

# Dell™ PowerConnect™ 34XX 시스템 사용 설명서

[소개](#)

[하드웨어 설명](#)

[PowerConnect 3424/P 및 PowerConnect 3448/P 설치](#)

[PowerConnect 3424/P 및 3448/P 구성](#)

[Dell OpenManage 스위치 관리자 사용](#)

[시스템 정보 구성](#)

[스위치 정보 구성](#)

[통계 보기](#)

[QoS\(서비스 품질\) 구성](#)

[참치 기능 상호작용 정보](#)

[용어집](#)

---

## 참고, 알림, 주의



**주:** 참고는 컴퓨터를 보다 효율적으로 사용하는데 도움이 되는 중요 정보를 제공합니다.



**알림:** 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.



**주의:** 주의는 위험한 상황, 심각한 부상 또는 사망할 우려가 있음을 알려줍니다.

---

본 설명서에 수록된 정보는 사전 통보 없이 변경될 수 있습니다.  
© 2005 Dell Inc. 저작권 본사 소유.

어떠한 경우에도 Dell Inc.의 사전 승인 없이 무단 복제하는 행위는 엄격하게 금지되어 있습니다.

본 설명서에 사용된 상표: Dell, Dell OpenManage, DELL 로고, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet 및 Latitude는 Dell Inc.의 상표입니다. Microsoft 및 Windows는 Microsoft Corporation의 등록 상표입니다.

본 설명서에서 특정 회사의 표시나 제품 이름을 지칭하기 위해 기타 상표나 상호를 사용할 수도 있습니다. Dell Inc.는 자사가 소유하고 있는 것 이외에 기타 모든 등록 상표 및 상표명에 대한 어떠한 소유권도 없습니다.

2005년 3월

[목차 페이지로 돌아가기](#)

## 소개

### Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [시스템 설명](#)
- [스태킹 개요](#)
- [기능 개요](#)
- [추가 CLI 설명서](#)

PowerConnect 3424/3448 및 PowerConnect 3424P/3448P는 스택 가능한 고급 다중 장치입니다. PowerConnect 단원은 독립 실행형 다중 층 전환 장치나 최대 6개의 스택링 구성요소를 가진 스택 가능한 장치로 작동할 수 있습니다.

이 **사용 설명서**에는 장치를 설치, 구성 및 유지하는 데 필요한 정보가 수록되어 있습니다.

## 시스템 설명

PowerConnect 3424/3448 및 PowerConnect 3424P/3448P는 융통성과 최소 관리를 결합하였습니다. PowerConnect 3424 및 3448 시리즈에는 다음의 장치 유형을 포함합니다.

- 1 [PowerConnect 3424](#)
- 1 [PowerConnect 3424P](#)
- 1 [PowerConnect 3448](#)
- 1 [PowerConnect 3448P](#)

### PowerConnect 3424

PowerConnect 3424는 24개의 10/100Mbps 포트, 2개의 SFP 포트 및 독립 실행형 장치에서 처리량을 전달하는 데 사용하거나 장치가 스택된 경우 스택링 포트에 사용하는 2개의 구리 포트를 제공합니다. 또한 하나의 RS-232 콘솔 포트도 제공합니다. PowerConnect 3424는 스택 가능한 장치이지만 독립 실행형 장치로도 작동합니다.

### PowerConnect 3424P

PowerConnect 3424P는 24개의 10/100Mbps 포트, 2개의 SFP 포트 및 독립 실행형 장치에서 처리량을 전달하는 데 사용하거나 장치가 스택된 경우 스택링 포트에 사용하는 2개의 구리 포트를 제공합니다. 또한 하나의 RS-232 콘솔 포트도 제공합니다. PowerConnect 3424P는 스택 가능한 장치이지만 독립 실행형 장치로도 작동합니다. PowerConnect 3424P는 PoE(이더넷 상의 전원)도 제공합니다.

그림 1-1. PowerConnect 3424 및 PowerConnect 3424P



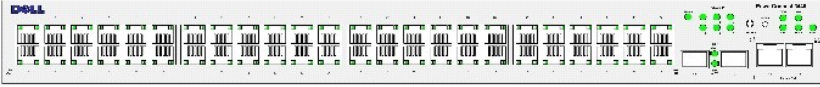
### PowerConnect 3448

PowerConnect 3448는 48개의 10/100Mbps 포트, 2개의 SFP 포트 및 독립 실행형 장치에서 처리량을 전달하는 데 사용하거나 장치가 스택된 경우 스택링 포트에 사용하는 2개의 구리 포트를 제공합니다. 또한 하나의 RS-232 콘솔 포트도 제공합니다. PowerConnect 3448는 스택 가능한 장치이지만 독립 실행형 장치로도 작동합니다.

### PowerConnect 3448P

PowerConnect 3448P는 48개의 10/100Mbps 포트, 2개의 SFP 포트 및 장치가 독립 실행형 모드일 경우 처리량을 전달하는 데 사용하거나 장치가 스택의 한 부분일 경우 스택링 포트에 사용하는 구리 포트 2개를 제공합니다. 또한 장치는 하나의 RS-232 콘솔 포트를 제공합니다. PowerConnect 3448P는 추가로 PoE를 제공합니다.

그림 1-2. PowerConnect 3448 및 PowerConnect 3448P



## 스태킹 개요

PowerConnect 3424/P 및 PowerConnect 3448/P 스택킹은 모든 스택 구성요소가 단일 단원인 것처럼 단일 점을 통해 다중 스위치 관리를 제공합니다. 모든 스택 구성요소는 스택을 관리하는 단일 IP 주소를 통해 액세스됩니다. 스택은 다음에서 관리합니다.

- 1 웹 기반 인터페이스
- 1 SNMP 관리 스테이션
- 1 CLI(명령줄 인터페이스)

PowerConnect 3424/P 및 PowerConnect 3448/P 장치는 스택당 최대 6개 단원의 스택킹을 지원하거나 독립 실행형 단원으로 작동할 수 있습니다.

스태킹 설정 동안, 한 스위치를 스택 마스터로 선택하고 다른 스택 구성요소를 백업 마스터로 선택할 수 있습니다. 모든 다른 장치는 스택 구성요소로 선택되고 고유 단원 ID가 할당됩니다.

각 스택 구성요소에 스위치 소프트웨어가 별도로 다운로드됩니다. 그러나, 스택의 모든 단원은 동일한 소프트웨어 버전을 실행해야 합니다.

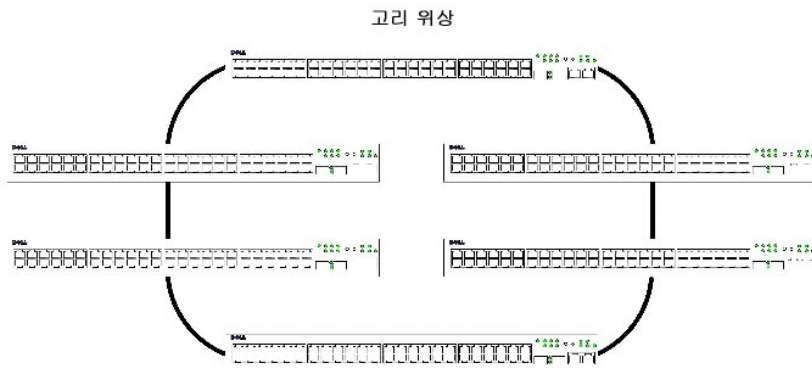
스위치 스택 및 구성은 스택 마스터에 의해 유지됩니다. 다음의 경우 스택 마스터는 최소 작동 영향으로 포트를 감지하고 재구성합니다.

- 1 단원 오류
- 1 내부 단원 스택킹 연결 오류
- 1 단원 삽입
- 1 스택킹 단원 제거

## 스택 위상 이해

PowerConnect 3400 시리즈는 링형 위상으로 작동합니다. 스택킹 링형 위상은 스택의 모든 장치가 상호 연결되어 원을 구성하는 곳입니다. 스택의 각 장치는 연결되어 있는 장치에 데이터를 송수신합니다. 패킷은 해당 목적지에 도착할 때까지 계속 스택을 통과합니다. 시스템은 처리량을 전송하는 최적의 경로를 발생합니다.

그림 1-3. 스택킹 고리형 위상



고리형 위상에서 발생된 대부분의 장애는 고리의 장치가 작동할 수 없게 되거나 연결이 끊긴 경우 발생합니다. PowerConnect 3424/P 및 PowerConnect 3448/P 스택을 통해 시스템은 시스템 장치 시간없이 자동으로 스택킹 오류 복구 위상으로 전환합니다. SNMP 메시지는 자동으로 생성되지만 스택 관리 동작은 필요하지 않습니다. 그러나, 스택킹 무결성을 확보하려면 스택킹 연결이나 스택 구성요소를 복구해야 합니다.

스테킹 문제를 해결한 후, 해당 장치를 중단없이 스택에 재연결할 수 있으며 링형 위상은 복원됩니다.

## 스테킹 오류 복구 위상

스테킹 위상에 오류가 발생하면 스택은 스테킹 오류 복구 위상으로 복구합니다. 스테킹 오류 복구 위상에서 장치는 체인 구조로 작동합니다. 스택 마스터가 패킷 전송 목적지를 결정합니다. 각 단원(맨 위 및 맨 아래 단원 제외)을 2개의 인접 단원에 연결합니다.

## 스테킹 구성요소 및 단원 ID


스테킹 단원 ID는 스테킹 구성에 필수입니다. 부팅 프로세스 동안 스테킹 작업이 결정됩니다. 작업 모드는 초기화 프로세스 동안에 선택한 단원 ID에 의해 결정됩니다. 예를 들면, 독립 실행형 모드를 선택했을 경우, 장치는 부트 업 프로세스에서 독립 실행형 장치로 부팅합니다.

장치 단원은 독립 실행형 단원의 기본 단원 ID와 함께 제공됩니다. 장치가 독립 실행형 단원으로 작동하는 경우, 모든 스테킹 LED는 꺼집니다.

다른 단원 ID를 선택한 경우 단원은 재설정되어도 지워지지 않고 계속 유효합니다.

단원 ID 1 및 단원 ID 2는 마스터 활성화 단원에 부여됩니다. 단원 ID 3-6은 스택 구성요소에 정의할 수 있습니다.


마스터 단원이 부팅되는 경우 또는 스택 구성요소를 삽입하거나 제거하는 경우에 마스터 단원은 스테킹 검색 프로세스를 초기화합니다.

 **주:** 같은 단원 ID를 가진 2개의 구성요소를 발견한 경우 스택은 계속 작동합니다. 그러나, 더 오랜 결합 시간을 가진 단원만이 스택을 결합합니다. 한 단원이 스택을 결합하는 데 실패했음을 알리는 메시지가 사용자에게 전송됩니다.

## 스테킹 구성요소 제거 및 교체

단원 1 및 단원 2는 마스터 활성화 단원입니다. 단원 1 및 단원 2는 마스터 장치나 백업 마스터 장치중 하나로 지정됩니다. 스택 마스터 할당은 구성 프로세스 동안 수행됩니다. 다음 결정 프로세스에 따라 한 마스터 활성화 스택 구성요소는 마스터로 선택되고 다른 하나는 백업 마스터로 선택됩니다.

- 1 하나의 스택 마스터 활성화 단원만 존재하는 경우, 해당 단원은 마스터로 선택됩니다.
- 1 2개의 마스터 활성화 스테킹 구성요소가 존재하며 그 중 하나가 스택 마스터로 수동으로 구성된 경우, 수동으로 구성된 구성요소는 스택 마스터로 선택됩니다.
- 1 2개의 마스터 활성화 단원이 존재하며 수동으로 마스터로 구성된 경우, 보다 긴 활성 상태 시간을 가진 단원이 스택 마스터로 선택됩니다.
- 1 2개의 마스터 활성화 단원이 존재하며 모두 수동으로 마스터로 구성된 경우, 보다 긴 활성 상태 시간을 가진 단원이 스택 마스터로 선택됩니다.
- 1 2개의 마스터 활성화 스테킹 구성요소가 같은 경과 시간을 가지면 단원 1이 스택 마스터로 선택됩니다.

 **주:** 2개의 구성요소가 10분 간격 내에 삽입되었을 경우 같은 경과 시간을 가진 것으로 간주됩니다.

예를 들면, 단원 2가 10분 주기의 처음 1분에 삽입되고 단원 1이 같은 주기의 제5분에 삽입되면 두 단원은 같은 경과 시간을 가진 것으로 간주됩니다. 같은 경과 시간을 가진 마스터 활성화 스택 구성요소가 2개 있을 경우 단원 1이 마스터로 선택됩니다.

스택 마스터 및 백업 마스터는 예열 대기 상태를 유지합니다. 예열 대기 상태는 오류 복구 발생 시 백업 마스터가 스택 마스터를 대체하도록 확보합니다. 이는 스택이 계속 정상적으로 작동하도록 보증합니다.

예열 대기 상태동안, 마스터 및 백업 마스터는 정적 구성으로만 동기화됩니다. 스테킹 마스터가 구성된 경우, 스택 마스터는 스테킹 백업 마스터를 동기화해야 합니다. 동적 구성은 저장되지 않습니다. 예를 들면, 동적으로 기억한 MAC 주소는 저장되지 않습니다.

스택의 각 포트는 구성 명령 및 구성 파일의 일부인 특정 단원 ID, 포트 유형, 포트 번호를 가집니다. 다음 항목을 포함하는 구성 파일은 장치 스택 마스터에서만 관리합니다.

- 1 플래쉬로 저장
- 1 구성 파일을 외부 TFTP 서버로 업로드
- 1 구성 파일을 외부 TFTP 서버에서 다운로드

**주:** 스택이 재설정 및/또는 포트가 더 이상 존재하지 않아도 모든 구성된 포트의 스택 구성은 저장됩니다.

재부팅할 때마다 위상 검색이 수행되고 마스터는 스택의 모든 단원을 기억합니다. 단원 ID는 단원에 저장되고 위상 검색을 통해 기억됩니다. 단원이 선택된 마스터없이 부팅을 시도하며 독립 실행형 모드로 작동하지 않는 경우 해당 장치는 부팅하지 않습니다.

구성 파일은 명시적 사용자 구성을 통해서만 변경합니다. 다음의 경우 구성 파일은 자동으로 수정되지 않습니다.

- 1 단원이 추가된 경우
- 1 단원이 제거된 경우
- 1 단원에 단원 ID가 재할당된 경우
- 1 단원이 스테킹 모드와 독립 실행형 모드 사이에서 전환하는 경우

시스템이 재부팅할 때마다 마스터 단원의 시작 구성 파일은 스택을 구성하는 데 사용됩니다.

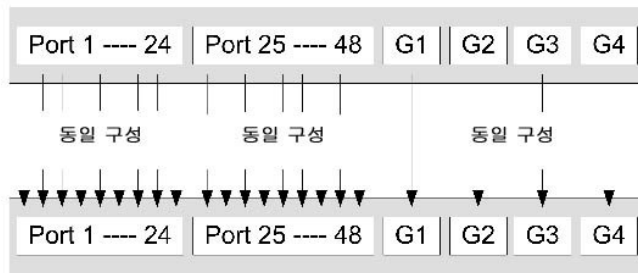
스택에서 스택 구성요소를 제거한 다음 같은 단원 ID를 가진 단원으로 교체하면 해당 스택 구성요소는 원래 단원 구성으로 구성됩니다. 물리적으로 존재하는 포트만이 PowerConnect OpenManage 스위치 관리자 홈 페이지에 표시되며 웹 관리 시스템을 통해 구성할 수 있습니다. 존재하지 않는 포트는 CLI 또는 SNMP 인터페이스를 통해 구성합니다.

## 스테킹 구성요소 교환

같은 단원 ID를 가진 스택 구성요소가 같은 단원 ID를 가진 기존 스택 구성요소를 교체하는 경우, 이전 장치 구성은 삽입된 스택 구성요소에 적용됩니다. 새로 삽입한 장치가 이전 장치보다 포트를 많이 또는 적게 가지고 있는 경우, 관련 포트 구성은 새 스택 구성요소에 적용됩니다. 예를 들면,

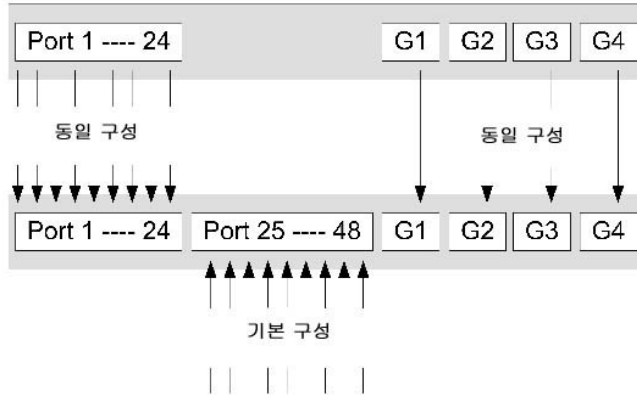
- 1 PowerConnect 3424/P가 PowerConnect 3424/P를 교체하는 경우, 모든 포트 구성은 원래대로 유지됩니다.
- 1 PowerConnect 3448/P가 PowerConnect 3448/P를 교체하는 경우, 모든 포트 구성은 원래대로 유지됩니다.

그림 1-4. PowerConnect 3448/P가 PowerConnect 3448/P를 교체



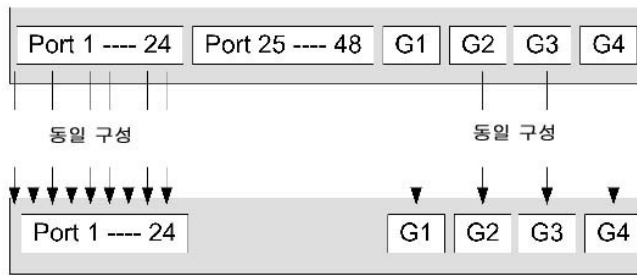
- 1 PowerConnect 3448/P가 PowerConnect 3424/P를 교체하는 경우, 첫 번째 3448/P 24 FE 포트가 3424/P 24 FE 포트 구성을 가집니다. GE 포트 구성은 원래대로 유지됩니다. 나머지 포트는 기본 포트 구성을 가집니다.

