙의 무게 중심이 아래에 있도록 하기 위해 무거운 장비일수록 랙의 아래쪽에 장착하도록 합니다.

2. 제품 설치하기

필요한 도구가 준비되었으면 다음과 같은 순서에 따라 장비를 19인치 랙에 설치합니다.

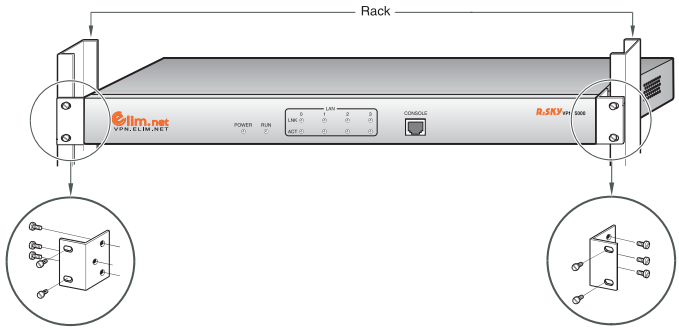
1. R2SKY 시리즈를 작업할 공간이 충분한 바닥이나 튼튼한 테이블 위에 놓습니다. 그리고, 빠진 준비물이 없는지 확인합니다.

2. R2SKY 시리즈의 양쪽 옆면을 보면 각각 3개의 나사 구멍이 있습니다. 다음 그림과 같이 이 나사 구멍에 맞추어서 브라켓을 대고, 접시 머리 나사를 사용하여 브라켓을 고정시킵니다.

3. 19인치 랙이 놓여진 장소가 장비를 장착하는 작업을 하는 데 불편하지 않을 정도로 여유가 있는지 확인합니다. 그리고, 19인치 랙에 스위치를 장착할 수 있는 10cm 정도의 수직 공간이 있는지 확인합니다.

4. 브라켓을 부착한 R2SKY 시리즈를 19인치 랙에 설치할 부분까지 들어 올립니다.

5. 장비에 장착된 브라켓을 19인치 랙의 구멍에 잘 맞춘 후, 4개의 바인더 머리 나사로 조여서 고정시킵니다.



2. 제품 설치하기

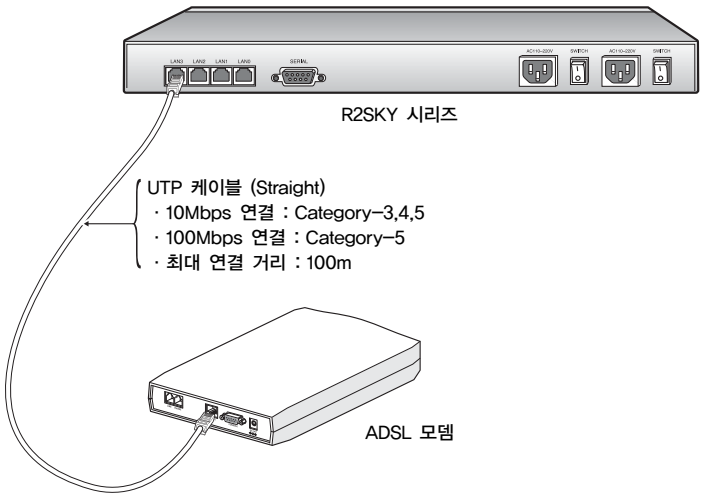
WAN 연결하기

이 절에서는 R2SKY 시리즈를 WAN에 연결하는 방법에 대해 살펴봅니다.

주의

케이블을 연결하는 장비들간의 거리가 본 매뉴얼에서 제시한 최대 거리보다 먼 경우에는 전송하는 데이터가 손실될 수 있습니다.

R2SKY 시리즈를 ADSL 망과 연결하는 경우에는 제품과 함께 제공된 straight 타입의 UTP 크로스케이블을 사용하여 다음 그림과 같이 R2SKY 시리즈의 뒷면에 있는 LAN1 ~ LAN3(4) 포트 중 하나와 ADSL 망에 연결되어 있는 ADSL 모뎀의 업링크(혹은 LAN) 포트와 연결합니다.



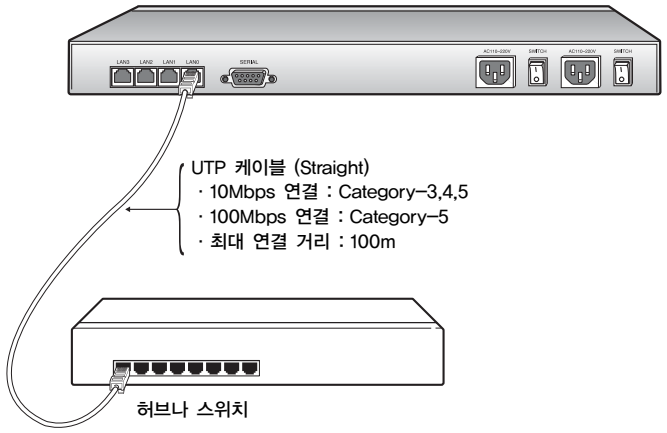
Tip 참고

제공되는 모뎀에 따라 간혹 Cross 타입의 UTP 크로스케이블을 사용해야 하는 경우도 있습니다.

케이블을 연결한 후에는 4장의 인터페이스 설정하기 절의 내용을 참고하여, ADSL 모뎀과 연결한 LAN 포트 인터페이스의 설정 작업을 수행하도록 합니다.

2. 제품 설치하기

R2SKY 시리즈를 통해 LAN에 속한 여러 PC에서 인터넷으로 접속하려면 제품과 함께 제공된 straight 타입의 UTP케이블을 사용하여 다음 그림과 같이 R2SKY 시리즈 뒷면에 있는 LAN0 포트를 LAN 허브나 스위치에 연결하면 됩니다.

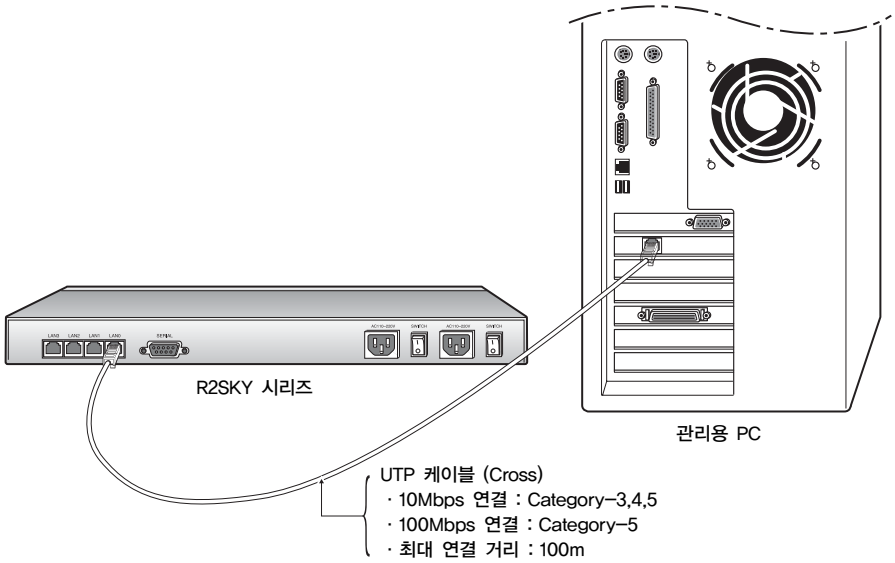


2. 제품 설치하기

관리용 PC 연결하기

앞에서 살펴본 것과 같이 R2SKY 시리즈의 LAN0 포트를 허브나 스위치와 연결하면 R2SKY 시리즈에 접속할 수 있는 모든 PC에서 웹 콘솔로 로그인할 수 있습니다. 웹 콘솔에서는 R2SKY 시리즈를 설정하거나 R2SKY 시리즈를 통해 송수신되는 트래픽을 다양한 방법으로 조회할 수 있습니다.

R2SKY 시리즈가 LAN과 연결되어 있지 않은 상태에서 웹 콘솔을 통해 장비를 설정하거나 모니터링 하려면 LAN0 포트를 직접 PC와 연결하면 됩니다. Cross 타입의 UTP 크로스케이블을 준비한 후 다음 그림과 같이 R2SKY 시리즈의 뒷면에 있는 LAN0 포트를 PC에 장착된 LAN 카드의 포트와 연결합니다.



Cross 타입의 UTP 크로스케이블에 대한 핀 연결은 부록 A의 내용을 참고합니다. 그리고, 웹 콘솔로 로그인하는 방법과 웹 콘솔의 메뉴를 사용하여 R2SKY 시리즈를 설정하거나 모니터링 하는 방법은 3장부터 설명됩니다.

2. 제품 설치하기

콘솔 터미널 연결하기

R2SKY 시리즈는 웹 콘솔을 통해 관리할 수도 있지만, CONSOLE 포트와 연결된 콘솔 터미널을 통해서 장비의 부팅 과정이나 동작 상태 등의 기본적인 모니터링 작업을 할 수 있습니다.

콘솔 터미널 구성하기

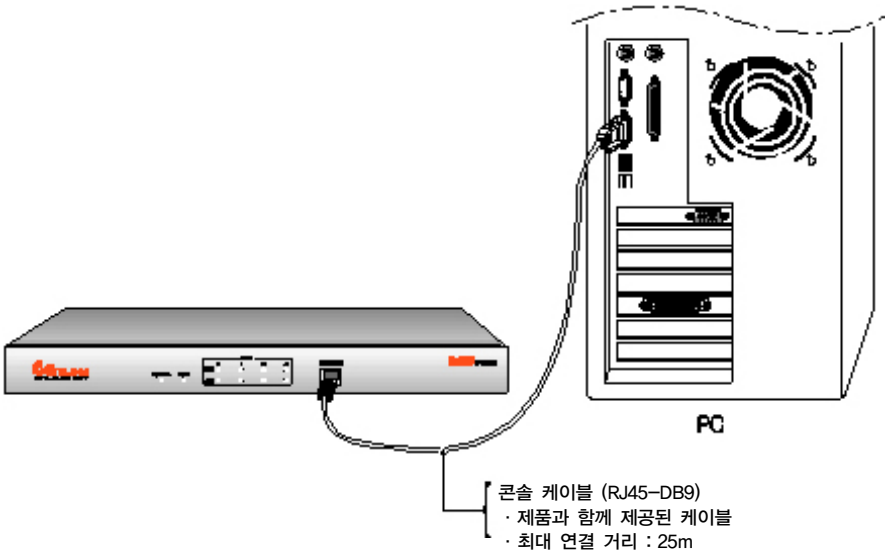
R2SKY 시리즈의 콘솔 터미널로 사용할 PC (PC에는 Hyper Terminal과 같은 터미널 에뮬레이터가 설치되어 있어야 합니다.)와 VT-100 터미널은 다음과 같이 구성되어 있어야 합니다.

항 목	설정 값
초당 비트 수	19200bps or 9600bps
데이터 비트	8bit
패리티 비트	없음
정지 비트	1bit
흐름 제어	없음

2. 제품 설치하기

콘솔 터미널 연결하기

제품과 함께 제공된 콘솔 케이블을 사용하여 R2SKY 시리즈의 CONSOLE 포트와 콘솔 터미널로 사용할 PC나 터미널의 시리얼 포트를 다음 그림과 같이 연결합니다.



Tip 참고

R2SKY 4000 장비의 CONSOLE 포트와 콘솔 터미널을 연결할 때에는 양쪽 커넥터가 각각 DB-9, RJ-11인 콘솔 케이블을 사용해야 합니다.

2. 제품 설치하기

전원 연결하기

주의

R2SKY 시리즈에 전원을 연결하기 전에 다음과 같은 사항을 확인하도록 합니다.

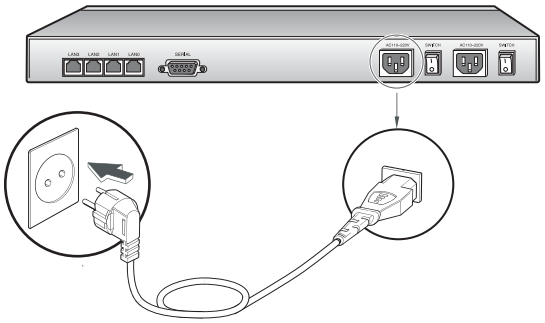
◦ 부록 B의 전원 관련 주의 사항에 설명된 내용에 따라 연결하고자 하는 전원이 적절한지 확인합니다.

◦ 스위치 뒷면에 있는 전원 스위치가 OFF 상태(O 방향)인지 미리 확인합니다.

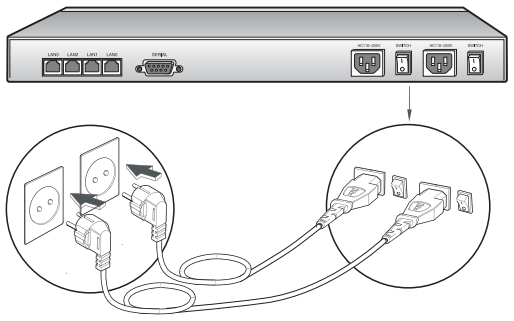
R2SKY 시리즈에 전원을 연결하는 방법은 다음과 같습니다.

1. R2SKY 시리즈의 전원 스위치가 OFF 상태(O 방향)인지 확인합니다.

2. 제품과 함께 공급된 전원 케이블을 장비 뒷면에 있는 전원 입력 단자에 연결합니다. 그리고, 전원 케이블의 플러그를 접지된 콘센트에 연결합니다.



3. R2SKY 5000의 경우에는 전원 이중화를 위해 제품과 함께 공급된 전원 케이블을 나머지 전원 입력 단자와 접지된 콘센트에 각각 연결합니다. 가능하면 2번 과정에서 연결한 전원 소스와 다른 전원 소스에 연결하는 것이 전원을 이중화하여 안전합니다.



2. 제품 설치하기

시스템 구동하기

설치 작업을 완료한 후에는 다음과 같은 순서대로 R2SKY 시리즈를 구동합니다.

1. 장비를 구동하기 전에 다음 사항들을 다시 한번 점검합니다.
   ◦ 장비가 랙이나 기타 장소에 안전하게 설치되어 있는지 확인합니다.
   ◦ 장비의 각 포트에 케이블이 바르게 연결되어 있는지 확인합니다.
   ◦ 전원 케이블이 바르게 연결되어 있는지 확인합니다.

2. 콘솔 터미널의 전원을 켜고, 설치된 터미널 에뮬레이터 프로그램을 실행합니다.

3. 장비에 있는 전원 스위치를 I 방향으로 눌러서 전원을 켭니다.

4. 냉각 팬이 돌아가는 소리가 들리는지 확인합니다.

5. 스위치에 전원이 정상적으로 공급되면 POWER LED에 불이 켜집니다.

6. 잠시 후, 장비의 초기화 과정이 시작되면 RUN LED에 불이 깜박이기 시작합니다.

7. 장비의 초기화가 정상적으로 완료되면 RUN LED가 꺼집니다.

8. 이제 R2SKY 시리즈가 정상적으로 설치 되었습니다. 계속해서 다음 장의 내용을 참고하여 웹 콘솔을 통해 LAN 포트와 장비를 설정하도록 합니다.

Chapter

3

웹 콘솔 살펴보기

이 장에서는 웹 콘솔로 로그인하는 방법과 웹 콘솔에 제공하는 기능을 살펴봅니다.

3. 웹 콘솔 살펴보기

사용하기 전에

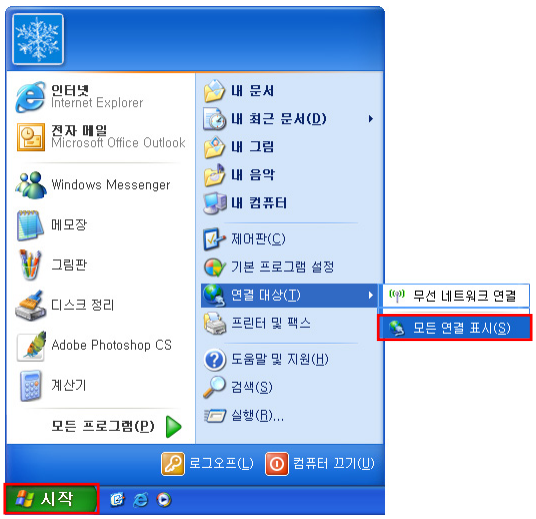
이 절에서는 웹 콘솔을 사용하기 위해 미리 해두어야 할 작업과 웹 콘솔로 로그인하는 방법, 그리고, 웹 콘솔의 화면 구성과 메뉴에 대해 간략하게 소개합니다.

PC의 IP 주소 설정하기

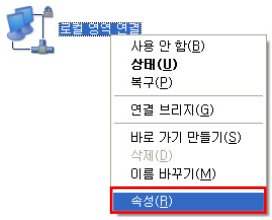
R2SKY 시리즈를 설정하기 위해 웹 콘솔로 로그인 하려면 먼저 사용자의 PC가 R2SKY 시리즈와 같은 LAN(ETHERNET)에 있어야 하고, 접속이 가능해야 합니다. R2SKY 시리즈는 기본적으로 IP 주소는 192.168.1.100, 서브넷은 255.255.255.0로 설정되어 있습니다. 그러므로, 웹 콘솔로 로그인할 PC의 IP 주소는 192.168.1.1 ~ 192.168.1.99 혹은 192.168.1.101 ~ 192.168.1.254의 범위에 속하는 값으로 서브넷은 255.255.255.0으로 설정해야 합니다.

다음은 Windows XP를 운영체제로 사용하는 PC의 IP 주소를 변경하는 방법입니다.

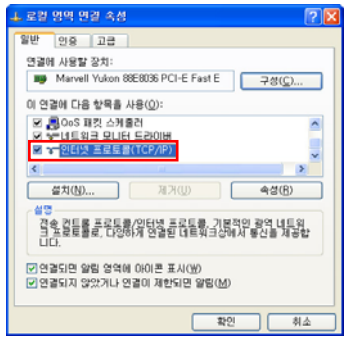
1. 바탕 화면에서 시작 버튼을 클릭하고 연결 대상 > 모든 연결 표시 메뉴를 선택합니다.



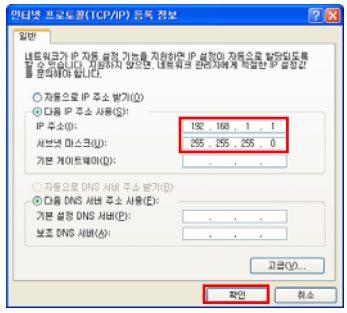
2. <네트워크 연결> 화면이 나오면 로컬 영역 연결 아이콘을 선택한 상태에서 마우스의 오른쪽 버튼을 클릭하여 속성 메뉴를 선택합니다.



3. <로컬 영역 연결 등록 속성> 화면이 나오면 '이 연결에 다음 항목을 사용'목록에서 인터넷 프로토콜 (TCP/IP)를 선택하고 [등록 정보] 버튼을 클릭합니다.



4. <인터넷 프로토콜 (TCP/IP) 등록 정보> 화면이 나오면 다음 IP 주소 사용 항목을 클릭한 후, IP 주소에 192.168.1.1~192.168.1.99나 192.168.1.101 ~ 192.168.1.254의 범위에 속하는 값을 입력합니다. 그리고, 서브넷 마스크에는 '255.255.255.0'를 입력한 후 [확인] 버튼을 클릭합니다.



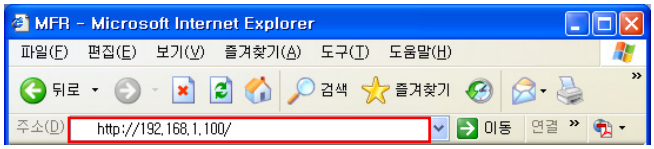
3. 웹 콘솔 살펴보기

웹 콘솔로 로그인하기

PC의 IP 주소를 변경한 후에는 다음과 같은 방법으로 R2SKY 시리즈를 구성할 수 있는 웹 콘솔로 로그인할 수 있습니다.

1. PC에 설치된 웹 브라우저를 실행합니다.

2. 웹 브라우저의 주소 입력란에 http://192.168.1.100을 입력한 후, [Enter] 키를 누릅니다.



3. ID와 PASS 항목에 각각 웹 콘솔 로그인 ID와 암호를 입력합니다. 그리고, [LOGIN] 버튼을 클릭합니다.

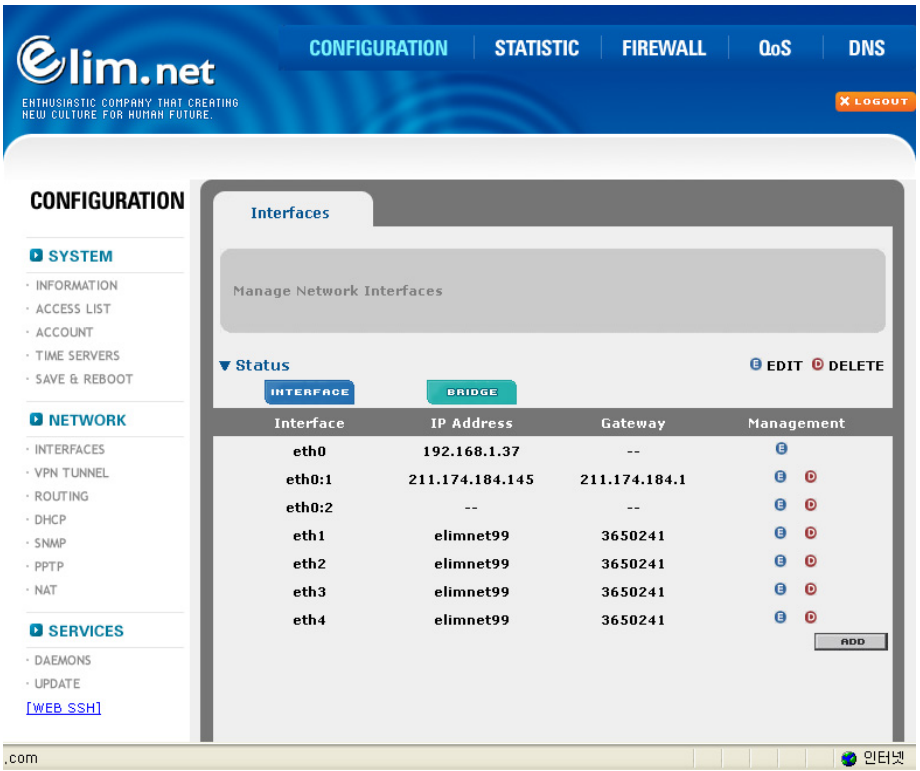
Tip 참고

R2SKY 시리즈에 기본으로 설정되어 있는 웹 콘솔 로그인 ID와 암호는 각각 'admin'과 'r2sky'입니다. 따라서 R2SKY 시리즈의 웹 콘솔로 처음 로그인하는 경우에는 ID 항목에 'admin'을 입력하고 PASS 항목에 'r2sky'을 입력하면 됩니다. 로그인 암호는 상황에 따라 변경될 수 있습니다.

3. 웹 콘솔 살펴보기

웹 콘솔로 로그인한 후에는 가급적이면 로그인 암호를 변경하는 것이 좋습니다. 웹 콘솔 로그인 암호를 변경하거나 새로운 사용자를 등록하는 방법은 다음 장의 웹 콘솔 사용자 암호 변경하기 절에 설명되어 있습니다.

4. 웹 콘솔 로그인 ID와 암호를 정확하게 입력하면 다음과 같은 웹 콘솔 화면이 나타납니다.

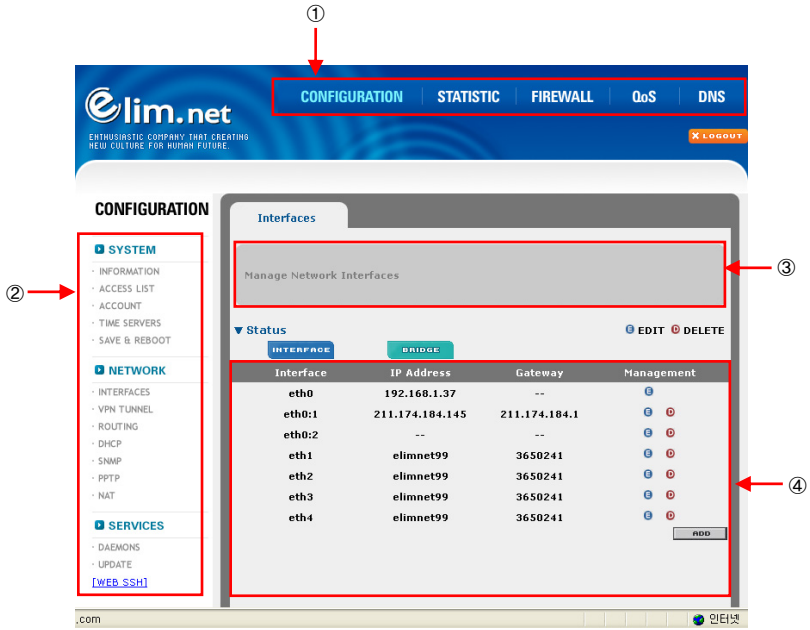


다음 절에서 웹 콘솔의 화면 구성과 웹 콘솔에서 제공하는 메뉴들의 종류와 기능에 대해 알아봅니다.

3. 웹 콘솔 살펴보기

웹 콘솔 화면 구성

R2SKY 시리즈의 웹 콘솔 화면은 다음과 같은 항목들로 구성되어 있습니다.



부분	기 능
①	웹 콘솔의 기본 메뉴, 여기에 있는 메뉴 항목을 클릭하면 ② 부분에 서브 메뉴가 출력됩니다.
②	② 부분에 있는 메뉴 항목의 서브 메뉴. 따라서, 메뉴를 선택할 때에는 ① 〉 ② 순서대로 클릭하면 됩니다.
③	선택한 메뉴에 대한 도움말이 출력되는 부분.
④	선택한 메뉴에 따라 설정 작업을 할 수 있는 항목들이나 모니터링한 결과 등이 출력되는 부분

3. 웹 콘솔 살펴보기

웹 콘솔 메뉴의 종류와 기능

다음은 R2SKY 시리즈의 웹 콘솔에서 지원하는 메뉴 항목과 기능을 정리한 표입니다.

메뉴			기능
CONFIGURATION	SYSTEM	INFORMATION	장비에 관련된 사람들(고객, 장비 판매자, 설치자, 관리자)의 정보와 PnN 인터페이스, Arrange IP에 대한 정보를 설정합니다.
		ACCESS LIST	웹 콘솔로 로그인하거나 특정 데몬에 액세스할 수 있는 IP어드레스 범위를 지정하기 위해 액세스 리스트를 정의합니다.
		ACCOUNT	사용자 계정을 추가하거나, 웹 콘솔 로그인 암호(admin 계정과 user 계정)를 변경합니다.
		TIME SERVERS	Primary와 secondary NTP 서버를 지정합니다.
		SAVE & REBOOT	변경된 설정을 플래쉬 메모리에 저장하거나 장비를 리부팅합니다.
	NETWORK	INTERFACES	각 인터페이스에 연결되는 망의 종류(ADSL 망, 케이블 망, 전용회선)에 따라 필요한 값을 설정합니다.
		VPN TUNNEL	VPN 터널을 추가하거나 삭제합니다.
		ROUTING	정적 라우트(static route)를 추가하거나 삭제합니다.
		DHCP	장비가 DHCP 서버로 동작하기 위해 필요한 값(할당할 IP 주소 범위와 서브넷 마스크, 기본 게이트웨이 주소, IP 주소 할당 시간)을 지정합니다.
		SNMP	장비의 SNMP 에이전트로 접속할 수 있는 호스트를 추가하거나 삭제합니다.
		PPTP	PPTP 서버를 구성합니다.
		NAT	DMZ, SNAT, DNAT을 설정합니다.
	SERVICES	DAEMONS	각종 데몬에 대한 상태 체크 및 변경, 부팅시 실행 여부 등을 설정합니다.
		UPDATE	장비의 버전을 체크하여 업데이트를 실시합니다.
		WEB SSH	웹에서 SSH를 사용하실 수 있습니다.

3. 웹 콘솔 살펴보기

메뉴			기능
STATISTIC	SYSTEM	GENERAL	장비의 기본적인 정보를 출력합니다.
	NETWORK	TUNNEL STATUS	터널의 현재 상태와 VPN 터널을 통해 송수신되는 패킷 사용량에 대한 통계 정보를 출력합니다.
		IFCONFIG	interface의 IP Address, MAC Address, Subnet 정보를 알려줍니다.
		ROUTING STATUS	routing 정보를 알려줍니다.
		ARP TABLE	장비를 사용하고 있는 IP 주소와 MAC 주소의 목록을 보여줍니다.
		DHCP LEASE	DHCP 설정 정보와 현재 클라이언트에게 할당된 IP 주소를 보여줍니다.
		ALIVE	whois, ping, traceroute 를 실행하실 수 있으며 그 결과를 알려줍니다.
		PPTP	pptp 동작시의 접속 시간, 아이디, 할당된 아이피, 접속 아이피 정보를 알려주며, Manage에서는 일시중지나 실행을 하실 수 있습니다.
	LOG	SYSTEM	터널의 up/down 로그 정보를 알려 줍니다.
		FIREWALL	방화벽에 대한 모니터링 정보를 알려줍니다.
		QOS	QoS에 대한 모니터링 정보를 알려줍니다.
	TRAFFIC	STATUS	인터페이스별 다운로드, 업로드 트래픽 정보를 실시간으로 알려줍니다.
	PNN	TRAFFIC ANALYSIS	호스트들의 업로드,다운로드에 대한 세션 및 트래픽 정보를 알려줍니다.
		NETWORK ANALYSIS	호스트들의 TCP,UDP 세션 정보를 알려줍니다.
FIREWALL	EZ2F	QUICK START	쉽고 빠르게 FIREWALL을 구성할 수 있게 해주는 메뉴입니다.
	ADVANCED	OBJECTS	방화벽 정책을 적용받을 호스트들을 오브젝트화(그룹화)합니다.
		CHAIN POLICY	각각의 CHAIN(FORWARD, INPUT, OUTPUT)에 대해 ACCEPT, DROP를 설정합니다.
		CHAIN FORWARD	FORWARD에 대한 정책을 수립합니다.
		CHAIN INPUT	INPUT에 대한 정책을 수립합니다.
		CHAIN OUTPUT	OUTPUT에 대한 정책을 수립합니다.
		ICMP	ICMP에 대한 정책을 수립합니다.
QoS	EZ2Q	BASIC	각 인터페이스에 대해 UPLOAD, DOWNLOAD 허용 트래픽을 설정합니다.

3. 웹 콘솔 살펴보기

메뉴			기능
		UPLOAD RULE	UPLOAD RULE을 수립하며 우선순위(1~7)을 설정합니다.
		DOWNLOAD RULE	DOWNLOAD RULE을 수립하며 우선순위(1~7)을 설정합니다.
DNS	DNS	GLOBAL SETTING	Recursion, Fetch-glue, Notify, Version, Allow-Transfer, Forwarders를 설정합니다.
		DNS SETTING	Master, Slave 설정합니다.
		DNS RELOAD	설정된 정보를 RELOAD합니다.

Tip 참고

웹 콘솔 화면에는 표시되어 있지만 위 표에서 설명하지 않은 메뉴 항목들은 현재 구현 중인 메뉴로, 다음 버전에서 지원될 예정입니다.

Chapter

4

제품 설정하기

이 장에서는 웹 콘솔의 'CONFIGURATION' 메뉴를 사용하여 R2SKY 시리즈를 설정하는 방법에 대해 설명합니다.

4. 제품 설정하기

이 장에서 다루는 내용은 다음과 같습니다.

◦ 고객과 관리자(장비와 관련된 사람들의) 정보 설정하기
◦ 액세스 리스트 관리하기
◦ 웹콘솔 사용자 암호 변경하기
◦ 시간 설정하기
◦ 설정 파일 관리하기
◦ 설정을 플래시 메모리에 저장하기
◦ 장비 재부팅하기
◦ 장비 셧다운하기
◦ 인터페이스 설정하기
◦ VPN 설정하기
◦ 라우팅 설정하기
◦ DHCP 설정하기
◦ 외부 서버로 로그 전송하기
◦ 데몬 상태 설정하기

고객과 관리자(장비와 관련된 사람들의) 정보 설정하기

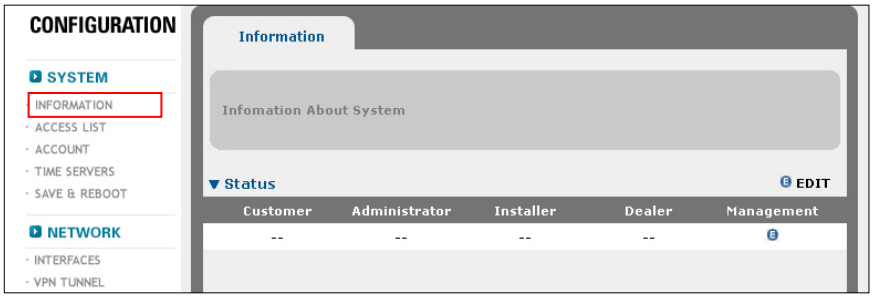
R2SKY 시리즈 웹 콘솔에서는 장비와 관련된 다음과 같은 정보를 입력하고 조회할 수 있습니다.

◦ 장비를 사용하는 고객
◦ 장비 관리자
◦ 장비 설치 담당자
◦ 장비 판매처
◦ 장비의 통계 정보를 조회할 수 있는 PnN 인터페이스

4. 제품 설정하기

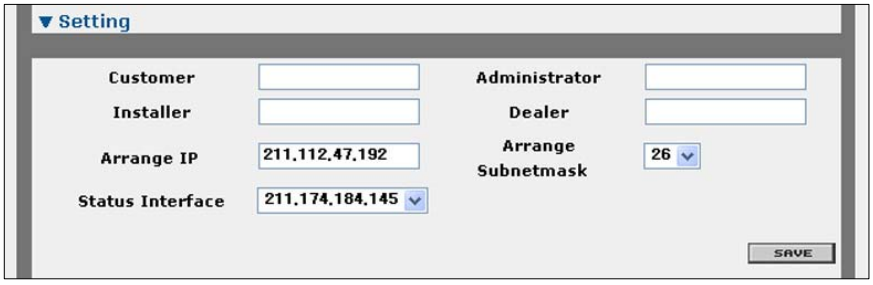
이러한 정보를 입력하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 CONFIGURATION - System - Information 메뉴를 클릭합니다. 그러면, 다음과 같은 <Information> 화면이 나타납니다.



2. 기본적으로 웹 콘솔에는 고객이나 관리자에 대한 정보가 입력되어 있지 않습니다. 이러한 정보를 입력하기 위해서 Management 항목에 있는 (E) 아이콘을 클릭합니다.

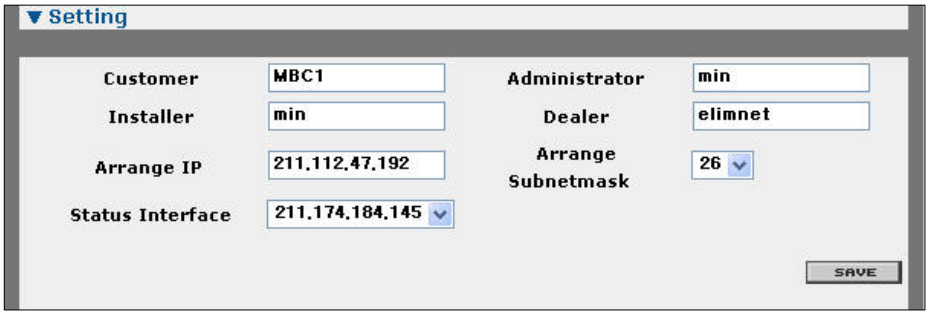
3. 그러면, 다음과 같이 정보를 입력할 수 있는 <Setting> 화면이 나타납니다. 그림 아래의 설명을 참고하여 각 항목의 값을 설정합니다.



4. 제품 설정하기

항 목	설 명
Customer	이 장비를 사용하는 고객의 정보를 입력합니다.
Administrator	이 장비를 관리하는 역할을 맡은 관리자에 대한 정보를 입력합니다.
Installer	이 장비를 설치한 설치 담당자에 대한 정보를 입력합니다.
Dealer	이 장비의 판매처에 대한 정보를 입력합니다.
Arrange IP	이 장비에 할당된 IP 대역을 입력합니다. Arrange IP를 입력하지 않으면, STATISTIC – System – Bandwidth 메뉴를 사용할 수 없습니다.
Arrange Subnetmask	이 장비에 할당된 네트워크 범위를 입력합니다.
status Interface	콤보 박스를 클릭한 후 가상 인터페이스를 선택합니다. STATISTIC – PnN 메뉴를 사용하여 통계 정보를 조회하려면 반드시 PnN 인터페이스를 지정해야 합니다. PnN 인터페이스로 지정할 인터페이스는 IP 주소와 넷 마스크 등이 설정되어 있어야 합니다. 해당 메뉴에 대한 적용은 장비의 용도에 따라 달라집니다.

4. 항목의 값을 모두 입력한 후 [SAVE] 버튼을 클릭합니다.



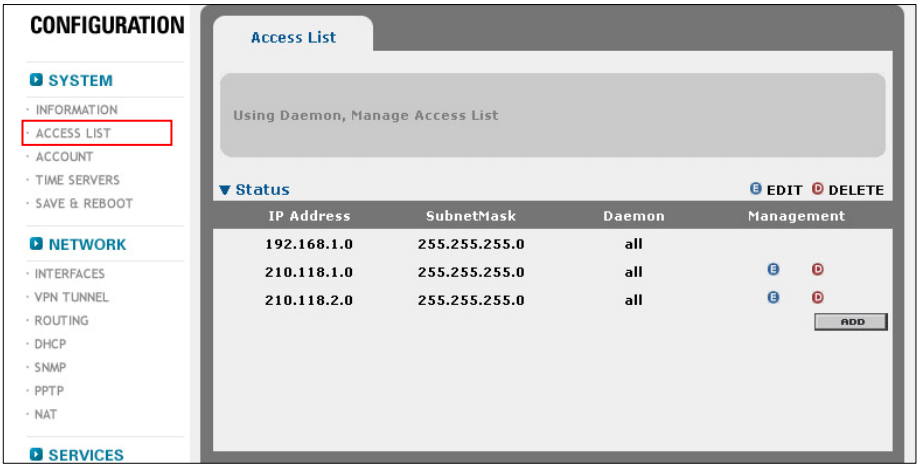
5. 그러면, <Information> 화면의 목록에 입력한 정보가 표시됩니다.

4. 제품 설정하기

엑세스 리스트 관리하기

R2SKY 시리즈는 데몬에 엑세스 리스트를 적용하여 특정한 호스트가 해당 데몬에 엑세스할 수 없도록 할 수 있습니다. 이 기능은 허용되지 않은 사용자의 엑세스나 해커의 의도된 공격으로부터 장비를 보호할 수 있게 해줍니다.

웹 콘솔에서 CONFIGURATION - System - Access List 메뉴를 클릭하면 현재 설정된 엑세스 리스트의 목록을 보여주는 다음과 같은 <Access List> 화면이 나타납니다.



다음 절에서는 <Access List> 화면에서 새로운 엑세스 리스트를 추가하거나 기존 엑세스 리스트를 수정 혹은 삭제하는 방법을 살펴봅니다.

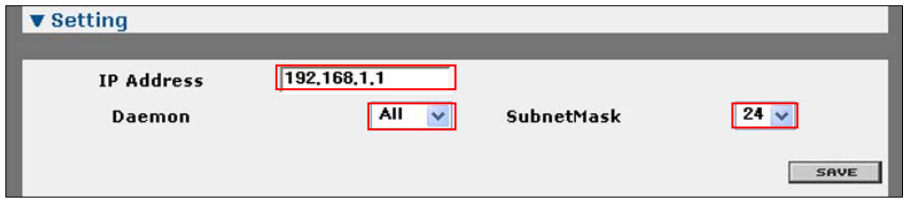
4. 제품 설정하기

엑세스 리스트 추가하기

특정 데몬에 적용될 엑세스 리스트를 추가하는 방법은 다음과 같습니다.

1. <Access List> 화면의 아래쪽에 있는 [ADD] 버튼을 클릭합니다.

2. 화면 아래쪽에 엑세스 리스트를 정의할 수 있는 <Setting> 화면이 나타납니다. 그림 아래에 있는 표의 설명을 참고하여 <Setting> 화면에 있는 각 항목들의 값을 설정합니다.



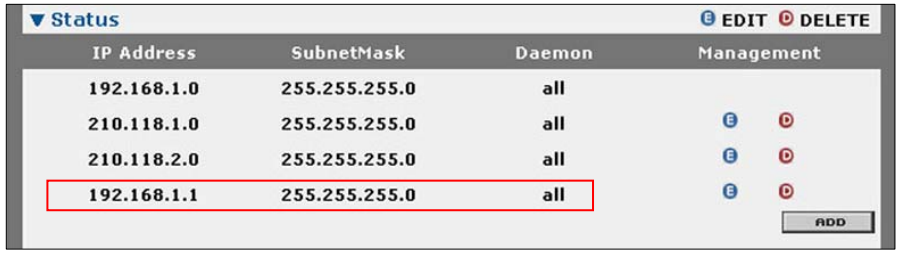
① IP Address : 엑세스 리스트에 추가할 네트워크의 번호나 호스트의 IP 주소를 입력합니다.

② Daemon : 콤보 박스를 클릭한 후 엑세스 리스트를 적용할 데몬을 선택합니다.

③ Subnet Mask : 콤보 박스를 클릭한 후 서브넷 마스크의 bit 수를 선택합니다.
- 24 : 255.255.255.0, 16 : 255.255.0.0, 8 : 255.0.0.0

3. [SAVE] 버튼을 클릭합니다.

4. 그러면, 다음과 같이 설정한 IP 주소가 선택한 데몬의 엑세스 리스트로 추가됩니다.

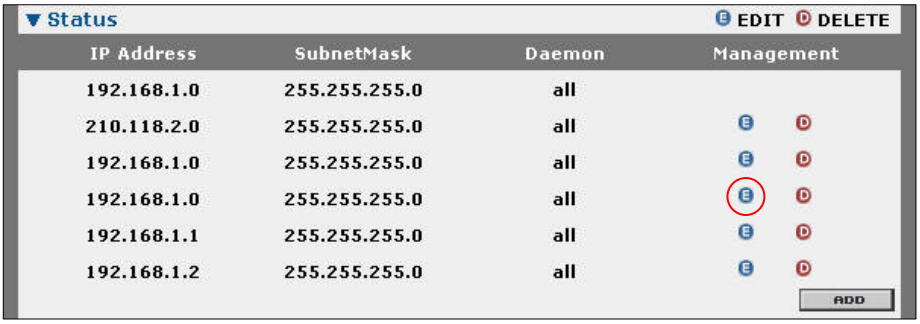


4. 제품 설정하기

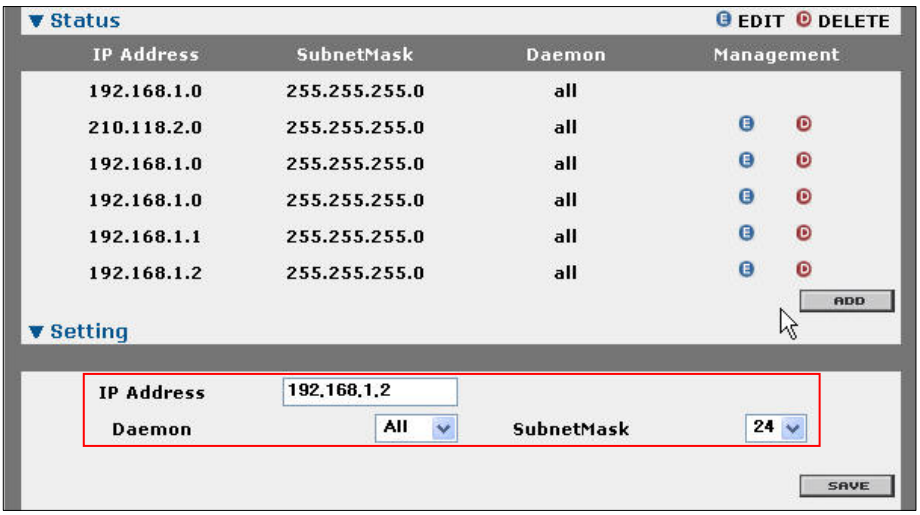
엑세스 리스트 수정하기

기존에 정의된 엑세스 리스트를 수정하는 방법은 다음과 같습니다.

1. <Access List> 화면의 엑세스 리스트 목록에서 수정할 엑세스 리스트의 Management 항목에 있는 (E) 버튼을 클릭합니다.

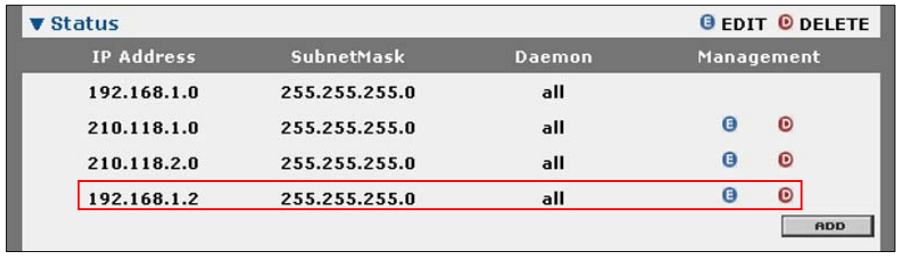


2. 선택한 엑세스 리스트의 설정 값을 수정할 수 있는 <Setting> 화면이 나타납니다. '엑세스 리스트 추가하기' 절에 설명되어 있는 내용을 참고하여 원하는 항목의 값을 수정합니다.



3. 항목을 모두 수정한 후, [SAVE] 버튼을 클릭합니다.

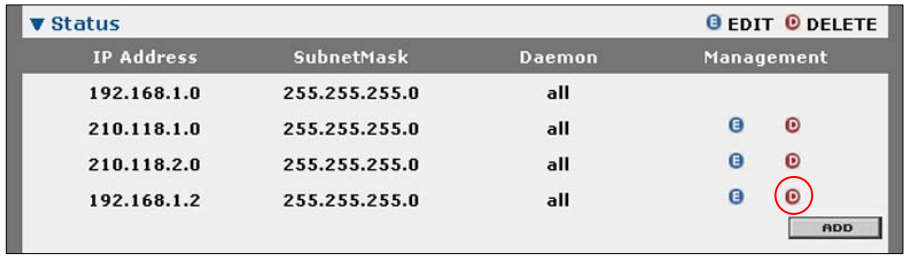
4. 그러면, 다음과 같이 변경된 엑세스 리스트의 설정 값이 화면에 표시됩니다.



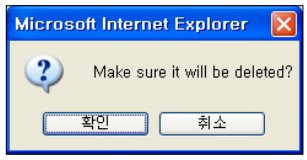
엑세스 리스트 삭제하기

정의되어 있는 엑세스 리스트를 삭제하는 방법은 다음과 같습니다.

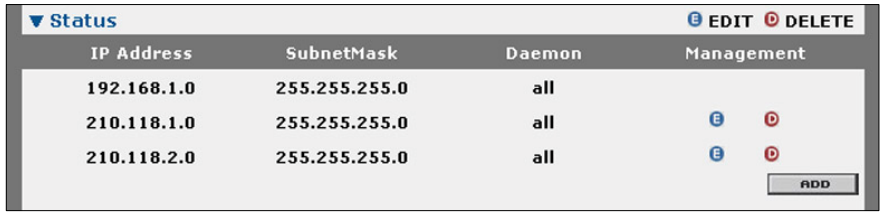
1. <Access List> 화면의 엑세스 리스트 목록에서 삭제할 엑세스 리스트의 Management 항목에 있는 (D) 버튼을 클릭합니다.



2. 다음과 같이 엑세스 리스트의 삭제를 확인하는 화면이 나타납니다. [확인]을 클릭합니다.



3. 그러면, 선택한 엑세스 리스트가 <Access List> 화면의 목록에서 삭제됩니다.



4. 제품 설정하기

웹 콘솔 사용자 암호 변경하기

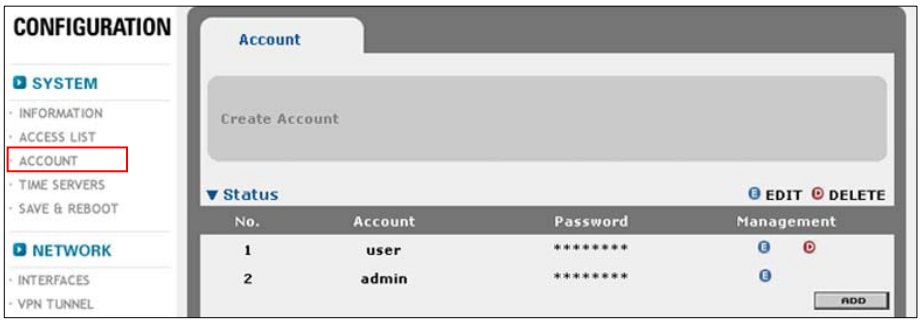
웹 콘솔로 로그인 하려면 반드시 사용자 ID와 암호를 입력해야 합니다. R2SKY 시리즈에는 기본으로 admin(암호는 r2sky)이라는 사용자와 user(암호는 r2sky)라는 두 사용자가 등록되어 있습니다. 웹 콘솔에서는 이 두 사용자의 암호를 변경할 수 있습니다. 최초로 웹 콘솔에 로그인한 후에는 가능하면 기본으로 설정되어 있는 암호를 다른 값으로 변경하는 것이 안전합니다.

Tip 참고

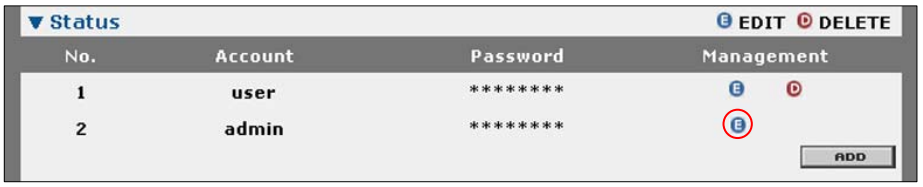
기본으로 설정되는 웹 콘솔 암호는 상황에 따라 변경될 수 있습니다.

다음은 웹 콘솔 사용자의 암호를 변경하는 방법입니다.

1. 웹 콘솔에서 CONFIGURATION - SYSTEM - ACCOUNT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Account> 화면이 나타납니다.

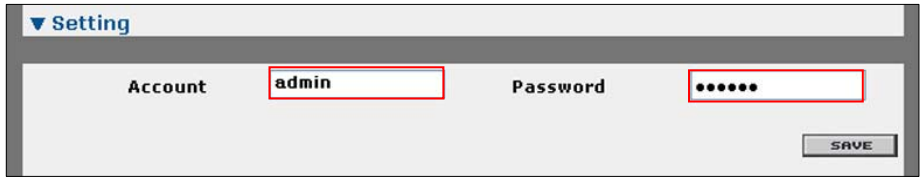


2. <Account> 화면의 Account 리스트 목록에서 수정할 Account 리스트의 Management 항목에 있는 (E) 버튼을 클릭합니다.



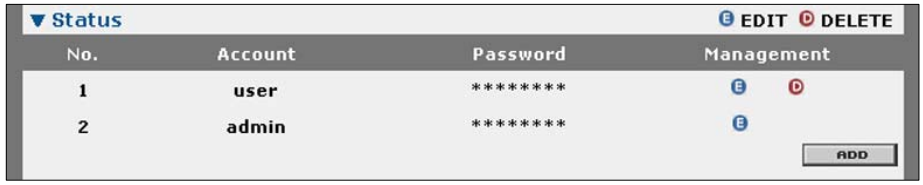
3. <Account> 화면에 있는 admin과 user 사용자의 Password 항목에 각각 admin과 user로 로그인할 때 사용할 새로운 암호를 입력합니다.

4. 제품 설정하기



4. 암호를 입력한 후 [SAVE] 버튼을 클릭합니다.

5. 암호가 성공적으로 변경되면 다음과 같은 화면이 나타납니다.



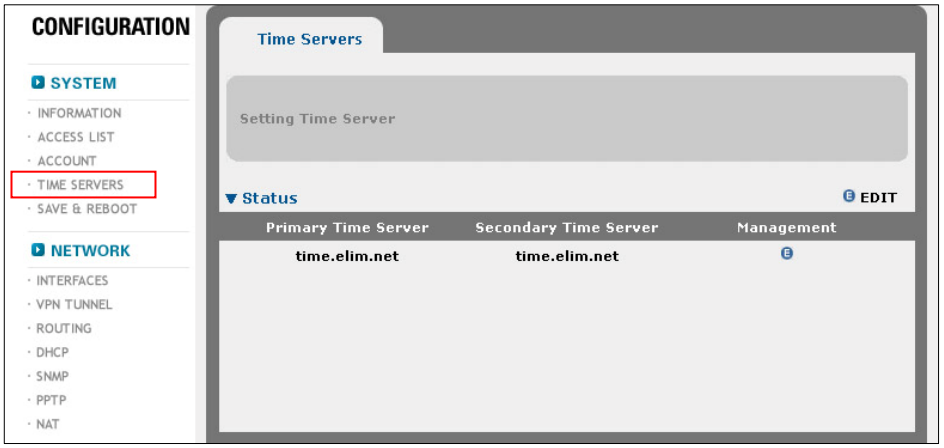
이 후부터는 웹 콘솔에서 로그아웃 한 후 다시 웹 콘솔로 로그인할 때 변경된 암호를 사용해야 합니다.

4. 제품 설정하기

시간 설정하기

R2SKY 시리즈는 장비의 내부 시간을 설정하거나 다른 장비와의 동기(Synchronization)를 맞추기 위해 정확한 시간을 제공해주는 NTP(Network Time Protocol) 서버를 사용할 수 있습니다. 기본적으로 사용되는 Primary 타임 서버(Time Server)와 백업용으로 사용되는 Secondary 타임 서버, 2개의 타임 서버를 지정할 수 있습니다. Secondary 서버는 Primary 서버에 문제가 발생한 경우에 바로 사용됩니다.

웹 콘솔에서 CONFIGURATION - TIME SERVERS 메뉴를 클릭하면 현재 설정되어 있는 타임 서버를 보여주고, 타임 서버를 설정할 수 있는 다음과 같은 <Time Servers> 화면이 나타납니다.



타임 서버 지정하기

기본적으로 R2SKY 시리즈는 Primary 타임 서버로 "time.elim.net", Secondary 타임 서버로 "time.elim.net"이 설정되어 있습니다. 다음과 같은 방법을 통해 기본으로 설정된 서버 대신 다른 서버를 타임 서버로 지정할 수 있습니다.

1. <Time Sever> 화면의 Management 항목에 있는 (E)를 클릭합니다.

2. 화면 아래쪽에 다음과 같이 타임 서버를 선택할 수 있는 <Setting> 화면이 나타납니다.

4. 제품 설정하기

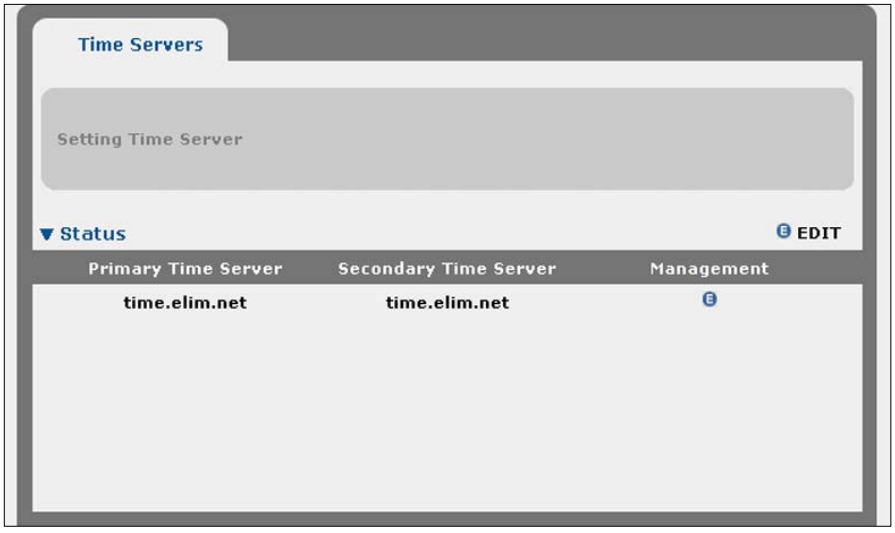
각 항목을 다음과 같이 설정합니다.

① Primary Time Server : Primary 타임 서버로 사용할 서버의 이름이나 IP 주소를 입력합니다.

② Secondary Time Server : Secondary 타임 서버로 사용할 서버의 이름이나 IP 주소를 입력합니다. Primary 타임 서버와 동일한 서버를 지정할 수 있습니다.

3. 타임 서버를 입력한 후 [SAVE] 버튼을 클릭합니다.

4. 그러면, <Time Servers> 화면에 선택한 타임 서버가 표시됩니다.

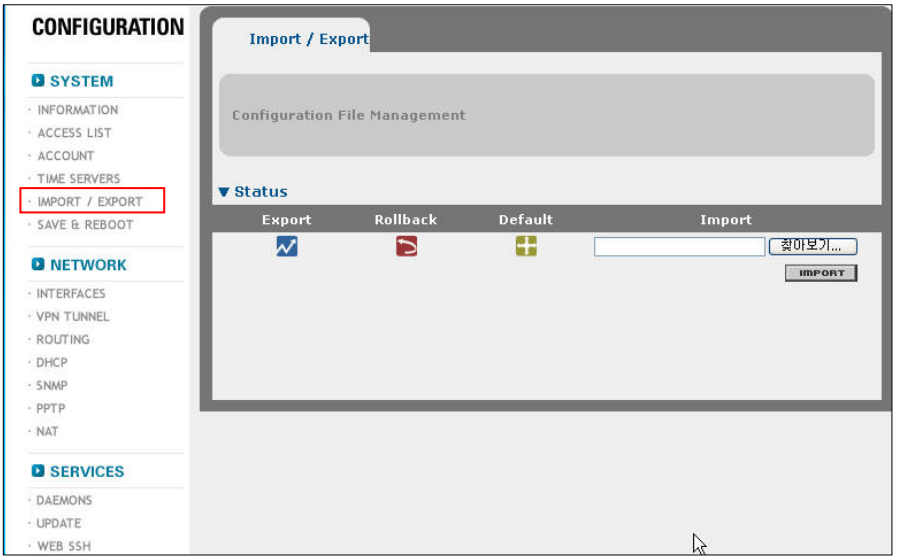


4. 제품 설정하기

설정 파일 관리하기

R2SKY 시리즈의 설정은 파일 형태로 장비에 저장됩니다. 설정이 파일로 관리되기 때문에 외부 서버에 설정을 백업해두거나(Export) 혹은 외부 서버에 저장된 설정 파일을 장비로 가져와서 저장할(Import) 수 있습니다. 그리고, 설정이 변경되기 직전의 설정과 장비 출하 시의 기본 설정을 별도의 파일로 저장해두기 때문에 필요한 경우 이전 설정(Rollback)이나 기본 설정(Default)을 다시 되돌릴 수 있습니다.

웹 콘솔에서 CONFIGURATION - SYSTEM - IMPORT / EXPORT 메뉴를 클릭했을 때 나타나는 <Import/Export> 화면에서 이러한 설정 파일과 관련된 작업들을 수행할 수 있습니다.



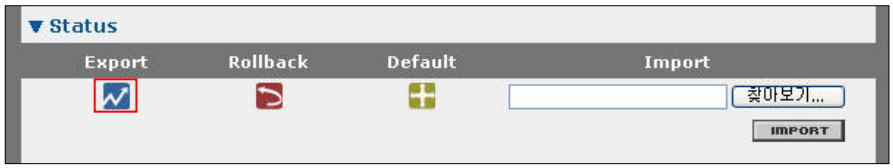
4. 제품 설정하기

설정 파일 Export하기

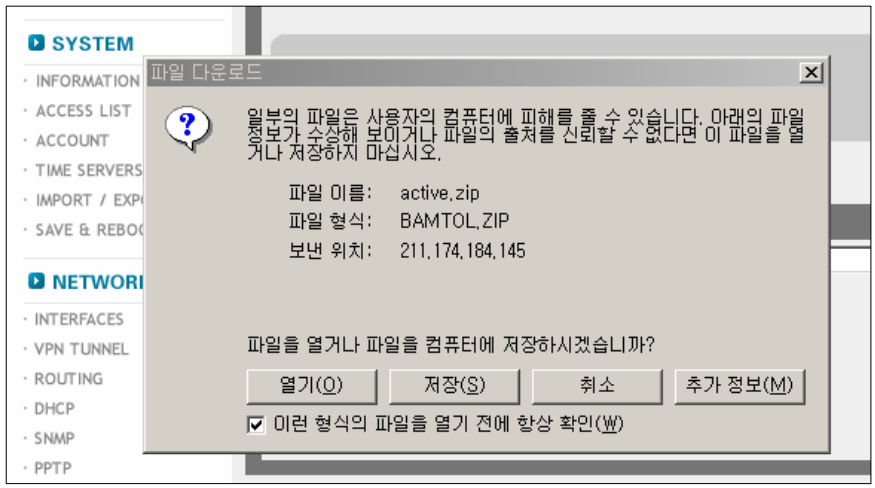
다음과 같은 방법으로 현재 장비 설정을 웹 콘솔을 실행한 호스트의 PC에 저장합니다.

1. 웹 콘솔에서 CONFIGURATION – SYSTEM - IMPORT / EXPORT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Import/Export> 화면이 나타납니다.

2. <Import/Export> 화면의 Export 항목에 있는 아이콘을 클릭합니다.

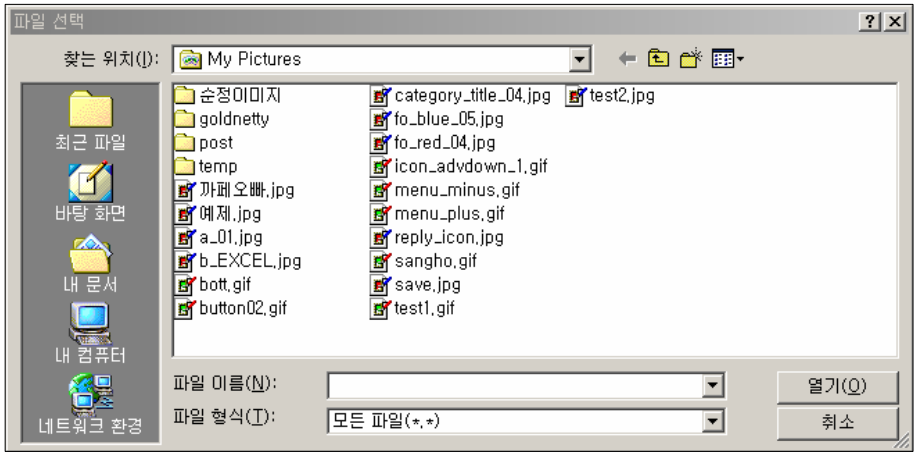


3. 다음과 같은 <파일 다운로드> 화면이 나타나면 [저장(S)] 버튼을 클릭합니다.



Export 아이콘을 클릭하면 위와 같은 파일 다운로드 화면이 나옵니다.

4. 다음과 같은 <다른 이름으로 저장> 화면이 나타나면 파일 이름에 설정을 저장할 파일 이름을 입력한 후 [저장(S)] 버튼을 클릭합니다.

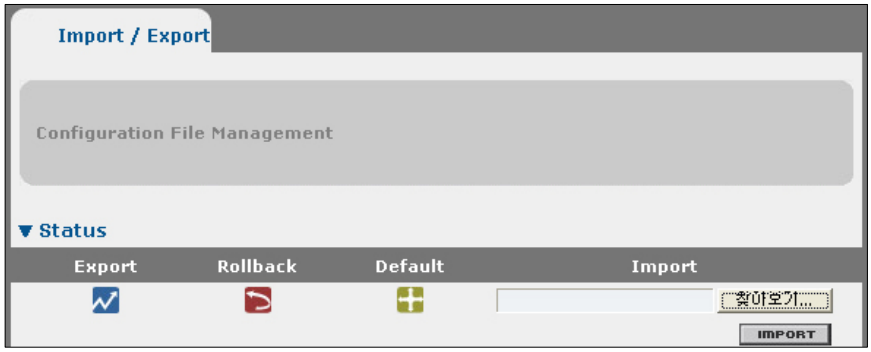


이렇게 저장된 설정 파일은 "Import" 기능을 통해 다시 장비로 읽어와서 장비에 적용될 수 있습니다. 설정 파일을 Import하는 방법은 다음 절에서 설명합니다.

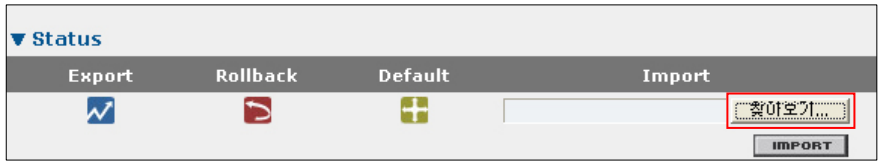
설정 파일 Import하기

설정 파일을 Import하는 것은 외부에 있는 설정 파일을 장비로 가져와서 장비의 설정 파일로 사용하는 것입니다. 웹 콘솔을 실행한 호스트의 PC에 Import할 설정 파일을 저장해둡니다. 그런 후에 웹 콘솔에서 다음과 같은 방법으로 설정 파일을 Import합니다.

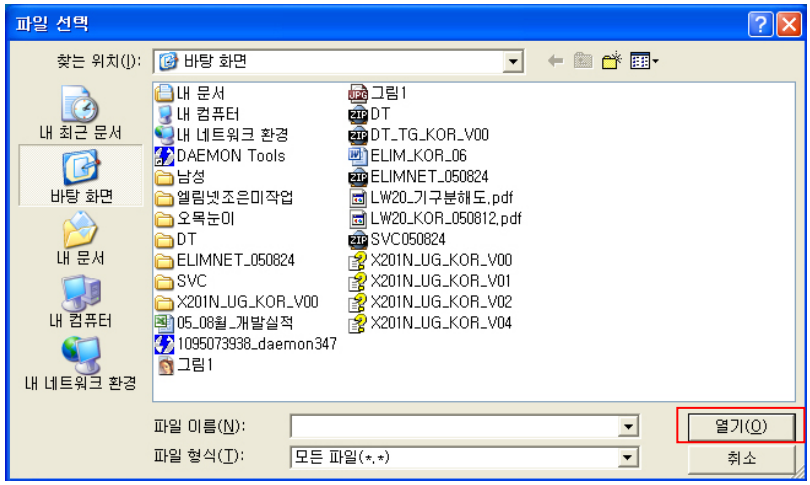
1. 웹 콘솔에서 CONFIGURATION - SYSTEM - IMPORT / EXPORT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Import/Export> 화면이 나타납니다.



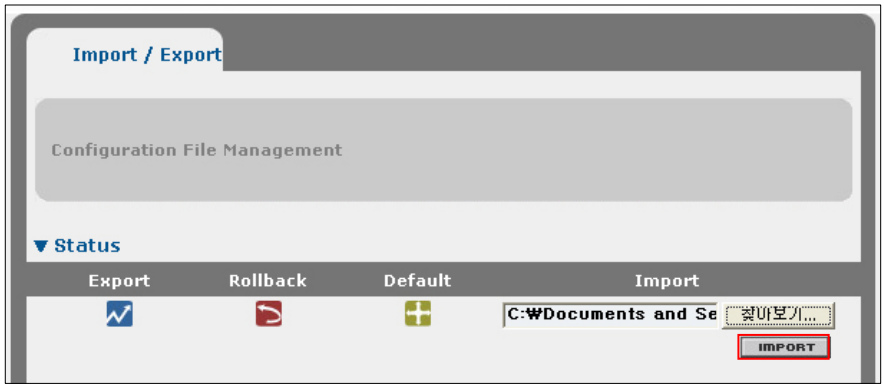
2. <Import/Export> 화면의 Import 항목에 있는 [찾아보기] 버튼을 클릭합니다.



3. 다음과 같은 <파일 선택> 화면이 나타나면 Import할 파일을 선택한 후 [열기(O)] 버튼을 클릭합니다.



4. 선택한 파일 이름이 Import 항목에 표시되면 아래에 있는 [IMPORT] 버튼을 클릭합니다.

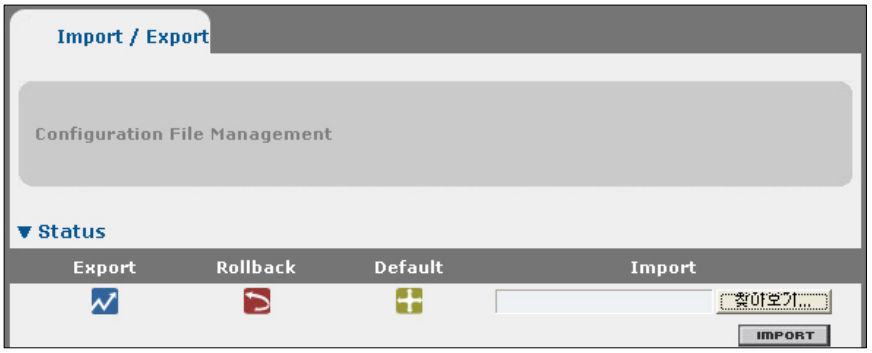


4. 제품 설정하기

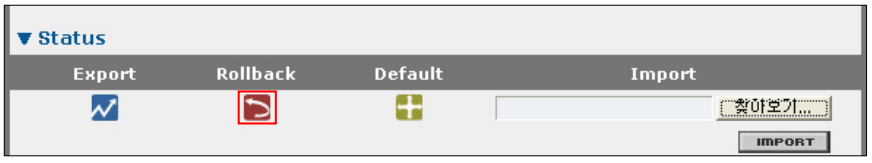
이전 설정 가져오기

R2SKY 시리즈는 현재 설정으로 변경되기 직전의 설정으로 다시 복구할 수 있습니다. 이러한 기능을 "Rollback"이라고 합니다. 웹 콘솔에서 이전의 설정으로 Rollback하는 방법은 다음과 같습니다.

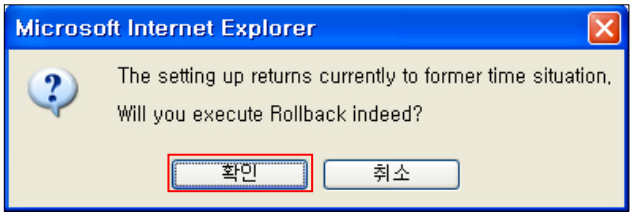
1. 웹 콘솔에서 CONFIGURATION – SYSTEM - IMPORT / EXPORT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Import/Export> 화면이 나타납니다.



2. <Import/Export> 화면의 Rollback 항목에 있는 아이콘을 클릭합니다.



3. 다음과 같이 Rollback 여부를 확인하는 화면이 나타납니다. [확인]을 클릭하면 이전 설정이 다시 복구 됩니다.

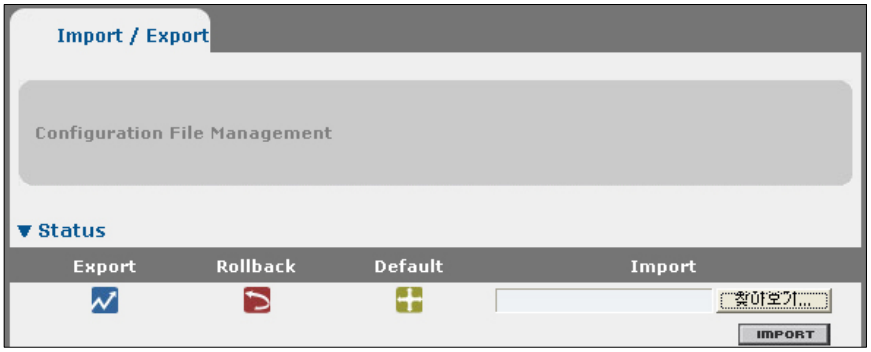


4. 제품 설정하기

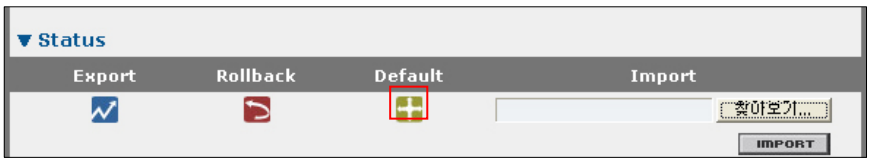
초기 설정 가져오기

웹 콘솔에서 장비의 설정을 출하 시의 초기 설정 값으로 되돌리는 방법은 다음과 같습니다.

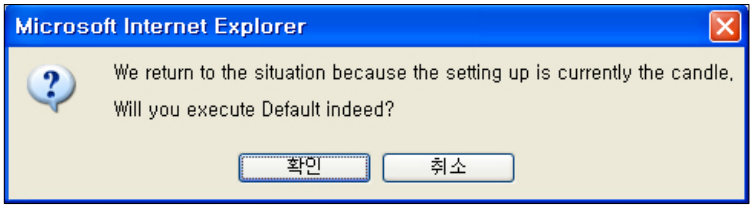
1. 웹 콘솔에서 CONFIGURATION - SYSTEM - IMPORT / EXPORT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Import/Export> 화면이 나타납니다.



2. <Import/Export> 화면의 Default 항목에 있는 아이콘을 클릭합니다.



3. 다음과 같이 장비를 초기 상태로 설정할지 여부를 확인하는 화면이 나타납니다. [확인]을 클릭하면 출하 시의 상태로 설정됩니다.



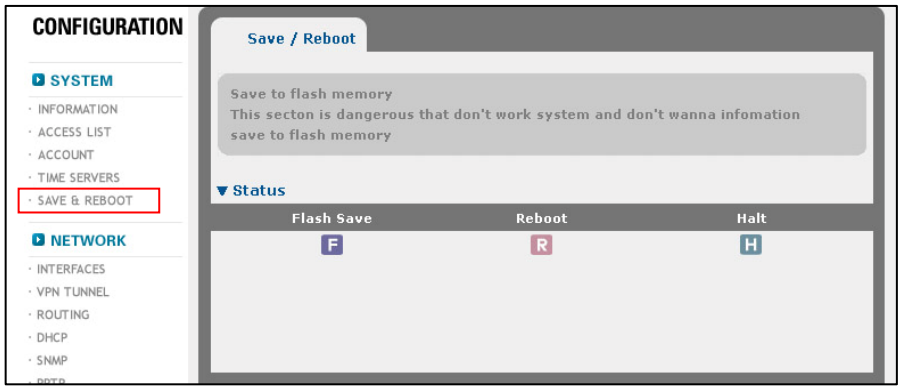
4. 제품 설정하기

설정을 플래시 메모리에 저장하기

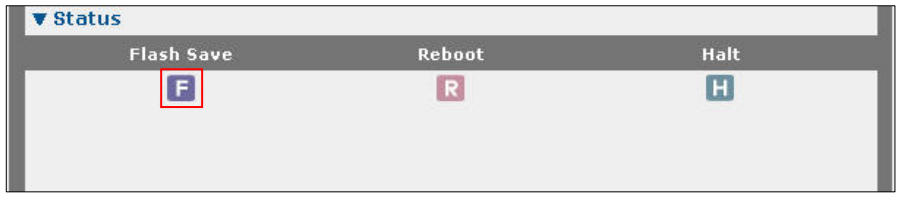
앞에서 살펴본 웹 콘솔의 설정 메뉴들을 사용하여 장비의 설정을 변경한 후에는 변경한 설정을 장비의 플래시 메모리에 저장해야 합니다. 플래시 메모리에 저장하지 않으면 장비가 리부팅 되는 경우 이전 설정으로 되돌아가게 됩니다.

변경된 설정을 플래시 메모리에 저장하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 CONFIGURATION - SYSTEM - SAVE & REBOOT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Save/Reboot> 화면이 나타납니다.



2. <Save/Reboot> 화면에서 Flash Save 항목에 있는 (F) 아이콘을 클릭합니다.



3. 다음과 같이 플래쉬 저장 여부를 확인하는 화면이 나타납니다. [확인]을 클릭합니다.

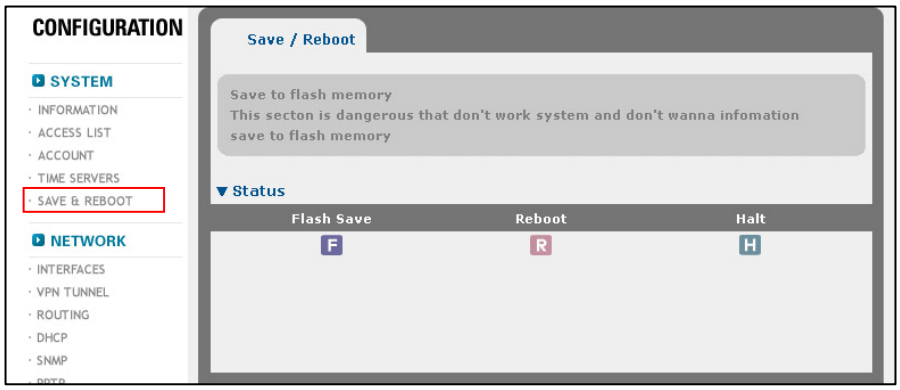
4. 장비의 설정이 플래쉬 메모리에 성공적으로 저장되면 이를 알려주는 다음과 같은 메시지 화면이 출력됩니다.