그림 1-5. PowerConnect 3424/P 포트가 PowerConnect 3448/P 포트를 교체



1 PowerConnect 3424/P가 PowerConnect 3448/P를 교체하는 경우, PowerConnect 3424/P 24 FE 포트가 첫 번째 24 FE PowerConnect 3448/P 포트 구성을 가집니다. GE 포트 구성은 원래대로 유지됩니다.

그림 1-6. PowerConnect 3448/P 포트가 PowerConnect 3424/P 포트를 교체



## 스택 마스터에서 백업 스택 마스터로 전환

다음의 경우가 발생하면 백업 마스터가 스택 마스터를 교체합니다.

- 1 스택 마스터에 오류가 발생했거나 스택에서 제거됩니다.
- 1 스택 마스터와 스테킹 구성요소의 연결이 끊어졌습니다.
- 1 웹 인터페이스나 CLI를 통해 소프트 전환을 수행합니다.

스택 마스터와 백업 마스터 사이의 전환이 제한 서비스 손실을 초래합니다. 오류가 발생한 경우 모든 동작 표는 다시 기억됩니다. 실행 구성 파일은 스택 마스터와 백업 마스터 사이에서 동기화되면 계속 백업 마스터에서 실행됩니다.

## 기능 개요

이 항목에서는 장치 기능을 설명합니다. 모든 업데이트한 장치 기능의 완전한 목록에 대한 정보는 최신 소프트웨어 버전 **발행 정보**를 참조하십시오.

## 이더넷상의 전원

PoE(이더넷상의 전원)는 네트워크 인프라를 업데이트하거나 수정하지 않고 기존 LAN 케이블로 연결된 장치에 전원을 공급합니다. PoE를 사용하면 네트워크 장치를 전원 옆에 배치할 필요가 없습니다. PoE는 다음 응용프로그램에 사용할 수 있습니다.

- 1 IP 전화
- 1 무선 액세스 점

- 1 IP 게이트웨이
- 1 PDA
- 1 오디오 및 비디오 원격 모니터링

PoE에 대한 자세한 내용은 [PoE 관리](#)를 참조하십시오.

## 헤드 라인 차단

HOL(헤드 라인) 차단은 동일한 송신 포트 자원에 대한 처리량 경쟁으로 인해 처리량 지연 및 프레임 손실이 발생하도록 합니다. HOL 차단 대기열 패킷과 대기열의 헤드에 있는 패킷은 대기열의 끝에 있는 패킷보다 빨리 전달됩니다.

## 흐름 제어 지원(IEEE 802.3X)

흐름 제어는 고속 장치가 패킷을 전송하는 것을 억제하도록 요청함으로써 저속 장치가 고속 장치와 통신할 수 있도록 합니다. 전송을 일시 중지하여 버퍼 오버플로를 방지합니다.

포트 또는 LAG에 흐름 제어를 구성하는 데 대한 정보는 "[포트 구성 정의](#)" 또는 "[LAG 매개변수 정의](#)"를 참조하십시오.

## 배압 지원

반이중 연결에서, 수신 포트는 연결을 점유함으로써 추가 처리량을 사용할 수 없게 하여 버퍼 오버플로를 방지합니다.

포트 또는 LAG에 흐름 제어를 구성하는 데 대한 정보는 "[포트 구성 정의](#)" 또는 "[LAG 매개변수 정의](#)"를 참조하십시오.

## VCT(가상 케이블 검사)

VCT는 오픈 케이블 및 케이블 부족과 같은 구리 연결 케이블 부설 중 발생한 문제를 감지하고 보고합니다. 케이블 검사에 대한 자세한 내용은 "[케이블 진단 프로그램 실행](#)"을 참조하십시오.

## MDI/MDIX 지원

장치는 자동 조정이 활성화된 경우 RJ-45 포트에 연결된 케이블이 교차되었는지 아니면 곧게 놓였는지 여부를 자동으로 감지합니다.

최종 스테이션의 표준 배선은 **MDI**(매체 의존 인터페이스)이고 허브 및 스위치의 표준 배선은 **MDIX**(크로스오버가 있는 매체 의존 인터페이스)입니다.

포트 또는 LAG에 MDI/MDIX를 구성하는 데 대한 정보는 "[포트 구성 정의](#)" 또는 "[LAG 매개변수 정의](#)"를 참조하십시오.

## 자동 조정

자동 조정을 사용하면 장치가 작업 모드를 보급하도록 할 수 있습니다. 자동 조정 기능은 점 대 점 연결 세그먼트를 공유하는 두 장치 사이에서 정보를 교환하는 방법 및 전송 용량을 최대로 사용하도록 두 장치를 자동으로 구성하는 방법을 제공합니다.

PowerConnect 3400 시리즈는 포트 통보를 제공하여 자동 조정을 향상시켰습니다. 포트 통보는 시스템 관리자가 통보된 포트 속도를 구성하도록 합니다.

자동 조정을 구성하는 데 대한 자세한 내용은 ["포트 구성 정의"](#) 또는 ["LAG 매개변수 정의"](#)를 참조하십시오.

## MAC 주소 지원 기능

### MAC 주소 용량 지원

장치는 최대 8K MAC 주소를 지원합니다. 장치는 시스템 사용에 특정 MAC 주소를 보유합니다.

### 정적 MAC 항목

MAC 항목은 수신 프레임에서 기억하는 대체 항목으로 브리지 표에 수동으로 입력할 수 있습니다. 이러한 사용자 정의된 항목은 에이징을 조건으로 하는 것이 아니며 재설치 또는 재부팅 후에도 유지됩니다.

자세한 내용은 ["정적 주소 정의"](#)를 참조하십시오.

### MAC 주소 자체 학습

장치는 수신 패킷에서 자동으로 MAC 주소를 학습할 수 있게 합니다. MAC 주소는 브리지 표에 저장됩니다.

### MAC 주소에 대한 자동 에이징

일정한 시간 동안 수신된 처리량이 없는 MAC 주소는 폐기됩니다. 이렇게 하면 브리지 표가 오버플로되는 것을 방지할 수 있습니다.

MAC 주소 에이징 아웃 시간을 구성하는 데 대한 자세한 내용은 ["동적 주소 보기"](#)를 참조하십시오.

### VLAN 인식 MAC 기반 전환

장치는 항상 VLAN 인식 브리징을 수행합니다. 프레임이 해당 대상 MAC 주소에만 기반하여 전달되는 위치에서 클래식 브리지(IEEE802.1D)는 수행되지 않습니다. 그러나, 태그화하지 않은 프레임에 비슷한 기능을 구성할 수 있습니다. 포트와 연관되지 않은 대상 MAC 주소에 전송된 프레임은 관련 VLAN의 모든 포트에 채도합니다.

### MAC 멀티캐스트 지원

멀티캐스트 서비스는 제한된 브로드캐스트 서비스로서 정보 배포의 일 대 다 및 다 대 다 연결을 허용합니다. 총 2 멀티캐스트 서비스는 단일 프레임 주소를 특정 멀티캐스트 주소로 지정하여 프레임 사본이 해당 포트에 전송합니다.

자세한 내용은 ["모든 매개변수로 멀티캐스트 할당"](#)을 참조하십시오.

## 총 2 기능

### IGMP 스누핑

IGMP 스누핑은 IGMP 프레임 내용을 장치에 의해 워크스테이션에서 업스트림 멀티캐스트 라우터로 전달되는 시점에 검사합니다. 프레임에서 장치는 멀티캐스트 세션의 워크스테이션 및 멀티캐스트 프레임을 전송하는 멀티캐스트 라우터를 식별합니다.



자세한 내용은 "[IGMP 스누핑](#)"을 참조하십시오.

## 포트 미러링

포트 미러링은 모니터되는 포트에서 모니터하는 포트에 수신 및 송신 패킷의 사본을 전달하여 네트워크 처리량을 모니터링하고 미러링합니다. 특정 소스 포트를 통해 모든 처리량의 사본을 수신하는 대상 포트를 지정합니다.

자세한 내용은 "[포트 미러링 세션 정의](#)"를 참조하십시오.

## 브로드캐스트 스톱 제어

스톱 제어를 사용하면 장치에 의해 접수 및 전달된 멀티캐스트와 브로드캐스트 프레임의 양을 제한할 수 있습니다.

총 2 프레임이 전달될 때 브로드캐스트 및 멀티캐스트 프레임은 관련 VLAN의 모든 포트에 채도합니다. 이는 대역폭을 점유하고 모든 포트에 연결된 모든 노드를 로드합니다.

자세한 내용은 "[스톱 제어 활성화](#)"를 참조하십시오.

## VLAN 지원 기능

### VLAN 지원

VLAN은 단일 브로드캐스트 도메인을 구성하는 전환 포트 모음입니다. 패킷은 VLAN 태그 또는 수신 포트와 패킷 내용에 기준으로 VLAN에 종속하는 것으로 분류됩니다. 공통 특성을 공유하는 패킷은 같은 VLAN에 분류될 수 있습니다.

자세한 내용은 "[VLAN 구성](#)"을 참조하십시오.

### 포트 기반 VLAN(가상 LAN)

포트 기반 VLAN은 수신 포트를 기준으로 하여 수신 패킷을 VLAN으로 분류합니다.

자세한 내용은 "[VLAN 포트 설정 정의](#)"를 참조하십시오.

### 전체 802.1Q VLAN 태그화 규약

IEEE 802.1Q는 가상 브리지 LAN, VLAN에서 제공한 서비스 및 이러한 서비스 관련 프로토콜과 알고리즘의 아키텍처를 정의합니다.

### GVRP 지원

GVRP(GARP VLAN 등록 프로토콜)은 IEEE 802.1Q 규격 VLAN 프루닝 및 802.1Q 트렁크 포트의 동적 VLAN 적성을 제공합니다. GVRP가 활성화된 경우, 장치는 활성 원본으로 사용하는 "[스패닝 트리 프로토콜 기능](#)" 위상의 일부인 모든 포트에서 VLAN 멤버십을 등록하고 보고합니다.

자세한 내용은 "[GVRP 매개변수 구성](#)"을 참조하십시오.

## 개인 VLAN

개인 VLAN 포트와 하나의 총 2 보안 기능은 동일한 브로드캐스트 도메인 내의 포트 사이에 격리를 제공합니다.

개인 VLAN에 대한 자세한 내용은 "[개인 VLAN 구성](#)"을 참조하십시오.

## 스패닝 트리 프로토콜 기능

### STP(스패닝 트리 프로토콜)

802.1d 스패닝 트리는 브리지와 L2 전달 루프를 자동으로 방지하고 해결하도록 허용하는 표준 총 2 스위치 요구사항입니다. 특별히 포맷한 프레임 및 포트의 선택적 활성화 및 비활성 전달을 사용하여 교환 구성 메시지를 전환합니다.

자세한 내용은 "[스패닝 트리 프로토콜 구성](#)"을 참조하십시오.

### 빠른 연결

STP는 수렴하는 데 최대 30-60초 소요합니다. 이 시간 동안 STP는 가능한 루프를 감지하여 상태 변경 사항이 보급되고 관련 장치가 응답하는 시간이 있도록 합니다. 많은 응용프로그램에 대해 30-60초의 응답 시간은 너무 길다. 빠른 연결은 이 지연을 우회하며 전달 루프가 발생하지 않는 네트워크 위상에서 사용할 수 있습니다.

포트 및 LAG의 빠른 연결 활성화에 대한 자세한 내용은 "[STP 포트 설정 정의](#)" 또는 "[정적 주소 정의](#)"를 참조하십시오.

### IEEE 802.1w 고속 스패닝 트리

스패닝 트리는 각 호스트가 해당 포트가 처리량을 활동적으로 전달하는지 확인하는 데 30-60초를 소요할 수 있습니다. RSTP(고속 스패닝 트리)는 전달 루프를 작성하지 않고 네트워크 위상의 사용을 감지하여 빠른 수렴을 활성화합니다.

자세한 내용은 "[고속 스패닝 트리 정의](#)"를 참조하십시오.

### IEEE 802.1s 다중 스패닝 트리

MSTP(다중 스패닝 트리) 작업은 VLAN을 STP 인스턴스에 매핑합니다. MSTP는 다른 로드 균형 시나리오를 제공합니다. 다양한 VLAN에 할당된 패킷은 MSTP 영역(MST 영역) 내에서 다른 경로에 따라 전송됩니다. 영역은 하나 이상의 프레임을 전송할 수 있는 MSTP 브리지입니다. 표준은 관리자 하위급 VLAN 처리량을 고유 경로에 할당하도록 합니다.

자세한 내용은 "[스패닝 트리 프로토콜 구성](#)"을 참조하십시오.

## 연결 집계

### 연결 집계

최대로 8개의 집계된 연결(각 연결은 최대 8개의 구성요소 포트를 포함)을 정의하여 단일 LAG(연결 집계 그룹)를 형성할 수 있습니다. 따라서 다음의 작업을 수행할 수 있습니다.

- 1 실제 연결 중단으로부터 내결함성 보호
- 1 고대역폭 연결
- 1 향상된 대역폭 세분성

## 1 고대역폭 서버 연결

LAG는 동일한 속도를 가지고 전이중 방식 작업으로 설정된 포트 구성됩니다.

자세한 내용은 "[LAG 매개변수 정의](#)"를 참조하십시오.

## 연결 집계 및 LACP

LACP는 연결을 통한 동등 교환을 사용하여 진행 중에 다양한 연결의 집계 기능을 결정하며 지정된 1쌍의 장치 사이에서 획득할 수 있는 집계 기능의 최고 레벨을 계속 제공합니다. LACP는 시스템 내에서 바인드한 포트를 자동으로 확인, 구성, 바인딩 및 모니터링합니다.

자세한 내용은 "[포트 집계](#)"를 참조하십시오.

## BootP 및 DHCP 클라이언트

DHCP는 설정 매개변수를 활성화하여 시스템 시작 시 네트워크 서버로부터 수신되도록 합니다. DHCP 서비스는 계속 진행 중인 프로세스입니다. DHCP는 BootP의 확장 서비스입니다.

DHCP에 대한 자세한 내용은 "[DHCP IP 인터페이스 매개변수 정의](#)"를 참조하십시오.

## 서비스 기능의 품질

### 서비스 등급 802.1p 지원

IEEE 802.1p 신호 기술은 데이터 링크/MAC 하위 층에서 네트워크 처리량을 표시하고 우선순위를 지정하기 위한 OSI 층 2 표준입니다. 802.1p 처리량은 분류된 후 대상으로 전송됩니다. 대역폭 예약 또는 제한은 설정되거나 강제 실행되지 않습니다. 802.1p는 802.1Q(VLAN) 표준의 파생 항목입니다. 802.1p는 IP 우선순위 IP 헤더 비트 필드와 비슷한 우선순위의 8개 레벨을 설정합니다.

자세한 내용은 "[서비스 품질 구성](#)"을 참조하십시오.

## 장치 관리 기능

### SNMP 경고 및 트랩 로그

시스템에서 심각도 코드 및 시간 소인과 함께 이벤트를 로그합니다. 이벤트를 SNMP 트랩으로 트랩 수신자 목록으로 전송합니다.

SNMP 경고 및 트랩에 대한 자세한 내용은 "[SNMP 매개변수 정의](#)"를 참조하십시오.

### SNMP 버전 1, 2 및 3

UDP/IP 프로토콜을 통한 SNMP(단순 네트워크 관리 프로토콜)는 시스템 액세스를 제어하며 커뮤니티 항목(각 항목은 커뮤니티 문자열 및 해당 액세스 권한으로 구성) 목록이 정의되었습니다. SNMP 보안에는 읽기 전용, 읽기/쓰기 및 슈퍼 등 3가지 레벨이 있습니다. 슈퍼 사용자만이 커뮤니티 표에 액세스할 수 있습니다.

자세한 내용은 "[SNMP 매개변수 정의](#)"를 참조하십시오.

## 웹 기반 관리

웹 기반 관리를 사용하면 임의의 웹 브라우저에서 시스템을 관리할 수 있습니다. 시스템에는 HTML 페이지 역할을 하며 시스템을 모니터링하고 구성할 수 있는 EWS(내포된 웹 서버)가 포함됩니다. 시스템은 웹 기반 입력을 구성 명령, MIB 변수 설정 및 기타 관리 관련 설정으로 내부 전환합니다.

## 구성 파일 다운로드 및 업로드

장치 구성은 구성 파일에 저장됩니다. 구성 파일은 시스템 와이드 및 포트 특정 장치 구성을 모두 포함합니다. 시스템에서 텍스트 파일로 저장 및 조작된 구성 파일을 CLI 명령 집합의 형식으로 표시할 수 있습니다.

자세한 내용은 "[파일 관리](#)"를 참조하십시오.

## TFTP 소형 파일 전송 프로토콜

장치는 TFTP를 통해 부팅 이미지, 소프트웨어 및 구성 업로드/다운로드를 지원합니다.

## 원격 모니터링

RMON(원격 모니터링)은 SNMP의 확장 서비스로서 포괄적 네트워크 치리량 모니터링 기능(네트워크 장치 관리 및 모니터링을 허용하는 SNMP와 반대)을 제공합니다. RMON은 현재 및 과거의 MAC 층 통계 자료와 제어 객체를 정의하는 표준 MIB로서 전체 네트워크를 통해 실시간 정보를 캡처하도록 합니다.