장비 재부팅하기

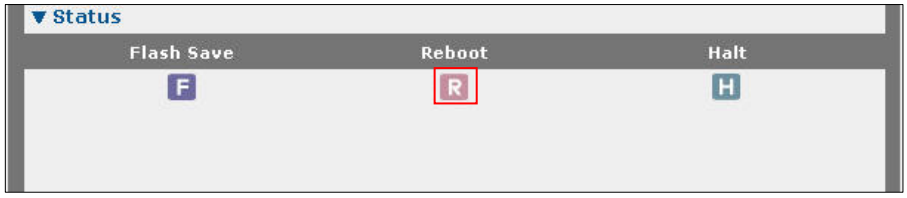
장비가 정상적으로 동작하지 않거나 그 밖에 필요한 경우에는 시스템을 다시 부팅해야 합니다. 멀리 떨어진 장소에서도 웹 콘솔을 통해 다음과 같은 방법으로 장비를 부팅할 수 있습니다.

다음은 웹 콘솔에서 장비를 재부팅하는 방법입니다.

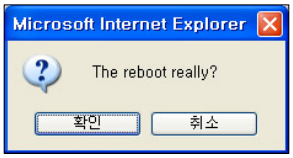
1. 웹 콘솔에서 CONFIGURATION - SYSTEM - SAVE & REBOOT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Save/Reboot> 화면이 나타납니다.



2. <Save/Reboot> 화면에서 Reboot 항목에 있는 (R) 아이콘을 클릭합니다.



3. 다음과 같이 장비의 재부팅 여부를 확인하는 화면이 나타납니다. [확인]을 클릭하면 장비가 재부팅됩니다.



주의

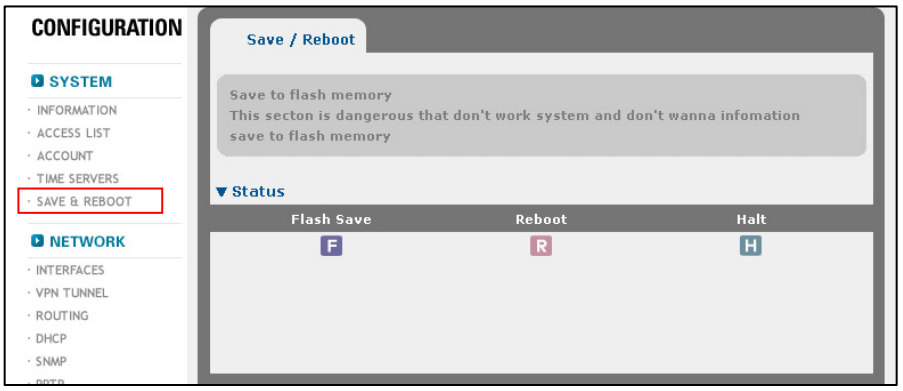
장비를 부팅하게 되면 장비를 통해 연결되어 있는 모든 사용자의 네트워크 연결이 끊어지게 되므로 반드시 필요한 경우에만 장비를 부팅하도록 합니다.

장비 셧다운하기

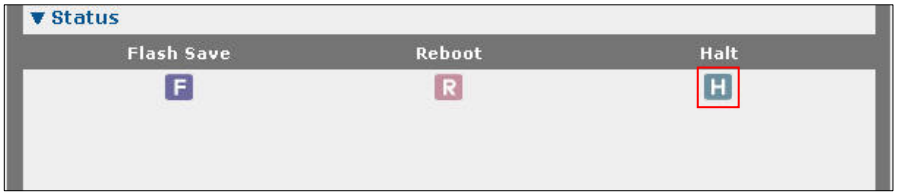
R2SKY 시리즈는 웹 콘솔에서 원격으로 셧다운 시킬 수 있습니다. 장비가 셧다운 된 상태에서는 전원 스위치를 꺼도 장비에 문제가 발생하지 않습니다.

다음은 웹 콘솔에서 장비를 셧다운하는 방법입니다.

1. 웹 콘솔에서 CONFIGURATION - SYSTEM - SAVE & REBOOT 메뉴를 클릭합니다. 그러면, 다음과 같은 <Save/Reboot> 화면이 나타납니다.



2. <Save/Reboot> 화면에서 Halt 항목에 있는 (H) 아이콘을 클릭합니다.



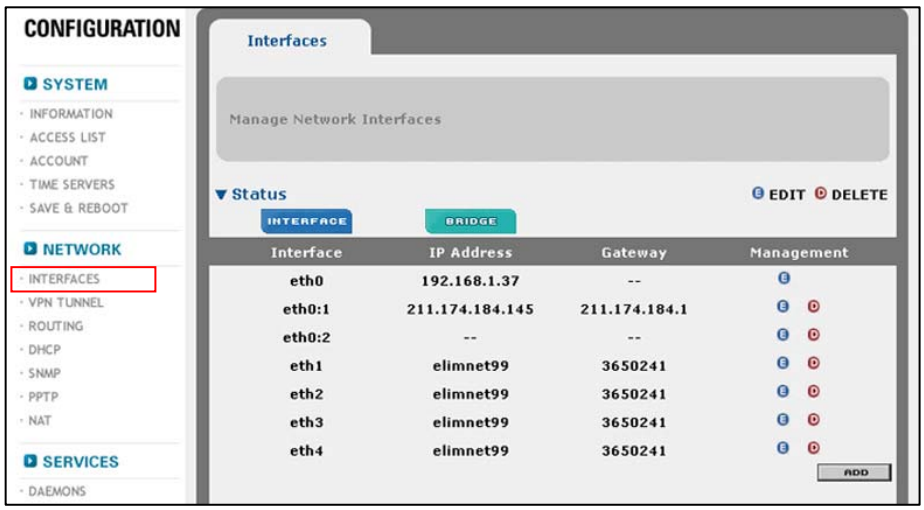
3. 다음과 같이 장비의 셧다운 여부를 확인하는 화면이 나타납니다. [확인]을 클릭하면 장비가 셧다운됩니다.

Tip 참고

장비가 셧다운 되면 웹 콘솔과의 접속도 끊어지게 됩니다.

인터페이스 설정하기

웹 콘솔에서 CONFIGURATION - NETWORK - INTERFACES 메뉴를 클릭하면 R2SKY 시리즈의 인터페이스를 설정할 수 있는 다음과 같은 <Interfaces> 화면이 나타납니다.



4. 제품 설정하기

기본적으로 R2SKY 시리즈의 인터페이스는 가상 인터페이스인 eth0만 활성화되어 있고 나머지 인터페이스들은 활성화되어 있지 않은 상태입니다. R2SKY 시리즈는 각 인터페이스를 다음과 같은 3가지 종류로 설정할 수 있습니다.

◦ PPPoE : ADSL 모뎀과 같이 계정 접속(PPPoE)을 이용한 설정 시 사용되는 인터페이스
◦ Cable : 케이블 모뎀 또는 자동 접속(dhcp) 방식을 이용한 설정 시 사용되는 인터페이스
◦ Static : 전용회선으로부터 받은 고정IP 또는 초고속 사업자로부터 받은 고정 IP 설정 시 사용되는 인터페이스

LAN

- eth0 : 관리용 인터페이스로 항상 192.168.1.100 의 IP가 설정 되어 있어야 합니다.
- eth0:1 : 엘림넷에서 할당 받은 고정 IP 또는 내부에서 사설로 사용할 IP 중 게이트웨이로 사용할 IP를 입력 합니다
- eth0:2 : 사용하려는 IP 블록이 추가 될 경우 사용합니다.

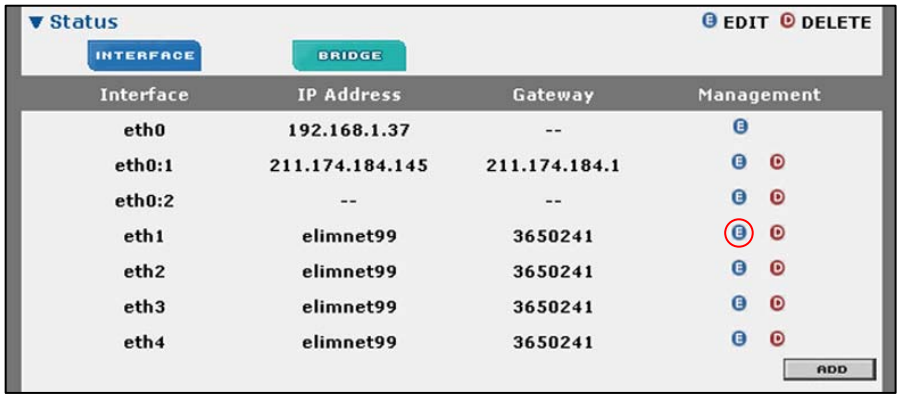
WAN

- eth1 : PPPOE, Cable, Static 중 선택하여 외부 망과 연결할 경우 사용합니다.
- eth2 : PPPOE, Cable, Static 중 선택하여 외부 망과 연결할 경우 사용합니다.
- eth3 : PPPOE, Cable, Static 중 선택하여 외부 망과 연결할 경우 사용합니다.
- eth4 : PPPOE, Cable, Static 중 선택하여 외부 망과 연결할 경우 사용합니다.

각 종류의 인터페이스를 설정하는 방법은 다음과 같습니다.

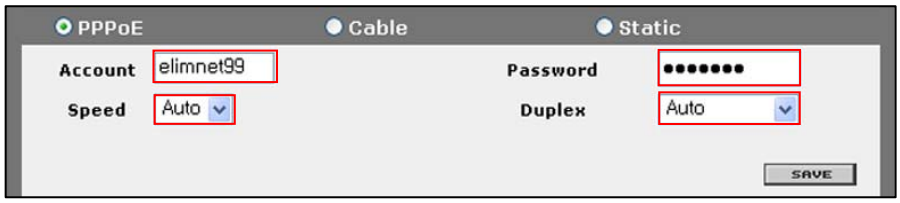
PPPoE 인터페이스 설정하기

1. <Interfaces> 화면의 인터페이스 목록에서 ADSL 망과 연결되는 PPPoE 인터페이스로 설정할 LAN 인터페이스(eth1 ~ eth4)를 선택한 후 (E)를 클릭합니다.



2. 그러면, 선택한 인터페이스를 PPPoE 인터페이스로 설정하기 위해 필요한 설정 값을 입력하는 항목들로 구성된 <Setting> 화면이 나타납니다. <Setting> 화면의 가장 위에 있는 3개의 라디오 버튼(PPPoE, Cable, Static) 중에서 'PPPoE'를 클릭합니다.

3. 그리고, 다음 설명을 참고하여 아래에 있는 항목들의 값을 지정합니다.



① Account : 사용자의 로그인 ID를 알파벳과 숫자를 사용하여 최대 20자 이내로 입력합니다.

② Password : 사용자의 로그인 암호를 입력합니다.

③ Speed : 콤보 박스를 클릭한 후 인터페이스의 전송 속도를 선택합니다.

- auto : 연결된 장비의 속도에 맞게 자동으로 설정.
- 10 : 10Mbps
- 100: 100Mbps

4. 제품 설정하기

④ Duplex : 콤보 박스를 클릭한 후 인터페이스의 전송 모드(duplex mode)를 지정합니다.

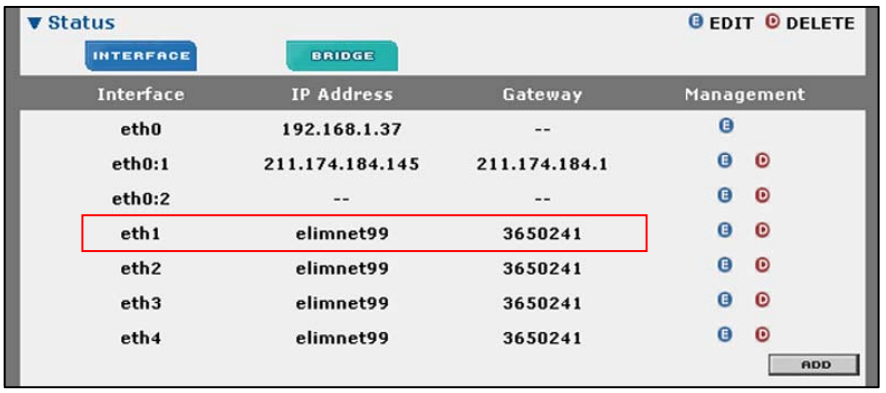
- Auto : 연결된 장비의 전송 모드에 맞게 자동으로 설정.
- Full duplex: 전이중 전송 모드(Full-duplex mode)
- Half duplex: 반이중 전송 모드(Half-duplex mode)

주의

③, ④번 항목은 특별한 경우를 제외하고는 Auto Mode로 설정할 것을 권장합니다.

4. 항목의 값을 모두 입력한 후 [SAVE] 버튼을 누릅니다.

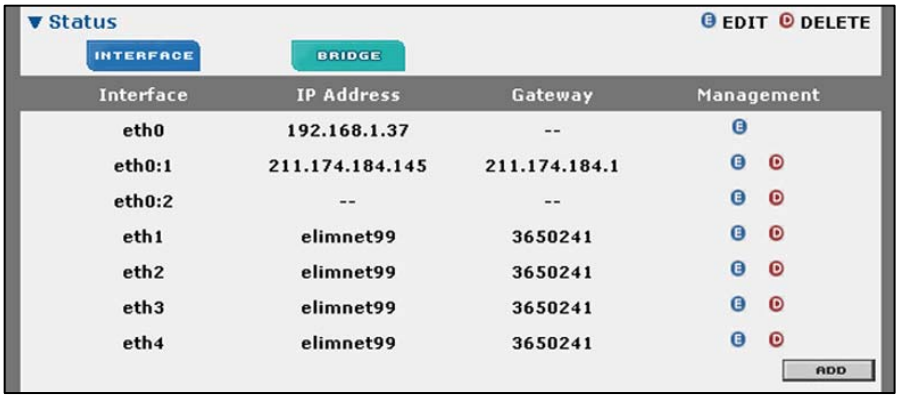
5. 정상적으로 PPPoE 인터페이스로 설정되면, 인터페이스 목록에 해당 인터페이스의 정보가 변경되어 출력됩니다.



4. 제품 설정하기

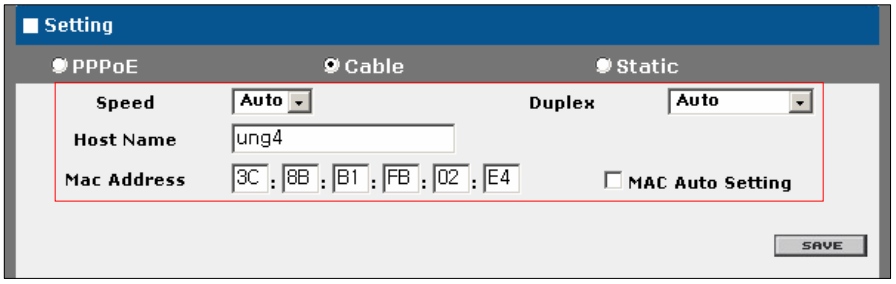
케이블 인터페이스 설정하기

1. <Interfaces> 화면의 인터페이스 목록에서 케이블망과 연결되는 케이블 인터페이스로 설정할 LAN 인터페이스(eth1 ~ eth4)를 선택한 후 (E)를 클릭합니다.



2. 그러면, 선택한 인터페이스를 케이블 인터페이스로 설정하기 위해 필요한 설정 값을 입력하는 항목들로 구성된 <Setting> 화면이 나타납니다. <Setting> 화면의 가장 위에 있는 3개의 라디오 버튼(PPPoE, Cable, Static) 중에서 'Cable'을 클릭합니다.

3. 그리고, 다음 설명을 참고하여 아래에 있는 항목들의 값을 지정합니다.



① Speed : 콤보 박스를 클릭한 후 인터페이스의 전송 속도를 지정합니다.

- Auto : 연결된 장비의 속도에 맞게 자동으로 설정.
- 10 : 10Mbps
- 100: 100Mbps

② Duplex : 콤보 박스를 클릭한 후 인터페이스의 전송 모드(duplex mode)를 지정합니다.
- Auto : 연결된 장비의 전송 모드에 맞게 자동으로 설정.
- Full duplex : 전이중 전송 모드(Full-duplex mode)
- Half duplex : 반이중 전송 모드(Half-duplex mode)

③ Host Name : 호스트 이름을 설정합니다.

④ MAC Address : 호스트의 MAC Address를 입력합니다.

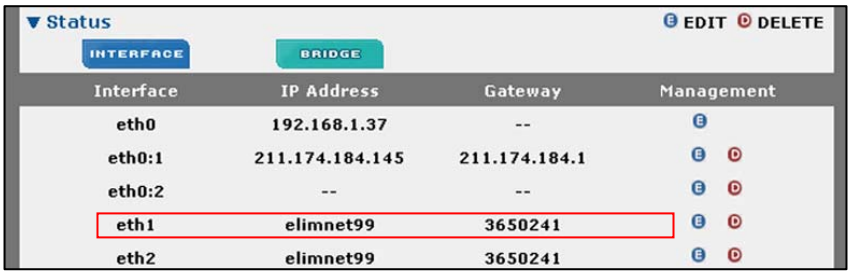
⑤ MAC Auto Setting : 자동으로 MAC Address를 생성하고자 할 경우 체크합니다.

주의

이 항목들은 특별한 경우를 제외하고는 AUTO MODE로 설정할 것을 권장합니다.

3. 항목의 값을 모두 입력한 후 [SAVE] 버튼을 누릅니다.

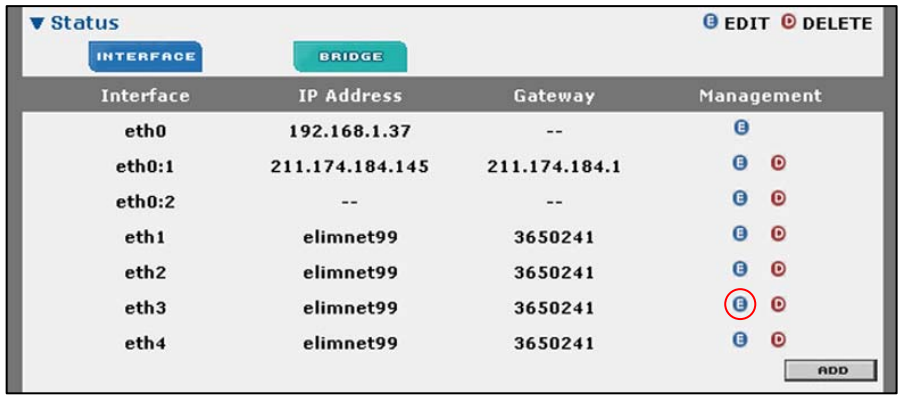
4. 정상적으로 케이블 인터페이스로 설정되면, 인터페이스 목록에 해당 인터페이스의 정보가 변경됩니다.



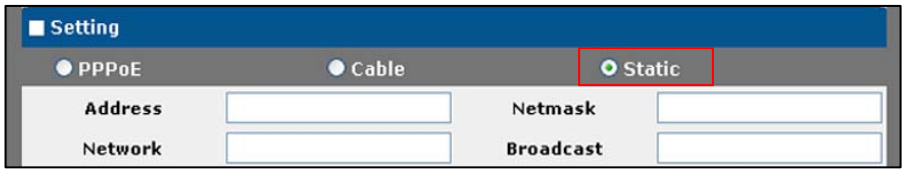
4. 제품 설정하기

전용회선 인터페이스 설정하기

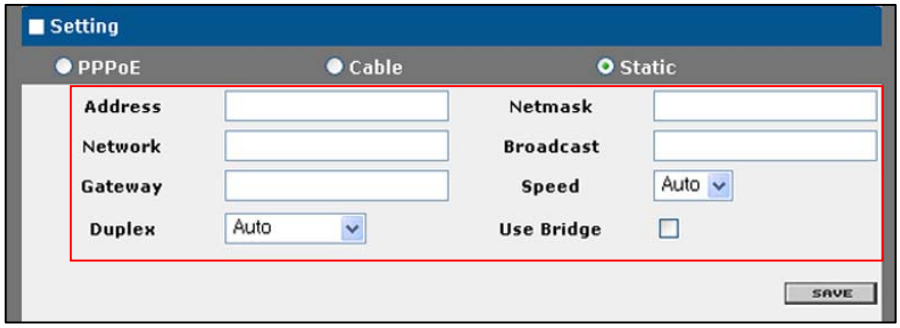
1. <Interfaces> 화면의 인터페이스 목록에서 전용회선과 연결되는 인터페이스로 설정할 인터페이스(eth0 ~ eth4)를 선택한 후 (E)를 클릭합니다.



2. 그러면, 선택한 인터페이스를 전용회선 인터페이스로 설정하기 위해 필요한 설정 값을 입력하는 항목들로 구성된 <Setting> 화면이 나타납니다. <Setting> 화면의 가장 위에 있는 3개의 라디오 버튼(pppoe, cable, static) 중에서 'static'을 클릭합니다.



3. 그리고, 다음 설명을 참고하여 아래에 있는 항목들의 값을 지정합니다.



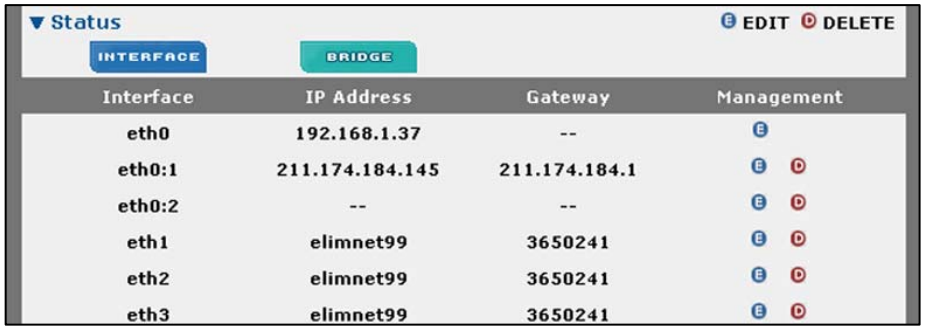
4. 제품 설정하기

① Address : 엘림넷으로부터 할당 받은 IP 주소를 입력합니다.
② Netmask : 엘림넷으로부터 할당 받은 서브넷 마스크 값을 입력합니다.
③ Network : 엘림넷으로부터 할당 받은 네트워크 주소를 입력합니다.
④ Broadcast : 엘림넷으로부터 할당 받은 브로드캐스트 주소를 입력합니다.
⑤ Gateway: 엘림넷으로부터 할당 받은 게이트웨이 주소를 입력합니다.
⑥ 인터페이스 : 콤보 박스를 클릭한 후 eth0 ~ eth4 중에서 전용회선과 연결되는 인터페이스를 선택합니다.
⑦ Speed : 인터페이스의 전송 속도를 지정합니다.
- Auto : 연결된 장비의 속도에 맞게 자동으로 설정.
- 10 : 10Mbps
- 100: 100Mbps
⑧ Duplex : 인터페이스의 전송 모드(duplex mode)를 지정합니다.
- Auto : 연결된 장비의 전송 모드에 맞게 자동으로 설정.
- Full : 전이중 전송 모드(Full-duplex mode)
- Half : 반이중 전송 모드(Half-duplex mode)
⑨ Use Bridge : Bridge를 구성하기 위해서는 구성하고자 하는 Interface에서 Use Bridge를 체크합니다.

주의

⑦, ⑧번 항목은 특별한 경우를 제외하고는 AUTO MODE로 설정할 것을 권장합니다.

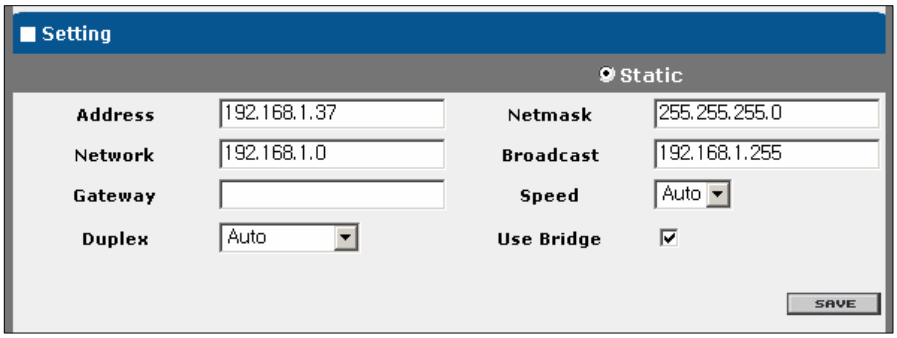
4. 정상적으로 전용회선 인터페이스로 설정되면, 인터페이스 목록에 해당 인터페이스의 정보가 변경되어 출력됩니다.



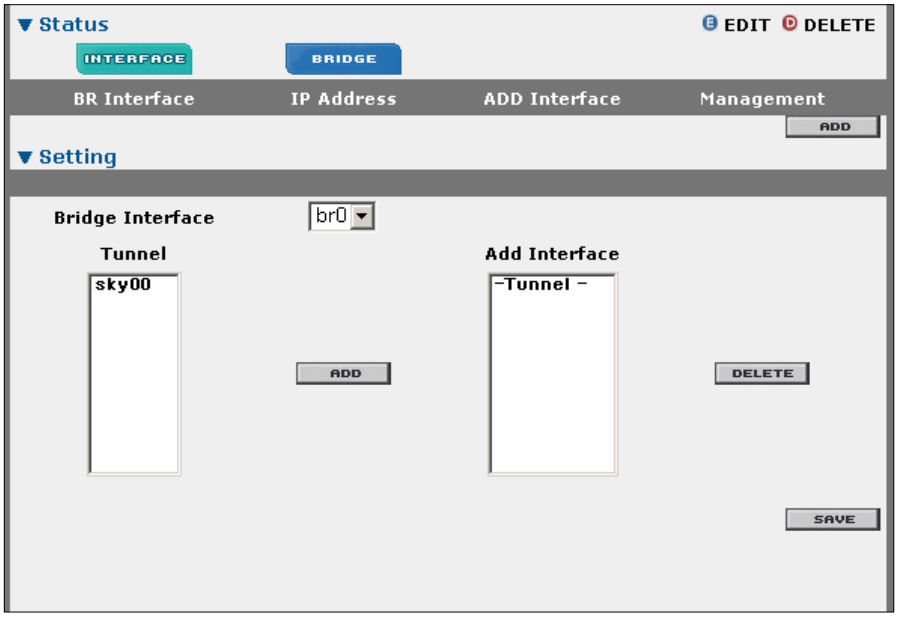
4. 제품 설정하기

Bridge 설정하기

Bridge를 구성하기 위해서는 구성하고자 하는 Interface에서 Use Bridge를 체크합니다.



ADD 버튼 : Bridge를 새로 생성합니다.



Bridge를 설정하기 위해 Bridge Interface와 Tunnel를 선택한 후 ADD버튼을 클릭하여 Add Interface부분에 설정하고자 하는 터널 인터페이스가 추가 되었다면 save를 눌러 저장합니다.

① Bridge Interface : Interface에서 Use Bridge를 체크 한 경우 리스트화 됩니다.

② Tunnel : Configuration >> Network >> VPN TUNNEL 에서 Setting한 TUNNEL이 리스트화 되어 나타납니다.

③ ADD : Tunnel를 선택한 후 ADD버튼을 클릭하면 Add Interface리스트에 등록이 됩니다.

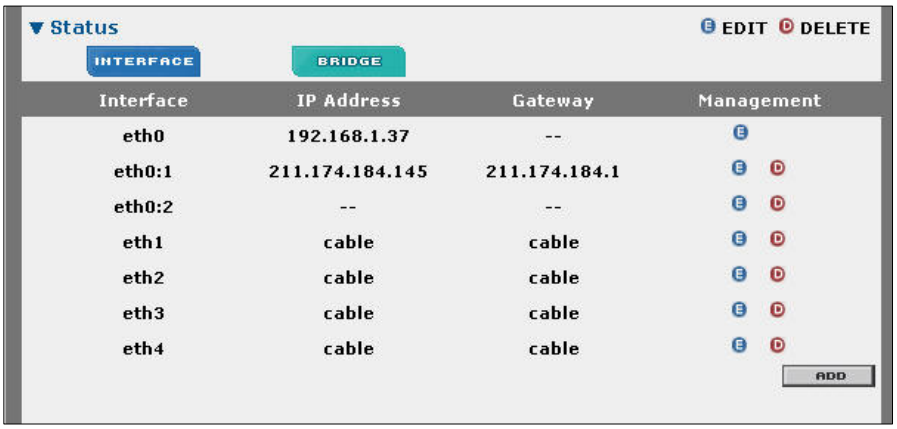
④ DELETE : Add Interface의 TUNNEL 리스트 중에서 제외하고자 할 때, 해당 TUNNEL을 선택한 후 DELETE버튼을 클릭하여 제외시킵니다.

⑤ SAVE : 모든 구성이 완료되었을 경우 SAVE를 클릭하여 해당 내용을 저장하고 시스템에 적용시킵니다.

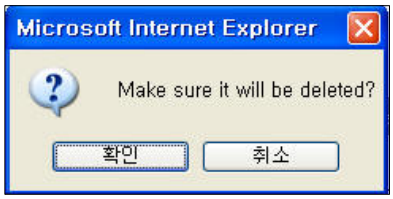
인터페이스 설정 삭제하기

다음과 같은 방법으로 설정된 인터페이스를 삭제할 수 있습니다.

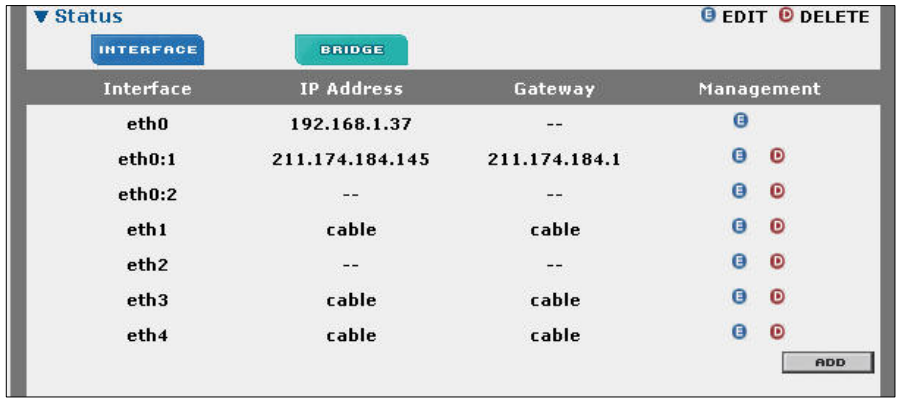
1. 인터페이스의 설정을 삭제하려면 <Interfaces> 화면의 인터페이스 목록에서 삭제할 인터페이스의(D)를 클릭합니다.



2. 다음과 같이 삭제 여부를 확인하는 화면이 나타나면 [확인]을 클릭합니다.



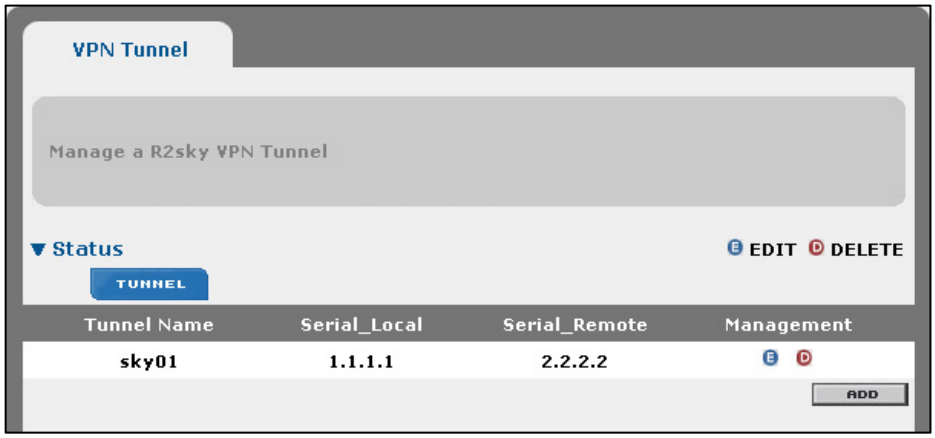
3. 선택한 인터페이스가 <Interfaces> 화면에서 지워진 것을 확인할 수 있습니다.



4. 제품 설정하기

VPN 설정하기

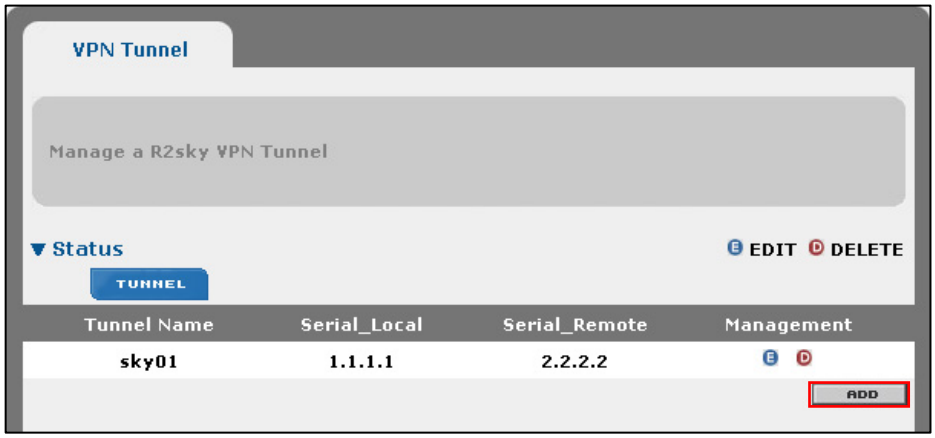
웹 콘솔에서 CONFIGURATION - NETWORK - VPN TUNNEL 메뉴를 클릭하면 VPN 터널을 설정할 수 있는 다음과 같은 <VPN Tunnel> 화면이 나타납니다.



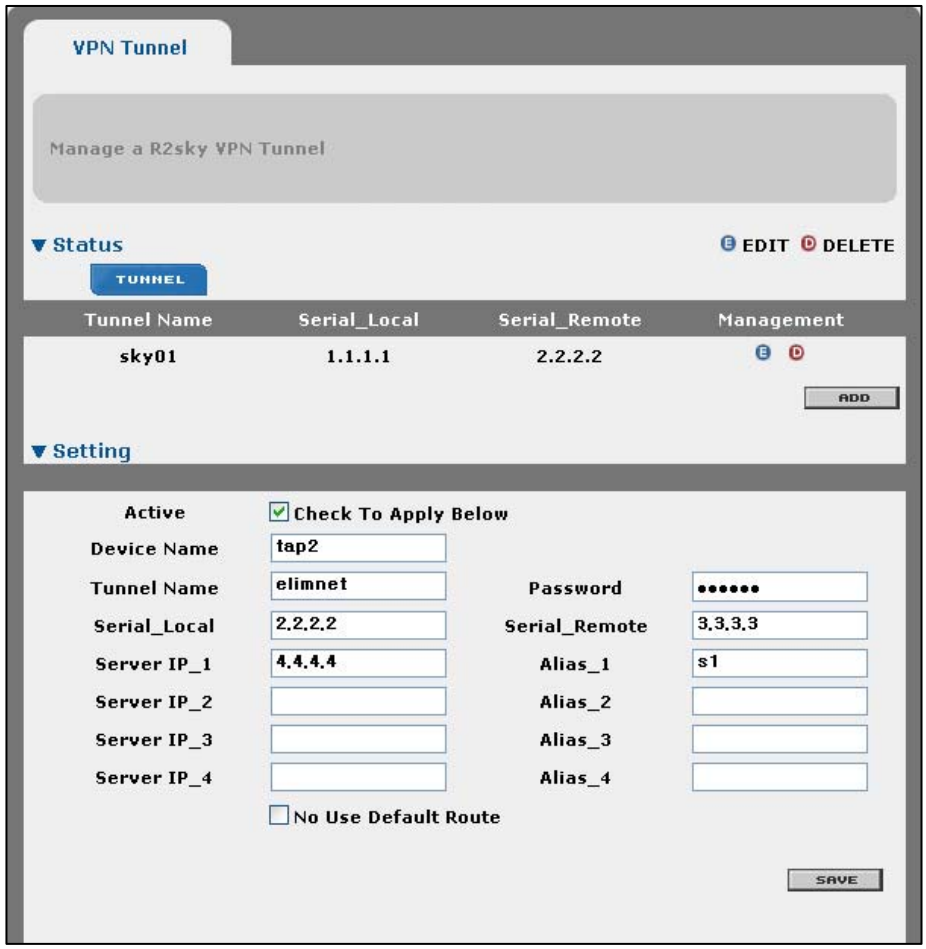
<VPN Tunnel> 화면에는 현재 정의되어 있는 VPN 터널의 목록이 출력됩니다. 기본적으로 R2SKY 시리즈에 정의되어 있는 VPN 터널은 없습니다. 새로운 VPN 터널을 추가하는 방법과 기존에 정의된 VPN 터널을 변경하거나 삭제하는 방법에 대해 알아봅니다.

VPN 터널 추가하기

1. <VPN Tunnel> 화면에서 VPN 터널 목록의 아래쪽에 있는 [ADD] 버튼을 클릭합니다.



2. 그러면, VPN 터널을 정의하는 데 필요한 값을 입력할 수 있는 <Setting> 화면이 나타납니다.



<Setting> 화면에 있는 각 항목들을 다음 설명을 참고하여 설정합니다.

① Device Name : Device Name은 물리적 인터페이스명(tap0,tap1,....tapX)을 입력 해 줍니다.

② Active : VPN 터널의 사용 여부를 지정합니다. 이 항목을 체크하면, 해당 VPN 터널이 실제로 사용됩니다.

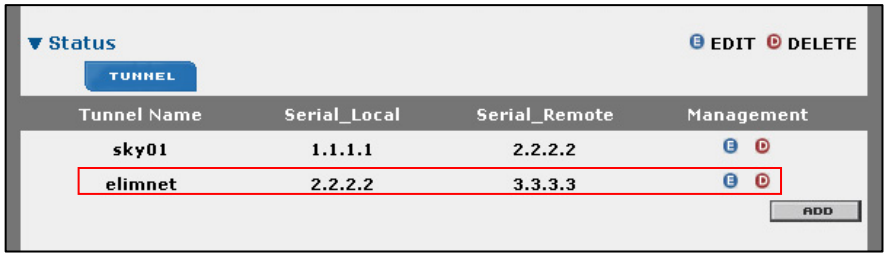
③ Tunnel Name : VPN 터널의 이름을 입력합니다. 반드시 sky로 시작하는 이름을 사용해야 합니다.

④ Password : VPN 터널의 암호를 입력합니다.
⑤ Serial Local : VPN 터널이 연결됐을 때 사용하는 이 장비의 시리얼 IP 주소를 입력합니다
⑥ Serial Remote : VPN 터널이 연결됐을 때 사용하는 VPN 서버의 시리얼 IP 주소를 입력합니다
⑦ Server IP_1 ~ 4 : 서버의 IP 주소를 입력합니다.
⑧ Alias_1 ~4 : 서버를 지칭할 수 있는 이름을 입력합니다.
⑨ No Use Default Route : No Use Default Route를 체크하게 되면 Route를 사용자가 직접추가 할 수 있습니다.

Routing은 IP Address와 Subnetmask를 입력하여 구성하게 됩니다.
Disable를 체크하고 save할 경우 해당 정보는 저장이 되나 시스템에 적용은 되지 않습니다.
Delete를 체크하고 save할 경우 해당 정보는 삭제됩니다.

3. 값을 모두 입력한 후 [SAVE] 버튼을 누릅니다.

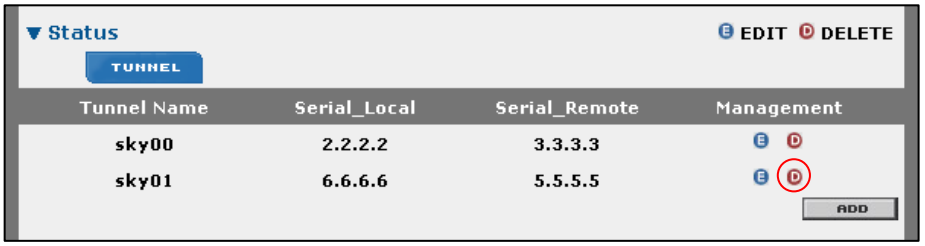
4. 정상적으로 VPN 터널이 추가되면 화면의 목록에 정의한 VPN 터널이 표시됩니다.



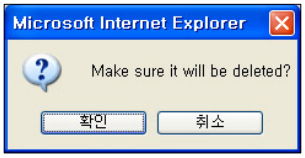
4. 제품 설정하기

VPN 터널 삭제하기

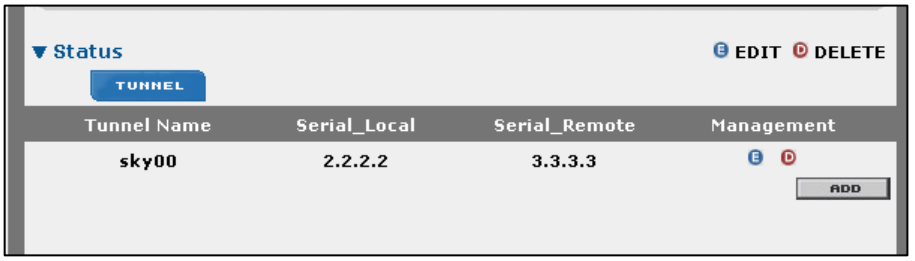
1. 장비에 정의된 VPN 터널을 삭제하려면 <VPN Tunnel> 화면의 목록에서 삭제할 VPN 터널의 Management 항목에 있는 (D)를 클릭합니다.



2. 다음과 같은 화면이 나타나면 [확인]을 클릭합니다.



3. 선택한 VPN 터널이 다음과 같이 <VPN Tunnel> 화면의 목록에서 지워집니다.



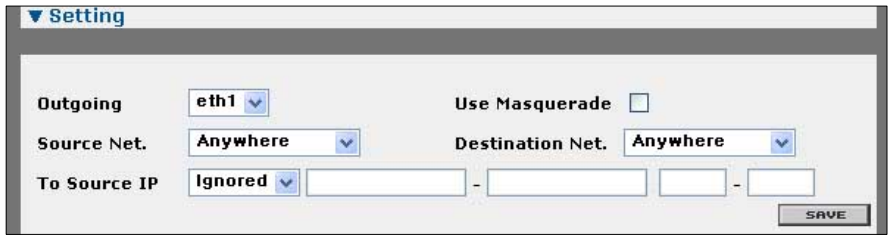
4. 제품 설정하기

SNAT 설정하기

전송되는 트래픽에 적용될 SNAT을 설정하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 NETWORK-NAT-SNAT 메뉴를 클릭합니다.
2. 다음과 같은 <SNAT> 화면이 나타납니다. <SNAT> 화면에는 현재 SNAT설정들이 출력됩니다.

3. [ADD] 버튼을 클릭합니다.
4. 그러면, 다음과 같이 SNAT을 설정할 수 있는 <Setting> 화면이 나타납니다.



다음 설명을 참고하여 각 항목의 값을 설정합니다.

① Outgoing : 콤보 박스를 클릭한 후 SNAT 기능을 동작 시킬 인터페이스를 지정합니다. 선택된 인터페이스를 통해 전송되는 트래픽에 SNAT 기능이 적용됩니다.

② Use _ Masquerade : Masquerade 기능의 사용 여부를 지정합니다. MASQUERADE기능은 ADSL과 케이블 TV 망처럼 동적 IP주소를 할당 받는 다이어업(Dial-up)계정에서 사용됩니다.

③ Source Net. : 콤보 박스를 클릭한 후 SNAT를 적용할 트래픽의 전송지 네트워크를 선택합니다.

Destination Net : 콤보 박스를 클릭한 후 SNAT를 적용할 트래픽의 전송지 네트워크를 선택합니다.

To Source IP : Outgoing ~ Destination Net. 항목에서 지정한 조건과 일치하는 전송 트래픽에 특정한 범위의 공인 IP 주소와 포트를 할당하고자 할 때 사용하는 항목입니다. 콤보 박스를 클릭하여 'Equals'를 선택한 후, 다음에 있는 2개의 입력란에 공인 IP주소의 범위를 입력하고, 그 뒤에 있는 2개의 입력란에 포트 범위를 입력합니다.

항목의 값을 설정한 후 [SAVE] 버튼을 클릭합니다.

<SNAT> 화면에서 추가된 SNAT 설정을 확인할 수 있습니다.

4. 제품 설정하기

DNAT 설정하기

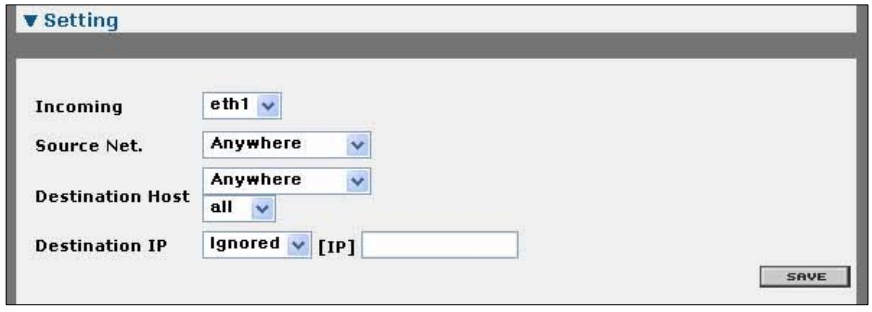
WAN에서 수신되는 트래픽에 적용될 DNAT을 설정하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 NETWORK-NAT-DNAT 메뉴를 클릭합니다.

2. 다음과 같은 <DNAT> 화면이 나타납니다. <DNAT> 화면에는 현재 SNAT설정들이 출력됩니다.

3. [ADD] 버튼을 클릭합니다.

4. 그러면, 다음과 같이 DNAT을 설정할 수 있는 <Setting> 화면이 나타납니다.



4. 제품 설정하기

다음 설명을 참고하여 각 항목의 값을 설정합니다.

① Incoming :콤보 박스를 클릭한 후 DNAT을 적용할 인터페이스를 지정합니다. 선택된 인터페이스를 통해 수신되는 트래픽에 DNAT 기능이 동작 됩니다.

② Source Net : 콤보 박스를 클릭한 후 DNAT을 적용할 트래픽의 전송지 네트워크를 선택합니다.

③ Destination : 콤보 박스를 클릭한 후 DNAT을 적용할 트래픽의 목적지 네트워크와 프로토콜의 종류를 선택합니다.

④ To Destination IP : Incoming~Destination Net. 항목에서 지정한 조건과 일치하는 전송 트래픽에 특정한 사설 IP주소와 포트를 할당하고자 할 때 사용하는 항목입니다. 콤보 박스를 클릭하여 'Equals'를 선택한 후, 다음에 있는 [IP] 입력란에 사설 IP조소를 입력하고, 그 뒤에 있는 [PORT]입력란에 포트 번호를 입력합니다.

5. 항목의 값을 설정한 후 [SAVE] 버튼을 클릭합니다.

6. <DNAT> 화면에서 추가된 DNAT 설정을 확인할 수 있습니다.

4. 제품 설정하기

DMZ Adding In Tunnel

DMZ : 로컬네트웍의 보안을 유지하고 외부에서 액세스 가능한 특정 호스트를 지정하고자 할 때 사용합니다.

① DMZ PC IP : 내부 특정 IP를 입력합니다.

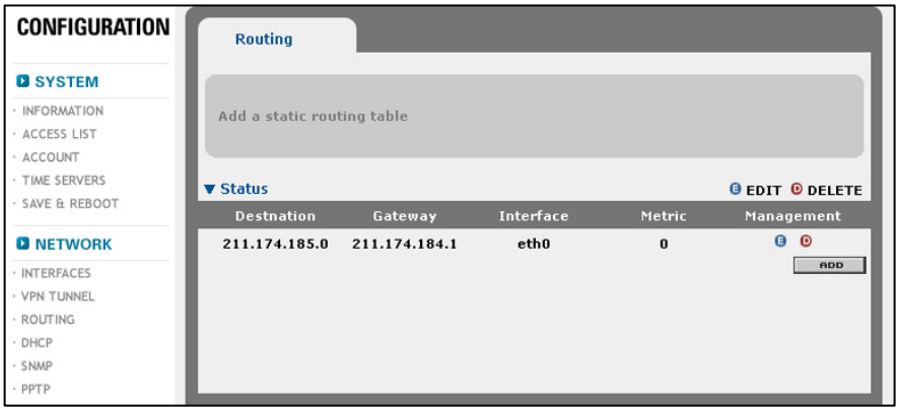
② DMZ PC Port : 내부에 적용하고자 하는 포트 번호를 입력합니다.

③ Public IP : 공인 IP를 입력합니다.

④ Public Port : 적용하고자 하는 포트 번호를 입력합니다.

라우팅 설정하기

웹 콘솔에서 CONFIGURATION - NETWORK - ROUTING 메뉴를 클릭하면 R2SKY 시리즈의 라우팅 테이블에 정적 라우트 엔트리(static route entry)를 추가할 수 있는 다음과 같은 <Routing> 화면이 나타납니다.

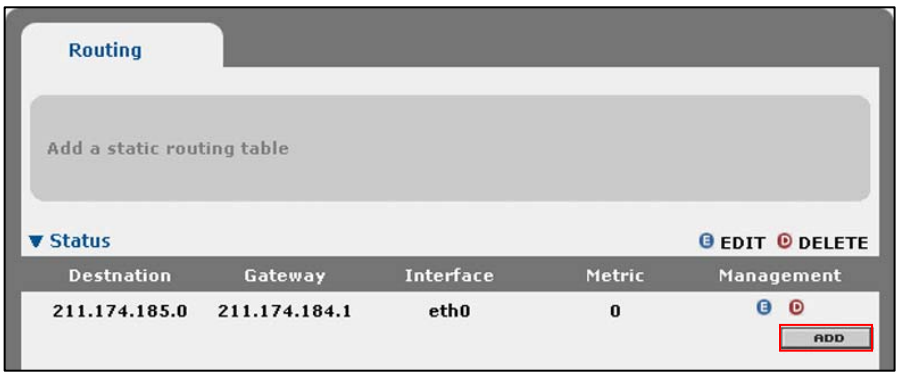


<Routing> 화면에는 현재 장비에 추가되어 있는 정적 라우트의 목록이 표시됩니다. 정적 라우트는 본사와 지사간의 특정 IP 블럭에 대한 라우팅을 직접 지정할 때 유용하게 사용 할 수 있습니다.

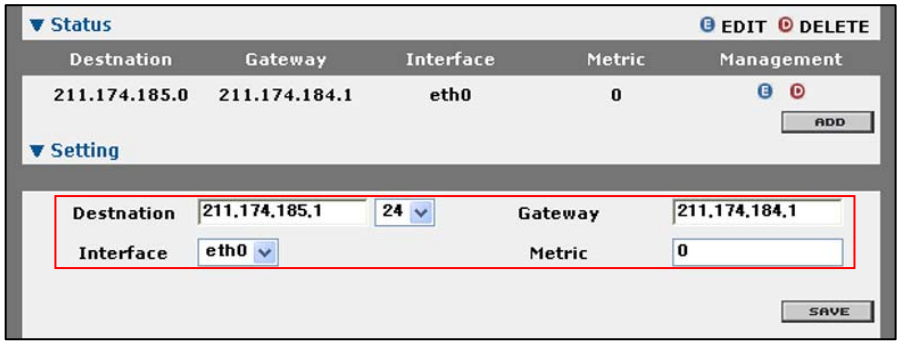
정적 라우트 추가하기

정적 라우트를 추가하는 방법은 다음과 같습니다.

1. [ADD] 버튼을 클릭합니다.

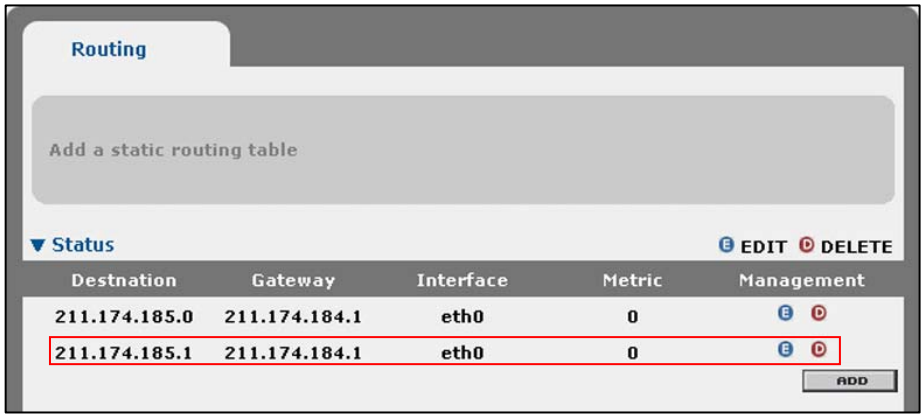


2. 화면 아래쪽에 다음과 같이 정적 라우트에 대한 설정 값을 입력할 수 있는 <Setting> 화면이 나타나면 아래 설정을 참고하여 각 항목의 값을 입력합니다.



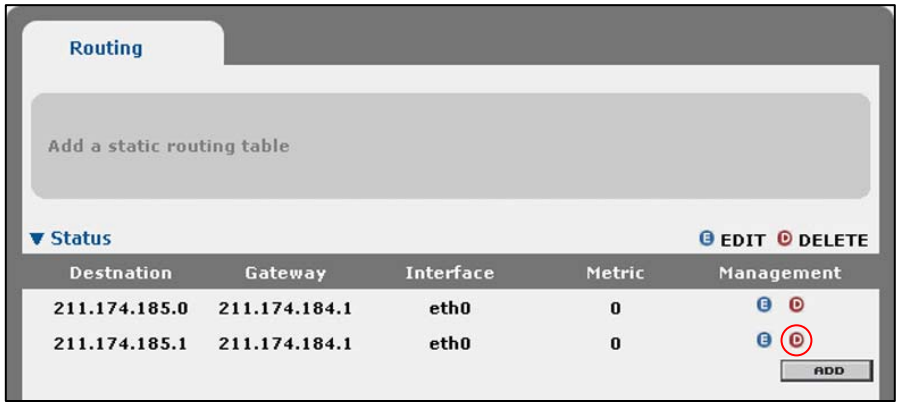
① Destination : 라우트의 목적지 주소를 입력합니다
② Gateway : 다음 경로의 주소를 입력합니다.
③ Interface : 인터페이스를 입력합니다.
④ Metric : 라우트의 메트릭 값을 입력합니다. 기본 값으로는 '0'을 입력하면 됩니다.

3. [SAVE] 버튼을 누르면 입력한 Static 라우트가 라우팅 테이블에 추가됩니다.

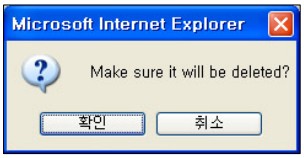


Static 라우트 삭제하기

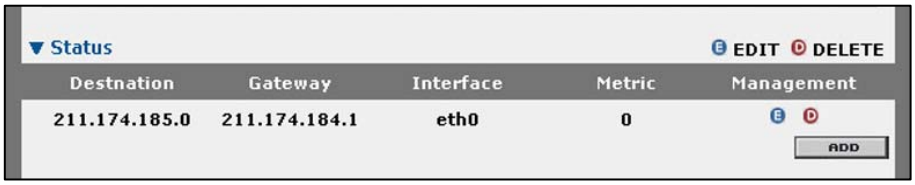
1. 라우팅 테이블에 추가된 Static 라우트를 삭제하려면 <Routing> 화면의 목록에서 삭제할 Static 라우트의 Management 항목에 있는 (D)를 클릭합니다.



2. 다음과 같은 화면이 나타나면 [확인]을 클릭합니다.

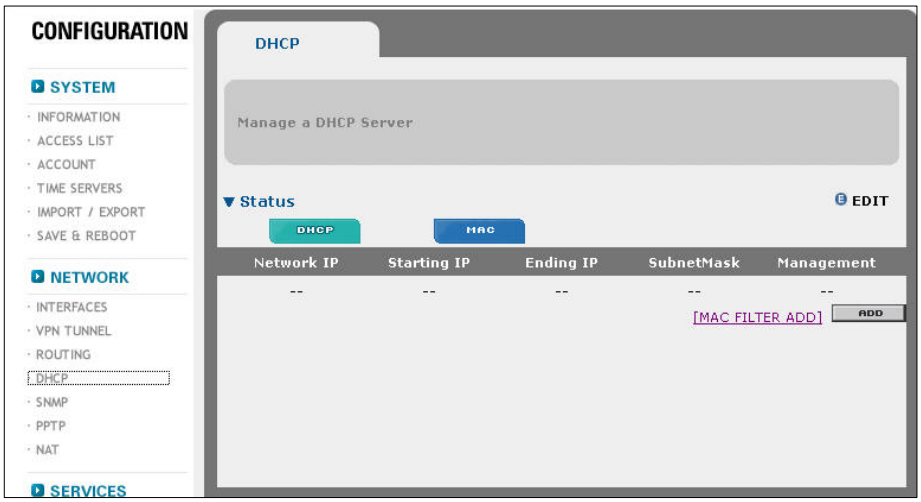


3. 선택한 정적 라우트가 다음과 같이 <Routing> 화면의 목록에서 지워집니다.



DHCP 설정하기

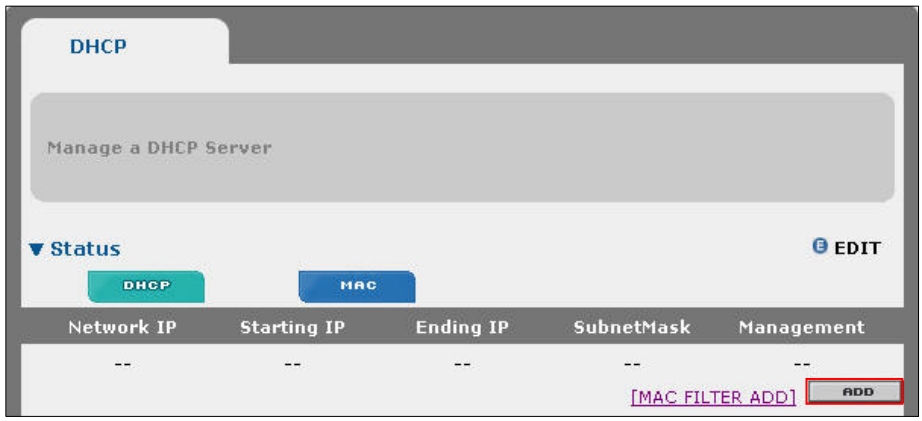
웹 콘솔에서 CONFIGURATION - NETWORK - DHCP 메뉴를 클릭하면 DHCP(Dynamic Host Control Protocol)를 설정할 수 있는 다음과 같은 <DHCP> 화면이 나타납니다.



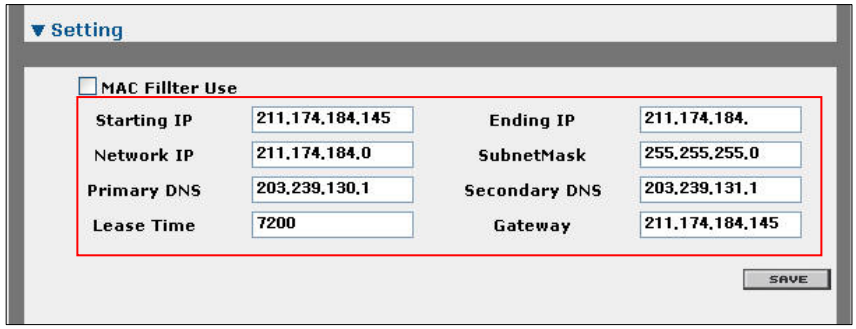
DHCP 설정하기

<DHCP> 화면에서 DHCP를 설정하는 방법은 다음과 같습니다.

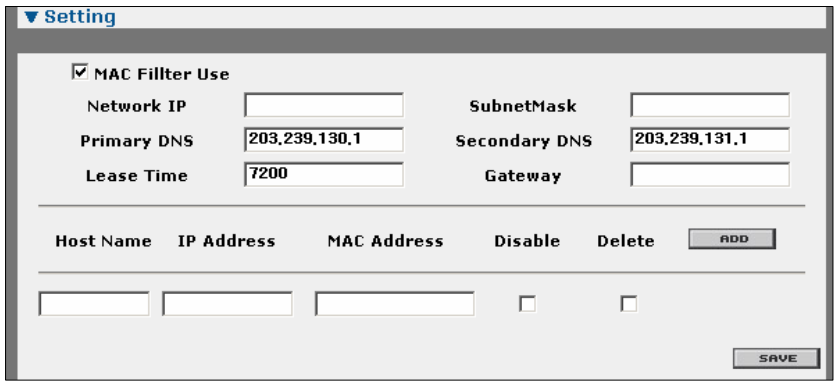
1. [ADD] 버튼을 클릭합니다.



2. 화면 아래쪽에 다음과 같이 DHCP에 대한 설정 값을 입력할 수 있는 <Setting> 화면이 나타나면 아래 설명을 참고하여 각 항목의 값을 입력합니다.



① Starting IP : DHCP 클라이언트에게 할당해줄 시작 주소를 입력합니다.
② Ending IP : DHCP 클라이언트에게 할당해줄 마지막 주소를 입력합니다.
③ Network IP : DHCP 클라이언트가 속한 서브넷의 네트워크 주소를 입력합니다.
④ Subnet Mask : DHCP 클라이언트에게 할당해줄 서브넷 마스크 값을 입력합니다.
⑤ Primary DNS : DHCP 클라이언트에게 할당해줄 Primary DNS를 입력합니다.
⑥ Secondary DNS : DHCP 클라이언트에게 할당해줄 Secondary DNS를 입력합니다.
⑦ Lease Time : 할당해준 IP 주소의 유효 시간을 입력합니다. 기본 값은 7200입니다.
⑧ Gateway : 해당 네트워크의 기본 게이트웨이를 입력합니다.



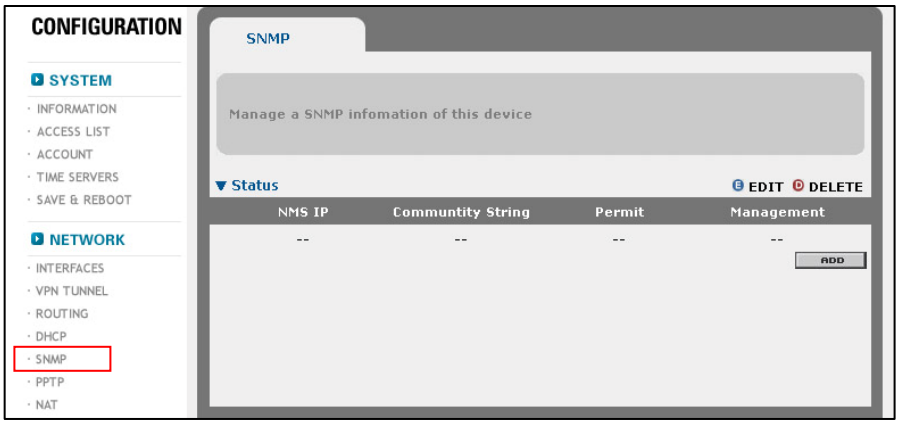
MAC Filter Use를 체크할 경우 MAC Address를 이용하여 해당 호스트에 IP를 지정 해 놓을 수 있습니다.

3. [SAVE] 버튼을 누르면 DHCP 설정이 장비에 바로 적용됩니다. DHCP 설정 정보는 <DHCP> 화면에서 확인할 수 있습니다.

SNMP 설정 사용하기

R2SKY 시리즈는 SNMP 기능을 제공합니다. 사용자들은 MRTG, RRD툴 등을 이용하여 복잡한 로그분석을 하지 않아도 손쉽게 네트워크 통계분석을 이용할 수 있습니다.

아래와 같이 콘솔에서 CONFIGURATION - NETWORK - SNMP 메뉴를 클릭합니다. 그러면, 다음과 같이 현재 설정된 SNMP 설정 목록을 보여주는 <SNMP> 화면이 나타납니다. 기본적으로 설정되어 있는 SNMP 설정은 없습니다.



다음 절에서 SNMP 설정을 추가하고, 수정 혹은 삭제하는 방법을 살펴봅니다.

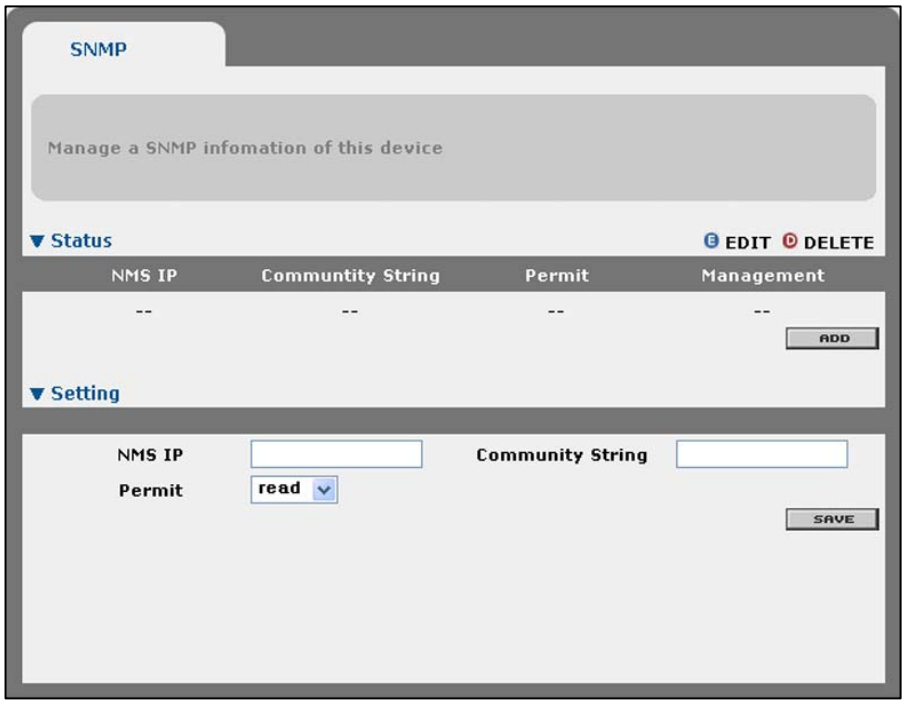
4. 제품 설정하기

SNMP 설정 추가하기

장비에 접속할 수 있는 SNMP 설정을 추가하는 방법은 다음과 같습니다.

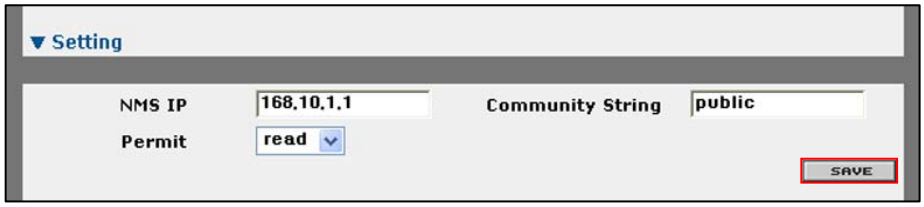
1. <SNMP> 화면의 아래쪽에 있는 [ADD] 버튼을 클릭합니다.

2. 화면 아래쪽에 추가할 SNMP 설정을 정의할 수 있는 <Setting> 화면이 나타납니다. 그림 아래에 있는 설명을 참고하여 <Setting> 화면에 있는 각 항목들의 값을 설정합니다.

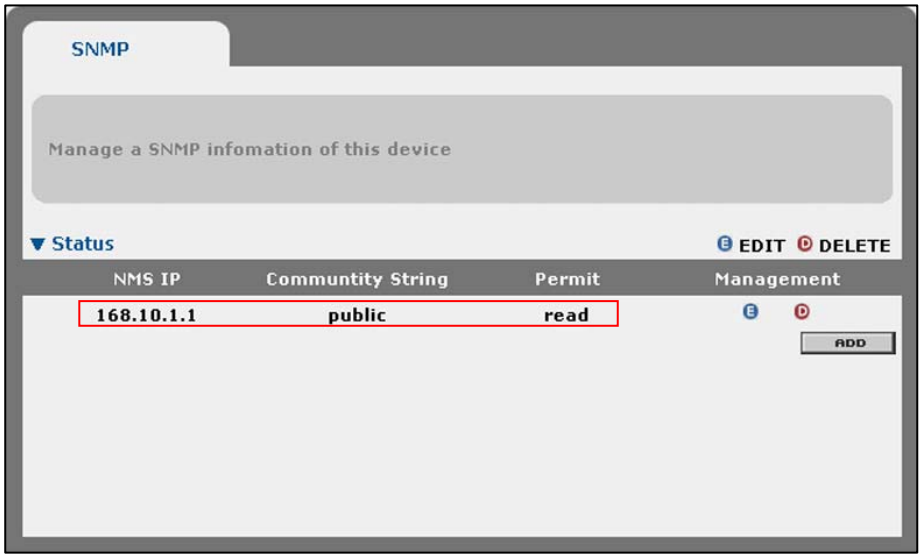


① Server IP : SNMP 정보를 이용할 호스트의 IP 주소를 입력합니다.
② Community String : 장비로 접속할 때 사용할 SNMP 커뮤니티 스트링을 입력합니다.
③ Permit : 콤보 박스를 클릭한 후 호스트에게 지정할 액세스 권한을 선택합니다.
- read : 장비의 현황을 조회할 수 있는 권한.
- write : 장비의 현황 및 설정을 조회하고 변경할 수 있는 권한.

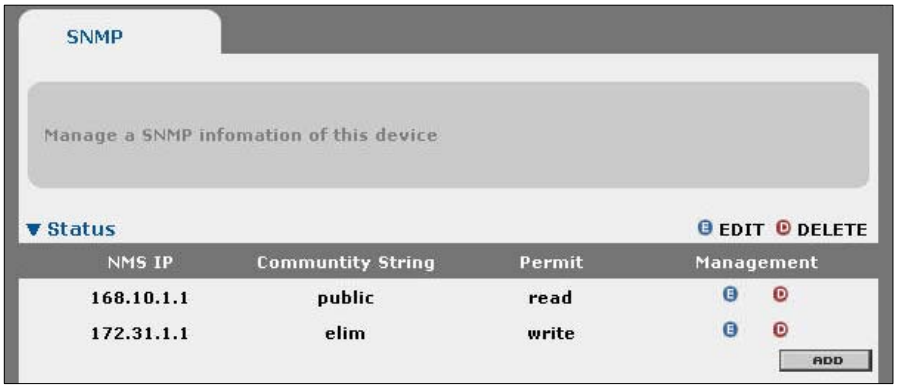
3. 항목의 값을 모두 입력한 후 [Save] 버튼을 클릭합니다.



4. 그러면, 다음과 같이 입력한 SNMP 설정이 <SNMP> 화면에 추가된 것을 확인할 수 있습니다.



5. 계속해서 다른 SNMP 설정을 추가로 지정하려면, 1 ~ 4번 과정을 동일하게 수행하면 됩니다. 다음 화면은 여러 개의 SNMP 설정이 추가된 <SNMP> 화면입니다.

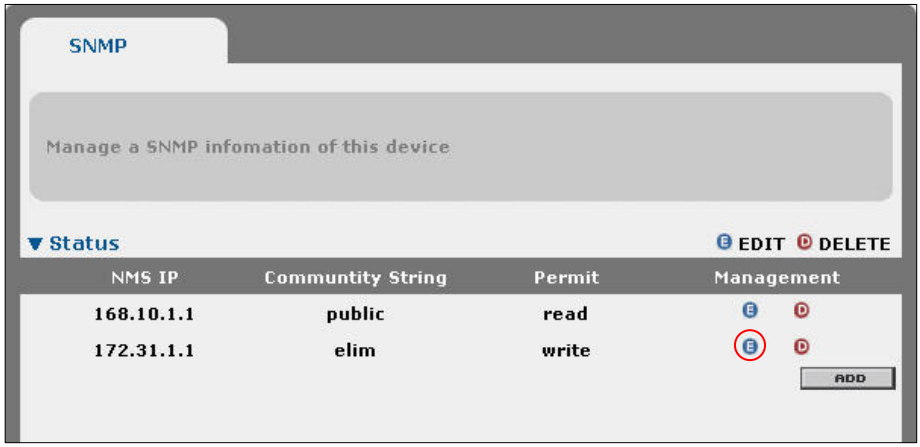


4. 제품 설정하기

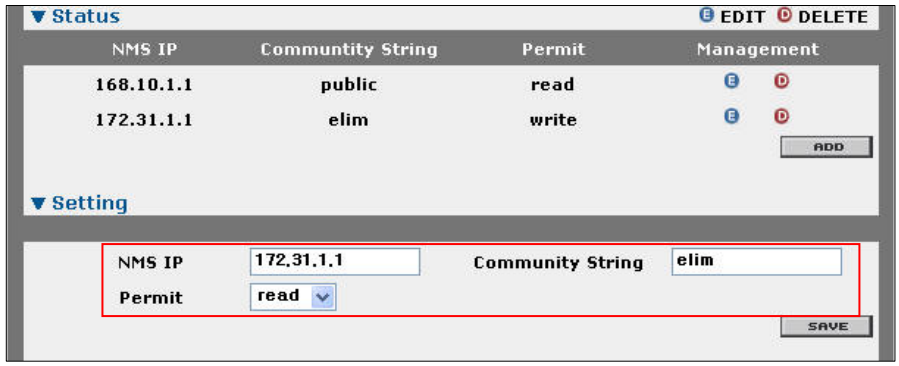
SNMP 설정 수정하기

기존에 정의된 SNMP 설정을 수정하는 방법은 다음과 같습니다.

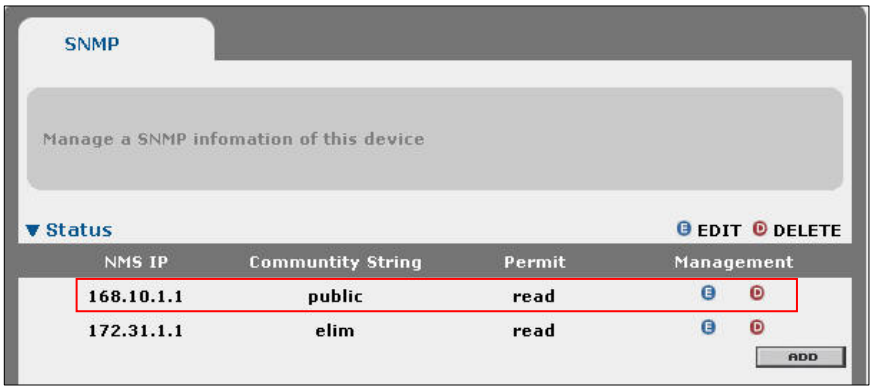
1. <SNMP> 화면의 SNMP 설정 목록에서 수정할 SNMP 설정의 Management 항목에 있는 (E) 버튼을 클릭합니다.



2. 선택한 SNMP 설정의 내용을 수정할 수 있는 <Setting> 화면이 나타납니다. 'SNMP 설정추가하기' 절에 설명되어 있는 내용을 참고하여 원하는 항목의 값을 수정한 후 [Save] 버튼을 클릭합니다.



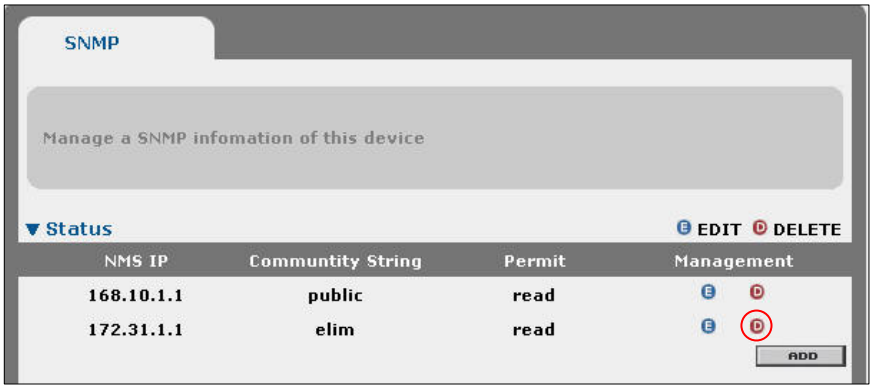
3. 그러면, 다음과 같이 변경된 SNMP 설정 값이 화면에 표시됩니다.



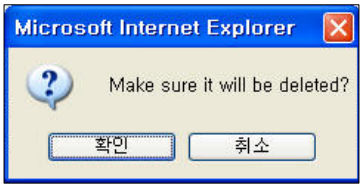
SNMP 설정 삭제하기

정의되어 있는 SNMP 설정을 삭제하는 방법은 다음과 같습니다.

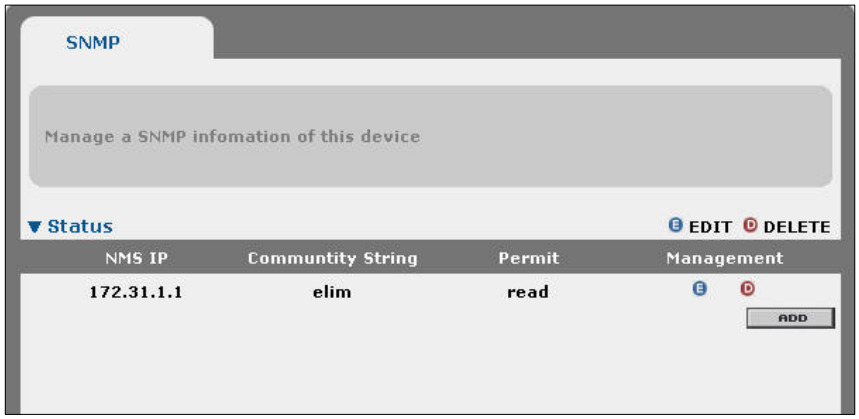
1. <SNMP> 화면의 SNMP 설정 목록에서 삭제할 SNMP 설정의 Management 항목에 있는 (D) 버튼을 클릭합니다.