자세한 내용은 "[통계 자료 보기](#)"를 참조하십시오.

## 명령줄 인터페이스

CLI(명령줄 인터페이스) 구문 및 시맨틱은 가능한 범위에서 일반 업체 관습을 따릅니다. CLI는 필수 및 옵션 요소로 구성됩니다. CLI 인터프리터는 명령 및 키워드 완성을 제공하여 사용자를 도와 입력을 줄입니다.

## Syslog

Syslog는 이벤트 알림을 활성화하여 이벤트 알림이 저장, 검사 및 결정되는 원격 서버에 전송되도록 하는 프로토콜입니다. 시스템에서 중요한 이벤트 알림을 실시간으로 전송하고 사후 사정을 위해 이러한 이벤트를 기록해 둡니다.

Syslog에 대한 자세한 내용은 "[로그 관리](#)"를 참조하십시오.

## SNTP

SNTP(단순 네트워크 시간 프로토콜)은 네트워크 이더넷 스위치 클럭 시간을 밀리초 단위까지 정확하도록 보증합니다. 시간 동기화는 네트워크 SNTP 서버에서 수행합니다. 시간 소스는 계층에 의해 설정됩니다. 계층은 참조 클럭에서 떨어진 거리를 정의합니다. 계층이 더 높을 수록(0이 최고) 클럭이 더 정확합니다.

자세한 내용은 "[SNTP 설정 구성](#)"을 참조하십시오.

## 도메인 이름 시스템

DNS(도메인 이름 시스템)은 사용자 정의된 도메인 이름을 IP 주소로 전환합니다. 도메인 이름을 DNS 서비스에 할당할 때마다 이름을 숫자 IP 주소로 전환합니다. 예를 들면,

www.ipexample.com은 192.87.56.2로 전환됩니다. DNS 서버는 도메인 이름 데이터베이스 및 해당 IP 주소를 유지합니다.

자세한 내용은 ["도메인 이름 시스템 구성"](#)을 참조하십시오.

## Traceroute

Traceroute는 전달 프로세스 동안 패킷이 전송되는 IP 라우트를 검색합니다. CLI Traceroute 유틸리티는 사용자 exec 또는 관리자 모드에서 실행할 수 있습니다.

## 보안 기능

### SSL

SSL(보안 소켓 층)은 프라이버시, 인증, 데이터 무결성을 통과하도록 데이터의 안전한 트랜잭션을 활성화하는 응용프로그램 레벨 프로토콜입니다. SSL은 인증서와 공개 및 개인 키에 의지합니다.

### 포트 기반 인증(802.1x)

포트 기반 인증은 외부 서버를 통해 포트 별로 인증 시스템 사용자를 활성화합니다. 인증되고 승인된 시스템 사용자만이 데이터를 전송하고 수신할 수 있습니다. 포트는 EAP(확장 가능 인증 프로토콜)을 사용하여 RADIUS(원격 인증 다이얼 인 사용자 서비스)를 통해 인증됩니다.

자세한 내용은 ["포트 기반 인증 구성"](#)을 참조하십시오.

### 잠긴 포트 지원

잠긴 포트는 특정 포트에서 특정 MAC 주소를 가진 사용자만 액세스 가능하도록 제한하여 네트워크 보안을 향상시킵니다. 이러한 주소는 수동으로 정의하거나 포트에 기억되어 있습니다. 프레임이 잠긴 포트에 감지되고 프레임 소스 MAC 주소가 해당 포트에 연결되지 않은 경우 보호 메커니즘이 호출됩니다.

자세한 내용은 ["포트 보안 구성"](#)을 참조하십시오.

### RADIUS 클라이언트

RADIUS는 클라이언트/서버 기반 프로토콜입니다. RADIUS 서버는 사용자 이름, 암호 및 계정 정보와 같은 사용자별 인증 정보를 포함하는 사용자 데이터베이스를 유지합니다.

자세한 내용은 ["SRADIUS 설정 구성"](#)을 참조하십시오.

### SSH

SSH(보안 셸)은 장치와의 안전한 원격 연결을 제공하는 프로토콜입니다. SSH 버전 2를 현재 지원합니다. SSH 서버 기능은 SSH 클라이언트를 활성화하여 장치와의 안전하고 암호화된 연결을 설정합니다. 이 연결은 내향 텔넷 연결과 비슷한 기능을 제공합니다. SSH는 장치 연결과 인증에 RSA 및 DSA 공개 키 암호화를 사용합니다.

### TACACS+

TACACS+는 장치에 액세스하는 사용자의 유효성 검사에 집중화 보안을 제공합니다. TACACS+는 RADIUS 및 기타 인증 프로세스와 일관성을 유지하는 동시에 집중화 사용자 관리 시스템을 제공합니다.

자세한 내용은 "[TACACS+ 설정 정의](#)"를 참조하십시오.

## 암호 관리

암호 관리는 향상된 네트워크 보안과 제고된 암호 제어를 제공합니다. SSH, 텔넷, HTTP, HTTPS 및 SNMP 액세스의 암호에 보안 기능이 할당됩니다. 암호 관리에 대한 자세한 내용은 "[암호 관리](#)"를 참조하십시오.

---

## 추가 CLI 설명서

설명서 CD에 있는 CLI 참조 안내서에서는 장치를 구성하는 데 사용하는 CLI 명령에 대한 정보를 제공합니다. 이 문서에서는 명령 설명, 구문, 기본값, 지침 및 예제에 대한 정보를 제공합니다.

---

[목차 페이지로 돌아가기](#)

## 하드웨어 설명

### Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [포트 설명](#)
- [실제 크기](#)
- [LED 정의](#)

## 포트 설명

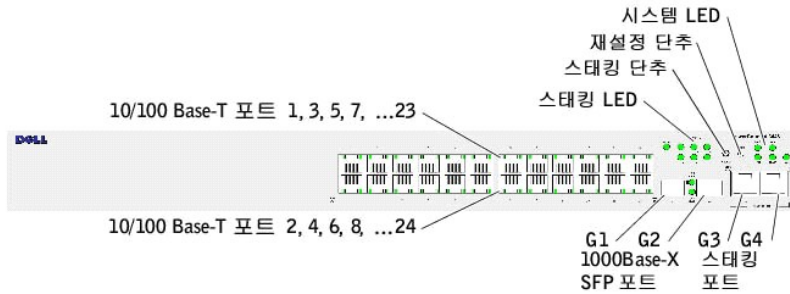
### PowerConnect 3424 포트 설명

PowerConnect 3424 장치는 다음과 같은 포트에 구성되었습니다.

- 1 24 고속 이더넷 포트 — 10/100Base-T 포트에 지정된 RJ-45 포트
- 1 2 광섬유 포트 — 1000Base-X SFP 포트에 지정됨
- 1 2 기가비트 포트 — 11000Base-T 포트에 지정됨
- 1 콘솔 포트 — RS-232 기반 포트

다음 그림은 PowerConnect 3424 전면 패널을 보여줍니다.

그림 2-1. PowerConnect 3424 전면 패널



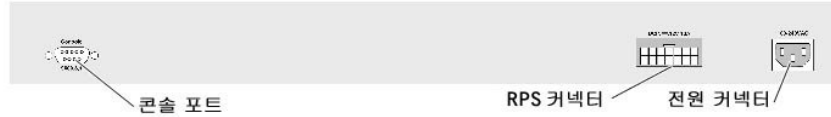
전면 패널에는 1~24 사이의 수로 표시된 RJ-45 포트 24개가 있습니다. 위쪽의 포트는 1~23 사이의 홀수로 표시되고 아래쪽의 포트는 2~24 사이의 짝수로 표시됩니다. 전면 패널에는 광섬유 포트인 G1 - G2 포트와 동선 포트인 G3 - G4 포트도 있습니다. G3 - G4 포트는 스택링 포트에 사용할 수 있거나 독립 실행형 장치에서 네트워크 처리량을 전달하는 데 사용됩니다.

전면 패널에는 2개의 단추가 있습니다. 스택 ID 단추는 장치 번호를 선택하는 데 사용됩니다. 두 번째 단추는 리셋 단추인데 장치를 수동으로 재시동하는 데 사용됩니다. 리셋 단추는 장치 전면 패널 표면에 나와 있지 않으므로 우연히 눌러 재시동될 염려가 없습니다. 전면 패널에는 모든 장치 LED가 있습니다.

다음 그림은 PowerConnect 3424 후면 패널을 보여줍니다.

그림 2-2. PowerConnect 3424 후면 패널

후면 패널에는 RPS 커넥터, 콘솔 포트 및 전원 커넥터가 있습니다.



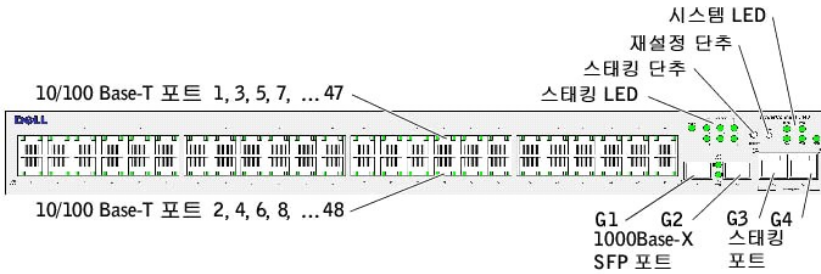
## PowerConnect 3448 포트 설명

PowerConnect 3448 장치는 다음과 같은 포트에 구성되었습니다.

- 1 48 FE 포트 — 10/100Base-T 포트에 지정된 RJ-45 포트
- 1 2 광섬유 포트 — 1000Base-X SFP 포트에 지정됨
- 1 2 기가비트 포트 — 11000Base-T 포트에 지정됨
- 1 콘솔 포트 — RS-232 콘솔 기반 포트

다음 그림은 PowerConnect 3448 전면 패널을 보여줍니다.

그림 2-3. PowerConnect 3448 전면 패널



전면 패널에는 1~48 사이의 수로 표시된 RJ-45 포트 48개가 있습니다. 위쪽의 포트는 1~47 사이의 홀수로 표시되고 아래쪽의 포트는 2~48 사이의 짝수로 표시됩니다. 전면 패널에는 광섬유 포트인 G1 - G2 포트와 동선 포트인 G3 - G4 포트도 있습니다. G3 - G4 포트는 스택킹 포트에 사용할 수 있거나 독립 실행형 장치에서 네트워크 처리량을 전달하는 데 사용됩니다.

전면 패널에는 2개의 단추가 있습니다. 스택 ID 단추는 장치 번호를 선택하는 데 사용됩니다. 두 번째 단추는 리셋 단추인데 장치를 수동으로 재시동하는 데 사용됩니다. 리셋 단추는 장치 전면 패널 표면에 나와 있지 않으므로 우연히 눌러 재시동될 염려가 없습니다. 전면 패널에는 모든 장치 LED가 있습니다.

다음 그림은 PowerConnect 3448 후면 패널을 보여줍니다.

그림 2-4. PowerConnect 3448 후면 패널



후면 패널에는 RPS 커넥터, 콘솔 포트 및 전원 커넥터가 있습니다.

## SFP 포트

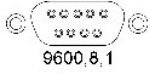
소형 폼팩터 연결 가능(SFP) 포트는 1000Base-SX 또는 LX로 지정된 복합 프로그램 가능 논리 장치(CPLD)를 통해 통신할 수 있는 2선식 직렬 인터페이스(TWIS)입니다.



## RS-232 콘솔 포트

1개의 터미널 연결용 DB-9 커넥터는 디버깅, 소프트웨어 다운로드 등에 사용됩니다. 기본 보드율은 9,600bps입니다. 보드율은 2400bps에서 최대 115,200bps까지 구성될 수 있습니다.

그림 2-5. 콘솔 포트



## 실제 크기

PowerConnect 3424/P 및 PowerConnect 3448/P 장치의 실제 크기는 다음과 같습니다.

PoE 모델:

- 1 폭 — 440mm(17.32인치)
- 1 깊이 — 387mm(15.236인치)
- 1 높이 — 43.2mm(1.7인치)

비 PoE 장치:

- 1 폭 — 440mm(17.32인치)
- 1 깊이 — 257mm(10.118인치)
- 1 높이 — 43.2mm(1.7인치)

## LED 정의

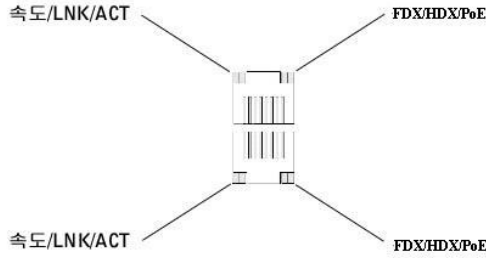
전면 패널에는 연결 상태, 전원 공급, 팬 및 시스템 진단 프로그램을 표시하는 발광 다이오드(LED)가 있습니다.

### 포트 LED

10/100/1000 Base-T 포트 및 10/100 Base-T 포트에는 각각 2개의 LED가 있습니다. 속도 LED는 포트의 왼쪽에 있고 연결/이중 방식/작동 LED는 포트의 오른쪽에 있습니다.

다음 그림은 PowerConnect 3424 /P 및 PowerConnect 3448/P 스위치에 있는 10/100 Base-T 포트 LED를 보여줍니다.

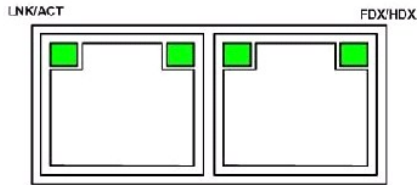
그림 2-6. RJ-45 동선 기반 10/100 BaseT LED



PowerConnect 3424 /P 및 PowerConnect 3448/P에 있는 RJ-45 100 Base-T 포트에는 LNK/ACT로 표시된 2개의 LED가 있습니다.

다음 그림은 100 Base-T LED를 보여줍니다.

그림 2-7. RJ-45 1000 BaseT LED



PowerConnect 3424 및 PowerConnect 3448용 RJ-45 LED 표시는 다음 표에 나와있습니다.

표 2-1. PowerConnect 3424 및 PowerConnect 3448 RJ-45 100BaseT LED 표시

LED	색상	설명
연결/작동/속도	녹색으로 켜져 있음	포트의 속도는 100Mbps입니다.
	녹색으로 깜박임	포트가 100Mbps 속도로 데이터를 전송하거나 수신하고 있습니다.
	황색으로 켜져 있음	포트의 속도는 10Mbps입니다.
	황색으로 깜박임	포트가 10Mbps 속도로 데이터를 전송하거나 수신하고 있습니다.
	꺼짐	현재 포트가 작동하지 않습니다.
FDX	녹색으로 켜져 있음	현재 포트가 전이중 방식 모드로 작동하고 있습니다.
	꺼짐	현재 포트가 반이중 방식 모드로 작동하고 있습니다.

PowerConnect 3424P 및 PowerConnect 3448P용 RJ-45 LED 표시는 다음 표에 나와있습니다.

표 2-2. PowerConnect 3424P 및 PowerConnect 3448P RJ-45 동선 기반 100BaseT LED 표시

LED	색상	설명
속도/연결/작동	녹색으로 켜져 있음	현재 포트가 100Mbps 속도로 연결됩니다.
	녹색으로 깜박임	현재 포트가 100Mbps 속도로 작동하고 있습니다.
	꺼짐	현재 포트가 10Mbps 속도로 작동하거나 또는 연결되지 않았습니다.
PoE	녹색으로 켜져 있음	전원 공급 장치(PD)가 감지되고 정상적인 부하에서 작동하고 있습니다. 전원 공급 장치에 대한 자세한 내용은 " <a href="#">이더넷 전원 장치 관리</a> "를 참조하십시오.
	호박색으로 켜져 있음	전원 공급 장치에 과부하나 부족이 발생했습니다. 이더넷 전원 장치 오류에 대한 자세한 내용은 " <a href="#">이더넷 전원 장치 관리</a> "를 참조하십시오.
	호박색으로 깜박임	전원 공급 장치 전원이 사전 정의된 전원 분배를 초과했습니다. 이더넷 전원 장치 전원 분배에 대한 자세한 내용은 " <a href="#">이더넷 전원 장치 관리</a> "를 참조하십시오.
	꺼짐	전원 공급 장치가 감지되지 않았습니다.

## 기가비트 포트 LED

다음 표는 기가비트(스테링 포트) LED에 대해 설명합니다.

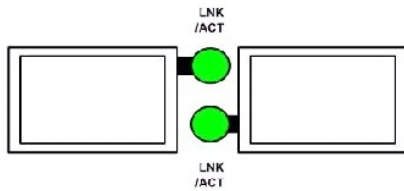
표 2-3. PowerConnect 3424 및 PowerConnect 3448 RJ-45 동선 기반 100BaseT LED 표시

LED	색상	설명
연결/작동/속도	녹색으로 켜져 있음	포트의 속도는 1000Mbps입니다.
	녹색으로 깜박임	포트가 1000Mbps 속도로 데이터를 전송하거나 수신하고 있습니다.
	황색으로 켜져 있음	포트의 속도는 10 또는 100Mbps입니다.
	황색으로 깜박임	포트가 10 또는 100Mbps 속도로 데이터를 전송하거나 수신하고 있습니다.
	꺼짐	현재 포트가 작동하지 않습니다.
FDX	녹색으로 켜져 있음	현재 포트가 전이중 방식 모드로 작동하고 있습니다.
	꺼짐	현재 포트가 반이중 방식 모드로 작동하고 있습니다.

## SFP LED

각 SFP 포트는 LNK/ACT로 표시된 LED가 1개씩 있습니다. PowerConnect 3424/P 및 PowerConnect 3448/P 장치에서 LED는 포트 사이에 있고 원형 모양입니다. 다음 그림은 각 장치에 있는 LED를 보여줍니다.

그림 2-8. SFP 포트 LED



SFP 포트 LED 표시는 다음 표에 나와있습니다.

표 2-4. SFP 포트 LED 표시

LED	색상	설명
연결/작동	녹색으로 켜져 있음	연결이 이루어졌습니다.
	녹색으로 깜박임	현재 포트가 데이터를 전송하거나 수신하고 있습니다.
	꺼짐	현재 포트가 연결되지 않았습니다.

## 시스템 LED

PowerConnect 3424 /P 및 PowerConnect 3448/P 장치의 시스템 LED는 전원 공급 장치, 팬, 온도 상태 및 진단 프로그램에 대한 정보를 제공합니다. 다음 그림은 시스템 LED를 보여줍니다.

그림 2-9. 시스템 LED



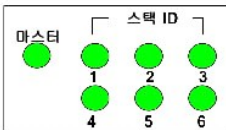
다음 표는 시스템 LED 표시에 대해 설명합니다.

표 2-5. 시스템 LED 표시등

LED	색상	설명
전원 공급 장치(PWR)	녹색으로 켜져 있음	스위치가 켜져 있습니다.
	꺼짐	스위치가 꺼져 있습니다.
예비 전원 공급 장치(RPS) (모델: 3424 및 3448)	녹색으로 켜져 있음	현재 RPS가 작동하고 있습니다.
	적색으로 켜져 있음	RPS에 오류가 발생했습니다.
	꺼짐	예비 전원 공급 장치를 연결하지 않았습니다.
예비 전원 공급 장치(RPS) (모델: 3424P 및 3448P)	녹색으로 켜져 있음	RPS는 현재 작동 중입니다.
	꺼짐	예비 전원 공급 장치에 고장이 발생했거나 연결되어 있지 않습니다.
진단 프로그램(DIAG)	녹색으로 깜박임	현재 시스템 진단 프로그램 검사가 진행 중입니다.
	녹색으로 켜져 있음	시스템 진단 프로그램 검사가 성공적으로 완료되었습니다.
	적색으로 켜져 있음	시스템 진단 프로그램 검사에 오류가 있습니다.
	꺼짐	시스템이 정상적으로 작동하고 있습니다.
온도(TEMP)	적색으로 켜져 있음	장치 온도가 허용 온도 범위를 초과했습니다.
	꺼짐	장치가 허용 온도 범위 내에서 작동하고 있습니다.
팬(FAN)	녹색으로 켜져 있음	모든 장치 팬이 정상적으로 작동하고 있습니다.
	적색으로 켜져 있음	하나 이상의 장치 팬이 작동하지 않습니다.

스테킹 LED는 스택의 장치 위치를 표시합니다. 다음 그림은 전면 패널에 있는 LED를 보여줍니다.

그림 2-10. 스테킹 LED



스테킹 LED는 1~6 사이의 숫자로 표시됩니다. 각 스테킹 장치에는 장치 ID 번호를 표시하는 스테킹 LED 표시등이 1개 있습니다. 스테킹 LED 1 또는 2가 켜져 있으면 장치가 스택 마스터나 백업 마스터임을 표시합니다.

표 2-6. 스테킹 LED 표시

LED	색상	설명
모든 스테킹 LED	꺼짐	현재 스위치는 독립 실행형 장치입니다.
스테킹 LED 1~6(S1~S6)	녹색으로 켜져 있음	장치가 스테킹 장치 N으로 지정되었습니다.
	꺼짐	장치가 스테킹 장치 N으로 지정되지 않았습니다.
스테킹 마스터 LED	녹색으로 켜져 있음	장치가 스택 마스터입니다.
	꺼짐	장치가 스택 마스터가 아닙니다.

## 전원 공급 장치

본 장치에는 내부 전원 공급 장치(AC 장치)와 PowerConnect 3424/P 및 PowerConnect 3448/P 장치를 PowerConnect EPS-470 장치에 연결하거나 PowerConnect 3424 및 PowerConnect 3448 장치를 PowerConnect RPS-600 장치에 연결하는 커넥터가 있습니다. PowerConnect 3424/P 및 PowerConnect 3448/P 장치에는 내부 전원 공급 장치(12볼트)가 있

습니다.

두 전원 공급 장치로 작동하는 것은 부하 분담에 의해 조절됩니다. 전원 공급 장치 LED는 전원 공급 장치 상태를 표시합니다.

PowerConnect 3424/P 및 PowerConnect 3448/P 장치는 470W(12V-48V)의 내부 전원을 공급하고 24 포트 PoE 장치에 전체 370W의 전원을 공급합니다.

## AC 전원 공급 장치

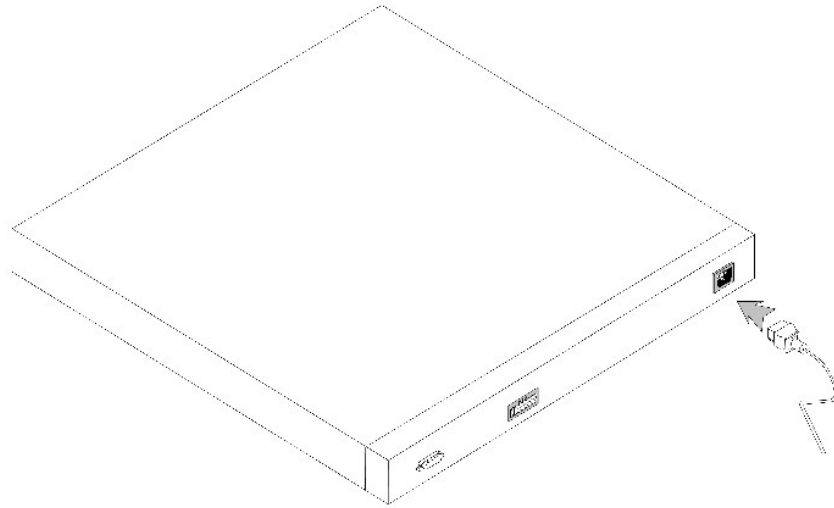
AC 전원 공급 장치는 90~264VAC, 47~63Hz 사이에서 작동합니다. AC 전원 공급 장치에는 표준 커넥터가 사용됩니다. 전면 패널에 있는 LED 표시등은 AC 장치가 연결되어 있는지를 표시합니다.

## DC 전원 공급 장치

PowerConnect 3424 및 PowerConnect 3448 스위치는 외장형 RPS-600 장치와 연결되어 예비 전원 옵션을 제공합니다. 구성은 필요하지 않습니다. 전면 패널 "RPS" LED는 외장형 RPS-600의 연결 여부를 표시합니다. RPS LED 정의는 표 2-5를 참조하십시오.

PowerConnect 3424/P 및 PowerConnect 3448/P 스위치는 외장형 EPS-470 장치와 연결되어 예비 전원 옵션을 제공합니다. 구성은 필요하지 않습니다. 전면 패널 "RPS" LED는 외장형 EPS-470의 연결 여부를 표시합니다. RPS LED 정의는 표 2-5를 참조하십시오.

### 그림 2-11. 전원 연결




장치가 기타 전원에 연결되면 전원 공급 장치 오류가 발생할 확률이 낮아집니다.

## 스택 ID 단추

장치의 전면 패널에는 스택 마스터 및 구성요소용 장치 ID를 수동으로 선택하는 데 사용하는 스택 ID 단추가 있습니다.

스택 마스터 및 구성요소는 장치를 부팅하는 15초 내에 선택해야 합니다. 스택 마스터를 15초 내에 선택하지 않으면 장치는 독립 실행형 모드로 부팅됩니다. 장치용 장치 ID를 선택하려면 장치를 재부팅하십시오.

스택 마스터가 1 또는 2의 장치 ID를 수신합니다. 장치 1 및 장치 2가 모두 있을 경우 선택되지 않은 장치가 백업 마스터의 기능을 수행합니다. 스택 구성요소는 별도 장치 ID(3~6)를 수신합니다. 예를 들어, 스택에 4개의 장치가 있는 경우, 마스터 장치는 1이나 2이고 백업 마스터는 마스터 장치의 장치 ID에 따라 1이나 2이며, 세 번째 구성요소는 3이고 네 번째 스택 구성요소는 4입니다.

 **주:** 장치는 독립 실행형 장치를 자동으로 감지하지 못합니다. 장치 ID가 이미 선택되었으면 스테킹 LED가 켜지지 않을 때까지 스택 ID 단추를 여러 번 누르십시오.

## 리셋 단추

PowerConnect 3424/P 및 PowerConnect 3448/P 스위치는 전면 패널에 리셋 단추가 있고 장치를 수동으로 재시동하는 데 사용됩니다. 마스터 장치가 재시동되면 전체 스택도 재시동됩니다. 구성요소 장치만 재시동되면 나머지 스테킹 구성요소는 재시동되지 않습니다.

스위치 단일 재시동 회로는 고 전력 소비 상태나 지압 상태에 의해 활성화됩니다.

## 환기 시스템

PoE 기능을 가진 PowerConnect 3424/P 및 PowerConnect 3448/P 스위치에는 5개의 내장형 팬이 있습니다. 비 PoE PowerConnect 3424 및 PowerConnect 3448 장치에는 2개의 내장형 팬이 있습니다. 하나 이상의 팬에 오류가 발생했는지를 표시하는 LED를 관찰하여 작동을 확인할 수 있습니다.

---

[목차 페이지로 돌아가기](#)

## PowerConnect 3424/P 및 PowerConnect 3448/P 설치

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- 1 장소 준비
- 1 포장 풀기
- 1 장치 장착
- 1 전원 공급 장치에 장치 연결
- 1 스택 설치
- 1 장치 시작 및 구성

### 장소 준비

PowerConnect 3424 /P 및 PowerConnect 3448/P 장치는 표준 48.26am(19인치) 장치 랙에 장착하거나, 테이블 윗면에 놓거나 벽면에 장착할 수 있습니다. 장치를 설치하기 전에 설치 장소가 다음과 같은 장소 요구사항을 만족하는지 확인하십시오.

- 1 **전원** — 설치하려는 장치 주위에 쉽게 접근할 수 있는 100~240VAC, 50~60Hz 콘센트가 있어야 합니다.
- 1 **일반** — 전면 패널에 있는 LED의 켜짐 상태를 확인하여 예비 전원 공급 장치(RPS)를 올바르게 설치합니다.
- 1 **PoE 모델** — 전면 패널에 있는 PoE LED의 켜짐 상태를 확인하여 RPS를 올바르게 설치합니다.
- 1 **틈새** — 운영자 액세스에 충분한 전면 틈새를 제공합니다. 케이블 연결, 전원 연결 및 환기에 틈새를 제공합니다.
- 1 **케이블 연결** — 케이블 연결은 무선 송신기, 브로드캐스트 증폭기, 전력 선 및 형광등 설비와 같은 전기 잡음을 피면하여 경유하도록 합니다.
- 1 **환경 요구사항** — 장치 작동시 주위 온도 범위는 0~50°C(32~122°F)이고 상대 습도는 최대 95%(부전도)입니다.


### 포장 풀기

#### 포장 내용물

장치 포장을 풀 때 다음 품목이 들어 있는지 확인하십시오.

- 1 장치/스위치
- 1 AC 전원 케이블
- 1 RS-232 교차 케이블
- 1 풀이 문은 고무 패드
- 1 랙 설치용 랙 장착 키트 또는 벽면 장착 키트
- 1 설명서 CD
- 1 제품 정보 안내

#### 장치 포장 풀기

 **주:** 장치의 포장 상자를 풀기 전에 포장을 점검하여 손상된 흔적이 있으면 즉시 보고하십시오.

- 1 상자를 깨끗한 평면에 놓으십시오.
- 1 상자를 열거나 상자 덮개를 제거하십시오.
- 1 장치를 상자에서 꺼내고 안전하고 깨끗한 표면에 놓으십시오.
- 1 모든 포장 재료를 제거하십시오.
- 1 장치와 주변기기가 손상되었는지 점검하십시오. 손상되었으면 즉시 보고하십시오.

## 장치 장착

다음의 장착 지시사항은 PowerConnect 3424/P 및 PowerConnect 3448/P 장치에 적용됩니다. 콘솔 포트는 후면 패널에 있습니다. 전원 커넥터는 후면 패널에 있습니다. 예비 전원 공급 장치(RPS)를 연결하는 것은 옵션이지만 연결하는 것이 좋습니다. RPS 커넥터는 장치의 후면 패널에 있습니다.

## 랙에 설치

**⚠ 주의:** 연결되어 있거나 스위치를 지원하는 장치에 대한 안전 지침은 제품 정보 안내에 있는 안전 지침을 참조하십시오.

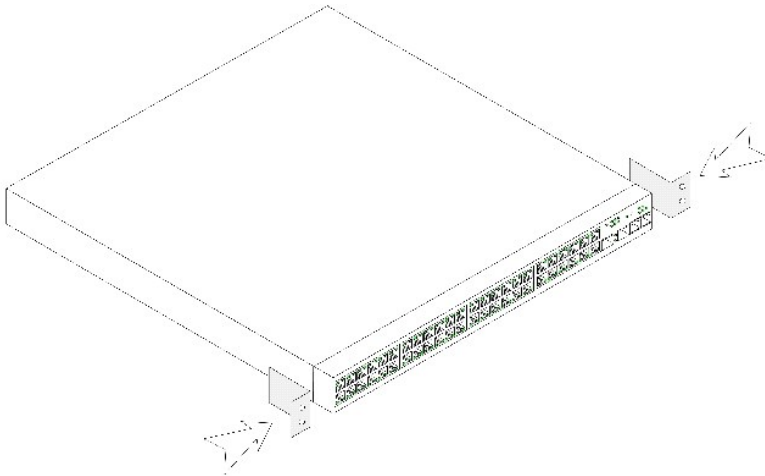
**⚠ 주의:** 랙 또는 캐비닛에 장치를 장착하기 전에 모든 장치의 케이블 연결을 끊으십시오.

**⚠ 주의:** 여러 장치를 랙에 장착할 때 상향식으로 장착하십시오.

1. 제공된 랙 장착 브래킷을 장치의 한쪽에 놓아 장치의 장착 구멍과 랙 장착 브래킷의 장착 구멍이 정렬되도록 하십시오.

다음 그림은 브래킷 장착 위치를 보여줍니다.

그림 3-1. 랙 장착용 브래킷 설치



2. 제공된 나사를 랙 장착 구멍에 넣고 드라이버로 조이십시오.
3. 장치의 다른쪽에 있는 랙 장착 브래킷에도 동일한 과정을 반복하십시오.
4. 장치를 48.26cm(19인치) 랙에 놓고 장치의 랙 장착 구멍과 랙의 장착 구멍이 정렬되도록 하십시오.
5. 랙 나사(제공되지 않음)를 사용하여 장치를 랙에 고정하십시오. 상단 나사 쌍을 조이기 전에 하단 나사 쌍을 조이십시오. 환기구를 막지 않도록 하십시오.

## 평면에 설치

장치를 랙에 설치하지 않는 경우 평면에 설치해야 합니다. 표면은 장치와 장치 케이블의 무게를 지탱할 수 있어야 합니다.

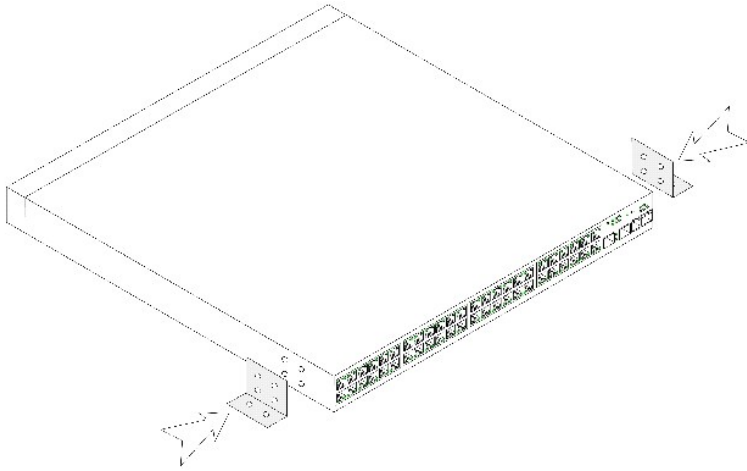
1. 풀이 묻은 고무 패드를 새시 일면의 표시된 위치에 각각 부착하십시오.
2. 장치를 평면에 놓고 각 옆면에 5.08cm(2인치), 뒤면에 12.7cm(5인치) 공간을 보장하십시오.
3. 장치가 올바르게 환기할 수 있도록 하십시오.

## 벽면에 장치 설치

1. 제공된 벽면 장착 브래킷을 장치의 한쪽에 놓아 장치의 장착 구멍과 랙 장착 브래킷의 장착 구멍이 정렬되도록 하십시오. 다음 그림은 브래킷 장착 위치를 보여줍니다.

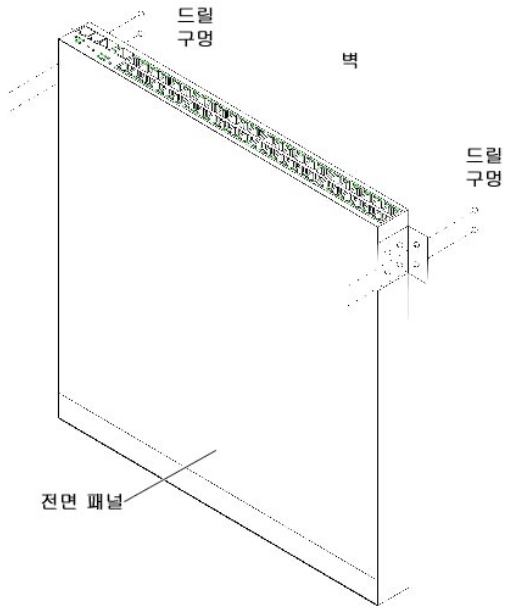


그림 3-2. 벽면 장착용 브래킷 설치



2. 제공된 나사를 랙 장착 구멍에 넣고 드라이버로 조입니다.
3. 장치의 다른쪽에 있는 벽면 장착 브래킷에도 동일한 과정을 반복합니다.
4. 장치를 설치할 벽면의 위치에 장치를 놓으십시오.
5. 장치를 고정할 나사의 위치를 벽면에 표기해 놓으십시오.
6. 구멍을 뚫고 모든 플러그(제공되지 않음)를 표기된 위치의 구멍에 맞추십시오.
7. 나사(제공되지 않음)를 사용하여 장치를 벽면에 고정하십시오. 환기구를 막지 않도록 하십시오.