2. 다음과 같이 SNMP 설정의 삭제를 확인하는 화면이 나타납니다. [확인]을 클릭합니다.



3. 그러면, 선택한 SNMP 설정이 <SNMP> 화면의 목록에서 삭제됩니다.



4. 제품 설정하기

데몬 상태 설정하기

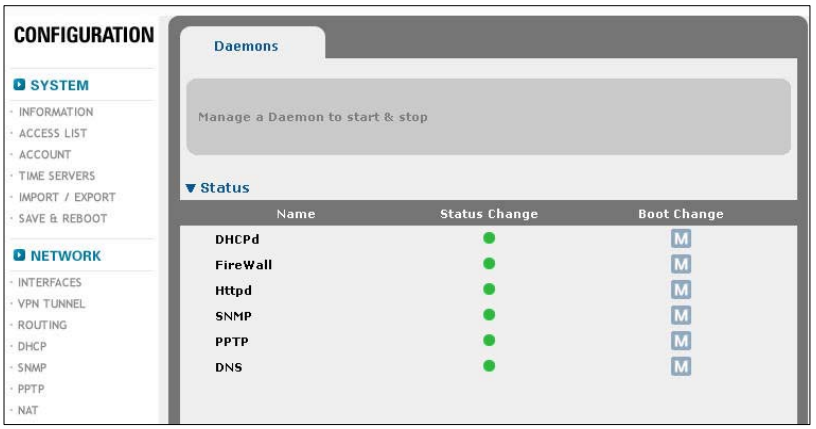
R2SKY 시리즈에는 다음과 같은 종류의 데몬(daemon)이 실행될 수 있습니다. 각 데몬이 장비에서 수행하는 기능과 기본적으로 설정되어 있는 동작 상태는 다음과 같습니다.

데몬의 종류	기 능	기본 동작 여부
SSHd	SSHd 접속 데몬	동작함
PnN	장비의 통계 정보 관련 데몬	동작하지 않음
DHCPd	DHCP 동작 관련 데몬	동작하지 않음
Firewall	방화벽 동작 관련 데몬	* 참고
Httpd	HTTP 관련 데몬	동작함
IDS	침입 방지를 위한 데몬	동작하지 않음
SNMP	SNMP 관련 데몬	동작하지 않음
Telnetd	텔넷 관련 데몬	동작하지 않음
Bandwidthd	Arrange IP 대역의 대역폭 사용량 수집과 관련된 데몬	동작함

Tip 참고

Firewall의 기본동작 여부는 현재 방화벽 설정의 적용 유무를 확인하여 Status에 표현합니다. 따라서 데몬을 스톱시키는 것은 모든 룰을 제거하게 되오니 주의하시기 바랍니다. XP의 경우 팝업창 허락가능으로 해 놓으시기 바랍니다.

웹 콘솔에서 CONFIGURATION - SERVICES - DAEMONS 메뉴를 클릭하면 현재 데몬의 동작 상태와 부트 상태를 보여주고 이를 변경할 수 있는 다음과 같은 <Daemons> 화면이 나타납니다.



4. 제품 설정하기

데몬 상태

<Service> 화면은 R2SKY 시리즈가 지원하는 각 데몬들의 동작 상태와 부트 모드를 다음과 같은 아이콘을 통해 표시해줍니다.

항 목	아이콘	의 미
Status		현재 동작 중인 데몬임을 표시해주는 아이콘
		현재 동작하고 있지 않은 데몬임을 표시해주는 아이콘
Status Change		현재 동작하고 있지 않은 데몬을 동작하도록 설정하는 아이콘
		현재 동작 중인 데몬을 동작하지 않도록 설정하는 아이콘
Boot Status		부트 상태가 Auto 모드인 데몬임을 표시해주는 아이콘
		부트 상태가 Manual 모드인 데몬임을 표시해주는 아이콘
Boot Change		부트 상태를 Manual 모드로 변경하는 아이콘
		부트 상태를 Auto 모드로 변경하는 아이콘

Tip 참고

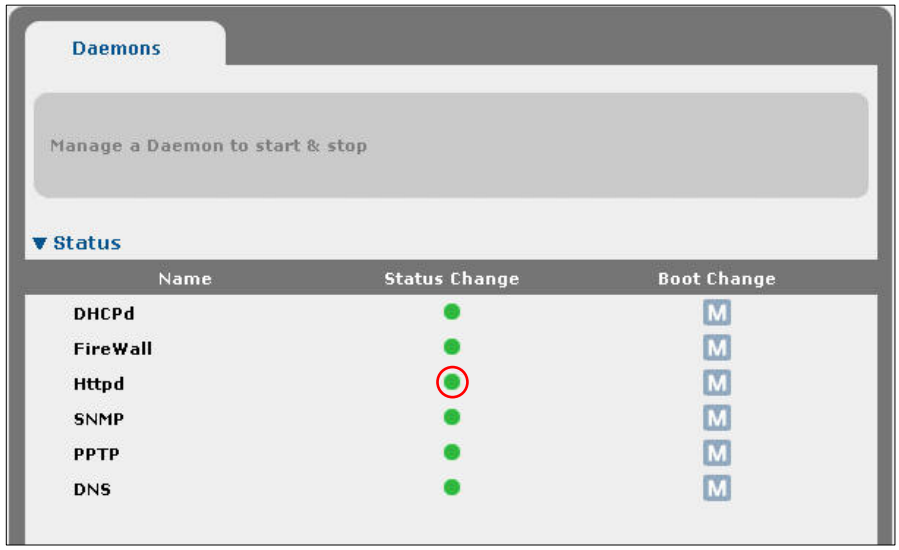
부트 모드는 장비가 부팅할 때 해당 데몬이 동작할지 여부를 나타냅니다. 부트 모드가 Auto인 데몬은 장비가 부팅될 때 자동으로 동작하게 되고, 부트 모드가 Manual인 데몬은 CONFIGURATION - SERVICES - DAEMONS 메뉴를 통해서 동작하도록 설정할 수 있습니다.

4. 제품 설정하기

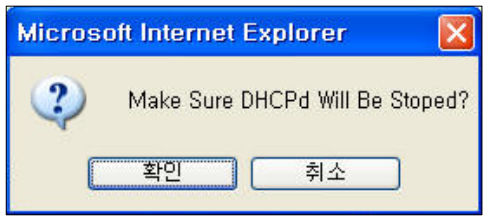
데몬의 동작 상태 변경하기

데몬의 동작 상태를 변경하는 방법은 다음과 같습니다.

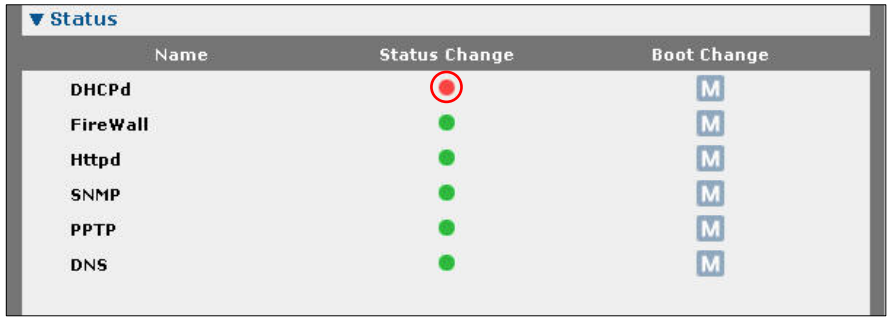
1. 동작 상태를 변경하려는 데몬의 Status Change 항목에 있는 아이콘을 클릭합니다.



2. 다음과 같은 확인 메시지가 나타납니다. [확인]을 클릭하면 지정한 데몬의 상태가 변경됩니다.



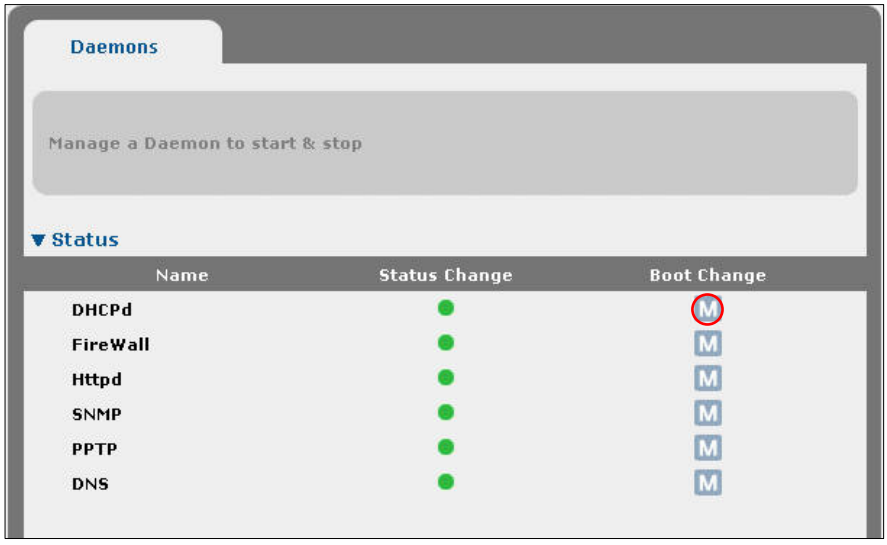
3. <Service> 화면의 Status 항목을 살펴보면, 데몬의 상태가 변경된 것을 확인할 수 있습니다.



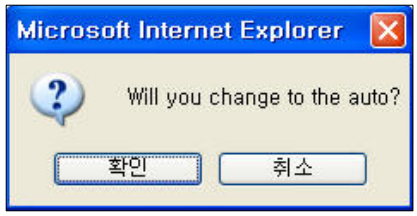
데몬의 부트 상태 변경하기

데몬의 부트 상태를 변경하는 방법은 다음과 같습니다.

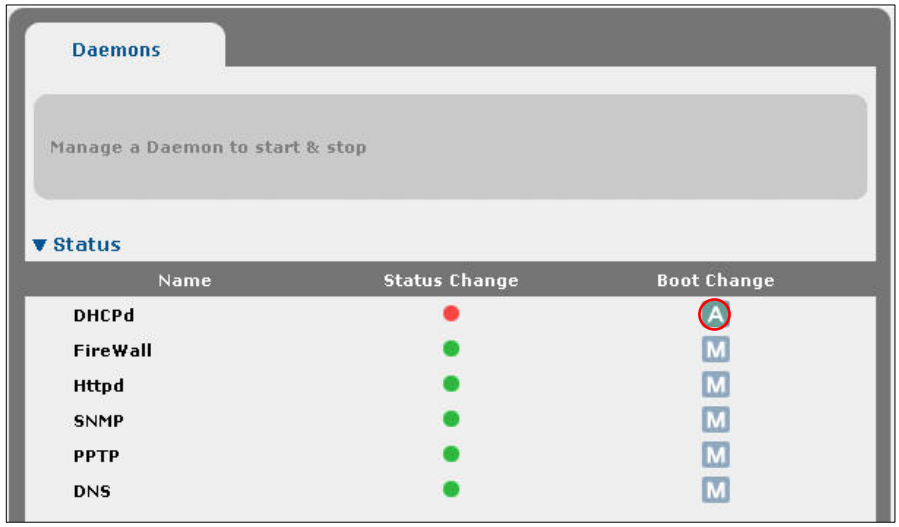
1. 부트 상태를 변경하려는 데몬의 Boot Change 항목에 있는 아이콘을 클릭합니다.



2. 다음과 같은 확인 메시지가 나타납니다. [확인]을 클릭하면 지정한 데몬의 부트 상태가 변경됩니다.



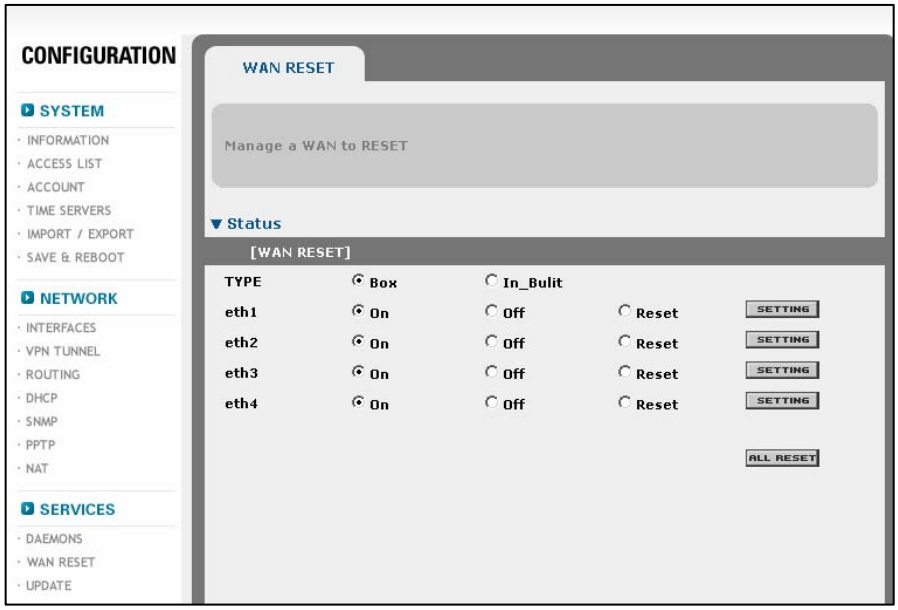
3. <Service> 화면의 Boot Status 항목을 살펴보면, 데몬의 부트 상태가 변경된 것을 확인할 수 있습니다.



4. 제품 설정하기

WAN RESET

초고속모뎀 장비를 컨트롤합니다.



TYPE : 컨트롤러의 타입을 선택합니다. Box:외장형, In-Bulit:내장형

ehX : 각 인터페이스에 대하여 전원의 상태를 선택한 후 setting버튼을 누릅니다.

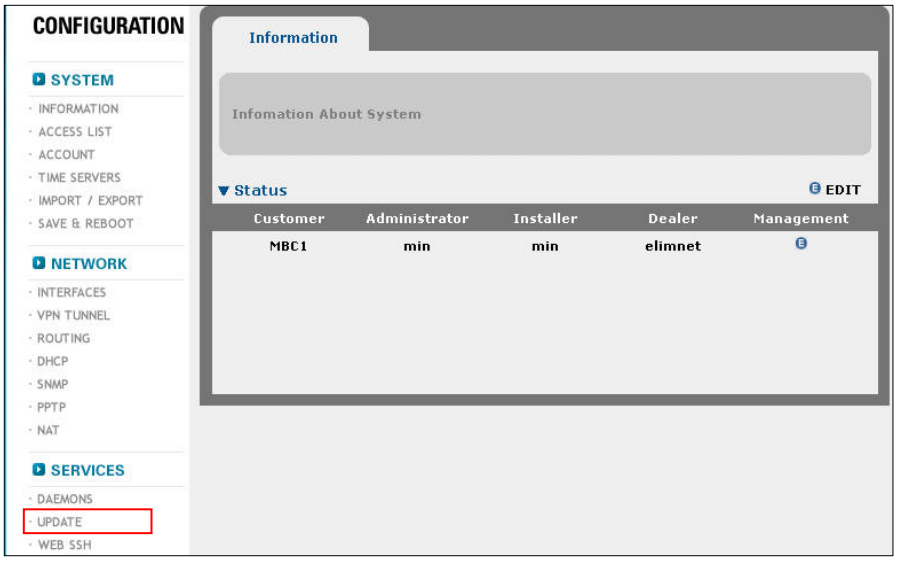
All RESET : 연결되어 있는 모든 모뎀에 대해 RESET을 합니다.

4. 제품 설정하기

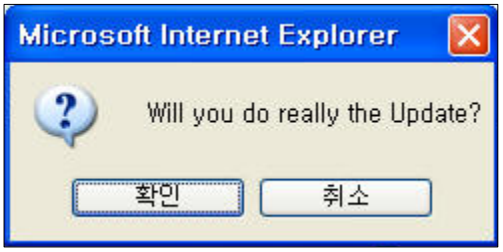
웹 콘솔 업데이트하기

웹 콘솔 프로그램의 업데이트 기능을 통하여 R2SKY 시리즈의 성능이나 기능이 추가되는 경우 최신의 버전으로 업데이트가 가능합니다. 최신의 웹 콘솔 프로그램으로 업데이트하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 CONFIGURATION - SERVICES - UPDATE 메뉴를 클릭합니다.



2. 다음과 같이 업데이트 여부를 확인하는 화면이 나타납니다. [확인]을 클릭합니다.



3. 잠시 후, 업데이트가 완료되면 다음과 같이 업데이트된 버전을 알려주는 화면이 나타납니다.

4. 제품 설정하기

Tip 참고

이미 최신 버전의 웹 콘솔 프로그램으로 업데이트되어 있는 경우에는 다음과 같은 화면이 나타납니다.

Chapter

5 트래픽 모니터링 하기

이 장에서는 웹 콘솔의 'STATISTIC' 메뉴를 사용하여 R2SKY 시리즈의 현재 설정 정보와 R2SKY 시리즈를 통해 송수신되는 트래픽 및 패킷에 대한 정보를 다양한 형태로 조회하는 방법에 대해 설명합니다.

5. 트래픽 모니터링하기

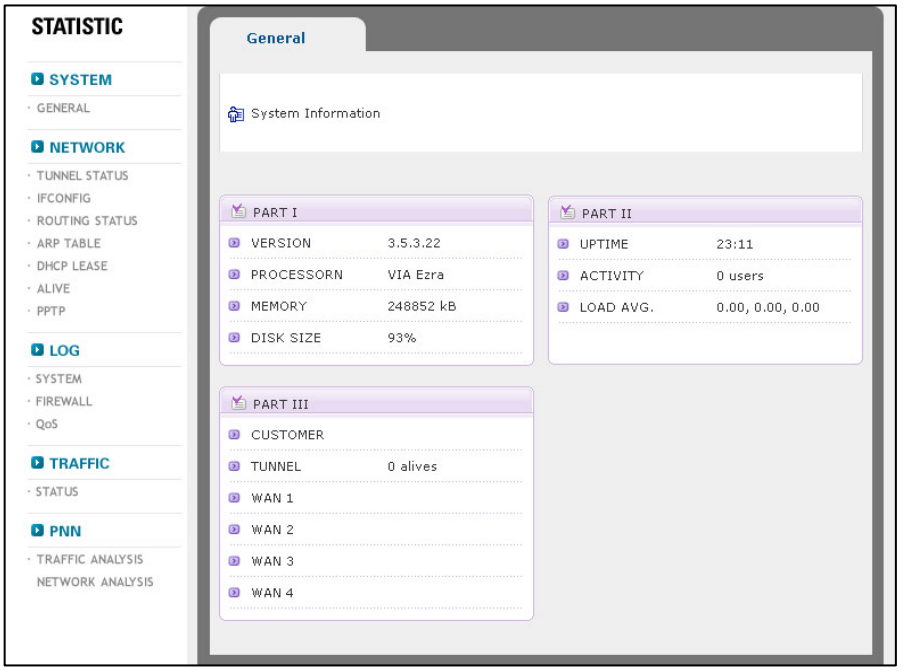
시스템 정보 출력하기

이 절에서는 STATISTIC- SYSTEM 메뉴의 서브 메뉴들을 사용하여 다음과 같은 정보를 출력하는 방법에 대해 알아봅니다.

◦ 시스템의 기본적인 정보
◦ Arrange IP 대역에 속한 호스트들의 사용 대역폭

장비의 기본적인 정보 보기

장비에 대한 기본적인 정보를 보려면 웹 콘솔에서 STATISTIC - SYSTEM - GENERAL 메뉴를 클릭합니다. 다음과 같이 <General> 화면이 나타나면서 장비의 하드웨어와 현재 설정 상태에 대한 간단한 정보들이 출력됩니다.



5. 트래픽 모니터링하기

<General> 화면에 출력된 항목들이 나타내는 정보는 다음과 같습니다.

항 목	설정 값
Version	웹 콘솔의 버전
Processor	프로세서의 종류
RAM	메모리의 크기 (KB)
DISK SIZE	플래시 메모리에서 현재 사용 중인 양 (%)
Customer	고객의 이름
Tunnel	현재 할당된 VPN 터널의 개수
Wan1 ~ Wan4	각 LAN 포트의 WAN 연결 상태
Uptime	장비가 부팅된 후부터 현재까지 경과한 시간 (분)
Activity	현재 장비에 연결되어 있는 사용자의 수
Load Avr	장비의 부하량

5. 트래픽 모니터링하기

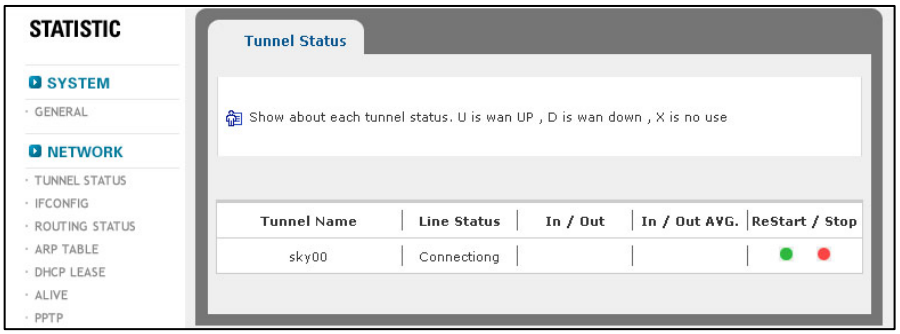
네트워크 모니터링하기

이 절에서는 STATISTIC- NETWORK 메뉴의 서브 메뉴들을 사용하여 다음과 같은 정보를 출력하는 방법에 대해 알아봅니다.

◦ VPN 터널의 상태와 VPN 터널을 통해 송수신되는 트래픽의 양
◦ TCP, UDP 세션 정보
◦ ARP 테이블의 내용
◦ DHCP 클라이언트에게 할당된 IP 주소에 대한 정보
◦ 로그 파일의 내용 (가장 최근의 200 line)
◦ 각 인터페이스의 IP 정보

VPN 터널 모니터링하기

현재 장비에 정의된 VPN 터널에 대한 상태 정보를 보려면 웹 콘솔에서 STATISTIC - NETWORK - TUNNEL STATUS 메뉴를 클릭합니다. 다음과 같은 <Tunnel> 화면이 나타나면서, 각 VPN 터널의 동작 상태와 터널을 통해 송수신되는 데이터에 대한 정보가 출력됩니다.



TUNNEL에 대한 상태를 확인 할 수 있으며, 해당 TUNNEL 상태를 Restart, Stop 할 수 있습니다.

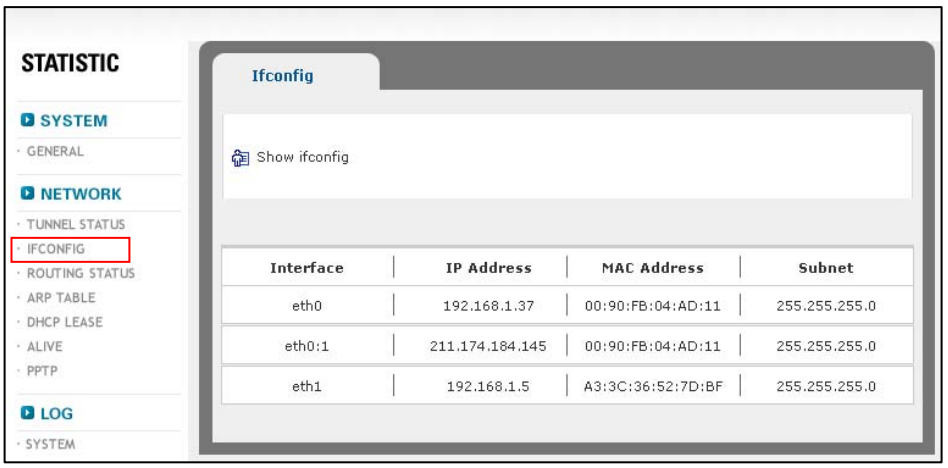
5. 트래픽 모니터링하기

<Tunnel> 화면에 출력된 각 항목들은 다음과 같은 정보를 나타냅니다.

항 목	의 미
No.	인덱스
Tunnel_name	터널의 이름
Line_status	각 라인의 터널 연결 상태. U : 터널과 연결되어 있는 라인. D : 터널과 연결되어 있지 않은 라인.
Input/Output	터널을 통해 송수신된 현재 트래픽
Input/Output AVG.	터널을 통해 송수신된 5분간의 평균 트래픽
Time	Input/Output 항목과 Input/Output AVG. 항목에 표시된 정보가 수집된 시간 간격. Time의 최대값은 5분입니다.

인터페이스의 IP 정보 보기

웹 콘솔에서 STATISTIC - NETWORK - IFCONFIG 메뉴를 클릭하면 다음과 같이 각 인터페이스의 IP 정보를 보여주는 <Ifconfig> 화면이 나옵니다.



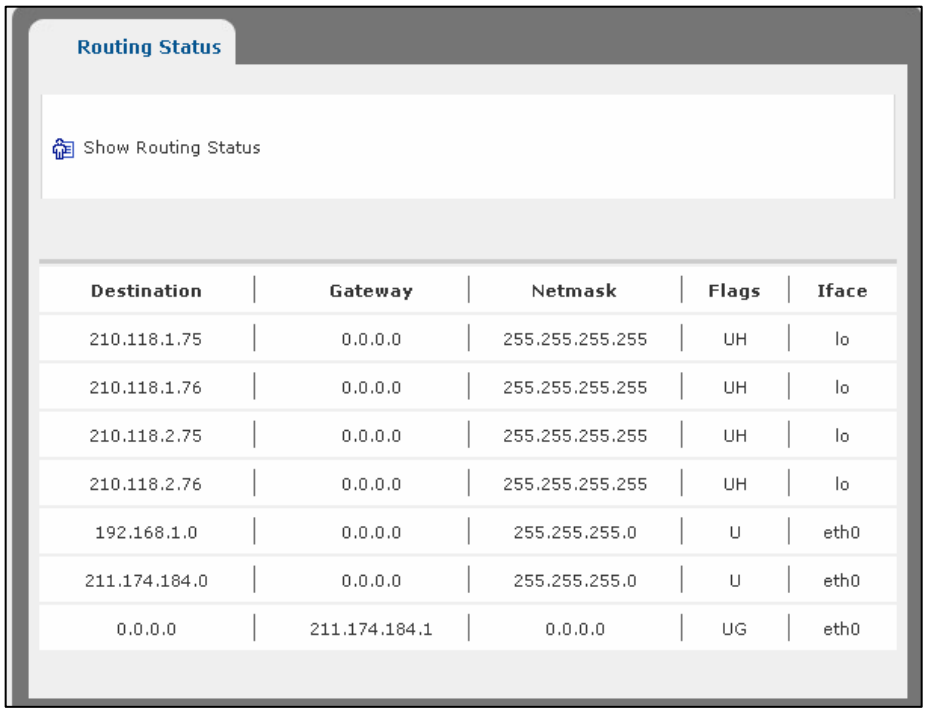
위 <Ifconfig> 화면에 출력된 인터페이스 중에서 상위 2개의 인터페이스는 사용자가 직접 IP 주소를 지정해준 Static 인터페이스입니다.

5. 트래픽 모니터링하기

그리고, 가장 아래에 있는 인터페이스는 PPPoE 인터페이스로 서비스 제공 업체로부터 할당 받은 IP 주소(inet addr 항목)가 출력됩니다. Ifconfig 메뉴는 이와 같이 PPPoE나 케이블 인터페이스의 IP 주소를 확인하는 데 이용하면 편리합니다.
다음 표는 <Ifconfig> 화면에 출력된 각 항목들이 나타내는 정보입니다.

항 목	의 미
encap	인터페이스의 종류. Ethernet인 경우에는 MAC 어드레스가 함께 출력됩니다 (HWaddr 항목).
inet addr	인터페이스의 IP 주소.
Bcast	인터페이스의 브로드캐스트 주소
P–t–P	인터페이스와 연결된 상대 인터페이스의 IP 주소.
Mask	인터페이스 IP 주소의 넷 마스크

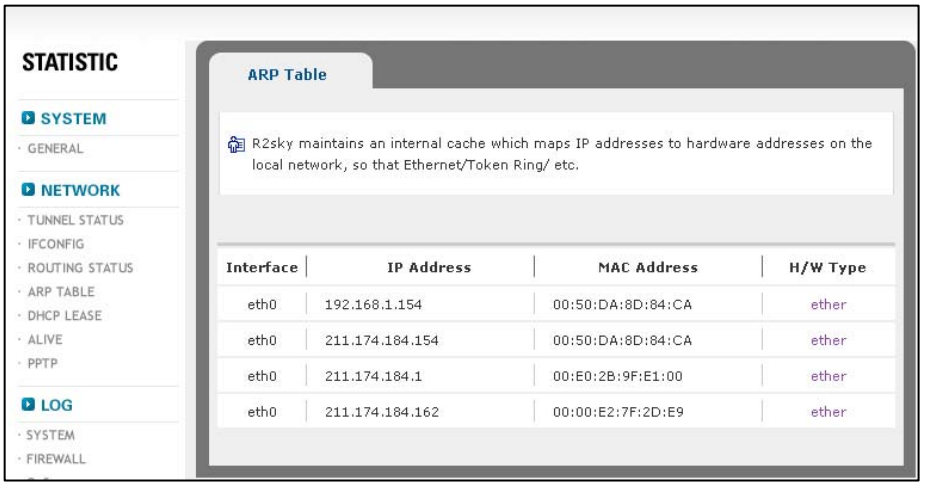
웹 콘솔에서 STATISTIC - NETWORK – ROUTING STATUS 메뉴를 클릭하면 라우팅 정보를 보여줍니다..



Destination : 목적지 정보를 보여줍니다.
Gateway : 게이트웨이 정보를 보여줍니다.
Netmask : 넷마스크 정보를 보여줍니다.
Flags : 플래그정보를 보여줍니다. (UH : 호스트, U : 클래스, UG : 게이트웨이)
Iface : 해당인터페이스 정보를 보여줍니다.

ARP 테이블 보기

ARP 테이블은 각 인터페이스를 통해 송수신되는 트래픽으로부터 학습한 MAC 주소와 IP 주소 간의 맵핑 테이블입니다. 장비는 ARP 테이블에 등록된 내용을 참고하여 MAC 주소를 IP 주소로 변환하여 보여줍니다.
ARP 테이블의 내용을 보려면 웹 콘솔에서 STATISTIC - NETWORK - ARP TABLE 메뉴를 클릭합니다. 그러면, 다음과 같이 ARP 테이블에 등록된 내용을 보여주는 <ARP Table> 화면이 나타납니다.



<ARP Table> 화면에 출력되는 ARP 테이블의 각 엔트리들은 다음 항목들로 구성되어 있습니다.

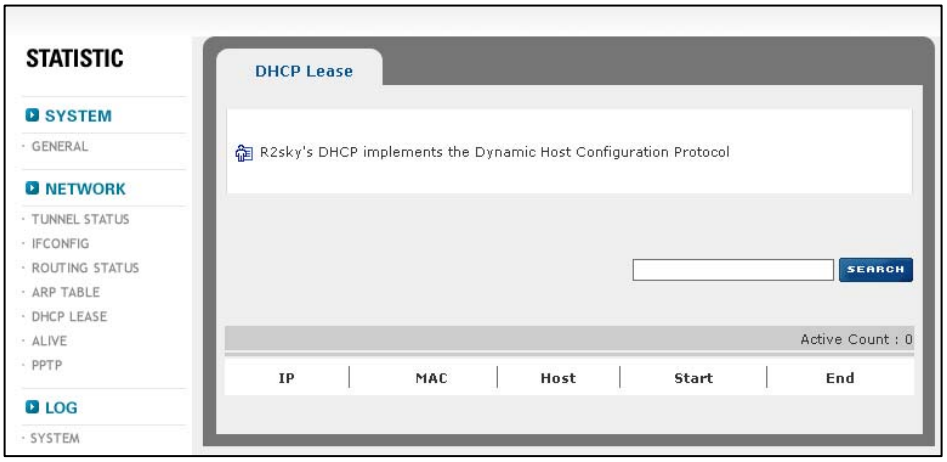
항 목	의 미
Interface	ARP 엔트리가 등록된(학습된) 인터페이스의 이름
IP Address	하드웨어 주소(MAC Address)에 맵핑되는 IP 주소
MAC Address	각 장비마다 고유한 하드웨어 주소
H/W Type	인터페이스의 종류 (ether : Ethernet)

Tip 참고

<ARP Table>에는 incomplete된 ARP 엔트리는 표시되지 않습니다.

DHCP 클라이언트에게 할당된 IP 주소 보기

CONFIGURATION - NETWORK - DHCP 메뉴를 사용하여 장비를 DHCP 서버로 사용하기 위한 설정 작업을 수행하면 DHCP 데몬이 실행되면서 DHCP 설정에 따라 클라이언트에게 IP 주소와 게이트웨이 주소, DNS 주소 등을 할당하게 됩니다. 현재 어떤 클라이언트에게 어떤 IP 주소가 할당되어 있는지를 살펴보려면, 웹 콘솔에서 STATISTIC - NETWORK - DHCP LEASE 메뉴를 클릭하면 됩니다. 그러면, 다음과 같이 현재 각 클라이언트에게 할당되어 있는 IP 주소들을 보여주는 <DHCP Lease> 화면이 나타납니다.



5. 트래픽 모니터링하기

<DHCP Lease> 화면에 출력된 각 항목들은 다음과 같은 정보를 나타냅니다.

항 목	의 미
IP Address	클라이언트에게 할당된 IP 주소
Start	IP 주소가 할당된 시간
End	IP 주소의 유효 시간. 이 시간이 지나면, 새로운 IP 주소를 할당 받게 됩니다.
MAC Address	클라이언트 PC의 MAC 주소(NIC의 MAC 주소)

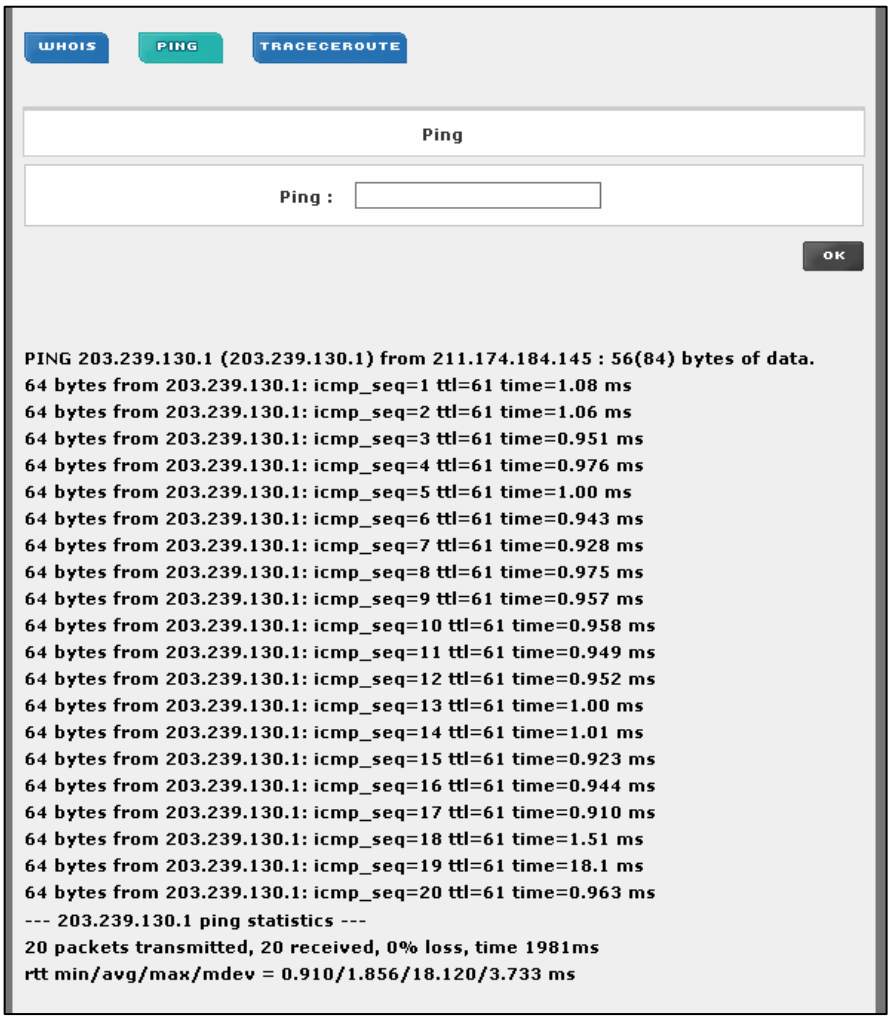
5. 트래픽 모니터링하기

ALIVE 내용 보기

CONFIGURATION - NETWORK - DHCP – ALIVE – WHOIS 메뉴를 통해 검색하고자 하는 도메인 IP Address를 입력하고 서버를 선택하면, 위와 같은 결과를 확인 하실 수 있습니다.

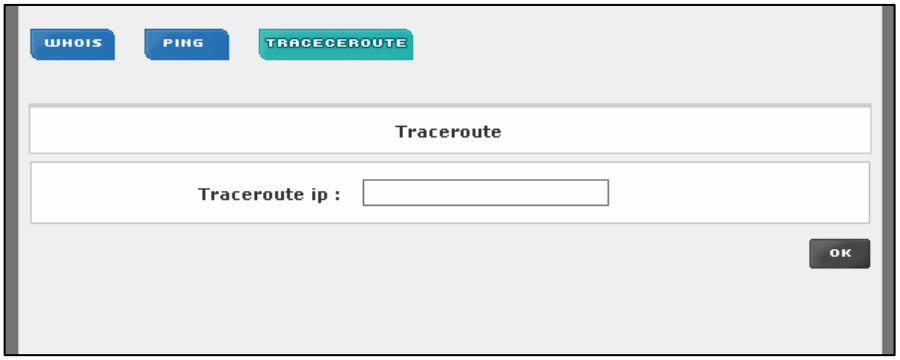
5. 트래픽 모니터링하기

CONFIGURATION - NETWORK - DHCP – ALIVE – PING 메뉴를 통해 특정 호스트와의 ping테스트를 실시합니다.