그림 3-3. 벽면에 장치 고정



## 터미널에 연결

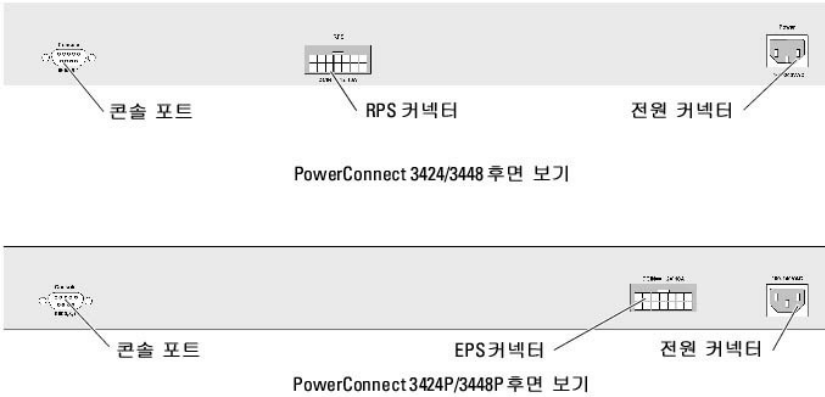
1. RS-232 교차 케이블을 ASCII 터미널이나 터미널 에뮬레이션 소프트웨어를 실행하는 데스크톱 시스템의 직렬 커넥터에 연결하십시오.
2. 케이블의 다른 끝에 있는 양 DB-9 커넥터를 장치 직렬 포트 커넥터에 연결하십시오.

## 전원 공급 장치에 장치 연결

제공되는 AC 전원 케이블을 후면 패널에 있는 AC 전원 커넥터에 연결하십시오.

**주:** 이 경우에는 전원 케이블을 접지된 AC 콘센트에 연결하지 마십시오. "[장치 시작 및 구성](#)"에서 자세히 설명한 단계에 따라 전원에 장치를 연결하십시오.

그림 3-4. 후면 패널 전원 커넥터



장치를 전원에 연결한 후 전면 패널의 LED를 살펴서 장치가 올바르게 연결되고 작동하는지 확인하십시오.

## 스택 설치

### 개요

각 장치는 독립 실행형 장치로 작동할 수 있거나 스택의 구성요소가 될 수 있습니다. 스택당 최대 6개의 장치나 최대 192개 포트가 지원됩니다.

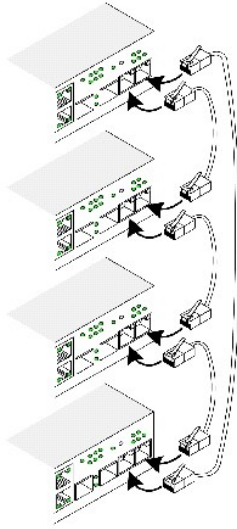
모든 스택에는 마스터 장치가 있고, 스택에 연결되어 있는 임의의 장치가 구성요소인 마스터 백업 장치도 있을 수 있습니다.

### 스태킹 PowerConnect 3400 직렬 스위치

각 PowerConnect 3400 직렬 스택에는 단일 마스터 장치가 포함되고 마스터 백업 장치가 있을 수 있으며 나머지 장치는 스택 구성요소로 간주됩니다.

PowerConnect 3400 직렬 스위치에는 스택용 RJ-45 기가비트 이더넷 포트(G3 및 G4)가 사용됩니다. 추가 장치 주변기기를 추가할 필요없이 스택용 용량이 장치에 추가됩니다. 장치를 함께 스택하려면, 표준 범주 5 케이블을 스택에 있는 맨 위 장치의 포트 G3과 스택에 있는 해당 장치의 바로 아래에 있는 장치의 포트 G4에 끼웁니다. 모든 장치가 연결될 때까지 이 과정을 반복합니다. 스택의 맨 아래에 있는 장치의 포트 G3을 스택의 맨 위에 있는 장치의 포트 G4에 연결합니다.

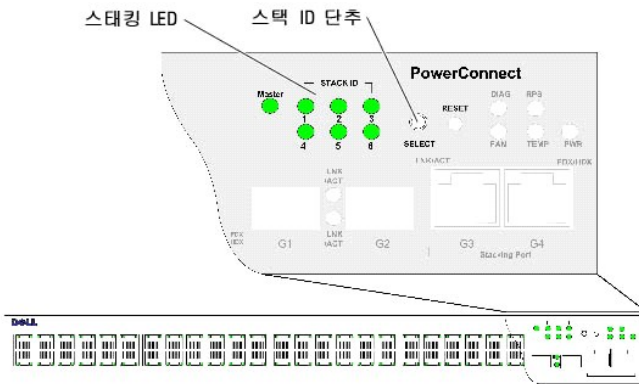
그림 3-5. 스택링 케이블 다이어그램



**주:** 스택킹 모드에서 G3 및 G4로 지정된 포트는 EWS에 표시되지 않습니다. 이 효과는 장치에서 나타나지 않습니다. 이는 포트가 다른 스택킹용 색인을 수신하기 때문입니다.

스택 장치 확인은 스택 ID 단추를 사용하여 장치 전면 패널에서 수행할 수 있습니다.

그림 3-6. 스택킹 구성 및 식별 패널



각 스택 장치에는 고유 장치 식별 ID가 있는데 스택에서 장치 위치 및 기능을 정의할 수 있습니다. 장치가 독립 실행형 장치이면 스택 LED는 켜지지 않습니다. 기본 설정은 독립 실행형입니다.

장치 ID는 스택 ID 단추를 사용하여 수동으로 구성합니다. 장치 ID는 스택 ID LED에 의해 표시됩니다. 장치 ID 1 및 2는 마스터 및 백업 마스터 장치용이고 장치 ID 3-6은 구성요소 장치용입니다.

## 장치 ID 선택 과정


장치 ID 선택 과정은 다음과 같습니다.

1. 독립 실행형/마스터 장치 콘솔 포트가 RS-232 교차 케이블을 통해 VT100 터미널 장치 또는 VT100 터미널 에뮬레이터에 연결되도록 하십시오.
2. AC 전원 소켓의 위치를 지정하십시오.
3. AC 전원 소켓을 비활성화하십시오.

4. 장치를 AC 전원 소켓에 연결하십시오.
5. AC 전원 소켓을 활성화하십시오.


장치가 시동하면 구성된 LED 번호(이전에 저장된 장치 ID에 해당)가 깜박이기 시작합니다. LED는 15초간 깜박입니다. 이 15초 동안에 해당 스택 ID LED가 켜질 때까지 스택 ID 단추를 눌러 해당 스택 ID를 선택합니다.


6. **선택 과정** — 스택 ID LED 번호를 확장하려면 스택 ID 단추를 계속하여 누르십시오. LED 6이 깜박일 때 스택 ID 단추를 누르면 장치가 독립 실행형으로 구성됩니다. 스택 ID 단추를 다시 누르면 스택 ID가 1로 확장되고 장치 1 및 장치 2는 마스터가 활성화된 장치로 됩니다. 마스터 선택 과정은 "[스태킹 개요](#)"를 참조하십시오.
7. **선택 과정 종료** — 15초간 깜박이는 기간이 시작되면 장치 ID 선택 과정은 완료됩니다. 스택 ID 단추는 응답이 없고 장치 ID는 이 기간의 마지막에 LED ID 깜박임으로 설정됩니다.

 **주:** 이러한 단계는 모든 스택 구성요소에 전원이 공급되고 해당 스택 ID가 선택될 때까지 한 번에 한 장치씩 수행해야 합니다. 한 번에 한 장치씩 단계를 수행하면 각 장치당 스택 ID를 선택하는 시간이 충분합니다. 그러나 전체 스택은 장치가 시동하기 전에 "[스태킹 케이블 다이어그램](#)"에 따라 케이블을 연결해야 합니다.

## 장치 시작 및 구성

모든 외부 연결을 완료한 후 장치에 터미널을 연결하여 장치를 구성하십시오. 추가 고급 기능 수행은 "[고급 구성](#)" 절에 설명되어 있습니다.

 **주:** 진행하기 전에 해당 제품의 발행 정보를 읽어보십시오. 발행 정보는 Dell 지원 웹 사이트인 [support.dell.com](http://support.dell.com)에서 다운로드하십시오.

 **주:** 최신 개정판의 사용자 설명서는 Dell 지원 웹 사이트인 [support.dell.com](http://support.dell.com)에서 참조하는 것이 좋습니다.

## 장치에 연결

장치를 구성하려면 장치가 콘솔에 연결되어 있어야 합니다. 그러나 장치가 스택의 부품이고 스택에 있는 마스터 장치라고 하는 장치만 터미널에 연결해야 합니다. 스택이 단일 장치로 작동하기에 마스터 장치만 구성됩니다.

## 장치에 터미널 연결


장치에는 장치 모니터링 및 구성용 터미널 에뮬레이션 소프트웨어를 실행하는 터미널 데스크탑 시스템에 연결할 수 있는 콘솔 포트가 제공됩니다. 콘솔 포트 커넥터는 데이터 터미널 장치(DTE) 커넥터로 구현된 수 DB-9 커넥터입니다.

콘솔 포트를 사용하려면 다음이 필요합니다.

1. 직렬 포트가 장착되어 있고 VT100 터미널 에뮬레이션 소프트웨어를 실행하는 VT100 호환 터미널 또는 데스크탑 또는 휴대용 시스템
1. 콘솔 포트용 양 DB-9 커넥터와 터미널용 적절한 커넥터를 가진 RS-232 교차 케이블

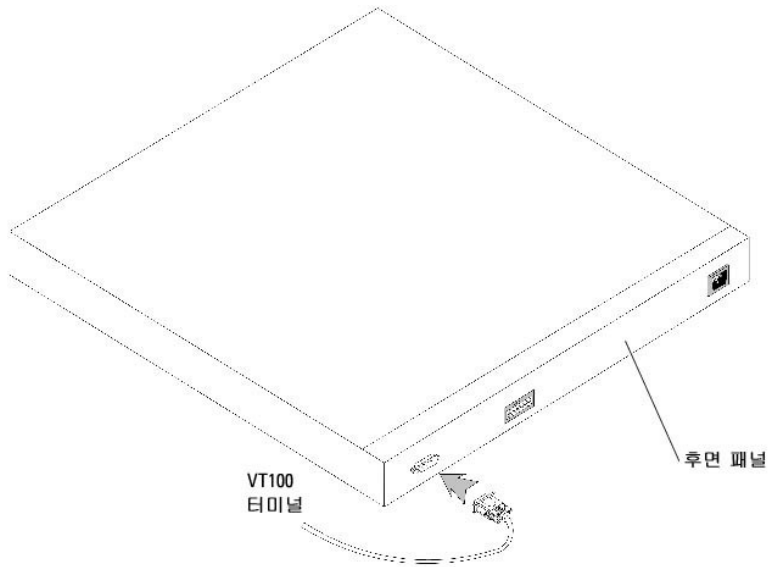
터미널을 장치 콘솔 포트에 연결하려면:


1. 제공된 RS-232 교차 케이블을 VT100 터미널 에뮬레이션 소프트웨어를 실행하는 터미널에 연결하십시오.
2. 적절한 직렬 포트(직렬 포트 1 또는 직렬 포트 2)를 선택하여 콘솔에 연결하십시오.
3. 데이터 속도를 9600보드로 설정하십시오.
4. 데이터 형식을 8 데이터 비트, 1 정지 비트 및 패리티가 없음으로 설정하십시오.
5. 흐름 제어를 없음으로 설정하십시오.
6. 속성에서, 에뮬레이션 모드에 VT100을 선택하십시오.
7. 기능, 화살표 및 Ctrl 키에 터미널 키를 선택하십시오. 터미널 키(Windows 키가 **아님**) 설정으로 하십시오.

 **주의사항:** Microsoft® Windows® 2000과 함께 하이퍼터미널을 사용하는 경우, Windows 2000 서비스 팩 2 이상이 설치되어 있는지 확인하십시오. Windows 2000 서비스 팩 2가 설치되어 있으면 화살표 키는 하이퍼터미널 VT100 에뮬레이션에서 올바르게 기능을 수행합니다. Windows 2000 서비스 팩에 대한 내용은 [www.microsoft.com](http://www.microsoft.com)으로 가십시오.

8. RS-232 교차 케이블의 양 커넥터를 마스터 장치/독립 실행형 장치에 있는 장치 콘솔 포트에 직접 연결하고 조임 고정 나사를 조이십시오. PowerConnect 3400 직렬 콘솔 포트는 후면 패널에 있습니다.

그림 3-7. PowerConnect 3400 직렬 콘솔 포트에 연결



 주: 콘솔은 스택에 있는 임의의 장치의 콘솔 포트에 연결될 수 있지만 스택 관리는 스택 마스터(장치 ID 1 또는 2)에서만 수행됩니다.

[목차 페이지로 돌아가기](#)

## PowerConnect 3424/P 및 3448/P 구성

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

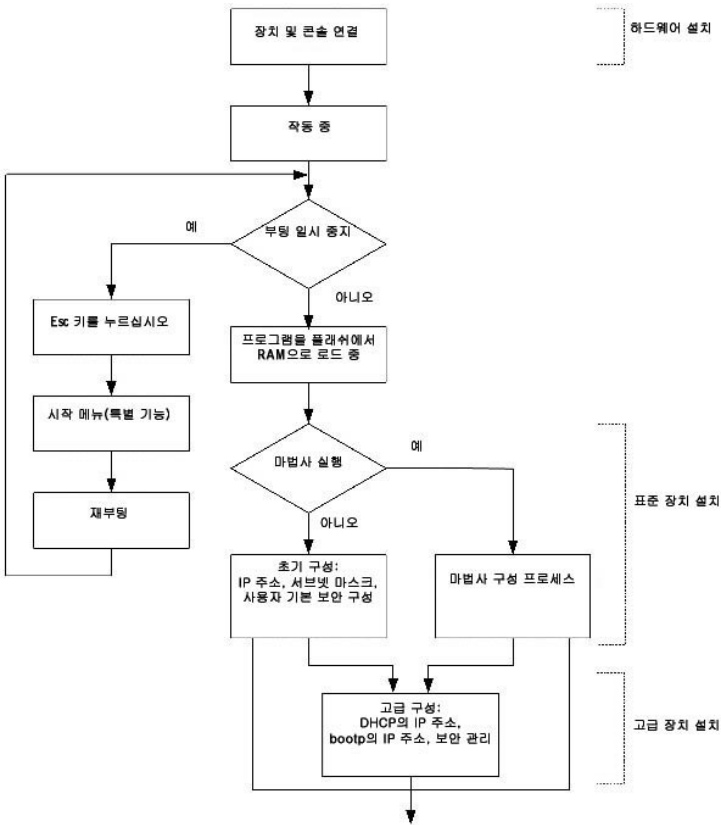
- [구성 절차](#)
- [고급 구성](#)
- [시작 절차](#)
- [포트 기본 설정](#)

### 구성 절차

모든 장치의 외부 연결이 완료된 후, 터미널이 장치에 연결되어 부팅 및 기타 절차를 감시합니다. 설치 순서 및 구성 절차는 다음 그림에 나와 있습니다.

**주:** 작업을 수행하기 전에 본 제품의 발행 정보를 읽어보십시오. [support.dell.com](http://support.dell.com)에서 발행 정보를 다운로드하십시오.

그림 4-1. 설치 및 구성 흐름





### 스위치 부팅

로컬 터미널이 이미 연결된 상태로 전원이 켜지면 스위치는 전원 공급 시 자체 검사(POST)를 진행합니다. POST는 장치가 초기화될 때마다 실행되며 장치가 완전히 부팅되기 전에 하드웨어 구성요소를 검사하여 장치가 충분히 작동 가능한지 여부를 결정합니다. 심각한 문제가 발견되면 프로그램 흐름이 중지됩니다. POST를 성공적으로 통과한 경우, 유효한 실행 가능한 이미지가 RAM에 로드됩니다. POST 메시지가 터미널에 표시되며 검사 성공이나 실패를 표시합니다.

부팅 프로세스는 약 30초 동안 실행됩니다.

## 초기 구성


 **주:** 작업을 수행하기 전에 본 제품의 발행 정보를 읽어보십시오. 발행 정보는 Dell 지원 웹 사이트인 [support.dell.com](http://support.dell.com)에서 다운로드하십시오.

 **주:** 초기 구성은 다음 조건을 가정합니다.

- n PowerConnect 장치는 구성된 적이 없으며 장치를 처음 받았을 때와 같은 상태입니다.
- n PowerConnect 장치를 정상적으로 부팅했습니다.
- n 콘솔 연결이 구성되고 콘솔 프롬프트가 VT100 터미널 장치의 화면에 표시됩니다.

초기 장치 구성은 콘솔 포트를 사용합니다. 초기 구성 후, 장치를 이미 연결된 콘솔 포트 또는 초기 구성 과정에서 정의한 인터페이스를 통해 원격으로 관리할 수 있습니다.