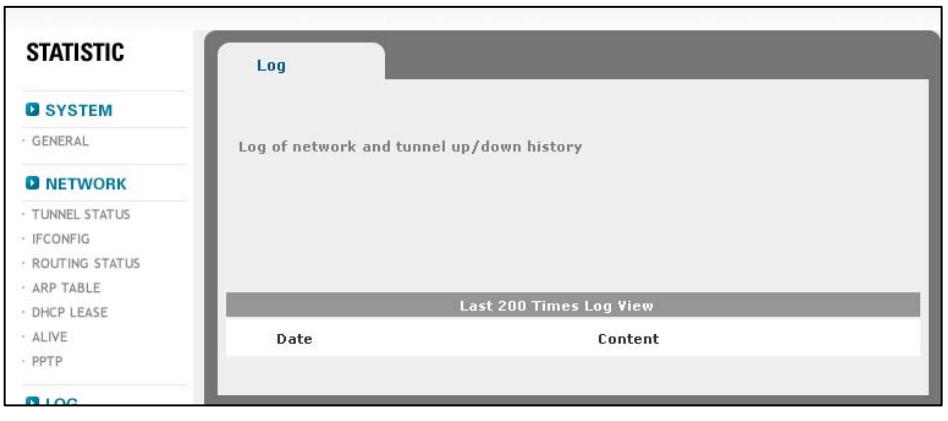
5. 트래픽 모니터링하기

CONFIGURATION - NETWORK - DHCP – ALIVE – PING 메뉴를 통해 최종 목적지까지 거치는 여러 라우터에 대한 경로 및 응답속도를 확인 하실 수 있습니다.



로그 내용 보기

장비에서 이벤트가 발생되면 이벤트에 대한 정보가 로그 파일에 기록됩니다. 이 로그 파일은 장비에 문제가 발생했을 때, 장비 관리자나 네트워크 관리자가 문제의 원인을 파악하는 데 유용하게 사용될 수 있습니다. 그리고, 장비로 접속한 사용자에 대한 기록과 변경된 장비 설정 등에 대한 정보가 모두 로그 파일에 남아있어서 어떤 사용자에 의해 장비의 어떤 설정이 수정되었는지도 쉽게 알 수 있습니다.
웹 콘솔에서 STATISTIC – LOG – SYSTEM 메뉴를 클릭하면 이러한 로그 파일의 내용 중 최근 200개를 보여주는 <Log> 화면이 나타납니다.

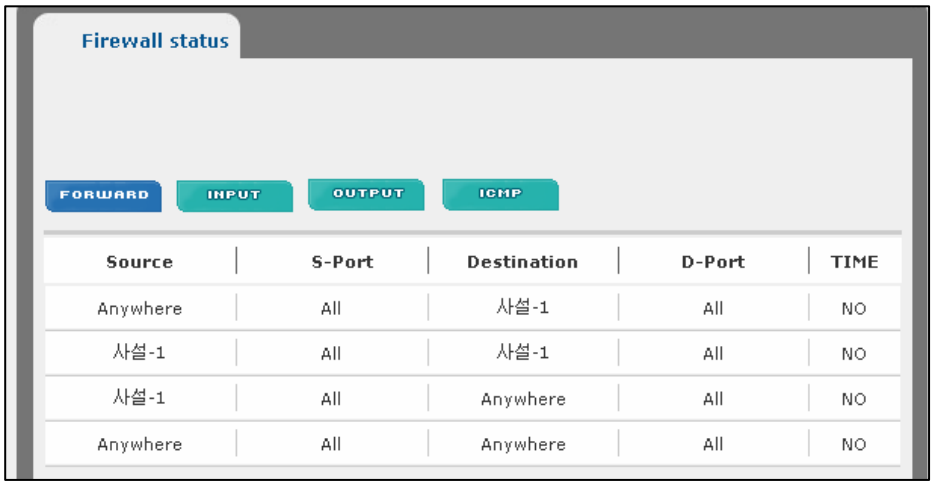


5. 트래픽 모니터링하기

<Log> 화면에 출력되는 항목들이 나타내는 정보는 다음과 같습니다.

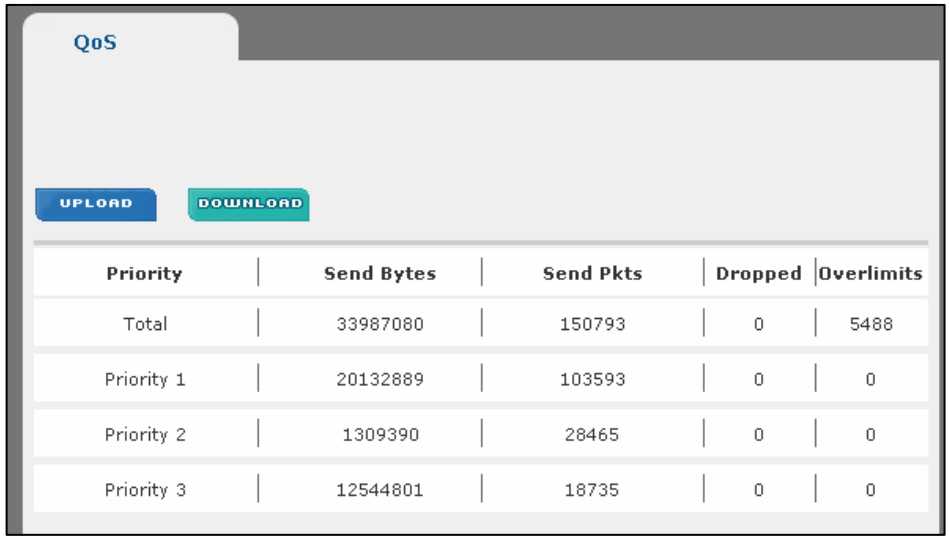
항 목	의 미
Today	오늘 하루 동안 Line_Down이나 Tunnel_Down이 발생한 횟수
This Week	이번 한 주 동안 Line_Down이나 Tunnel_Down이 발생한 횟수
Line_Down	인터페이스와 연결된 링크가 다운된 횟수
Tunnel_Down	VPN 터널이 연결 종료된 횟수
Last 200 Times Log View	최근에 발생한 200개의 이벤트에 대한 정보. 이벤트가 발생한 시간, 이벤트가 발생한 위치(부분), 발생한 이벤트에 대한 정보가 표시됩니다.

웹 콘솔에서 STATISTIC - LOG - FIREWALL STATUS 메뉴를 클릭하면 Firewall에 대한 상태를 볼 수 있습니다.
좀 더 상세한 보고자 한다면, 항목을 클릭하여 볼 수 있습니다.



5. 트래픽 모니터링하기

웹 콘솔에서 STATISTIC - LOG - QOS 메뉴를 클릭하면 QOS에 대한 상태를 볼 수 있습니다.
좀 더 상세한 보고자 한다면, 항목을 클릭하여 볼 수 있습니다.



Priority	Send Bytes	Send Pkts	Dropped	Overlimits
Total	33987080	150793	0	5488
Priority 1	20132889	103593	0	0
Priority 2	1309390	28465	0	0
Priority 3	12544801	18735	0	0

5. 트래픽 모니터링하기

트래픽의 통계 정보 보기

이 절에서 살펴볼 내용은 다음과 같습니다.

◦ 각 호스트에서 전송한 트래픽에 대한 정보
  - 전송한 트래픽을 프로토콜 종류별로 정리한 통계 정보
  - 전송한 TCP, UDP 트래픽을 어플리케이션 종류별로 정리한 정보
  - 각 호스트의 데이터 전송 속도와 초당 전송 패킷의 개수
  - 각 호스트의 시간대별 데이터 전송 양

◦ 각 호스트를 통해 송수신된 멀티캐스트 트래픽 정보

◦ 각 인터페이스를 통해 송수신된 트래픽을 다양하게 분석한 통계 정보

◦ 최근 1시간과 하루 동안 처리된 트래픽의 양을 출력하는 그래프

◦ 각 인터넷 도메인을 통해 송수신된 트래픽을 프로토콜 종류별로 정리한 통계 정보

◦ IP 트래픽에 대한 정보
  - WAN → LAN으로 수신된 IP 트래픽 정보
  - LAN → WAN으로 전송된 IP 트래픽 정보
  - LAN 내부에서 송수신되는 IP 트래픽 정보

◦ IP 프로토콜에 대한 정보
  - IP 프로토콜의 분포
  - 동작 중인 TCP 세션의 정보
  - 로컬 서브넷에 동작 중인 라우터에 대한 정보

수신된 트래픽의 통계 정보 보기

이 절에서는 각 호스트로 수신된 트래픽에 대한 다음 정보들을 출력하는 방법에 대해 알아봅니다.

◦ 수신된 트래픽을 프로토콜 종류별로 정리한 통계 정보

◦ 수신된 TCP, UDP 트래픽을 어플리케이션 종류별로 정리한 정보

◦ 각 호스트의 데이터 수신 속도와 초당 수신 패킷의 개수

◦ 각 호스트의 시간대별 데이터 수신 양

5. 트래픽 모니터링하기

프로토콜 종류별 수신 트래픽 보기

웹 콘솔에서 STATISTIC - PNN - TRAFFIC ANALYSIS 메뉴를 클릭합니다. 그러면 다음과 같이 ARP Table 에 등록되어 있는 Host에 대한 UPLOAD, DOWNLOAD 트래픽 정보를 제공합니다.

IP List	[Packets]	[Bytes]
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.170	1	60
210.182.131.177	50	4200
192.168.20.5	4	240
203.239.130.1	4	240
220.73.146.185	19	24727
222.122.84.41	5	437
192.168.20.5	14	924
192.168.20.5	5	676
222.122.84.42	6	3604
220.73.156.106	7	3580

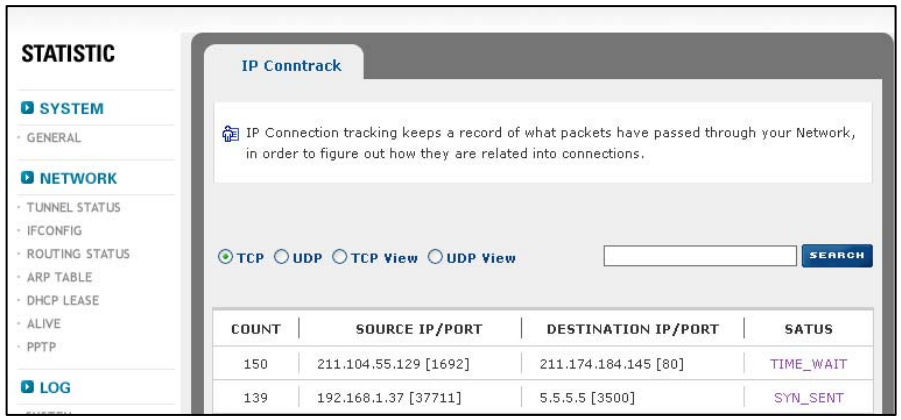
5. 트래픽 모니터링하기

TCP/UDP 세션 보기

현재 장비에 맺어진 TCP 세션과 UDP 세션을 출력하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 STATISTIC - PNN – NETWORK ANALYSIS 메뉴를 클릭합니다.

2. 다음과 같은 <IP Conntrack> 화면이 나타납니다.



3. 다음 설명을 참고하여 출력하고자 하는 정보에 따라 목록 위에 있는 4개의 라디오 버튼(TCP, UDP, TCP_VIEW, UDP_VIEW) 중 하나를 클릭합니다.

◦ TCP : 현재 장비에 맺어진 TCP 세션들을 출력합니다. 이 때, 전송지 IP와 목적지 IP가 동일하고 포트만 다른 세션들은 하나의 라인으로 출력하며 Count가 증가합니다.

◦ UDP : 현재 장비에 맺어진 UDP 세션들을 출력합니다. 이 때, 전송지 IP와 목적지 IP가 동일하고 포트만 다른 세션들은 하나의 라인을 출력하며 Count가 증가합니다.

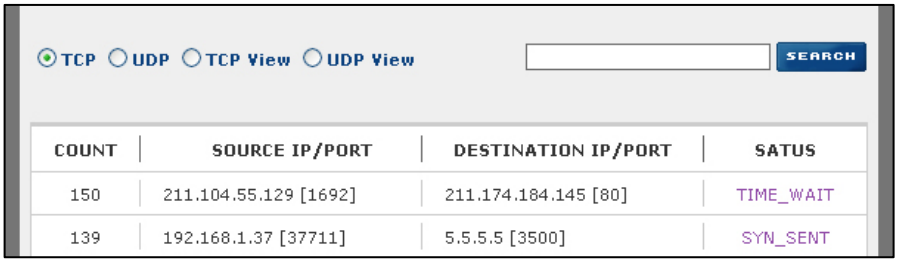
◦ TCP VIEW : 현재 장비에 맺어진 TCP 세션들을 모두 출력합니다.

◦ UDP VIEW : 현재 장비에 맺어진 모든 UDP 세션들을 모두 출력합니다.

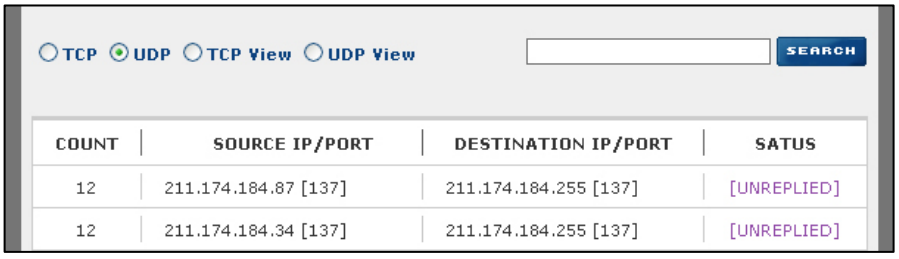
5. 트래픽 모니터링하기

다음은 각 라디오 버튼을 선택했을 때 출력되는 정보입니다.

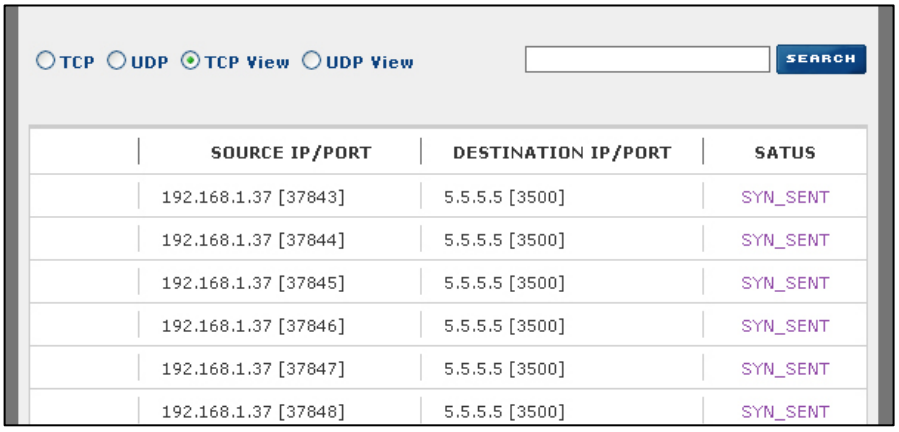
<TCP를 선택한 경우>



<UDP를 선택한 경우>

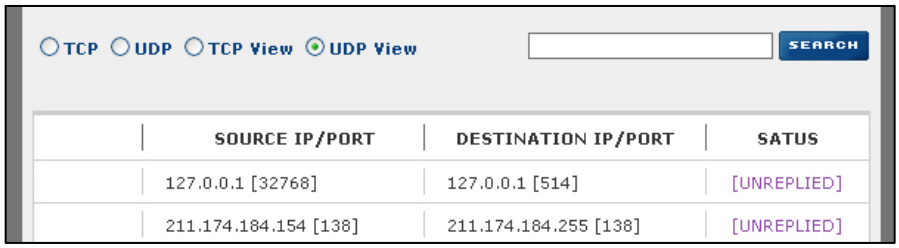


<TCP_VIEW를 선택한 경우>



5. 트래픽 모니터링하기

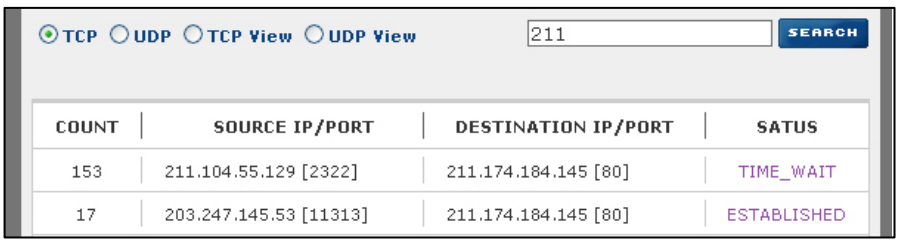
<UDP_VIEW를 선택한 경우>



출력된 각 항목들이 나타내는 정보는 다음과 같습니다.

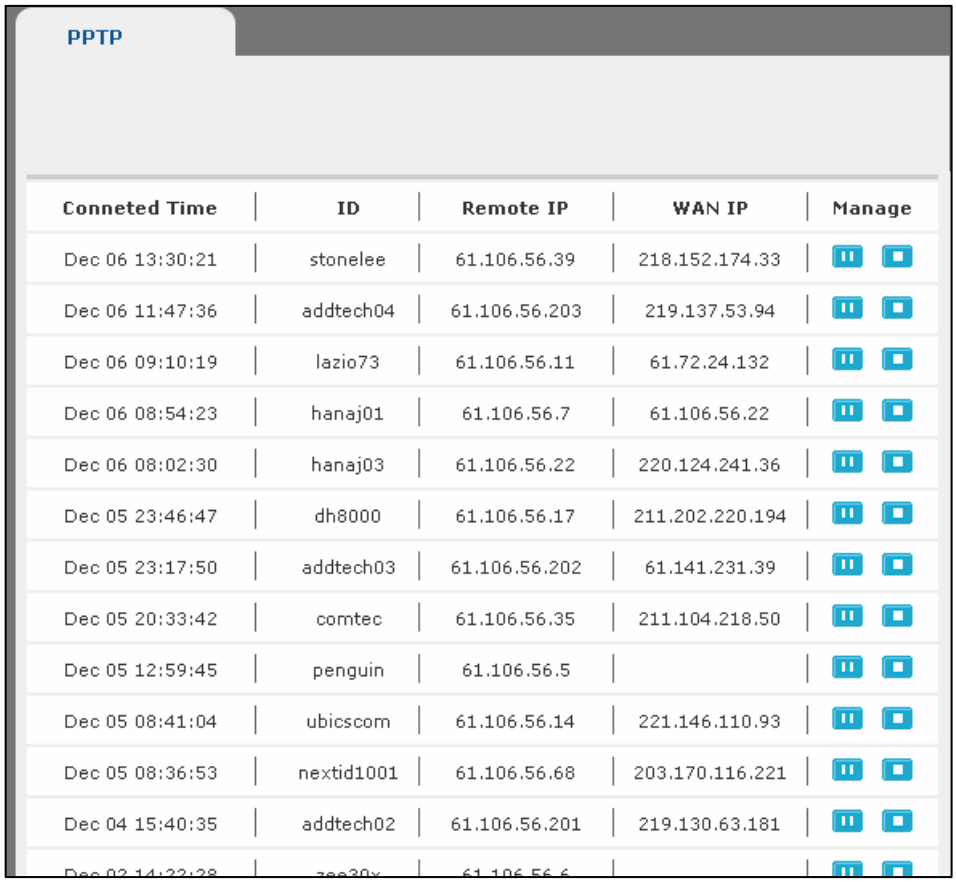
항 목	의 미
Count	왼쪽에 있는 Count 항목은 동일한 전송지 IP 주소와 목적지 IP 주소를 가진 TCP/UDP 세션의 개수입니다.
Source IP / PORT	TCP 세션이나 UDP 세션이 맺어진 전송지 IP 주소와 포트 번호
Destination IP / PORT	TCP 세션이나 UDP 세션이 맺어진 목적지 IP 주소와 포트 번호
Status	설정 상태 – ESTABLISHED : 정상적으로 연결되고 Data 송수신이 이루어지고 있는 상태 – ASSURED : Data 흐름 없이 연결되어 있는 상태 – TIME_WAIT : 연결 대기 상태 – SYN_SENT : 세션을 맺기 위해 시도하고 있는 상태

5. 라디오 버튼의 오른쪽에 있는 검색란을 이용하면 IP 주소와 포트 번호를 사용하여 TCP나 UDP 세션을 검색할 수 있습니다.
4개의 라디오 버튼 중에 검색할 대상을 선택한 후 입력란에 검색할 값을 입력하고 [SEARCH] 버튼을 클릭합니다. 그러면, 다음과 같이 입력한 값이 포함된 세션의 정보가 출력됩니다.



5. 트래픽 모니터링하기

웹 콘솔에서 STATISTIC - SYSTEM – PPTP 메뉴를 클릭하면 현재 서버에 접속되어 있는 정보를 보여줍니다.



Connected Time : 접속시간
ID : 접속 아이디
Remote IP : 할당된 IP
WAN IP : 접속아이디의 IP
Manage : 일시 정지 및 정지 기능

Chapter

6 방화벽(Firewall) 설정하기

이 장에서는 웹 콘솔의 'FIREWALL' 메뉴를 사용하여 특정한 서비스의 트래픽을 필터링하는 방법을 살펴봅니다.

6. 방화벽(Firewall) 설정하기

이 장에서는 웹 콘솔의 'FIREWALL'메뉴를 사용하여 특정한 서비스의 트래픽을 필터링하는 방법을 살펴봅니다.

Firewall Quick Start

R2SKY 시리즈는 방화벽에 대해 잘 알지 못하는 사용자들도 웹 콘솔에서 쉽게 방화벽을 설정할 수 있도록 Quick Start 메뉴를 제공합니다. Quick Start 메뉴에는 다음과 같이 자주 사용되는 서비스들이 미리 등록되어 있습니다.

서비스	설 명	포 트
FTP	파일 전송 서비스	21
Telnet	원격 로그인 서비스	23
Web	WWW(World Wide Web) 서비스	80
Pop3	메일 전송 서비스	110
SMTP	메인 수신 서비스	25
News	뉴스 서비스	119
Windows_File_Share	윈도우의 파일 공유 서비스	
V_Share	P2P 파일 공유 서비스	
Guruguru		
Donkey		
Soribada		
PD_BOX		
Pop_Folder		
Puruna		
MSN	Messenger 서비스	
(온라인 채팅 서비스)		
Nate_ON		
SayClub		
DAUM		
BuddyBuddy		

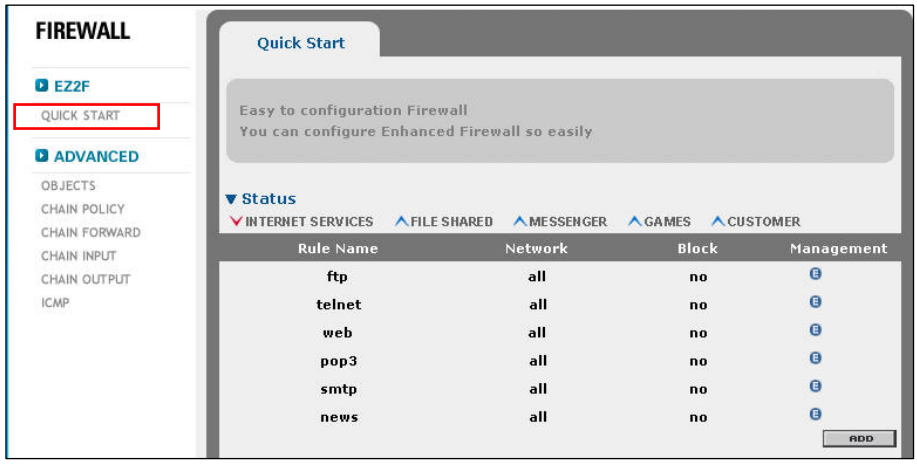
6. 방화벽(Firewall) 설정하기

서비스	설 명	포 트
Gunie	Messenger 서비스	
AOL		
ICQ		

서비스	설 명	포 트
Starcraft	네트워크 게임 서비스	
Diablo		
Lineage		
Lineage2		
Mu		
Fortress2		

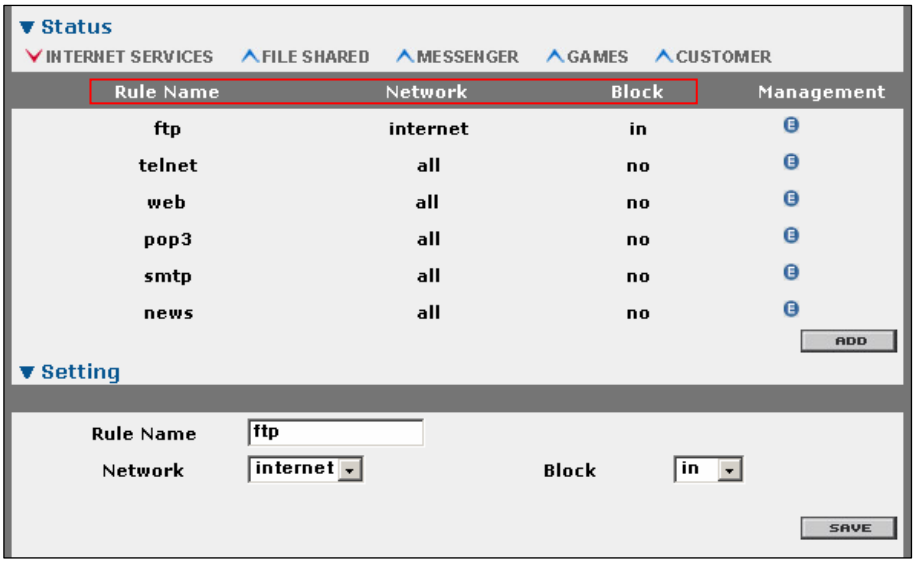
기본적으로는 이 서비스들이 모두 사용할 수 있도록 설정되어 있습니다.
사용자 네트워크의 정책에 따라 특정 서비스에 방화벽을 적용하여 서비스의 사용 여부를 변경하려면 다음과 같이 Quick Start 메뉴를 사용하면 됩니다.

1. 웹 콘솔에서 FIREWALL - EZ2F - QUICK START 메뉴를 클릭합니다.



6. 방화벽(Firewall) 설정하기

QUCIK START는 FIREWALL의 일반적인 사항들을 정리하여 사용자가 손쉽게 정책을 설정할 수 있습니다.

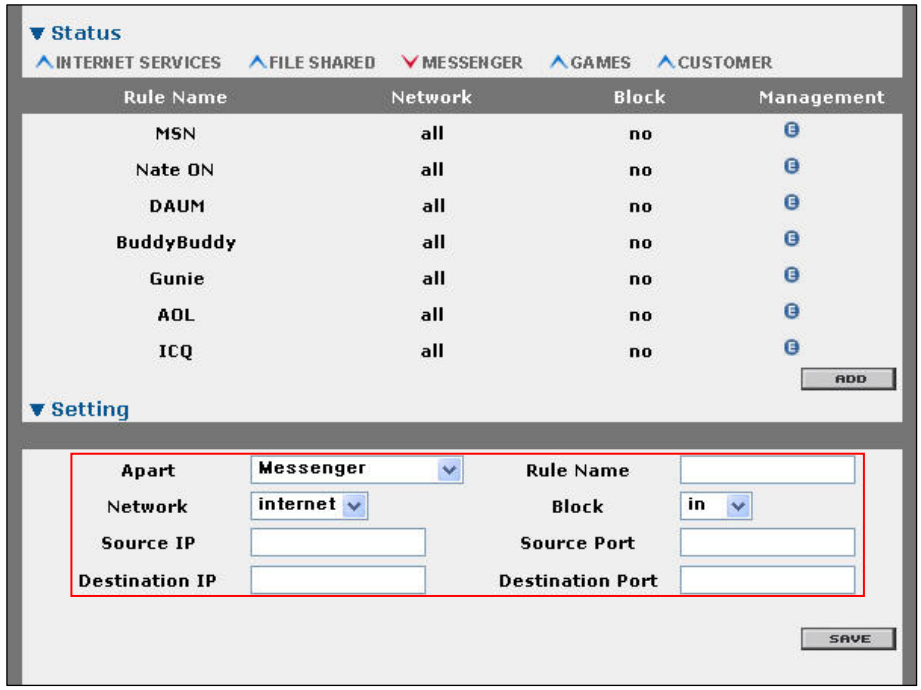


2. 자주 이용되는 IP, Port에 대해 따로 Object를 생성하지 않고 손쉽고,빠르게 Firewall을 설정 하실 수 있습니다.

◦ Rule Name : 일반적인 룰의 이름을 의미합니다.
◦ Network : LAN -> LAN범위 내에서 Firewall을 설정합니다.
Tunnel -> Tunnel범위 내에서 Firewall을 설정합니다.
All -> LAN, Tunnel에 대한 Firewall을 설정합니다.
◦ Block : in -> 들어오는 네트웍을 차단합니다.
Out -> 나가는 네트웍을 차단합니다.
All -> in, out 모두를 차단합니다.
No -> 차단하지 않습니다.

6. 방화벽(Firewall) 설정하기

3. 원하는 서비스의 설정을 끝낸 후 화면 아래에 있는 [SAVE] 버튼을 클릭하면 변경된 설정이 장비에 바로 적용됩니다.

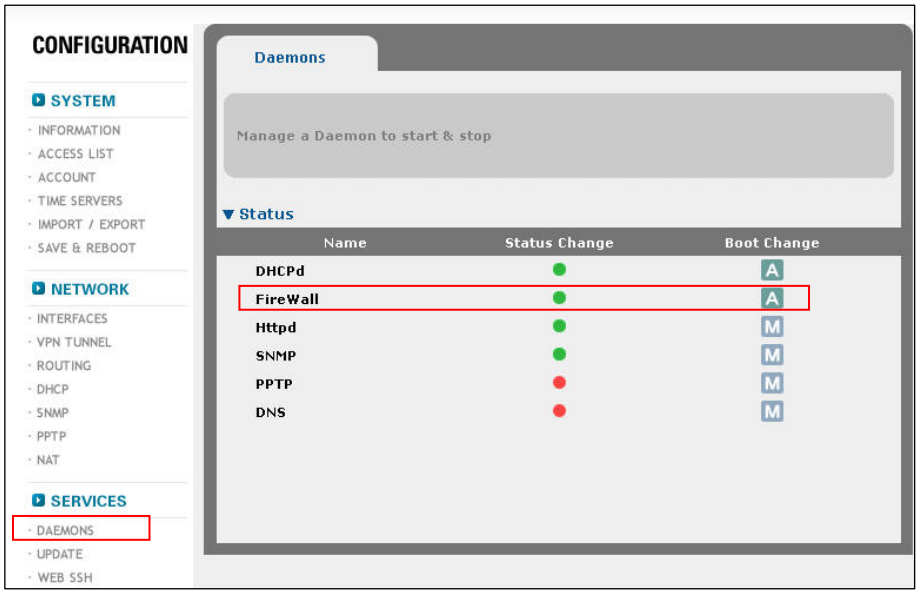


기본적으로 제공되는 룰외에 사용자가 직접 정의하고자 하는 룰을 설정합니다.

Apart : 해당 룰을 어느 항목(INTERNET SERVICES, FILE SHARED, MESSNGER, GAMES, CUSTOMER)에 위치 시킬 것인지 선택합니다.

◦ Rule Name : 룰 이름을 설정합니다.
◦ Network : LAN, Tunnel, All 중에서 설정합니다.
◦ Block : 네트웍의 흐름을 설정합니다.
◦ Source IP : 네트웍의 출발지 IP Address를 설정합니다.
◦ Source IP : 네트웍의 출발지 Port를 설정합니다.
◦ Destination IP : 네트웍의 목적지 IP Address를 설정합니다.
◦ Destination Port : 네트웍의 목적지 Port를 설정합니다.

4. 방화벽이 동작하고 있는지 확인하려면 CONFIGURATION - SERVICE - DAEMON 메뉴를 클릭한 후 Firewall 데몬의 상태가 "Running"인지 살펴봅니다.



트래픽 필터링 설정하기

Quick Start 메뉴를 사용하지 않고 직접 특정 트래픽을 필터링할 수 있도록 설정하는 방법을 살펴봅니다. R2SKY 시리즈의 웹 콘솔에서 트래픽 필터링 기능을 설정하는 과정은 다음과 같습니다.

1. 대상(Object) 등록하기
   먼저 필터링을 적용할 트래픽을 지정하기 위해 필요한 대상(object)을 등록합니다. 등록할 수 있는 대상에는 네트워크, 호스트(사용자), 서비스가 있습니다.

2. Chain Forward 정의하기
   네트워크와 호스트, 서비스 등을 등록한 후에는 이 값들을 사용하여 특정한 트래픽을 지정하고, 해당 트래픽을 어떻게 처리할 것인지를 정의한 정책(policy)을 추가해야 합니다. 이러한 정책을 Forward라고 하고, Forward 정책의 모음(group)을 Chain Forward라고 합니다.

3. Chain Policy 정의하기
   Chain Forward를 정의한 후에는 Chain Forward의 정책들에 적용되지 않는 나머지 트래픽을 처리할 방법을 설정합니다. Chain Policy는 Chain Forward에 의해 처리된 트래픽 이외의 트래픽들을 어떻게 처리할지 정의된 정책입니다. Chain Forward에 있는 어떤 Forward의 조건과도 일치하지 않는 트래픽은 Chain Policy에 정의된 action에 따라 처리됩니다.

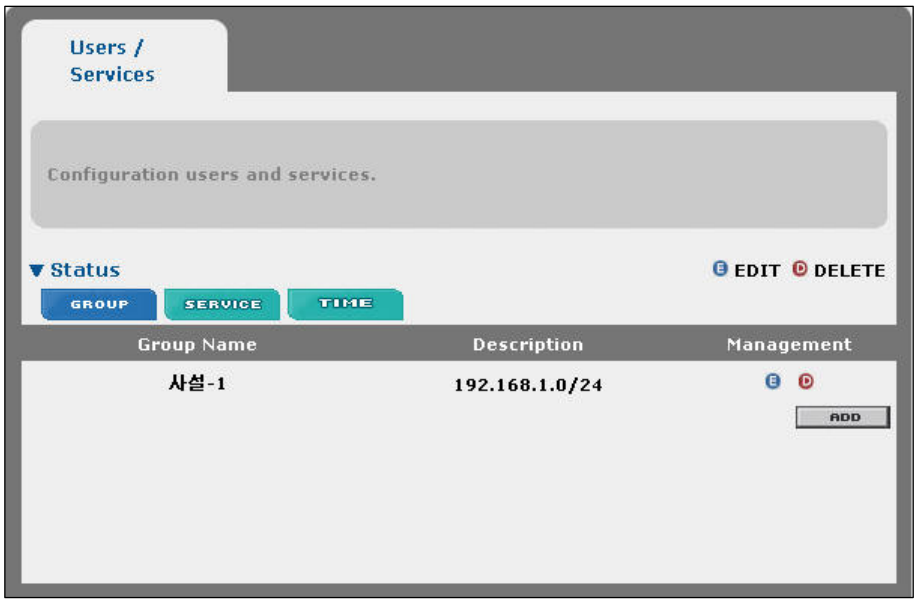
다음 절에서는 각 과정의 설정 방법에 대해 상세히 알아봅니다.

대상(네트워크, 사용자, 서비스) 등록하기

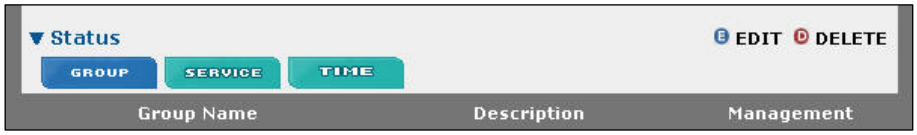
다음과 같은 방법으로 필터링을 적용할 트래픽을 지정할 때 사용될 네트워크와 사용자, 그리고 서비스를 등록합니다.

1. 웹 콘솔에서 FIREWALL - FILTER - USER/SERVICE 메뉴를 클릭합니다.

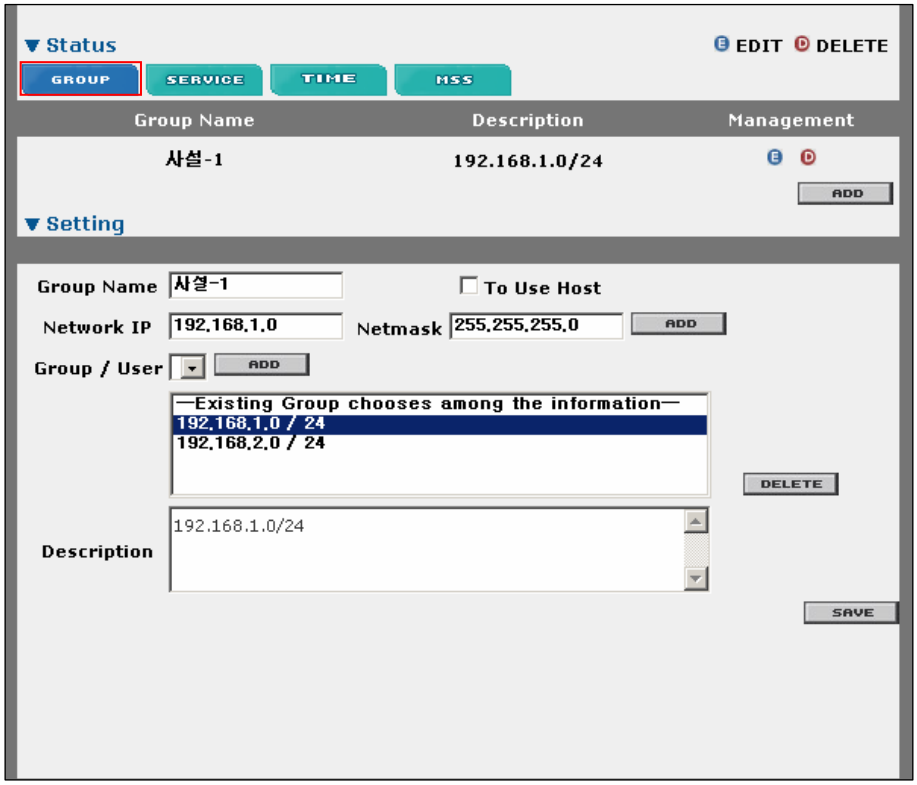
2. 다음과 같은 <User/Service> 화면이 나타납니다. <User/Service> 화면에는 현재 등록되어 있는 네트워크 목록이 출력됩니다.



3. 목록 바로 위에 있는 GROUP, USER, SERVICE 중에서 등록하고자 하는 대상을 선택합니다.