장치가 처음으로 부팅된 경우거나 장치가 구성되지 않아 구성 파일이 비어 있는 경우에 설치 마법사를 사용하라는 프롬프트가 표시됩니다. 설치 마법사는 초기 장치 구성 과정을 안내하며, 장치의 속도를 증가하고, 최대한 빨리 실행되도록 합니다.

 **주:** 장치를 구성하기 전에 다음 정보를 네트워크 관리자에게 문의하십시오.

- n 장치를 관리하는 VLAN 1 인터페이스에 지정되는 IP 주소(기본값으로, 각 포트는 VLAN 1의 구성요소임)
- n 네트워크의 IP 서브넷 마스크
- n 기본 라우트를 구성하기 위한 기본 게이트웨이(다음 홉 라우터) IP 주소
- n SNMP 커뮤니티 문자열 및 SNMP 관리 시스템 IP 주소(선택 사항)
- n 사용자 이름 및 암호

설치 마법사는 초기 스위치 구성 과정을 안내하며, 시스템의 속도를 증가하고, 최대한 빨리 실행되도록 합니다. 설치 마법사를 생략하고 장치 CLI 모드를 통해 장치를 수동으로 구성할 수 있습니다.

설치 마법사는 다음 필드를 구성합니다.

- 1 SNMP 커뮤니티 문자열 및 SNMP 관리 시스템 IP 주소(선택 사항)
- 1 사용자 이름 및 암호
- 1 장치 IP 주소
- 1 기본 게이트웨이 IP 주소

다음 내용이 표시됩니다.


```
Welcome to Dell Easy Setup Wizard
```


```
The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. The system will prompt you with a default answer; by pressing enter, you accept the default. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration.
```

```
Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+z].
```

[N]을 입력하면 설치 마법사가 종료됩니다. 60초 동안에 응답이 없으면 설치 마법사는 자동으로 종료되며 CLI 콘솔 프롬프트가 표시됩니다.

[Y]를 입력하면 설치 마법사는 초기 장치 구성 과정에 대화식 안내를 제공합니다.

 주: 60초 동안에 응답이 없고 BootP 서버가 네트워크에 있는 경우, BootP 서버에서 하나의 주소를 불러옵니다.

 주: 언제든지 [ctrl+z]를 입력하여 설치 마법사를 종료할 수 있습니다.

## 마법사 단계 1

다음 내용이 표시됩니다.

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network Manager) you can
```

- 1 Setup the initial SNMP version 2 account now.
- 1 Return later and setup additional SNMP v1/v3 accounts.

For more information on setting up SNMP accounts, please see the user documentation.

```
Would you like to setup the SNMP management interface now? (Y/N)[Y]Y
```

[N]을 입력하여 단계 2로 이동하십시오.

[Y]를 입력하여 설치 마법사를 계속하십시오. 다음 내용이 표시됩니다.

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the
particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to
this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems. For more information on adding
management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used: [Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: [0.0.0.0]
```

다음 내용을 입력하십시오.

- 1 SNMP 커뮤니티 문자열(예: Dell\_Network\_Manager)
- 1 관리 시스템의 IP 주소(A.B.C.D) 또는 임의의 관리 스테이션에서 관리할 수 있는 와일드카드 주소(0.0.0.0)

 주: 0으로 시작되는 IP 주소 및 마스크는 사용할 수 없습니다.

Enter 키를 누르십시오.

## 마법사 단계 2


다음 내용이 표시됩니다.

```
Now we need to setup your initial privilege (Level 15) user account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

다음 내용을 입력하십시오.



- 1 사용자 이름(예: "관리자")
- 1 암호 및 암호 확인

 주: 첫 번째와 두 번째 입력한 암호가 다른 경우, 사용자가 같은 암호를 입력할 때까지 프롬프트가 표시됩니다.

Enter 키를 누르십시오.

### 마법사 단계 3

다음 내용이 표시됩니다.

```
Next, an IP address is setup.
```

```
The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch.To setup an IP address:
```

```
Please enter the IP address of the device (A.B.C.D):[1.1.1.1]
```

```
Please enter the IP subnet mask (A.B.C.D or nn): [255.255.255.0]
```

IP 주소 및 IP 서브넷 마스크를 입력하십시오. 예를 들면, IP 주소로 1.1.1.1을 입력하고 IP 서브넷 마스크로 255.255.255.0을 입력하십시오.

Enter 키를 누르십시오.

### 마법사 단계 4

다음 내용이 표시됩니다.

```
Finally, setup the default gateway.
```

```
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
```

기본 게이트웨이를 입력하십시오.

Enter 키를 누르십시오. 다음 내용이 표시됩니다(예제로 제공한 매개변수가 사용됨).

```
This is the configuration information that has been collected:
```

```
=====
```

```
SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2
```

```
=====
```

## 마법사 단계 5

다음 내용이 표시됩니다.

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: (Y/N)[Y]Y
```

[N]을 입력하여 설치 마법사를 다시 시작하십시오.

[Y]를 입력하여 설치 마법사를 완료하십시오. 다음 내용이 표시됩니다.

```
Configuring SNMP management interface
Configuring user account.....
Configuring IP and subnet.....
```

```
Thank you for using Dell Easy Setup Wizard. You will now enter CLI mode.
```

## 마법사 단계 6

CLI 프롬프트가 표시됩니다.

---

## 고급 구성

이 절에서는 IP 주소의 동적 할당 및 인증, 승인 및 계정(AAA) 메커니즘에 기반한 보안 관리에 관한 정보를 제공하며, 다음 항목이 포함됩니다.

- 1 DHCP를 통한 IP 주소 구성
- 1 BOOTP를 통한 IP 주소 구성
- 1 보안 관리 및 암호 구성

DHCP 및 BOOTP를 통해 IP 주소를 구성하거나 수신하는 경우, 이러한 서버에서 수신한 구성 정보에는 IP 주소가 포함되며 서브넷 마스크 및 기본 게이트웨이도 포함될 수 있습니다.

## DHCP 서버에서 IP 주소 불러오기

DHCP 프로토콜을 사용하여 IP 주소를 불러오는 경우, 장치는 DHCP 클라이언트로 작동합니다. 장치가 재설정된 경우, DHCP 명령은 구성 파일에 저장되지만 IP 주소는 저장되지 않습니다. IP 주소를 DHCP 서버에서 불러오려면 다음 단계를 수행하십시오.

- 1 IP 주소를 불러오려면 DHCP 서버 또는 DHCP 서버가 있는 서브넷에 임의의 포트를 선택하고 연결하십시오.
- 2 다음 명령을 입력하여 IP 주소를 수신하는 데 사용되는 선택된 포트를 사용하십시오. 다음 예제에서 명령은 구성에 사용되는 포트 종류를 기반으로 합니다.
  - 1 동적 IP 주소 할당:

```
console# configure
```

```
console(config)# interface ethernet 1/e1
```

```
console(config-if)# ip address dhcp hostname powerconnect
```

```
console(config-if)# exit
```

```
console(config)#
```

1 VLAN에서 동적 IP 주소 할당:

```
console# configure
```

```
console(config)# interface ethernet vlan 1
```

```
console(config-if)# ip address dhcp hostname device
```

```
console(config-if)# exit
```

```
console(config)#
```

인터페이스는 IP 주소를 자동으로 수신합니다.


3. IP 주소를 확인하려면 다음 예제에서 표시한 것처럼 **show ip interface** 명령을 입력하십시오.


```
console# show ip interface
```


```
IP Address I/F Type
```

```
-----
```

```
100.1.1.1/24 vlan 1 dynamic
```

 **주:** DHCP 서버에 IP 주소를 불러오기 위해 장치 구성을 삭제할 필요는 없습니다.

 **주:** 구성 파일을 복사하는 경우, 동일한 DHCP 서버 또는 동일한 구성을 가지고 있는 DHCP 서버에 연결된 인터페이스에서 DHCP를 활성화하는 명령을 포함한 구성 파일을 사용하지 마십시오. 이러한 경우에 장치는 새 구성 파일을 불러오며, 그 파일로부터 부팅합니다. 장치는 새 구성 파일의 명령에 따라 DHCP를 활성화하며 DHCP는 동일한 파일을 다시 로드하도록 명령합니다.

 **주:** DHCP IP 주소를 구성하는 경우, 이 주소가 동적으로 할당되며 `ip address dhcp` 명령은 구성 파일에 저장됩니다. 마스터 오류 이벤트가 발생하면 백업은 DHCP 주소를 다시 불러오도록 시도합니다. 이러한 경우, 다음 중 하나의 결과가 발생할 수 있습니다.

- n 동일한 IP 주소가 할당될 수 있습니다.
- n 관리 스테이션과의 연결을 잃을 수 있는 부동한 IP 주소가 할당될 수 있습니다.
- n DHCP 서버가 다운될 수 있으므로 IP 주소 불러오기 오류가 발생되거나, 관리 스테이션과의 연결을 잃을 수 있습니다.


## BOOTP 서버에서 IP 주소 수신

표준 BOOTP 프로토콜이 지원되고 장치가 자동으로 IP 호스트 구성을 네트워크의 임의의 표준 BOOTP 서버에서 다운로드할 수 있게 합니다. 이러한 경우, 장치는 BOOTP 클라이언트로 작동합니다.

IP 주소를 BOOTP 서버에서 불러오려면:

1. IP 주소를 불러오려면 BOOTP 서버 또는 이러한 서버를 포함한 서브넷에 포트를 선택하고 연결하십시오.
2. 시스템 프롬프트에서 **delete startup configuration** 명령을 입력하여 플래쉬에서 시작 구성을 삭제하십시오.

장치는 구성 없이 재부팅되며 60초 내에 BOOTP 요청 전송을 시작합니다. 장치는 IP 주소를 자동으로 수신합니다.

 **주:** 장치 재부팅이 시작된 경우, ASCII 터미널 또는 키보드에서 임의로 입력하면 완료되기 전에 자동으로 BOOTP 프로세스가 취소되며 장치는 BOOTP 서버에서 IP 주소를 수신하지 않습니다.

다음 예제는 프로세스에 대해 설명합니다.

```
console> enable
```

```
console# delete startup-config
```

```
Startup file was deleted
```

```
console# reload
```

```
You haven't saved your changes. Are you sure you want to continue (y/n) [n]?
```

```
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

```
*****
```

```
/* the device reboots */
```

IP 주소를 확인하려면 **show ip interface** 명령을 입력하십시오.

장치는 이제 IP 주소로 구성됩니다.

## 보안 관리 및 암호 구성

사용자 액세스 권한, 특권 및 관리 방법을 관리하는 인증, 승인 및 계정(AAA) 메커니즘을 통해 시스템 보안을 제어합니다. AAA는 로컬 및 원격 사용자 데이터베이스를 모두 사용합니다. 데이터 암호화는 SSH 메커니즘을 통해 제어합니다.


시스템은 기본 암호가 구성되지 않은 상태로 전송되며 모든 암호는 사용자가 정의합니다. 사용자 정의 암호를 잃은 경우, **Startup** 메뉴에서 암호 복구 절차를 시작할 수 있습니다. 이 절차는 로컬 터미널에만 적용되며 장치에 암호를 입력하지 않고 로컬 터미널에서 장치에 한 번 액세스할 수 있습니다.


## 보안 암호 구성


보안 암호는 다음 서비스에 구성할 수 있습니다.

- 1 터미널
- 1 텔넷
- 1 SSH
- 1 HTTP

## 1 HTTPS

 **주:** 암호는 사용자가 정의합니다.

 **주:** 사용자 이름을 작성하는 경우, 기본 우선권은 1이며 액세스할 수 있지만 구성 권한은 없습니다. 우선권을 15로 설정하여 장치에 대한 액세스 및 구성 권한을 활성화합니다. 사용자 이름은 암호가 없이 특권 레벨 15를 지정할 수 있지만 항상 암호를 지정하는 것이 좋습니다. 지정된 암호가 없는 경우, 특권 사용자는 임의의 암호로 웹 인터페이스에 액세스할 수 있습니다.

 **주:** 암호 관리 명령으로 효력을 잃은 암호나 만료된 암호를 배제하여 암호를 보호할 수 있습니다. 자세한 내용은 "[보안 관리 및 암호 구성](#)"을 참조하십시오.

### 초기 터미널 암호 구성

초기 터미널 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)# aaa authentication login default line
```

```
console(config)# aaa authentication enable default line
```

```
console(config)# line console
```

```
console(config-line)# login authentication default
```

```
console(config-line)# enable authentication default
```

```
console(config-line)# password george
```

1 터미널 세션을 통해 처음으로 장치에 로그인하는 경우, 암호 프롬프트에 george를 입력하십시오.

1 장치의 모드를 활성화로 변경하는 경우, 암호 프롬프트에 george 를 입력하십시오.

### 초기 텔넷 암호 구성

초기 텔넷 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)# aaa authentication login default line
```

```
console(config)# aaa authentication enable default line
```

```
console(config)# line telnet
```

```
console(config-line)# login authentication default
```

```
console(config-line)# enable authentication default
```

```
console(config-line)# password bob
```

1 텔넷 세션을 통해 처음으로 장치에 로그인하는 경우, 암호 프롬프트에 bob를 입력하십시오.

1 장치 모드를 활성화로 변경하는 경우, bob를 입력하십시오.

## 초기 SSH 암호 구성

초기 SSH 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password jones.
```

- 1 SSH 세션을 통해 처음으로 장치에 로그인하는 경우, 암호 프롬프트에 jones를 입력하십시오.
- 1 장치 모드를 활성화로 변경하는 경우, jones를 입력하십시오.

## 초기 HTTP 암호 구성

초기 HTTP 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)# ip http authentication local

console(config)# username admin password user1 level 15
```


## 초기 HTTPS 암호 구성:

초기 HTTPS 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)# ip https authentication local

console(config)# username admin password user1 level 15
```


HTTPS 세션을 사용하기 위해 터미널, 텔넷 또는 SSH 세션을 사용하도록 구성하는 경우 다음 명령을 한 번 입력하십시오.

 **주:** 페이지 내용이 표시되도록 웹 브라우저에서 SSL 2.0 이상을 활성화하십시오.

```
console(config)# crypto certificate generate key_generate

console(config)# ip https server
```

처음 http 또는 https 세션을 활성화하는 경우, 사용자 이름에는 admin을 입력하고 암호에는 user1을 입력하십시오.

 주: Http 및 Https 서비스에는 레벨 15 액세스가 필요하며 구성 레벨 액세스에 직접 연결됩니다.

---

## 시작 절차

### 시작 메뉴 절차

시작 메뉴의 절차는 소프트웨어 다운로드, 플래쉬 제어 및 암호 복구가 포함됩니다. 진단 절차는 기술 지원 담당자 전용이며 설명서에 포함되지 않습니다.

장치 부팅 중에 시작 메뉴를 시작할 수 있습니다. 사용자 입력은 POST 검사가 끝나는 즉시 시작됩니다.

시작 메뉴를 시작하려면:

1. 전원을 켜고 자동 부팅 메시지를 보십시오.

\*\*\*\*\*

\*\*\*\*\* SYSTEM RESET \*\*\*\*\*

\*\*\*\*\*

Boot1 Checksum Test.....PASS

Boot1 Checksum Test.....PASS

Flash Image Validation Test.....PASS

BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49

Carrier board, based on PPC8247

128 MByte SDRAM. I-Cache 16 KB. D-Cache 16 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

2. 자동 부팅 메시지가 표시될 때 <Enter> 키를 눌러 시작 메뉴로 가십시오. 시작 메뉴 절차는 ASCII 터미널 또는 Windows HyperTerminal을 사용하여 수행할 수 있습니다.

[1] Download Software

[2] Erase Flash File


[3] Password Recovery Procedure


[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back

다음 절은 사용 가능한 시작 메뉴 옵션에 대해 설명합니다.

 **주:** 시작 메뉴에서 옵션을 선택하는 경우, 타임 아웃에 유의하십시오. 36초(기본값) 내에 선택하지 않은 경우, 장치는 타임 아웃됩니다. 기본값은 CLI를 통해 변경할 수 있습니다.

 **주:** 기술 지원 담당자만이 진단 모드(**옵션[4]**)를 실행할 수 있습니다. 때문에 진단 모드 시작은 본 안내서에서 설명하지 않습니다.

## 소프트웨어 다운로드 - 옵션[1]

소프트웨어 다운로드 절차는 새 버전을 다운로드하여 손상된 파일을 교체, 시스템 소프트웨어를 업데이트 또는 업그레이드하는 경우에 실행됩니다. 시작 메뉴에서 소프트웨어를 다운로드 하려면:

1. 시작 메뉴에서 [1]을 누르십시오. 다음 프롬프트가 표시됩니다.

Downloading code using XMODEM

\*\*\*\*\*

\*\*\* Running SW Ver. 1.0.0.30 Date 09-Jan-2005 Time 14:30:02

\*\*\*\*\*

HW version is

Base Mac address is : 00:00:b0:45:54:00

Dram size is : 128M bytes

Dram first block size is : 36864K bytes

Dram first PTR is : 0x1C00000

Flash size is: 16M

Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.



Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev. 0.0

-----

-- Unit Number 1 Standalone --

-----

BOXP\_high\_appl\_init: dpssIpcInitStandAlone

Tapi Version: v1.3.1.6P\_01\_03

Core Version: v1.3.1.6P\_01\_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is completed


01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed - operational.

01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: FAN# 1 status changed - operational.

2. 하이퍼터미널을 사용하는 경우, 하이퍼터미널 메뉴 막대에서 전송을 클릭하십시오.
3. 파일 이름 필드에서 다운로드하려는 파일의 파일 경로를 입력하십시오.
4. 프로토콜 필드에서 Xmodem 프로토콜이 선택되었는지 확인하십시오.
5. 전송을 누르십시오. 소프트웨어가 다운로드됩니다.