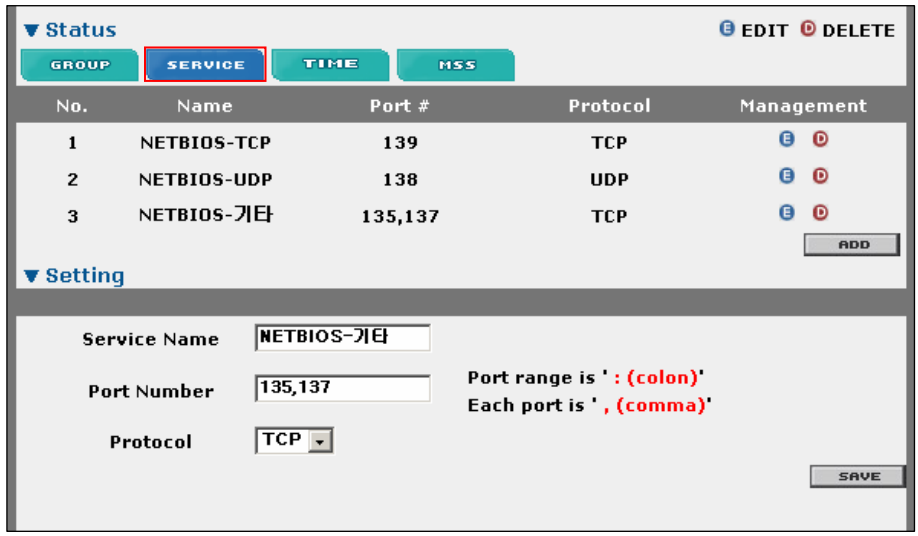


FIREWALL, QoS, NAT의 Source, Destination Host에 대한 리스트들을 세팅합니다.
각각의 그룹리스트를 클릭하면 세팅 되어 있는 호스트들의 정보를 확인 할 수 있습니다.



6. 방화벽(Firewall) 설정하기

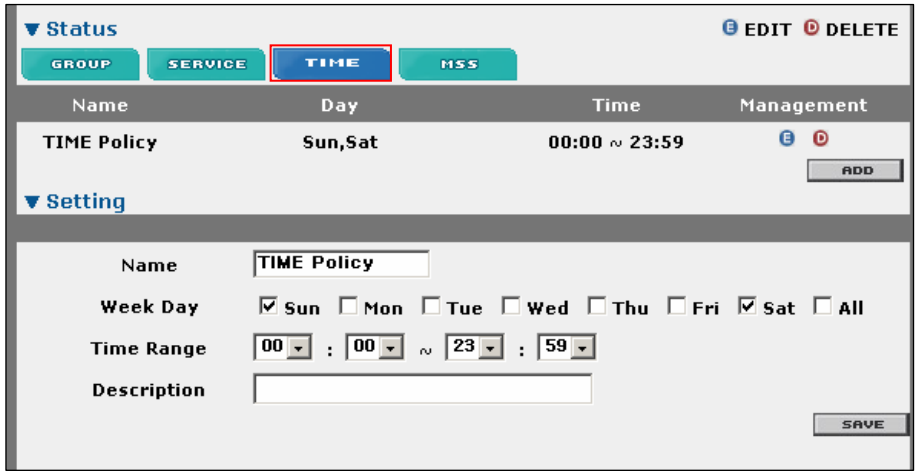
Group Name : 식별이 용이한 그룹 이름을 입력합니다.
To Use Host : 단일 Host를 사용하고자 할 때 체크를 합니다.
Network IP : IP Address를 입력합니다.
Netmask : Netmask를 입력합니다.
[ADD]버튼 : 해당 정보를 리스트에 추가합니다.
Group/User : 기존에 Setting되어 있는 그룹을 추가하고자 할 때 해당 리스트에서 선택 후 ADD를 합니다.
[DELETE]버튼 : 리스트에서 삭제하고자 할 때 클릭합니다.
Description : 그룹에 대한 설명 및 요약정보를 입력합니다.



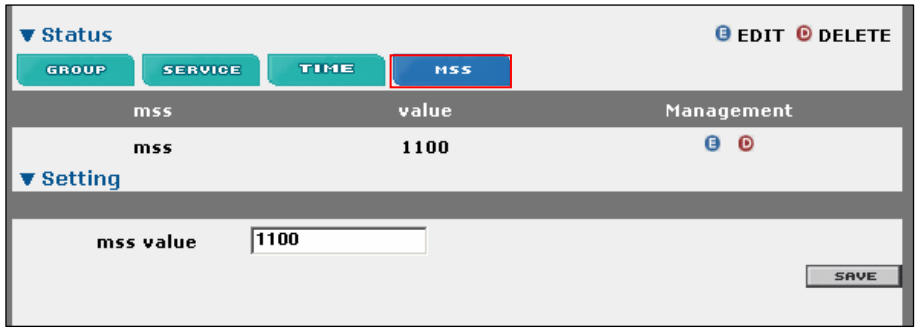
FIREWALL, QoS, NAT의 Source, Destination Port에 대한 리스트들을 설정합니다.

Service Name : 식별이 용이한 이름을 입력합니다.
Port Number : Port Number를 입력합니다. 포트가 range일때는 : (콜론)으로 설정을 하며, range가 아닌 복수의 포트일때는 ,(콤마)로 설정합니다.
Protocol : TCP / UDP를 설정합니다.

6. 방화벽(Firewall) 설정하기



Name : 식별이 용이한 이름을 설정합니다.
Week Day : 룰이 적용될 요일을 설정합니다.
Time Range : 룰이 적용될 시간을 설정합니다.
Description : 설명 및 요약 정보를 설정합니다.



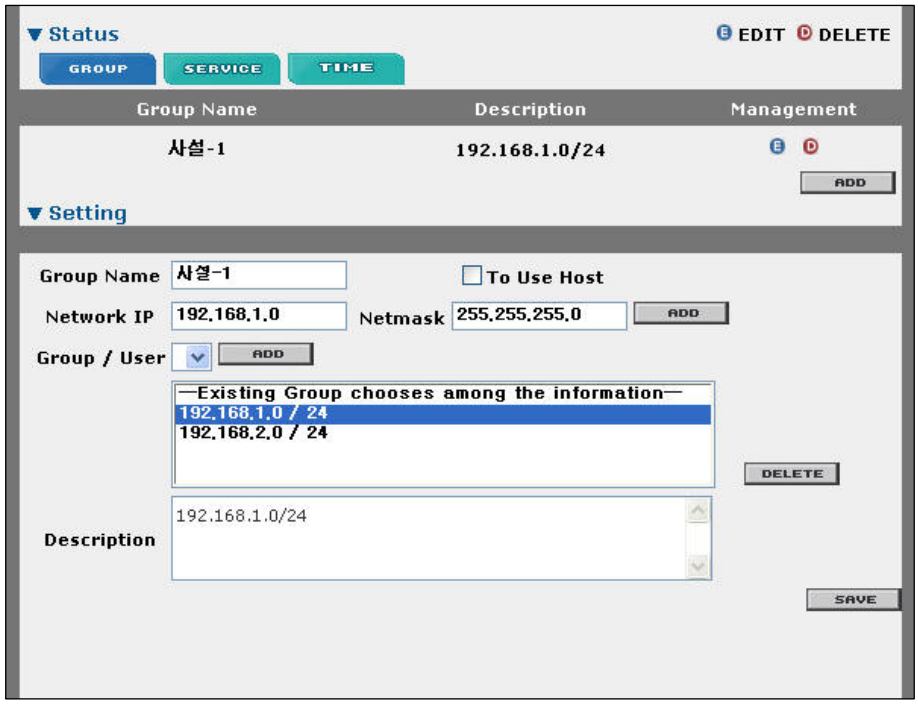
Default MSS 값을 변경하는 기능입니다.
변경된 상태에서 Default 값을 사용하고자 할 때는 삭제를 하면 됩니다.
mss value : 변경하고자 하는 값을 설정합니다.

4. 그런 후에 [ADD] 버튼을 클릭합니다.

5. 화면 아래에 선택한 항목(네트워크, 사용자, 서비스)에 대한 설정 값을 입력할 수 있는 <Setting> 화면에 나타납니다. 다음 설명을 참고하여 각 항목의 값을 지정합니다.

6. 방화벽(Firewall) 설정하기

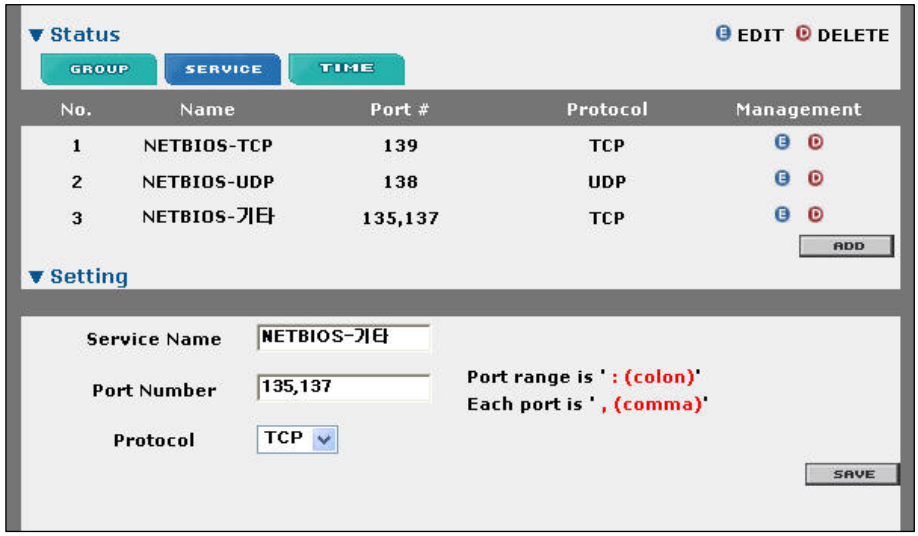
네트워크를 추가하는 경우



① Group Name 항목에 추가할 네트워크의 이름을 입력합니다.
② IP_Address 항목에 추가할 네트워크의 IP 주소를 입력합니다.
③ S.M 항목에 추가할 네트워크의 서브넷 마스크 값을 입력합니다.
④ [ADD] 버튼을 클릭합니다.
⑤ 여러 개를 한꺼번에 등록하는 경우에는 1 ~ 4번 과정을 여러 번 반복하면 됩니다.
⑥ Description 항목에 추가하는 네트워크에 대한 간략한 정보를 입력합니다.
⑦ [SAVE] 버튼을 클릭합니다.

6. 방화벽(Firewall) 설정하기

서비스를 추가하는 경우



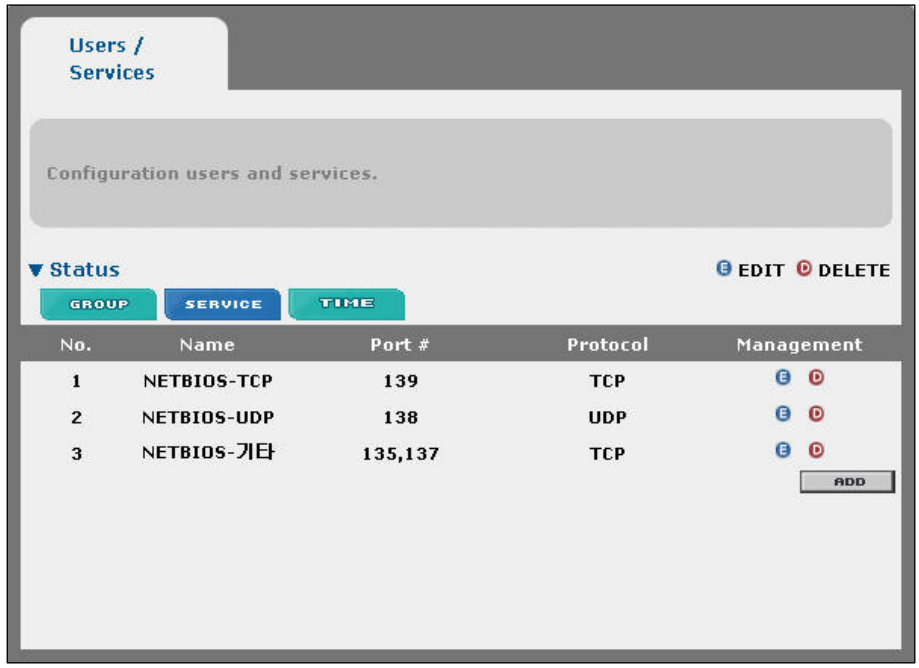
① Service Name 항목에 추가할 서비스의 이름을 입력합니다.

② Port Number 항목에 추가할 서비스에 사용되는 포트의 번호를 입력합니다. 여러 개의 포트를 입력하는 경우에는 ','를 사용하면 됩니다.

③ Protocol 항목의 콤보 박스를 클릭한 후 서비스의 프로토콜 종류를 선택합니다.

④ [SAVE] 버튼을 클릭합니다.

6. <User/Service> 화면에서 추가한 네트워크, 사용자, 서비스들을 확인할 수 있습니다.



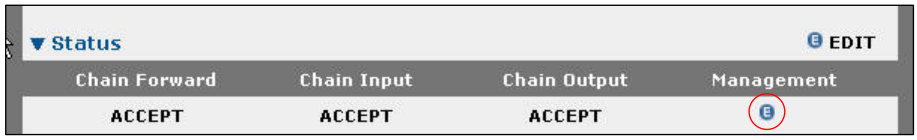
Chain Policy 설정하기

Chain Policy를 설정하는 방법은 다음과 같습니다.

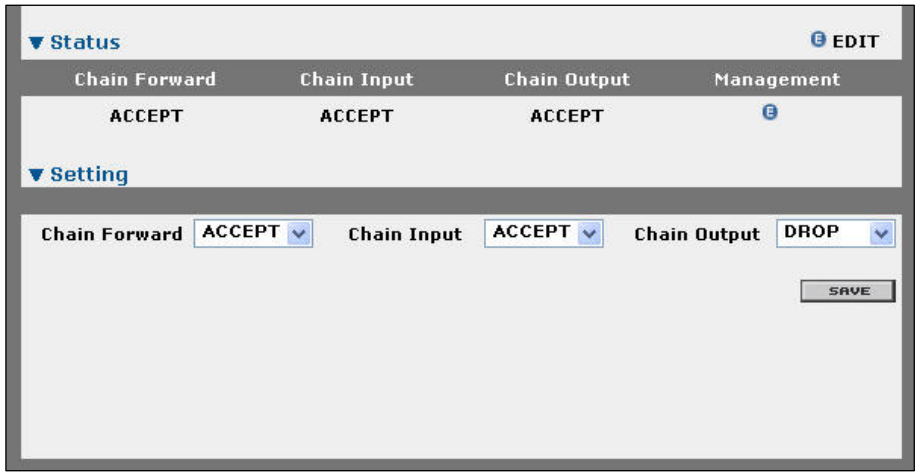
1. 웹 콘솔에서 FIREWALL - FILTER - CHAIN POLICY 메뉴를 클릭합니다.

2. 다음과 같은 <Chain Policy> 화면이 나타납니다. <Chain Policy> 화면에는 현재 정의된 Chain Policy가 출력됩니다.

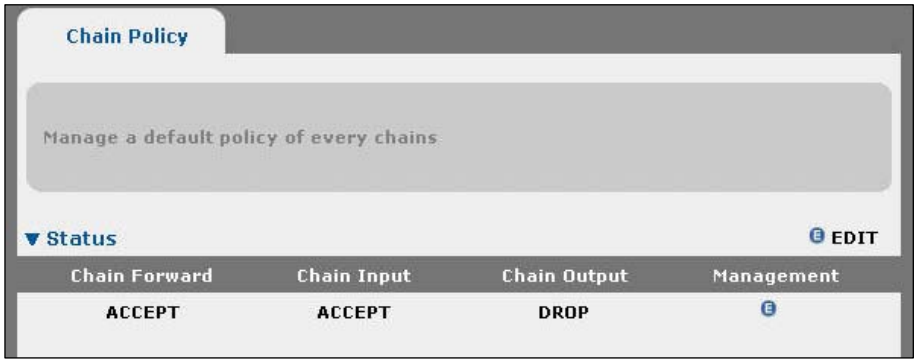
3. Management 항목에 있는 (E)를 클릭합니다.



4. 그러면, 다음과 같이 Chain Policy를 설정할 수 있는 <Setting> 화면이 나타납니다. Chain Forward 항목의 콤보 박스를 클릭한 후 ACCEPT와 DROP, 2가지 방법 중 하나를 선택합니다. ACCEPT를 선택한 경우에는 Chain Forward에 의해 처리되지 못한 트래픽이 모두 받아들여지고, DROP을 선택한 경우에는 모두 폐기됩니다.



5. [SAVE] 버튼을 클릭하면, <Chain Policy> 화면에서 변경된 설정을 확인할 수 있습니다.



6. 방화벽(Firewall) 설정하기

Chain Forward 설정하기

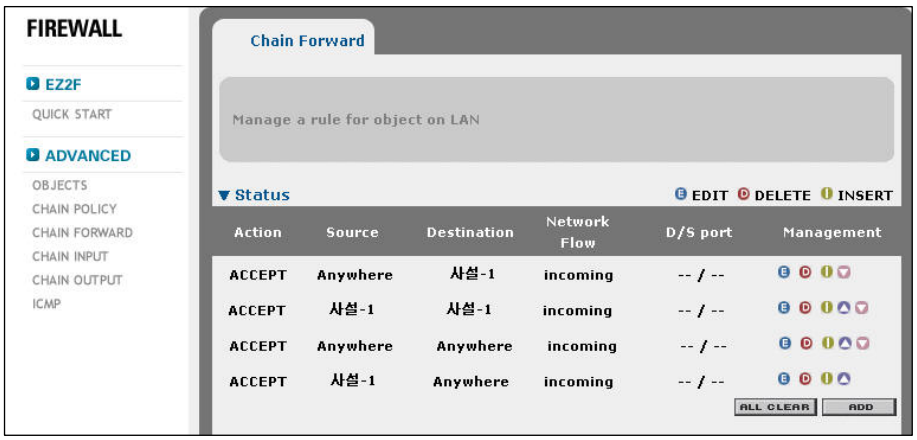
이 절에서는 Forward 정책을 추가하고, 수정하고, 삭제하는 방법에 대해 살펴봅니다.

Forward 정책 추가하기

Chain Forward에 Forward 정책을 추가하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 FIREWALL - FILTER - CHAIN FORWARD 메뉴를 클릭합니다.

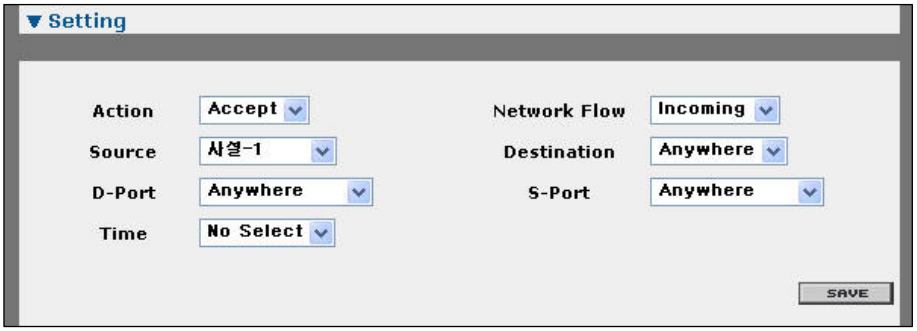
2. 다음과 같은 <Chain Forward> 화면이 나타납니다. <Chain Forward> 화면에는 현재 정의된 Forward 정책들이 출력됩니다.



3. Forward 정책을 삽입할 위치의 Manage 항목에 있는 (I) 아이콘을 클릭하거나 [ADD] 버튼을 클릭합니다. (I) 아이콘을 클릭한 경우에는 해당 Forward 정책의 다음 위치에 새로운 정책이 추가되고, [ADD] 버튼을 클릭한 경우에는 가장 아래쪽에 새로운 정책이 추가됩니다. Forward 정책의 위치가 가지는 의미는 "Forward 정책 우선 순위 변경하기" 절의 내용을 참고합니다.

4. 추가할 Forward 정책에 대한 정보를 입력할 수 있는 <Setting> 화면이 나타납니다.

6. 방화벽(Firewall) 설정하기



다음 설명을 참고하여 각 항목의 값을 설정합니다.

1. Action 항목에 이 Forward 정책의 조건에 일치하는 트래픽의 처리 방법을 지정합니다.
   - accept : 해당 트래픽을 받아들입니다.
   - drop : 해당 트래픽을 폐기합니다.
2. 나머지 5개의 항목들에서는 이 Forward 정책을 적용할 트래픽의 조건을 지정합니다. 이 조건에 만족하는 트래픽은 ① Action 항목에서 지정한 대로 처리됩니다. 항목을 Anywhere를 선택하면 해당 조건은 무시됩니다.

2-1. Network Flow : 수신되는 트래픽에 적용할지 전송되는 트래픽에 적용할지 지정합니다.
   - Incoming : 수신되는 트래픽
   - Outgoing : 전송되는 트래픽

2-2. Source : 정책을 적용할 트래픽의 전송지 네트워크를 선택합니다.

2-3. Destination : 정책을 적용할 트래픽의 목적지 호스트를 선택합니다.

2-4. D-Port : 정책을 적용할 트래픽의 목적지 서비스 포트를 선택합니다.

2-5. S-Port : 정책을 적용할 트래픽의 전송지 서비스 포트를 선택합니다.

5. 조건을 보다 상세하게 설정해야 하는 경우에는 [Advanced] 버튼을 클릭합니다. 그러면, 다음과 같이 5개의 항목이 추가로 나타납니다.

6. 방화벽(Firewall) 설정하기

아래 설명을 참고하여 각 항목의 값을 설정합니다. 항목을 조건으로 사용하지 않는 경우에는 "ignored"를 선택합니다.

① Connection State : 어떤 상태의 링크를 통해 송수신되는 트래픽에 정책을 적용할 것인지 지정합니다.
- new : 새로운 접속을 만드는 패킷
- established : 이미 연결되어 있던 링크
- related : 기존 접속의 부분은 아니지만 연관성을 가진 패킷으로 ICMP에러나, ftp접속을 형성하는 패킷
- invalid : 어떤 이유이건 확인할 수 없는 패킷

② Fragmentation : 나누어져 있는(framgentated) 패킷에 정책을 적용할지 여부를 지정합니다.
- equals : 나눠져 있는 패킷에만 정책 적용
- Not_equals : 나눠져 있지 않은 패킷에만 정책 적용

③ Ethernet : 오른쪽 입력란에 MAC 어드레스를 입력한 후, 이 MAC 어드레스와 일치하는 호스트에만 정책을 적용할지를 지정합니다.
- equals : 입력한 MAC 어드레스와 일치하는 호스트에만 정책 적용
- Not_equals : 입력한 MAC 어드레스와 일치하지 않는 호스트에만 정책 적용

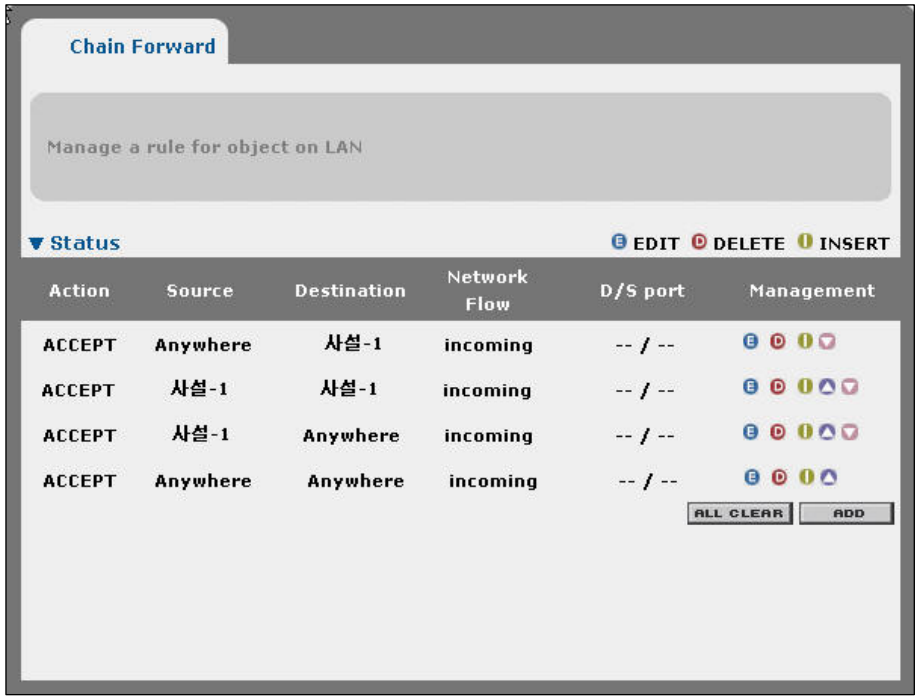
④ Packet Type : 오른쪽 콤보 박스에서 선택한 종류의 ICMP 패킷에 정책을 적용할지 여부를 지정합니다.
- equals : 선택한 종류의 패킷에만 정책 적용
- Not_equals : 선택한 종류의 패킷이 아닌 경우에만 정책 적용

⑤ Service Type : 오른쪽 콤보 박스에서 선택한 종류의 서비스 패킷에 정책을 적용할지 여부를 지정합니다.

- equals : 선택한 종류의 패킷에만 정책 적용
- Not_equals : 선택한 종류의 패킷이 아닌 경우에만 정책 적용

6. 항목의 값을 모두 설정한 후 [SAVE] 버튼을 클릭합니다.

7. <Chain Forward> 화면에서 추가한 Forward 정책을 확인할 수 있습니다.



6. 방화벽(Firewall) 설정하기

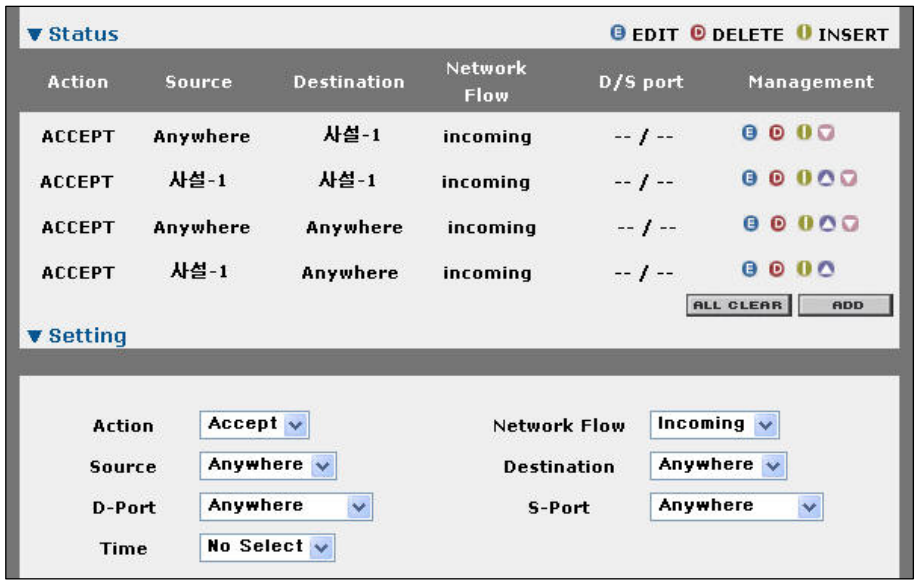
Forward 정책 수정하기

정의되어 있는 Forward 정책을 수정하는 방법은 다음과 같습니다.

1. 웹 콘솔에서 FIREWALL - FILTER - CHAIN FORWARD 메뉴를 클릭합니다.

2. 다음과 같은 <Chain Forward> 화면이 나타납니다. <Chain Forward> 화면에 출력된 Forward 정책 중에서 수정할 정책의 Manage 항목에 있는 (E) 버튼을 클릭합니다.

3. 선택한 Forward 정책의 현재 설정을 보여주는 <Setting> 화면이 나타납니다. 앞에서 살펴본 "Forward 정책 추가하기" 절의 내용을 참고하여 원하는 항목의 값을 다시 설정합니다.



4. 원하는 항목의 값을 모두 변경한 후 [SAVE] 버튼을 클릭합니다.

5. <Chain Forward> 화면에서 변경된 Forward 정책을 확인할 수 있습니다.

Forward 정책 우선 순위 변경하기

Forward chain이 정의되어 있으면, 트래픽이 전송되거나 수신될 때, 가장 위에 있는 Forward 정책의 조건을 트래픽과 비교하게 됩니다. 만약 트래픽이 해당 정책의 조건에 만족되면 정책의 action에 따라 처리되고, 그렇지 않으면 다음 위치에 있는 Forward 정책의 조건과 비교하게 됩니다. 가장 마지막에 있는 Forward 정책의 조건과도 일치하지 않으면 Chain policy에 정의된 action에 따라 처리됩니다.

이와 같이 트래픽은 Forward 정책의 순서에 따라 비교되므로, 다른 Forward 정책보다 우선적으로 트래픽과 비교해야 하는 Forward 정책은 위쪽에 위치해야 합니다. 그렇지 않는 정책은 아래쪽으로 위치해야 합니다. 기본적으로 정의된 순서에 따라 Forward 정책이 위치하게 되므로 가장 먼저 정의된 정책이 가장 위에 놓여져서 가장 높은 우선 순위를 가지게 됩니다.

이러한 Forward 정책의 위치는 다음과 같은 방법으로 변경할 수 있습니다.

1. 웹 콘솔에서 FIREWALL - FILTER - CHAIN FORWARD 메뉴를 클릭합니다.

2. 다음과 같은 <Chain Forward> 화면이 나타납니다.

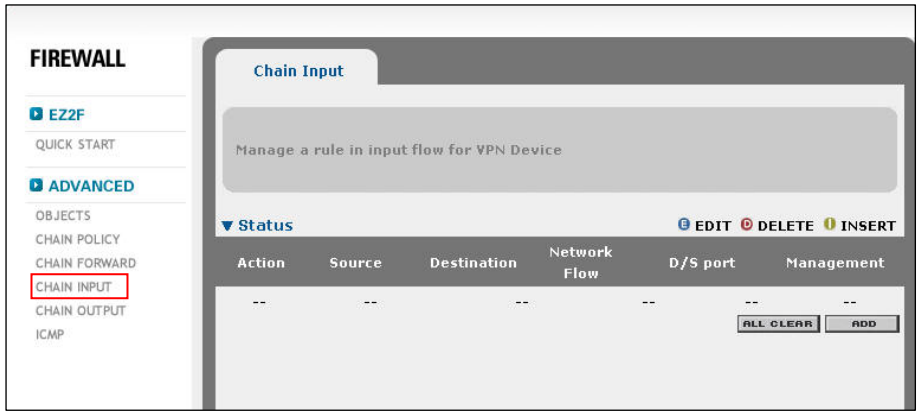
6. 방화벽(Firewall) 설정하기

<Chain Forward> 화면에 출력된 Forward 정책 중에서 위치를 변경할 정책의 Manage 항목에 있는 다음 아이콘들을 클릭합니다.

- ▼ : 이 아이콘을 클릭하면, 선택한 Forward 정책이 한 단계 위의 위치로 이동합니다.
- ▲ : 이 아이콘을 클릭하면, 선택한 Forward 정책이 한 단계 아래로 이동합니다.

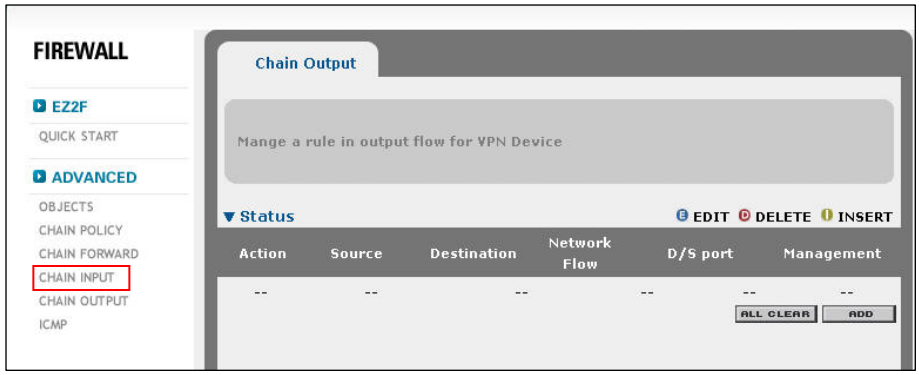
3. [SAVE] 버튼을 눌러서 변경 사항을 장비에 적용합니다.

<FIREWALL – ADVANCED – CHAIN INPUT>

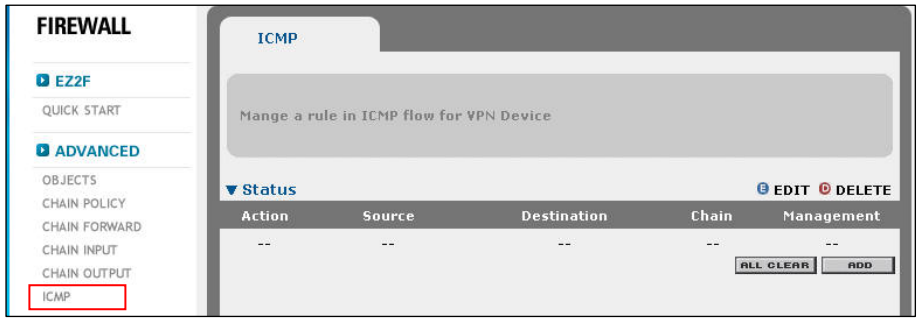


6. 방화벽(Firewall) 설정하기

<FIREWALL – ADVANCED – CHAIN OUTPUT>



<FIREWALL – ADVANCED – ICMP>



Chapter

7

QoS(Quality of Service) 설정하기

이 장에서는 웹 콘솔의 'QoS" 메뉴를 사용하여 R2SKY 시리즈에 QoS 기능을 설정하는 방법을 소개합니다.QoS 기능은 다음 버전에서 지원될 예정입니다.

7. QOS(Quality of Service)설정하기

QOS

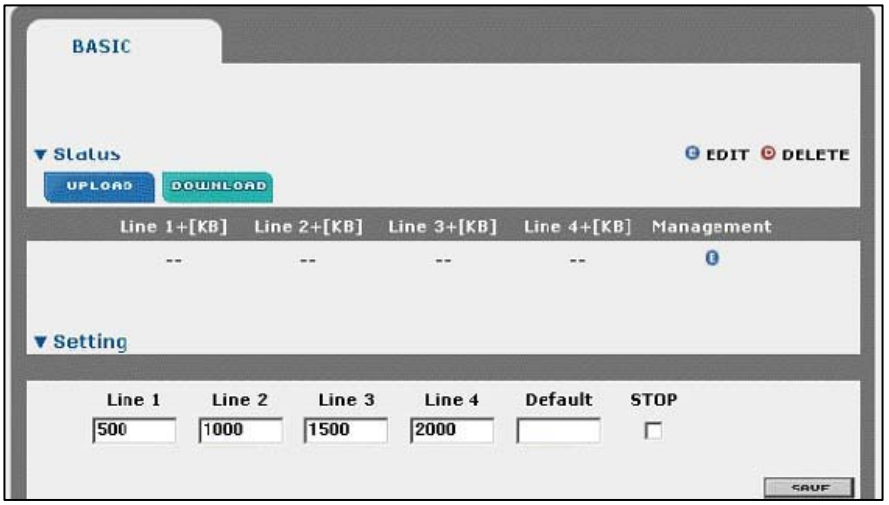
R2SKY 시리즈 웹콘솔에서 QOS기능을 설정하는 과정은 다음과 같습니다.

1. 대상(OBJECT) 등록하기
   먼저 QOS를 적용할 대상(OBJECT)를 등록합니다.
2. BASIC설정
   현재 각 라인의 다운로드 bandwidth, 업로드 bandwidth를 등록합니다
3. UPLOAD RULE, DOWNLOAD RULE
   네트워크와 호스트, 서비스(오브젝트)등을 등록한 후에는 이 값들을 보장해줄 대역폭과 우선순위를 지정하는 곳 입니다.

우선순위에 다른 각 서비스에 할당되는 대역폭

다음 절에서는 각 과정의 설치방법에 대해서 상세하게 알아봅시다

1. 대상(OBJECT)등록하기
   방화벽 설정의 대상(OBJECT) 설정과 같습니다. 각각의 대상(OBJECT)는 방화벽부분과 공유됩니다.
2. BASIC (업로드, 다운로드 bandwith를 지정합니다)



7. QOS(Quality of Service)설정하기

LINE1 초고속 ADSL의 해당 밴드위스를 적어주세요
LINE2 초고속 ADSL의 LINE1 + LINE2 의 해당 밴드위스를 넣어주세요
LINE3 초고속 ADSL의 LINE1 + LINE2 + LINE3 의 해당 밴드위스를 넣어주세요
LINE4 초고속 ADSL의 LINE1 + LINE2 + LINE3 + LINE4 의 해당 밴드위스를 넣어주세요

디폴트는 LINE1 LINE2 LINE3 LINE4를 셋팅 하지 않고 현재의 밴드위스를 적어 넣는 곳입니다

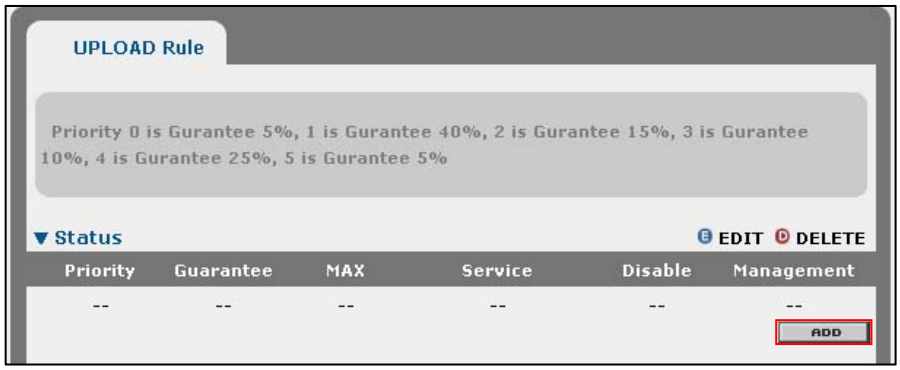
Stop은 QOS 적용하기 싫으면 클릭하세요
다운로드 쪽 bandwith 지정 위와 동일합니다.

3. UPLOAD RULE

7. QOS(Quality of Service)설정하기

1. 웹 콘솔에서 QOS-UPLOAD RULE을 클릭합니다.

2. ADD button을 누릅니다.



3. 화면 아래에 선택한 QOS 규칙에 대한 설정 값을 입력 할 수 있는 Setting 화면이 나옵니다.

7. QOS(Quality of Service)설정하기

다음 설명을 참고하여 각 항목의 값을 지정합니다.

1. priority – 조건을 만족하는 트래픽의 우선 순위를 지정합니다.
2. Source PORT – destination 항목은 추가하는 QOS규칙을 적용할 트래픽을 정의하는 항목들입니다. 이 항목들에 설정된 조건과 일치하는 트래픽에 이 QOS 규칙이 적용됩니다. 항목의 값을 Antwhere로 지정하면 해당항목의 조건은 무시됩니다. 하지만 Source PORT와 Destination PORT항목 중 하나는 반드시 ANYWHERE가 아닌 다른 값으로 설정해야 합니다.
   - 2.1 Source PORT : select 박스를 클릭한 후 QOS규칙을 적용할 트래픽의 전송지 서비스를 선택합니다.
   - 2.2 Destination PORT : select 박스를 클릭한 후 QOS규칙을 적용할 트래픽의 목적지 서비스를 선택합니다.
   - 2.3 Source IP : select 박스를 클릭한 후 QOS규칙을 적용할 트래픽의 전송호스트를 선택합니다.
   - 2.4 Destination IP : select 박스를 클릭한 후 QOS규칙을 적용할 트래픽의 전송지 호스트를 선택합니다.