 **주:** 소프트웨어가 다운로드된 후, 장치가 자동으로 재부팅됩니다.

## 플래시 파일 지우기 - 옵션 [2]

일부 경우에는 장치 구성을 지워야 합니다. 구성을 지우면 CLI, EWS 또는 SNMP를 통해 구성된 모든 매개변수는 재구성되어야 합니다.

장치 구성을 지우려면:

1. 시작 메뉴에서 2초 내에 [2]를 눌러 플래시 파일을 지우십시오. 다음 메시지가 표시됩니다.

WARNING: About to erase a Flash file.

Are you sure (Y/N)? y

2. [Y]를 누르십시오. 다음 메시지가 표시됩니다.

Write Flash file name (Up to 8 characters, Enter for none.):config

File config (if present) will be erased after system initialization

=====  
Press Enter To Continue  
=====

3. config를 플래쉬 파일 이름으로 입력하십시오. 구성이 지워지고 장치가 재부팅됩니다.
4. 장치 초기 구성을 반복하십시오.


### 암호 복구 - 옵션 [3]

암호를 잃어버린 경우, 시작 메뉴에서 암호 복구 절차를 실행할 수 있습니다. 절차 실행 시 암호가 없이 장치에 한 번 액세스할 수 있습니다.

로컬 터미널에서만 입력하는 암호를 잃어버린 경우 복구하려면:

1. 시작 메뉴에서 [3]을 입력하고 <Enter> 키를 누르십시오. 암호가 삭제됩니다.  
선택 항목을 입력하고 'ESC' 키를 눌러 종료하십시오.

현재 암호는 무시됩니다!

 **주:** 장치 보호를 확보하기 위해 적용 가능한 관리 방법에 대한 암호를 재구성하십시오.

### 진단 모드 실행 - 옵션 [4]

기술 지원 담당자 전용

### 터미널 보드울 설정 - 옵션 [5]

터미널 보드울을 설정하려면 [5]를 입력하고 <Enter> 키를 누르십시오.

선택 항목을 입력하고 'ESC' 키를 눌러 종료하십시오.

새 장치 보드울 설정: 38,400

## TFTP 서버를 통해 소프트웨어 다운로드

이 절에는 TFTP 서버를 통해 장치 소프트웨어(시스템 및 부팅 이미지)를 다운로드하는 데 관한 지시사항이 포함됩니다. TFTP 서버는 소프트웨어를 다운로드하기 전에 구성되어야 합니다.

### 시스템 이미지 다운로드

장치는 시스템 이미지의 사본이 저장된 플래쉬 메모리 영역에서 시스템 이미지의 압축을 푸는 경우에 부팅 및 작동됩니다. 새 이미지는 다운로드된 후, 기타 시스템 이미지 사본을 위해 할당된 기타 영역에 저장됩니다.





console# reload

This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?

6. y를 입력하십시오. 장치가 재부팅됩니다.

---

## 포트 기본 설정

장치 포트 구성에 관한 일반 정보에는 자동 조정 메커니즘에 대한 간단한 설명과 전환 포트의 기본 설정이 포함됩니다.

## 자동 조정

자동 조정은 모든 10/100/1000BaseT 전환 포트의 속도 자동 감지, 이중 모드 및 흐름 제어를 활성화합니다. 자동 조정은 각 포트당 기본값으로 활성화됩니다.

자동 조정은 두 연결 파트너 사이에서 구성된 메커니즘인데 한 포트에서 전송율, 이중 모드 및 흐름 제어(흐름 제어 기본값은 비활성화됨) 기능을 해당 파트너에게 알려줄 수 있습니다. 그러면 두 포트는 그들 사이의 최대 공통 범위로 작동합니다.

자동 조정을 지원하지 않는 NIC를 연결했거나 자동 조정으로 설정하지 않은 경우, 장치 전환 포트 및 NIC는 모두 수동으로 동일한 속도 및 이중 모드로 설정해야 합니다.

연결 다른쪽의 스테이션이 전이중 방식으로 구성된 장치 100BaseT 포트와 자동 조정을 시도하는 경우, 자동 조정은 스테이션이 반이중 방식으로 작동하도록 시도하게 합니다.

## MDI/MDIX

장치는 모든 전환 10/100/1000Base 포트에서 직선 및 교차 케이블의 자동 감지를 지원합니다. 이 기능은 자동 조정의 일부이며 자동 조정이 활성화되면 활성화됩니다.

MDI/MDIX(교차 매체 종속 인터페이스)가 활성화된 경우, 케이블 선택의 오류 자동 수정을 사용할 수 있으며, 직선 케이블 및 교차 케이블 사이의 구별점을 감소합니다. 최종 스테이션에 대한 표준 배선은 MDI(매체 종속 인터페이스)이며, 허브 및 스위치에 대한 표준 배선은 MDIX입니다.

## 흐름 제어

장치는 전이중 모드로 구성된 포트에 대해 802.3x 흐름 제어를 지원합니다. 기본값으로, 이 기능은 비활성화됩니다. 포트당 이 기능을 활성화할 수 있습니다. 흐름 제어 메커니즘은 수신 측이 전송 측에 신호를 보내어 전송을 일시적으로 중지하여 버퍼 오버플로를 방지할 수 있게 합니다.

## 배압

장치는 반이중 모드로 구성된 포트에 대해 배압 기능을 지원합니다. 기본값으로, 이 기능은 비활성화됩니다. 포트당 이 기능을 활성화할 수 있습니다. 배압 메커니즘은 전송 측이 추가 처리량을 일시적으로 전송하지 못하게 합니다. 수신 측은 연결을 점유하여 추가 처리량에 대해 사용 불가능하게 할 수 있습니다.

## 전환 포트 기본 설정

다음 표에는 포트 기본 설정이 나와있습니다.

표 4-7 포트 기본 설정

기능	기본 설정
포트 속도 및 모드	10/100BaseT 구리: 자동 조정 100Mbps 전이종 방식 10/100/1000BaseT 구리/SFP: 자동 조정 1000Mbps 전이종 방식
포트 전달 상태	활성화
포트 태그화	태그화 없음
흐름 제어	끄기(임구에서 비활성화)
배암	끄기(임구에서 비활성화)

---

[목록 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

## Dell OpenManage 스위치 관리자 사용


Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [응용프로그램 시작](#)
- [인터페이스 이해](#)
- [스위치 관리자 단추 사용](#)
- [필드 정의](#)
- [CLI를 통해 장치에 액세스](#)
- [CLI 사용](#)


이 항목에서는 Dell OpenManage 스위치 관리자 사용자 인터페이스에 대한 소개를 제공합니다.

---

### 응용프로그램 시작

 **주:** 응용프로그램을 시작하기 전에 IP 주소를 정의해야 합니다. 자세한 내용은 [초기 구성](#)을 참조하십시오.

1. 웹 브라우저를 여십시오.
2. 주소 표시줄에 장치의 IP 주소를 입력하고 키를 누르십시오.
3. **로그인** 창이 표시되면 사용자 이름과 암호를 입력하십시오.

 **주:** 암호는 대소문자를 구분하며 알파벳과 숫자로 구성됩니다.

4. **확인**을 클릭하십시오.

Dell OpenManage™ 스위치 관리자 홈 페이지가 표시됩니다.

---

### 인터페이스 이해

홈 페이지에는 다음 뷰가 들어 있습니다.

1. 트리 뷰 — 홈 페이지 왼쪽에 있는 트리 뷰는 기능 및 해당 구성요소의 확장 가능한 뷰를 제공합니다.
1. 장치 뷰 — 홈 페이지의 오른쪽에 있는 장치 뷰는 장치 뷰, 정보나 표 영역 및 구성 지시사항을 제공합니다.

그림 5-1. 스위치 관리자 구성요소

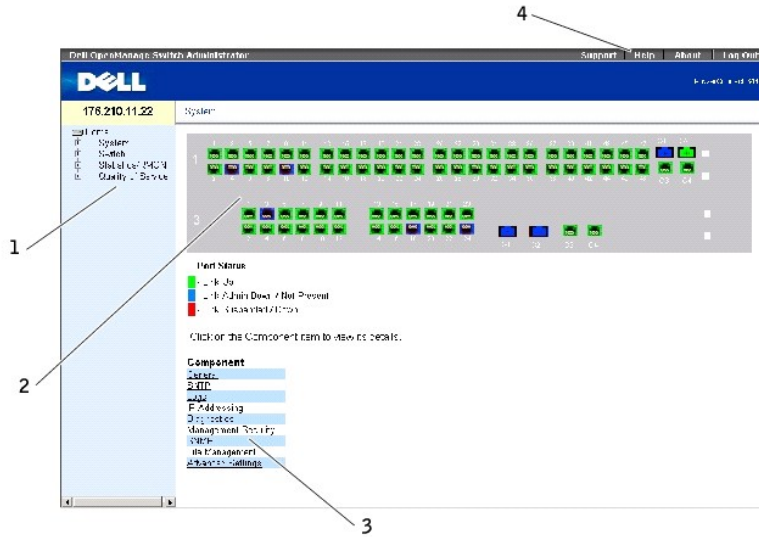


표 5-8 인터페이스 구성요소를 해당 번호와 함께 나열합니다.

표 5-8. 인터페이스 구성요소

구성요소	설명
1	트리 뷰에는 여러 가지 장치 기능 목록이 들어 있습니다. 트리 뷰의 브랜치를 확장하여 특정 기능의 모든 구성요소를 볼 수 있거나 축소하여 기능의 구성요소를 숨길 수 있습니다. 수직 막대를 오른쪽으로 끌어서 트리 영역을 확장하여 구성요소의 전체 이름을 표시할 수 있습니다.
2	장치 뷰는 장치 포트, 현재 구성 및 상태, 표 정보 및 기능 구성요소에 대한 정보를 제공합니다. 선택된 옵션에 근거하여 장치 뷰의 맨 아래 영역에서는 다른 장치 정보 및/또는 매개변수 구성 대화상자를 표시합니다.
3	구성요소 목록에는 기능 구성요소의 목록을 포함합니다. 트리 뷰의 기능을 확장하여 구성요소를 볼 수도 있습니다.
4	정보 단추는 장치 정보 및 Dell 지원에 액세스하도록 합니다. 자세한 내용은 <a href="#">정보 단추</a> 를 참조하십시오.

## 장치 표시

홈 페이지에는 장치 전면 패널의 그래픽 표시가 들어 있습니다.

그림 5-2. PowerConnect 장치 포트 표시등




포트 색상은 특정 포트가 현재 활성 상태인지 표시합니다. 포트는 다음의 색상으로 될 수 있습니다.

표 5-9. PowerConnect 포트 및 스택링 표시등

구성요소	설명
포트 표시등	
녹색	포트는 현재 활성 상태입니다.
적색	포트에 오류가 발생했습니다.



정색	포트는 현재 비활성 상태입니다.
적색	장치는 현재 스택에 연결되지 않았습니다.

 **주:** 포트 LED는 OpenManage 스위치 관리자의 PowerConnect 전면 패널에 반영되지 않습니다. LED 상태는 실제 장치 보기에 의해서만 결정됩니다. 그러나 스테킹 LED는 스테킹 포트 상태를 표시합니다. LED에 대한 자세한 내용은 [LED 정의](#)를 참조하십시오.

## 스위치 관리자 단추 사용

이 항목에서는 OpenManage 스위치 관리자 인터페이스에 있는 단추를 설명합니다. 인터페이스 단추는 다음 범주로 분류됩니다.

### 정보 단추

정보 단추는 OpenManage 스위치 관리자 인터페이스에 대한 정보뿐만 아니라 온라인 지원 및 온라인 도움말도 사용하도록 합니다.

표 5-10. 정보 단추

단추	설명
지원	<a href="http://support.dell.com">support.dell.com</a> 에서 Dell 지원 페이지를 여십시오.
도움말	장치 구성 및 관리에 도움이 되는 정보가 들어있는 온라인 도움말. 온라인 도움말 페이지는 문맥에 의존합니다. 예를 들어, IP 주소 페이지가 열린 경우, <b>도움말을 클릭하면</b> 해당 페이지에 대한 도움말 항목이 표시됩니다.
정보	버전, 빌드 번호 및 Dell 저작권 정보가 들어있습니다.
로그아웃	로그아웃 창을 여십시오.

### 장치 관리 단추

장치 관리 단추는 장치를 쉽게 구성하는 방법에 대한 정보를 제공하며 다음을 포함합니다.

표 5-11. 장치 관리 단추

단추	설명
변경 사항 적용	장치에 세트 변경 사항을 적용합니다.
추가	표 또는 대화상자에 정보를 추가합니다.
델넷	델넷 세션을 시작합니다.
쿼리	쿼리 표.
전체 표시	장치 표를 표시합니다.
왼쪽 화살표/오른쪽 화살표	목록 사이에서 정보를 이동합니다.
새로 고침	장치 정보를 새로 고칩니다.
전체 카운터 재설정	통계 카운터를 지웁니다.
인쇄	<b>네트워크 관리 시스템</b> 페이지 및/또는 표 정보를 인쇄합니다.
끝기	통계 차트를 즉석 생성합니다.

## 필드 정의

사용자 정의된 필드는 OpenManage 스위치 관리자 웹 페이지에서 별도로 설명하지 않은 경우 1~159개 문자를 포함할 수 있습니다. 다음을 제외한 모든 글자 또는 문자는 사용할 수 있습니다.

- 1 \
- 1 /
- 1 :
- 1 \*


1 ?  
1 <  
1 >  
1 |

---

## CLI를 통해 장치에 액세스

터미널 포트에 직접 연결하거나 텔넷 연결을 통해 장치를 관리할 수 있습니다. 텔넷 연결을 통해 액세스한 경우 CLI 명령을 사용하기 전에 장치에 IP 주소를 정의하고 장치 액세스에 사용된 워크스테이션을 장치에 연결하십시오.


초기 IP 주소 구성에 대한 자세한 내용은 "[초기 구성](#)"을 참조하십시오.

 **주:** CLI를 사용하여 원격으로 장치에 액세스하기 전에 장치에 소프트웨어를 다운로드하십시오.

## 터미널 연결

1. 장치 전원을 켜고 시동이 완료될 때까지 기다리십시오.
2. console> 프롬프트가 표시된 경우 enable를 입력하고 키를 누르십시오.
3. 장치를 구성하고 필요한 명령을 입력하여 필요한 작업을 완료하십시오.
4. 완료하면 관리자 EXEC 모드 명령 **끝내기**를 입력하십시오.

세션이 종료됩니다.

 **주:** 다른 사용자가 관리자 EXEC 명령 모드의 시스템에 로그인한 경우, 현재 사용자는 로그오프되고 새 사용자가 로그인됩니다.

## 텔넷 연결

텔넷은 터미널 에뮬레이션 TCP/IP 프로토콜입니다. RS-232 터미널은 TCP/IP 프로토콜 네트워크를 통해 가상으로 로컬 장치에 연결할 수 있습니다. 텔넷은 원격 로그인이 필요한 로컬 로그인 터미널의 대안입니다.

장치는 최대 4개의 동시 텔넷 세션을 지원하여 장치를 관리합니다. 모든 CLI 명령은 텔넷 세션에서 사용할 수 있습니다.

텔넷 세션을 시작하려면:

1. 시작 > 실행을 선택하십시오.

실행 창이 열립니다.

2. 실행 창의 열기 필드에 텔넷 <IP 주소>를 입력하십시오.
3. 확인을 클릭하십시오.

텔넷 세션이 시작됩니다.

---

## CLI 사용

이 항목에서는 CLI 사용에 대한 정보를 제공합니다.

## 명령 모드 개요

CLI는 명령 모드로 나뉩니다. 각 명령 모드에는 특정 명령 세트가 있습니다. 터미널 프롬프트에 물음표를 입력하면 해당 특정 명령 모드에 사용할 수 있는 명령 목록이 표시됩니다.

각 모드에서 특정 명령은 한 명령 모드에서 다른 명령 모드로 탐색하는 데 사용됩니다.

CLI 세션 초기화 동안, CLI 모드는 사용자 EXEC 모드입니다. 명령의 제한된 하위 세트만이 사용자 EXEC 모드에서 사용할 수 있습니다. 이 레벨은 터미널 구성을 변경하지 않는 작업을 위해 예정되며 CLI와 같은 구성 하위 시스템에 액세스하는 데 사용됩니다. 다음 레벨인 관리자 EXEC 모드를 시작하려면 암호가 필요합니다(구성된 경우).

관리자 EXEC 모드는 장치 전역 구성에 액세스하도록 합니다. 장치의 특정 전역 구성일 경우, 다음 레벨인 전역 구성 모드를 시작하십시오. 암호가 필요하지 않습니다.


전역 구성 모드는 전역 레벨에서 장치 구성을 관리합니다.

인터페이스 구성 모드는 실제 인터페이스 레벨에서 장치를 구성합니다. 하위 명령이 필요한 인터페이스 명령은 하위 인터페이스 구성 모드라 불리는 다른 레벨이 있습니다. 암호가 필요하지 않습니다.

## 사용자 EXEC 모드

장치에 로그인한 후 EXEC 명령 모드는 활성화됩니다. 사용자 레벨 프롬프트는 꺾쇠 괄호(>)가 뒤에 따르는 호스트 이름으로 구성되었습니다. 예를 들어:

```
console>
```

 **주:** 초기 구성 동안 수정되지 않은 경우 기본 호스트 이름은 콘솔입니다.

사용자 EXEC 명령을 사용하면 원격 장치에 연결하고 임시적으로 터미널 설정을 변경하고 기본 검사를 수행하고 시스템 정보를 나열할 수 있습니다.

사용자 EXEC 명령을 나열하려면 명령 프롬프트에 물음표를 입력하십시오.