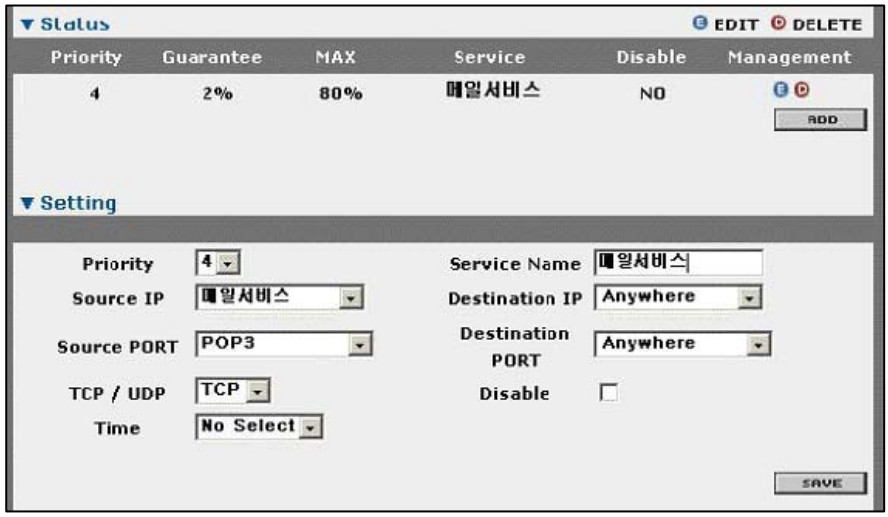
4. 항목을 모두 설정한 후 [SAVE] 버튼을 클릭합니다.

5. 추가된 QOS규칙을 확인할 수 있습니다.

정의 되어 있는 QOS 규칙을 수정하는 방법은 다음과 같습니다.

1. 추가된 QOS규칙의 Manage 항목에 있는 [E] 버튼을 클릭합니다.

2. 선택한 QOS규칙의 현재 설정을 보여주는 [Setting> 화면이 나타납니다. 앞에서 살펴본 내용대로 질의 내용을 참고하여 원하는 항목의 값을 다시 설정합니다.



3. 원하는 항목의 값을 모두 변경한 후 [Save] 버튼을 클릭합니다.

7. QOS(Quality of Service)설정하기

QOS 규칙 우선 순위 변경하기

QOS 구칙이 정의되어 있으면 트래픽이 전송되거나 수신될 때 가장 위에 있는 QOS규칙의 조건을 트래픽과 비교하게 됩니다. 만약 트래픽이 해당 정책의 조건에 만족되려면 QOS규칙에 정해진 대역폭과 우선순위를 할당 받게 되고 그렇지 않으면 다음 QOS규칙의 조건과 비교하게 됩니다.

이와 같이 트래픽은 QOS규칙의 순서에 따라 비교 되므로 다른 QOS규칙보다 우선적으로 트래픽과 비교해야 하는 QOS규칙은 위쪽에 위치해야 합니다. 그렇지 않는 QOS규칙은 아래쪽으로 위치해야 합니다. 기본적으로 정의된 순서에 따라 QOS규칙이 위치하게 되는데 가장 먼저 정의된 QOS규칙이 가장 위에 놓여져서 가장 높은 우선순위를 가지게 됩니다.
이러한 QOS규칙의 위치는 다음과 같은 방법으로 변경할 수 있습니다.

1. 웹 콘솔에서 QOS – UPLOAD RULE 메뉴를 클릭합니다.
2. 다음과 같은 <rules>화면이 나타납니다.
3. <rules>화면이 출력된 QOS규칙 중에서 위치를 변경할 규칙의 Manage항목에 있는 다음 아이콘들을 출력합니다.
   : - 이 아이콘을 클릭하면 선택한 QOS규칙이 한 단계 위의 위치로 이동합니다.
   : - 이 아이콘을 클릭하면 선택한 QOS규칙이 한 단계 아래로 이동합니다.
4. 아이콘을 클릭 할 때마다 QOS규칙의 위치가 화면에 변경되어 표시 됩니다.

정의된 QOS규칙이 다음과 같은 방법으로 삭제할수 있습니다.
1. 웹 콘솔에서 QOS-UPLOAD RULE 메뉴를 클릭합니다.
2. 다음과 같은 화면이 나타납니다. 화면에 출력된 QOS규칙 중에서 삭제할 규칙의 Manage항목에 있는 (D)아이콘을 클릭합니다.
3. 선택한 QOS규칙의 삭제여부를 확인하는 다음과 같은 화면이 나타납니다.
   [확인]을 클릭합니다.
4. 다음과 같이 선택된 QOS규칙이 화면에서 삭제된 것을 확인할 수 있습니다.

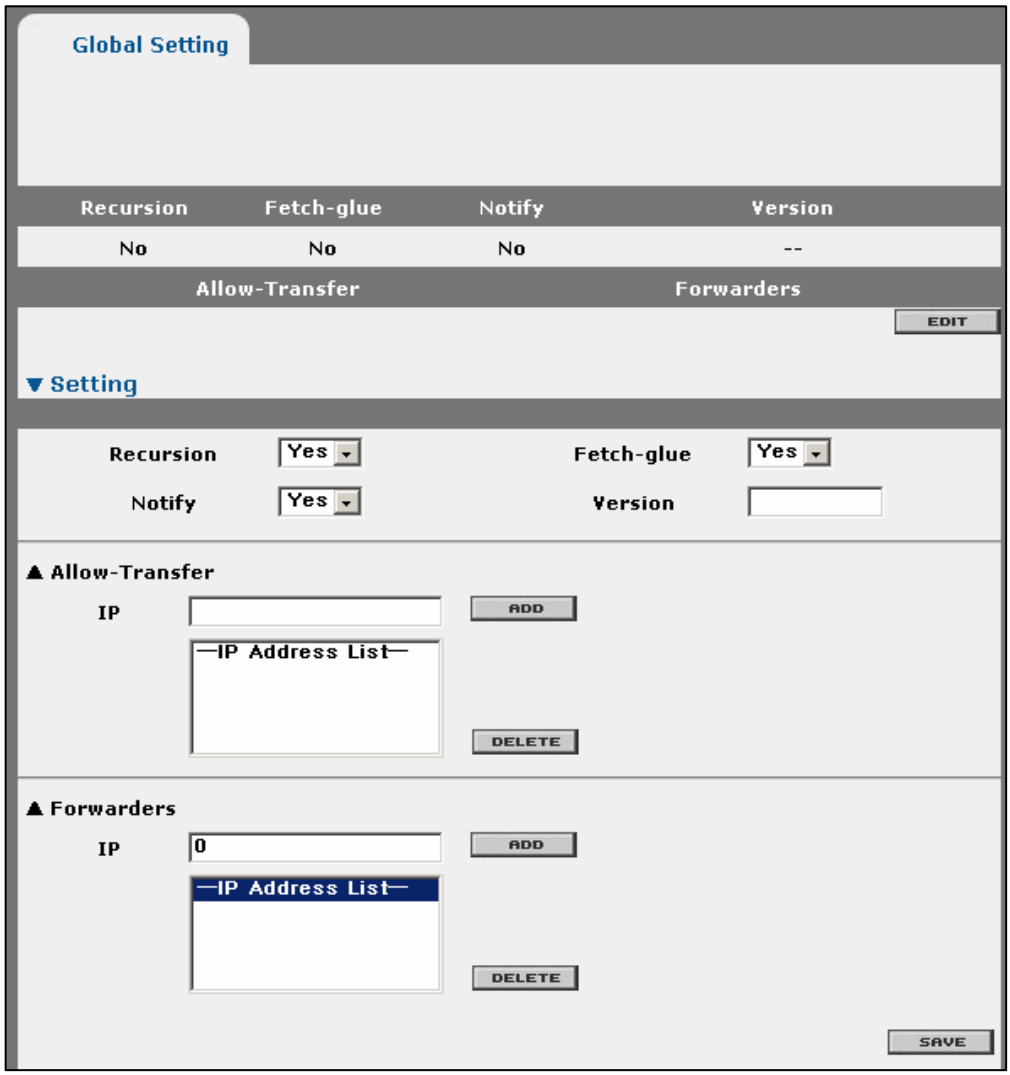
Chapter

8

DNS 설정하기

8. DNS 설정하기

웹 콘솔에서 DNS - DNS – GLOBAL SETTING 메뉴를 클릭합니다.



allow-transfer : DNS 영역의 전달을 주어진 IP 주소로 제한합니다.

Notify : Primary와 Secondary 네임서버의 동적 동기화를 가능하게 합니다.

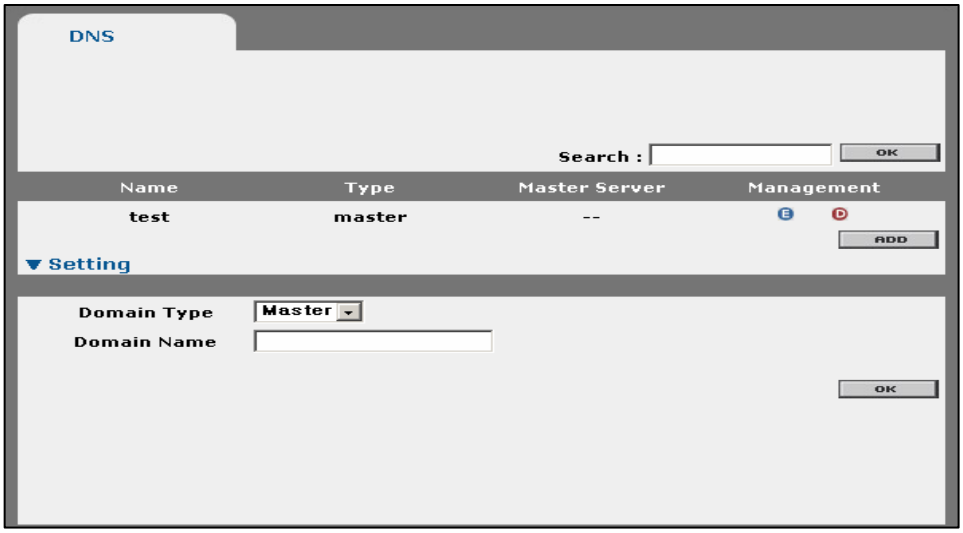
Forwarders : 스스로 응답할 수 없는 질의를 지정한 서버로 보냅니다..

Recursion : 재귀 기능

Fetch-glue : 응답 시 붙박이 데이터를 가져올지 말지 결정합니다..

8. DNS 설정하기

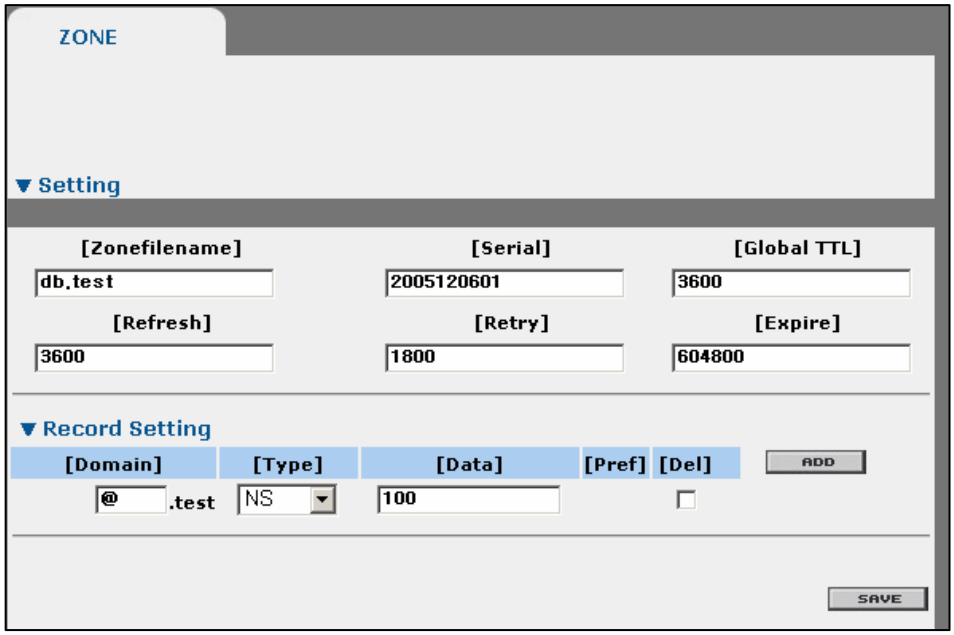
웹 콘솔에서 DNS - DNS - DNS SETTING 메뉴를 클릭합니다.



Domain Type : Master(특정zone과 관련된 모든 정보에 대한 권한을 가진다.)
Slave(마스터 서버로부터 해당 zone의 모든 정보를 전송 받는다.)
Domain Name : 도메인 이름을 입력합니다.

8. DNS 설정하기

Master Setting일 경우



Zonefilename : DNS Server가 가지고 있는 정보를 소유하는 파일

Serial : Serial은 Secondary가 Zone 파일의 수정여부를 알 수 있도록 하기 위함입니다. Serial의 표기는 증가하는 임의 숫자보단 일반적으로 최종 수정 일을 YYYYMMDDNN의 형식으로 표기합니다

Global TTL : 도메인의 캐시 값을 의미합니다.

Refresh : Primary측의 Zone 데이터베이스 수정여부를 Secondary가 검사하는 주기입니다.

Retry : Secondary측에서, Primary와 연결이 안될 경우, 재 시도 시간 주기입니다.

8. DNS 설정하기

Expire : Secondary가 Expire로 지정된 시간 동안 Primary에 연결하지 못할 경우, 오래된 백업카피의 자료가 더 이상 유효하지 않다고 보고, 해당 도메인에 대한 답변을 하지 않습니다.

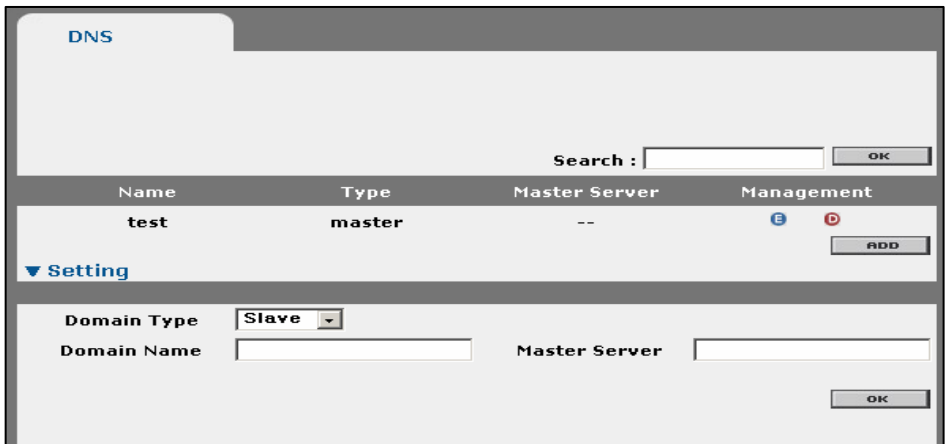
Record Setting에서 추가하고자 하는 레코드 타입을 결정하여 레코드를 추가합니다.

- NS는 (NAME SERVER) 레코드를 말합니다. 즉 네임서버임을 지정하는 레코드입니다.

- A (Address) 즉, 도메인 명을 IP 주소로 지정할 때 쓰입니다

- PTR 역으로 IP주소를 도메인 명으로 지정할 때 쓰입니다.
- CNAME은 일종의 별명(alias)를 지정할 때 쓰입니다. Canonical Name 레코드입니다.
- MX는 메일 익스체인저를 지정합니다.

Slave Setting일 경우



Appendixt A

제품과 케이블 사양

이 장에서는 R2SKY 시리즈의 제품 사양과 제품 설치 시 사용되는 케이블에 대한 사양이 정리되어 있습니다.

A. 제품과 케이블 사양

제품 사양

항목		사 양	
		R2SKY 4000	R2SKY 5000
프로세서 성능		2.0GHz	800MHz
제품 높이		2U	1U
콘솔 포트		1개의 콘솔 포트(CONSOLE, RJ-11)	1개의 콘솔 포트(CONSOLE, RJ-45)
최대 세션 수		1,250,000	2,344,000
LAN 포트		4(5)개의 10/100Base-TX 포트(LAN0 ~ 3(4), RJ-45)	
메모리		· 메인 메모리 : 256MBit · 플래시 메모리 : 64MBit	
LED	시스템 상태	· POWER : 전원 공급 상태 (초록색, 켜짐) · RUN : 플래시 메모리 액세스 상태 (빨간색, 깜박임)	
	포트 상태	· LINK : 상대 장비와의 연결 상태 (초록색, 켜짐) · ACT: 데이터 송수신 여부 (주황색, 깜박임)	
포장물품	랙설치 kit	· 접시 머리 나사 6개 · 바인드 머리 나사 4개 · 랙 브라켓 2개	
	케이블	· 콘솔 케이블 1개 · 전원 케이블 : R2SKY 4000(1개), R2SKY 5000(2개) · UTP 크로스케이블(straight 타입) 2개	
	매뉴얼	· 사용 설명서 1부	
사용환경	온도	· 규정 동작 온도 : 0~50° C · 동작 가능 온도 : -10~50° C · 보관 온도 : -40~80° C	
	습도	· 동작 습도 : 15~95% (40° C, 비응결 시) · 보관 습도 : 15~95% (65° C, 비응결 시)	

A. 제품과 케이블 사양

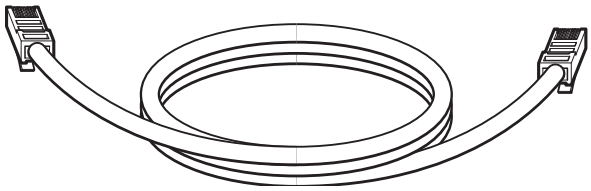
항 목	사 양	
	R2SKY 4000	R2SKY 5000
전원	· 주파수 : 50/60Hz · 입력 전압 : 100~240VAC · 소비 전력 : 최대 200W (R2SKY 5000에서 이중화할 경우 최대 200W 추가) · 전원 이중화 (R2SKY 5000)	
보안 기능	· 액세스 리스트 (access list) · 방화벽	
관리 기능	· 콘솔 – Remote : Telnet 및 Web 기반의 콘솔 (in-band) – Local : RS232 콘솔 포트 (out-band) · LED – 시스템 상태 LED : POWER, RUN – 포트 상태 LED : LINK, ACT · SNMP v1/v2c	
부가 기능	· DHCP 서버 · QOS	

A. 제품과 케이블 사양

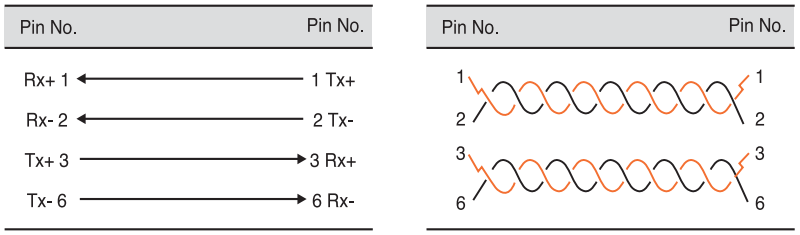
케이블 사양

Twisted Pair 케이블

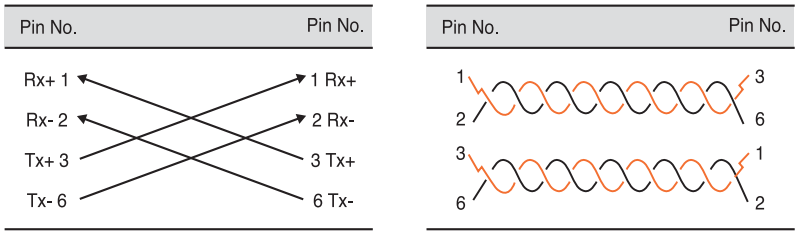
R2SKY 시리즈에 있는 LAN 포트들(LAN0 ~ LAN3(4))은 다음 그림과 같이 양쪽이 RJ-45 커넥터로 된 twisted pair 케이블을 사용하여 다른 장비와 연결합니다.



Twisted pair 케이블에는 shield가 되어 있는지 여부에 따라 UTP(unshielded twisted pair) 케이블과 STP(shielded twisted pair) 케이블의 2가지 종류가 있습니다. 그리고, 양쪽 커넥터의 핀 연결 방식에 따라 straight 타입과 cross 타입으로 나눠집니다. Straight 타입은 양쪽 커넥터에 있는 8개의 핀 모두 같은 번호의 핀과 연결된 것이고, cross 타입은 이와 달리 서로 다른 번호의 핀들이 연결된 것입니다. 일반적으로 사용되는 straight 타입과 cross 타입의 핀 연결은 다음과 같습니다.



Straight 타입



Cross 타입

A. 제품과 케이블 사양

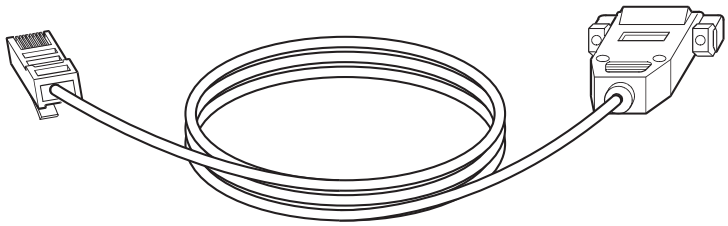
R2SKY 시리즈에 있는 LAN 포트들은 허브나 스위치와 같은 네트웍 장비의 포트와 연결하는 경우에는 straight 타입을, NIC(Network Interface Card)을 장착한 PC와 같은 단말과 연결할 때에는 cross 타입을 사용합니다.

Twisted pair 케이블은 선의 굵기에 따라 category로 분류됩니다. 연결할 장비가 10Mbps 이하의 속도를 지원하는 경우에는 category-3 혹은 4 정도의 케이블을 사용하면 되고, 100Mbps까지 지원하는 경우에는 category-5를 사용해야 합니다.

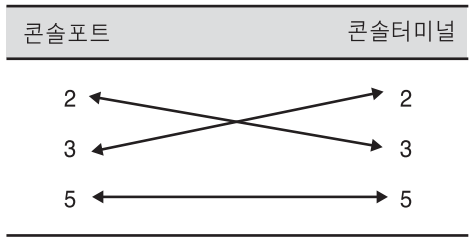
콘솔 케이블

R2SKY 5000

R2SKY 5000에 있는 CONSOLE 포트와 콘솔 터미널을 직접 연결할 때에는 다음과 같이 한쪽이 RJ-45, 다른 한쪽이 DB-9 커넥터인 콘솔 케이블을 사용합니다.



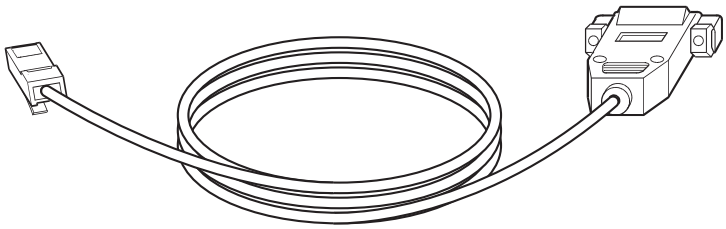
콘솔 케이블은 기본적으로 장비와 함께 제공되는 데, 케이블 양쪽 커넥터의 핀 연결은 다음과 같습니다.



A. 제품과 케이블 사양

R2SKY 4000

R2SKY 4000에 있는 CONSOLE 포트와 콘솔 터미널을 직접 연결할 때에는 다음과 같이 한쪽이 RJ-11, 다른 한쪽이 DB-9 커넥터인 콘솔 케이블을 사용합니다.



콘솔 케이블은 기본적으로 장비와 함께 제공됩니다.

Appendixt B

제품 설치 및 사용시 주의사항

이 장에서는 R2SKY 시리즈를 설치하기 전에 숙지하고 있어야 하는 설치/사용시 주의 사항과 설치 장소가 갖추어야 하는 환경에 대해 설명합니다.

B. 제품 설치 및 사용시 주의사항

주의 사항

경고

이 절에는 R2SKY 시리즈를 설치하고 사용할 때 신체적 손상을 일으킬 수 있는 상황에 대비하여 사용자가 기본적으로 알고 있어야 할 주의 사항에 관해 설명하고 있습니다. R2SKY 시리즈를 설치하거나 사용하기 전에 반드시 여기에서 설명한 내용을 숙지해두도록 합니다.

일반적인 주의 사항

◦ 제품을 설치하는 도중이나 설치한 후에도 제품이 설치된 주변을 깨끗하고 먼지가 없도록 유지해야 합니다.
◦ 제품의 덮개를 열었을 때에는 덮개를 안전한 곳에 놓아두어야 합니다.
◦ 사람이 부상을 당할 수도 있으므로 도구나 케이블 등을 통로에 놓아두지 않도록 합니다.
◦ 제품을 설치할 때 헐렁한 옷이나 넥타이, 스카프, 옷 소매 등이 제품에 끼일 수 있으므로 헐렁한 옷은 입지 않도록 하고, 넥타이나 스카프는 늘어지지 않도록 하며, 소매는 접어서 올리도록 합니다.
◦ 사람이나 장비에 손상을 입힐 수 있는 어떤 행동도 하지 않도록 합니다.
◦ 제품의 성능 확장이나 고장 수리를 위해 제품의 덮개를 열고 작업해야 하는 경우에는 반드시 구입처로 연락하여 전문가의 도움을 받도록 합니다.

전원 관련 주의 사항

◦ 제품에 전원을 연결할 때는 배선에 과부하가 걸리지 않는지 먼저 확인하도록 합니다.
◦ 제품에 전원을 연결할 때에는 반지나 목걸이, 시계와 같은 장신구를 착용하지 않도록 합니다. 이러한 장신구가 전원이나 그라운드에 연결되면 부품이 타버릴 위험이 있습니다.
◦ 작업하는 공간에서 위험이 발생할 소지가 있는지 항상 확인하도록 합니다. 젖은 바닥이나 접지되지 않은 전원 확장 케이블, 닳아서 내부가 보이는 전원 코드, 안전 접지 시설이 되어 있지 않은 바닥 등이 있는지 반드시 확인합니다.

B. 제품 설치 및 사용시 주의사항

AC 전원

◦ 본 제품은 TN 전원 시스템에 연결하도록 설계되어 있습니다. TN 전원 시스템이란 전원 콘센트에 있는 2구 중 1구가 접지에 직접 연결되어 있는 배전 시스템입니다. 제품과 함께 공급되는 전원 코드의 AC 플러그에는 접지 기능이 있습니다.

◦ 전원 코드와 전원 콘센트는 화재와 같은 긴급 상황 발생시 주요 전원 차단 장치의 역할을 하므로, 언제라도 전원 콘센트에서 전원 코드를 뽑을 수 있도록 전원 콘센트 앞에 물건을 쌓아 두거나 막아놓지 않도록 합니다.

DC 전원

◦ DC 전원 공급기는 UL 1950과 CSA 950, EN 60950, 그리고 IEC 60950 표준에 따른 SELV (Safety Extra-Low Voltage) 요구 조건을 만족하는 사양의 외부 DC 전원 공급기나 정류기에 연결하도록 합니다.

◦ DC 고정 배선에는 화재와 같은 긴급 상황 발생 시 바로 사용할 수 있는 양극(-48 VDC, GND) 차단 장치를 연결하도록 합니다.

◦ DC 전원 공급기를 설치하거나 제거하기 전에는 반드시 DC 회로에 전원을 차단했는지 확인합니다. 안전을 위해 DC 회로 차단기의 스위치를 OFF로 두고 테이프로 감아 우연한 접촉으로 인해 스위치가 ON으로 바뀌지 않도록 합니다.

◦ DC 전원 케이블 마감 장치는 배선 크기에 맞아야 하며 절연체와 도체를 모두 조일 수 있어야 합니다.

◦ DC 터미널 블록에 연결되는 DC 전원 케이블이 닿아서 노출된 부분이 없는지 확인하도록 합니다. 케이블의 노출된 부분에는 위험한 수준의 전기가 흐르기 때문에 인체가 닿지 않도록 주의하도록 합니다.

예비 전원

예비 전원 공급기가 장착된 제품을 구입한 경우, 2개의 전원 공급기를 각각 다른 입력 전원에 연결합니다. 그러면 2개의 전원 공급기 중 하나가 고장 났을 때에도 계속해서 장비를 운영할 수 있습니다.

B. 제품 설치 및 사용시 주의사항

정전기 관련 주의 사항

정전기는 장비나 회로에 큰 손상을 입힐 수 있는 요인입니다. 전자 부품을 잘못 다루었을 때 발생하게 되는 정전기는 제품이 일시적으로 오동작하게 하거나 혹은 아예 사용할 수 없게 만들기도 합니다. 그러므로, 제품의 회로를 건드리는 경우에는 정전기 방지를 위해 반드시 다음과 같은 조치를 취하도록 합니다.

◦ 정전기 방지용 스트랩을 착용하고 스트랩의 한쪽 끝은 정전기 방전용 잭이나 제품에 부착된 나사와 같이 도포되지 않은 철 구성 요소에 연결시키도록 합니다.
◦ 정전기 방지용 스트랩이 없는 경우에는 제품의 금속 부분을 손으로 만져서 사용자 자신을 접지하도록 합니다.
◦ 각종 카드의 부품이나 커넥터의 핀을 손으로 절대 만지지 않도록 하며 보드를 만질 때에는 보드의 모서리나 앞면 패널을 이용하도록 합니다.
◦ 카드와 의류가 서로 닿지 않게 합니다. 정전기 방지용 스트랩은 신체의 정전기에 대해서만 보드를 보호하므로 의류에서 발생할 수 있는 정전기는 제품 손상의 원인이 될 수 있습니다.
◦ 안전을 위해 주기적으로 전정기 방지용 스트랩의 저항 값이 1 ~ 10Mohms 사이의 값인지 확인하도록 합니다.

설치 및 서비스 관련 주의 사항

◦ 제품을 설치하기 전에 전원 스위치를 OFF(O 방향)로 두고, 전원 케이블과 포트에 연결되어 있는 케이블은 모두 빼내도록 합니다.
◦ 제품 설치 시 반지나 목걸이, 시계와 같은 장신구를 착용하지 않도록 합니다. 이러한 장신구가 전원이나 그라운드에 연결되면 부품이 타버릴 위험이 있습니다.
◦ 손이나 금속제 공구로 백플레인이나 보드를 만지지 않도록 합니다.
◦ 잠재적 위험이 예상되는 장소에서 혼자 작업하는 일이 없도록 합니다.
◦ 잠재적으로 인체에 위해 하거나 장비를 불안정하게 할 수 있는 어떤 행동도 하지 않도록 합니다.

B. 제품 설치 및 사용시 주의사항

전원 차단 시

제품에 공급되는 전원을 차단하고자 하는 경우에는 다음과 같은 점에 유의합니다.

◦ 제품을 구동시키기 전에 실내에 긴급 전원 차단 스위치를 배치하도록 합니다.

◦ 바로 교체할 수 없는 부품에 관한 작업은 전원을 끄고 회로의 전원 연결을 해제해야 합니다. 제품에 ON/OFF 스위치가 없는 경우에는 전원 코드를 뽑은 상태에서 작업하도록 합니다.

◦ 제품에 공급되는 전원을 완전히 차단하려면 모든 전원 공급 장치에 대한 전원 연결을 해제하도록 합니다.

◦ DC 전원 공급기의 경우, 회로 차단기를 찾아 회로 차단기의 스위치를 OFF로 바꾸고, 회로 차단기의 스위치 OFF로 둔 상태에서 테이프로 감아 고정시키도록 합니다.

◦ 전원 케이블이 연결된 상태에서 전원 공급기를 만지지 않도록 합니다. 전원 스위치를 꺼도 전원 케이블이 연결되어 있으면 전원 공급기 내에 라인 전압이 존재합니다.

접지

◦ AC 전원 공급기를 장착한 제품은 반드시 접지 되어 있는 AC 전원 콘센트에 연결하도록 합니다.

◦ 제품과 함께 공급되는 전원 코드의 AC 전원 플러그에 부착되어 있는 접지용 도체를 제거하지 않도록 합니다.

◦ 시스템을 접지하도록 합니다.

케이블 연결

제품의 각 포트에 케이블을 연결할 때는 다음과 같은 사항에 주의하도록 합니다.

◦ 전화선을 설치하거나 변경할 때 감전 사고를 당하지 않도록 주의합니다.

◦ 번개가 치는 날에는 케이블을 연결하거나 연결된 케이블을 빼내는 등의 작업을 하지 않도록 합니다.

◦ 전화선이 네트워크 인터페이스에서 분리되기 전에는 비절연 상태의 전화선이나 단말기를 손으로 만지지 않도록 합니다.

◦ 시스템 전원과 관계없이 WAN 포트의 경우, 위험한 네트워크 전압이 존재할 수 있습니다. 따라서 케이블을 분리할 때에는 시스템에서 먼 곳에 있는 WAN 포트의 케이블을 먼저 분리하도록 합니다.

◦ 가스가 누출된 장소 근처에서는 전화를 사용하지 않도록 합니다.
◦ 특별히 습기에 강하도록 설계된 잭이 아닌 경우에는 습기가 많은 장소에서는 전화 잭을 설치하지 않도록 합니다.

전자파 간섭 (EMI)

전자기장에서 특정 거리로 배선을 할 경우, 전자기장과 배선 신호 사이에 전자파 간섭(EMI- Electromagnetic Interface)이 발생할 수 있으므로 다음과 같은 점에 유의합니다.

◦ 잘못된 배선은 라디오 주파수 간섭(RFI-Radio Frequency Interference)을 발생시킬 수 있습니다.
◦ 특히 조명이나 라디오 송신기에서 발생하는 EMI 시스템의 신호 구동기와 수신기를 파괴할 수 있으며 배선과 시스템을 통해 서지 전력을 전도시켜 전기 사고가 발생할 수 있습니다.
설치 장소에서 강한 전자파 간섭이 발생하는 경우, 이를 개선하려면 RFI 전문가와 상의하도록 합니다.

랙 설치 관련 주의 사항

19인치 랙에 제품을 설치할 때에는 다음과 같은 점에 유의합니다.

◦ 가능하면 양쪽 옆면과 위, 아랫면이 모두 뚫려있는 개방형 랙을 사용하는 것이 좋습니다. 만약 제품을 밀폐형 랙에 설치해야 하는 경우에는 통풍이 잘 되는지 확인하도록 합니다.
◦ 밀폐형 랙을 사용하는 경우에는 랙에 적절한 통풍 장치가 있는지 확인합니다. 밀폐형 랙의 옆면에는 공기 흡입구가 있어야 하고, 랙에 팬을 부착하여 차가운 공기가 공급될 수 있어야 합니다.
◦ 통풍 팬이 위에 달려있는 밀폐형 랙은 아래 쪽에 장착되어 있는 시스템에서 발생한 초과열이 위로 올라가서 위에 설치되어 있는 시스템의 내부로 들어갈 수 있으므로 주의합니다.
◦ 랙에 이미 설치되어 있는 장비나 케이블이 전원 공급기나 냉각 팬의 공기 흐름을 방해하지 않도록 위치를 잘 조정합니다.
◦ 랙에 안정적으로 제품을 장착할 수 있도록 랙을 바닥에 볼트로 단단히 고정시키도록 합니다.
◦ 무거운 장비일수록 랙의 아래 쪽에 장착하도록 합니다.

B. 제품 설치 및 사용시 주의사항

제품 운반 시 주의 사항

제품을 포장 박스에서 꺼내어 설치 장소로 운반하거나 설치 장소를 변경하는 경우, 제품을 들어 올릴 때는 다음과 같은 점에 유의합니다.

◦ 제품을 옮기기 전에 전원을 끄고 각 포트에 연결된 케이블을 분리하도록 합니다.

◦ 제품을 옮길 작업자의 경우, 발을 바닥에 단단히 고정시키고 제품의 중량이 작업자의 두 발에 균일하게 분배되었는지 확인하도록 합니다.

◦ 허리를 편 상태를 유지하면 천천히 제품을 들어올립니다. 이 때 허리를 구부려 제품을 들어올리면 허리에 손상이 갈 수 있으므로 허리 대신 무릎을 구부려 제품을 들어올리도록 합니다.

◦ 제품의 중량에 따라 다음과 같이 필요한 인원의 작업자가 함께 제품을 들어서 옮기거나 기중기를 이용하도록 합니다.

제품의 무게	필요한 인원
18Kg 이하	1명
18~32Kg	2명
32~55Kg	3명
55Kg 이상	기중기 이용

제품 폐기 관련 주의 사항

제품을 폐기할 때는 중앙정부 및 지방 자치단체의 규정을 준수하여 시스템 본체와 전원 공급기 및 각종 부품을 폐기하도록 합니다.

B. 제품 설치 및 사용시 주의사항

설치 장소

설치 장소의 환경

R2SKY 시리즈를 안전하게 설치하고 사용하기 위해서는 설치 장소가 다음과 같은 요건들이 갖추어져 있어야 합니다.

◦ 시스템을 설치하는 중이거나 설치한 후에도 먼지가 없이 항상 깨끗하게 유지되어야 합니다.

◦ 직사광선이 비치지 않는 서늘한 장소에 시스템을 설치하고, 장비나 도구를 사람들이 왕래하는 장소에서 멀리 떨어지게 두어서 다치지 않도록 합니다.

◦ 다음과 같은 온도와 습도가 항상 일정하게 유지되는 장소여야 합니다.

항 목	값
동작 온도	0~50℃
보관 온도	-40~80℃
동작 습도	15~95% (45℃, 비응결 시)
보관 습도	15~95% (65℃, 비응결 시)

전원 공급

◦ R2SKY 시리즈는 다음과 같은 전원이 공급되는 장소에 설치해야 합니다.

항 목	값
입력 전압	110~220VAC
입력 전압 범위	88~264VAC
주파수	50/60Hz

◦ 설치 장소에 공급되는 전원이 깨끗한지 확인합니다. 스파크나 노이즈가 많은 전원이 공급되는 경우에는 전원 조절 장치를 설치하는 것이 좋습니다.

◦ 스위치 근처에 전원 콘센트를 두어서 전원 케이블을 쉽게 연결할 수 있도록 해야 합니다.

◦ 배선에 과부하가 걸리지 않도록 전원 공급 장치를 연결할 때 주의를 기울이도록 합니다.

Rev.00

elim.net

(주)엘림넷

서울시 서대문구 충정로3가 32-11 엘림넷 빌딩
TEL:02-3149-4900 FAX:02-3149-4998
http://www.elim.net

elimnet Bldg, 32-11 Chungjeongno 3-ga,
Seodaemun-Ku, Seoul 120-837,Korea
TEL:02-3149-4900 FAX:02-3149-4998
http://www.elim.net