## 관리자 EXEC 모드

권한 액세스는 무단 액세스를 방지하고 작동 매개변수를 확인하도록 보호될 수 있습니다. 암호는 화면에 표시되며 대소문자를 구분합니다.

관리자 EXEC 모드 명령을 사용하고 나열하려면:

1. 프롬프트에 **enable**을 입력하고 키를 누르십시오.
2. 암호 프롬프트가 표시되면 암호를 입력하고 키를 누르십시오.

관리자 EXEC 모드 프롬프트는 호스트 이름 뒤에 #으로 형태로 표시됩니다. 예를 들어:

```
console#
```

관리자 EXEC 명령을 나열하려면 명령 프롬프트에 물음표를 입력하십시오.

관리자 EXEC 모드에서 사용자 EXEC 모드로 돌아가려면 **disable**을 입력하고 키를 누르십시오.

다음 예제는 관리자 EXEC 모드에 액세스한 다음 사용자 EXEC 모드로 돌아가는 데 대해 설명합니다.

```
console> enable
```

```
암호 입력: *****
```

```
console#
```

```
console# disable
```

```
console>
```

**끝내기** 명령을 사용하여 이전 모드로 돌아가십시오. 예를 들면, 인터페이스 구성 모드에서 전역 구성 모드로, 전역 구성 모드에서 관리자 EXEC 모드로 돌아갑니다.

## 전역 구성 모드

전역 구성 명령은 특정 프로토콜 또는 인터페이스가 아닌 시스템 기능에 적용됩니다.

전역 구성 모드에 액세스하려면 관리자 EXEC 모드 프롬프트에서 **configure** 명령을 입력하고 키를 누르십시오. 전역 구성 모드는 호스트 이름 뒤에 (config) 및 파운드 기호 #가 오는 형태로 표시됩니다.

```
console(config)#
```

전역 구성 명령을 나열하려면 명령 프롬프트에 물음표를 입력하십시오.

전역 구성 모드에서 관리자 EXEC 모드로 돌아가려면 **exit** 명령을 입력하거나 키를 누른 상태에서 키를 누르십시오.

다음 예제는 전역 구성 모드에 액세스한 다음 관리자 EXEC 모드로 돌아가는 방법에 대해 설명합니다.

```
console#
```

```
console# configure
```

```
console(config)# exit
```

```
console#
```

CLI 모드의 전체 목록에 대해서는 **Dell™ PowerConnect™ 3424/P 및 PowerConnect 3448/P CLI 설명서**를 참조하십시오.

---

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

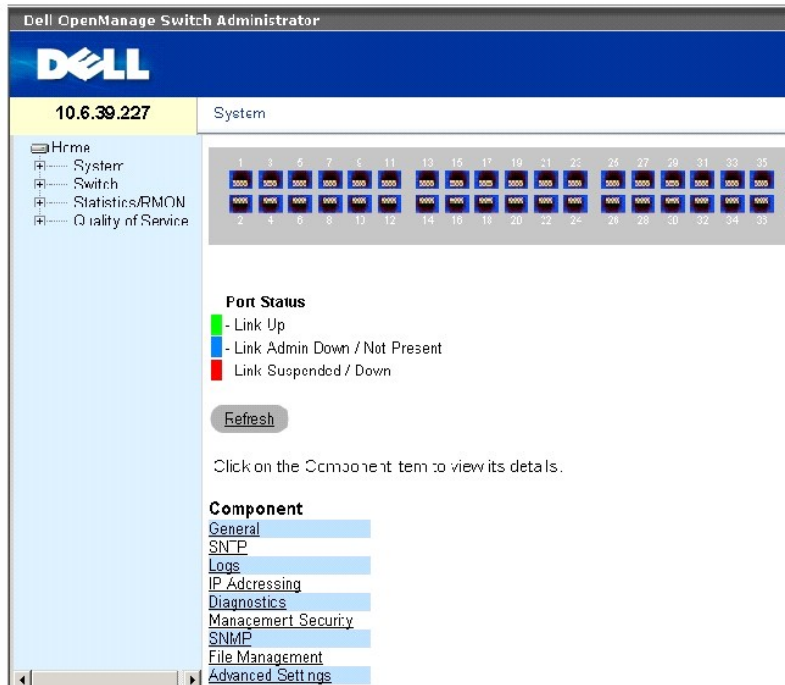
## 시스템 구성 정보

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [일반 스위치 정보 정의](#)
- [SNTP 설정 구성](#)
- [로그 관리](#)
- [IP Addressing 정의](#)
- [케이블 진단 실행](#)
- [스위치 보안 관리](#)
- [SNMP 매개변수 정의](#)
- [파일 관리](#)
- [일반 설정 구성](#)

이 절에서는 보안 기능을 포함하는 시스템 매개변수 정의, 스위치 소프트웨어 다운로드 및 스위치 재설정에 관한 정보를 제공합니다. **System** 페이지를 열려면 트리 뷰에서 **System**을 클릭하십시오.

그림 6-1. 시스템



## 일반 스위치 정보 정의

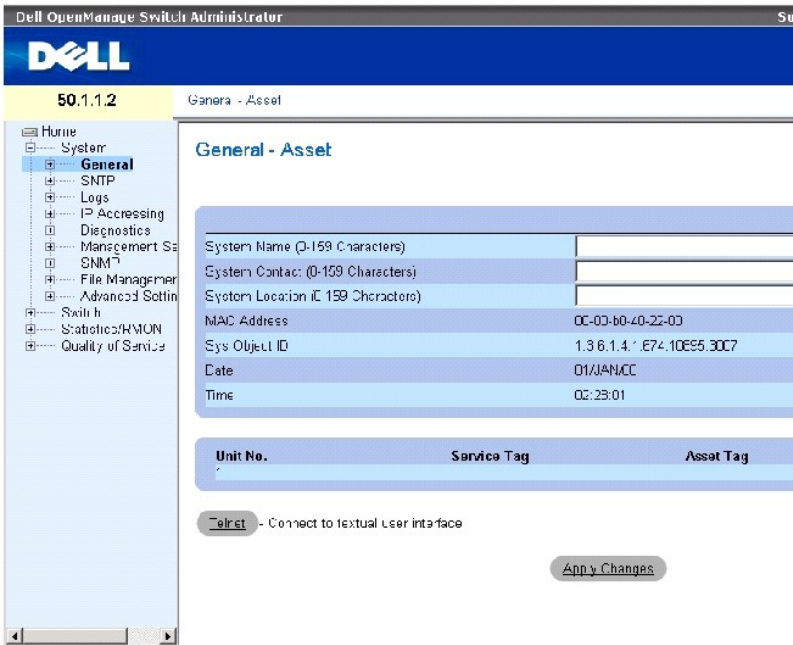
**General** 페이지에는 네트워크 관리자가 스위치 매개변수를 구성할 수 있는 페이지에 대한 링크가 들어 있습니다.

## 스위치 자산 정보 보기

**Asset** 페이지에는 시스템 이름, 위치 및 담당자, 시스템 MAC 주소, 시스템 개체 ID, 날짜, 시간 및 시스템 가동 시간을 포함한 일반 장치 정보를 구성하고 보는 데 필요한 매개변수가 들어 있

습니다. [Asset](#) 페이지를 열려면 트리 뷰에서 System → General → Asset을 클릭하십시오.

그림 6-2. 자산



[Asset](#) 페이지에는 다음 필드가 들어 있습니다.

**System Name (0-159 Characters)** — 사용자가 정의한 장치 이름을 정의합니다.

**System Contact (0-159 Characters)** — 문의할 담당자 이름입니다.

**System Location (0-159 Characters)** — 현재 실행 중인 시스템이 있는 위치입니다.

**MAC Address** — 장치 MAC 주소입니다.

**Sys Object ID** — 업체에서 기업의 네트워크 관리 서브시스템을 인증하는 ID입니다.

**Date (DD/MM/YY)** — 현재 날짜. 형식은 일, 월, 연도입니다. 예를 들면, 10/OCT/03은 2003년 10월 10일을 표시합니다.

**Time (HH:MM:SS)** — 시간을 표시합니다. 형식은 시간, 분, 초입니다. 예를 들면 20:12:21은 오후 8시 12분 21초를 표시합니다.

**Unit No.** — 장치 자산 정보가 표시되는 단위의 번호입니다.

**Service Tag** — 장치를 수리할 때 사용되는 서비스 참조 번호입니다.

**Asset Tag (0-16 Characters)** — 사용자가 정의한 장치 참조입니다.

Serial No.— 장치의 일련 번호입니다.

## 시스템 정보 정의

1. [Asset 페이지](#)를 여십시오.
2. 관련 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

시스템 매개변수가 정의되고 장치가 업데이트됩니다.

## 텔넷 세션 시작

1. [Asset 페이지](#)를 여십시오.
2. **Telnet**을 클릭하십시오.

텔넷 세션이 시작됩니다.

## CLI 명령을 사용하여 장치 정보 구성

다음 표에서는 [Asset](#) 페이지에 표시된 필드를 보고 설정하는 CLI 명령을 요약합니다.

표 6-12. 자산 CLI 명령

CLI 명령	설명
hostname name	장치 호스트 이름을 표시하거나 수정합니다.
snmp-server contact text	시스템 담당자를 설정합니다.
snmp-server location text	장치가 있는 위치에 대한 정보를 입력합니다.
clock set hh:mm:ss day month year	시스템 클럭 및 날짜를 수동으로 설정합니다.
show clock [detail]	시스템 클럭의 시간 및 날짜를 표시합니다.
show system id	서비스 태그 정보를 표시합니다.
show system	시스템 정보를 표시합니다.
asset-tag 텍스트	장치 자산 태그를 설정합니다.
show stack <1-6>	시스템 스택 정보를 표시합니다.
show system [unit 단위]	시스템 정보를 표시합니다.
show system id [unit 단위]	시스템 ID 정보를 표시합니다.

다음은 CLI 명령을 사용하여 장치 호스트 이름, 시스템 담당자 및 장치 위치를 정의하고 시스템 클럭의 시간 및 날짜를 설정하는 예입니다.

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York
```

```

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2

Console# clock set 13:32:00 7 Mar 2002

Console# show clock

15:29:03 Jun 17 2002

```

다음은 CLI 명령을 사용하여 독립형 장치의 시스템 정보를 표시하는 예입니다.

console# show system id	
Service tag	:
Serial number	: 51
Asset tag	:
console# show system	
System Description:	Ethernet Switch
System Up Time (days, hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK



Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

다음은 CLI 명령을 사용하여 스택 장치의 시스템 정보를 표시하는 예입니다.

console# <b>show system id</b>					
Unit	Serial number	Asset tag	Service tag		
----	-----	-----	-----		
1	893658972	mkt-1	89788978		
2	893658973	mkt-2	89788979		
3	893658974	mkt-3	89788980		
4	893658975	mkt-4	89788981		
5	893658976	mkt-5	89788982		
6	893658977	mkt-6	89788983		
console# <b>show system</b>					
Unit	Type				
----	-----				
1	PowerConnect 3424				
2	PowerConnect 3424				
3	PowerConnect 3428				

4	PowerConnect 3424P				
5	PowerConnect 3424P				
6	PowerConnect 3424P				
Unit	Main Power Supply	Redundant Power Supply			
	-----	-----			
1	OK				
2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
	-----	-----	-----	-----	-----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)	Temperature Sensor Status			
	-----	-----			

1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		

## 시스템 시간 설정 정의

**Time Synchronization** 페이지에는 로컬 하드웨어 클럭과 외부 SNTP 클럭의 시스템 시간 매개변수를 정의하는 필드가 들어 있습니다. 시스템 시간이 외부 SNTP 클럭을 사용하여 유지될 경우 외부 SNTP 클럭에 오류가 발생하면 시스템 시간은 로컬 하드웨어 클럭으로 전환됩니다. 그러면 장치에서 일광 절약 시간제를 사용할 수 있습니다. 다음은 국가별 일광 절약 시간제의 시작 및 종료 시간을 표시한 목록입니다.

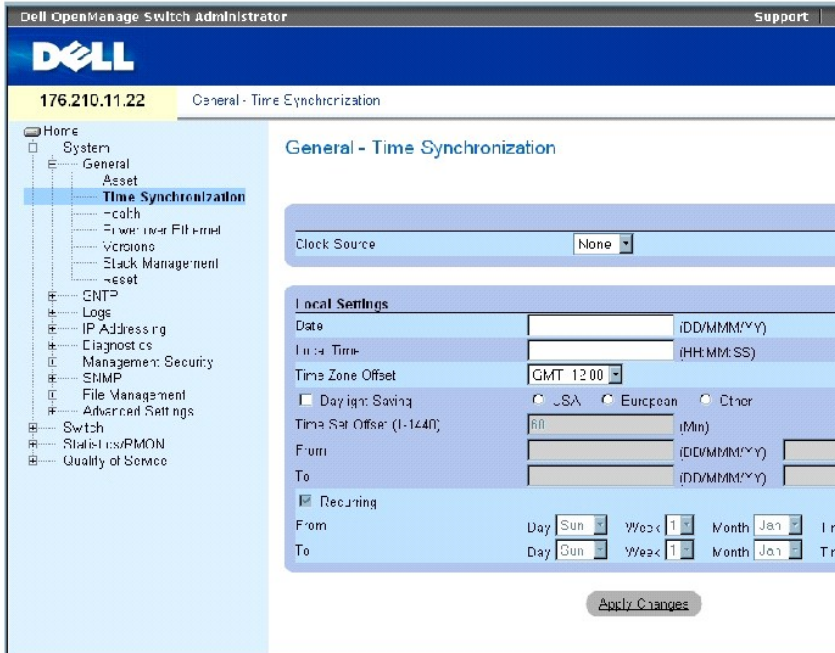
- 1 알바니아 — 3월 마지막 주~10월 마지막 주
- 1 호주 — 10월 31일~3월 31일
- 1 호주의 태즈메이니아 주 — 10월 1일~3월 31일
- 1 아르메니아 — 3월 마지막 주~10월 마지막 주
- 1 오스트리아 — 3월 마지막 주~10월 마지막 주
- 1 바하마 — 4월~10월(미국 서머 시간제와 병행)
- 1 벨로루시 — 3월 마지막 주~10월 마지막 주
- 1 벨기에 — 3월 마지막 주~10월 마지막 주
- 1 브라질 — 10월 세 번째 일요일~3월 세 번째 토요일. 일광 절약 시간제 기간에 브라질 남동부 대부분의 지역에서는 한 시간을 앞당겨 사용합니다.
- 1 칠레 — 이스터 섬, 3월 9일~10월 12일. 3월 첫 번째 일요일 또는 3월 9일 이후
- 1 중국 — 중국은 일광 절약 시간제를 실시하지 않습니다.
- 1 캐나다 — 4월 첫 번째 일요일~10월 마지막 일요일. 일광 절약 시간제는 주정부와 준주정부에서 관리합니다. 특정 지자체 지역에서는 예외도 있습니다.
- 1 쿠바 — 3월 마지막 일요일~10월 마지막 일요일
- 1 키프로스 — 3월 마지막 주~10월 마지막 주
- 1 덴마크 — 3월 마지막 주~10월 마지막 주
- 1 이집트 — 4월 마지막 금요일~9월 마지막 목요일
- 1 에스토니아 — 3월 마지막 주~10월 마지막 주
- 1 핀란드 — 3월 마지막 주~10월 마지막 주
- 1 프랑스 — 3월 마지막 주~10월 마지막 주
- 1 독일 — 3월 마지막 주~10월 마지막 주
- 1 그리스 — 3월 마지막 주~10월 마지막 주
- 1 헝가리 — 3월 마지막 주~10월 마지막 주
- 1 인도 — 인도는 일광 절약 시간제를 실시하지 않습니다.
- 1 이란 — 3월 1일~9월 1일
- 1 이라크 — 4월 1일~10월 1일
- 1 아일랜드 — 3월 마지막 주~10월 마지막 주
- 1 이스라엘 — 해마다 다릅니다.
- 1 이탈리아 — 3월 마지막 주~10월 마지막 주
- 1 일본 — 일본은 일광 절약 시간제를 실시하지 않습니다.

- 1 요르단 — 3월 마지막 주~10월 마지막 주
- 1 라트비아 — 3월 마지막 주~10월 마지막 주
- 1 레바논 — 3월 마지막 주~10월 마지막 주
- 1 리투아니아 — 3월 마지막 주~10월 마지막 주
- 1 룩셈부르크 — 3월 마지막 주~10월 마지막 주
- 1 마케도니아 — 3월 마지막 주~10월 마지막 주
- 1 멕시코 — 4월 첫 번째 일요일 2시~10월 마지막 일요일 2시
- 1 몰도바 — 3월 마지막 주~10월 마지막 주
- 1 몬테네그로 — 3월 마지막 주~10월 마지막 주
- 1 네덜란드 — 3월 마지막 주~10월 마지막 주
- 1 뉴질랜드 — 10월 첫 번째 일요일~3월 첫 번째 일요일 또는 15일 이후
- 1 노르웨이 — 3월 마지막 주~10월 마지막 주
- 1 파라과이 — 4월 6일~9월 7일
- 1 폴란드 — 3월 마지막 주~10월 마지막 주
- 1 포르투갈 — 3월 마지막 주~10월 마지막 주
- 1 루마니아 — 3월 마지막 주~10월 마지막 주
- 1 러시아 — 3월 마지막 주~10월 마지막 주
- 1 세르비아 — 3월 마지막 주~10월 마지막 주
- 1 슬로바키아 공화국 — 3월 마지막 주~10월 마지막 주
- 1 남아프리카 — 남아프리카는 일광 절약 시간제를 실시하지 않습니다.
- 1 스페인 — 3월 마지막 주~10월 마지막 주
- 1 스웨덴 — 3월 마지막 주~10월 마지막 주
- 1 스위스 — 3월 마지막 주~10월 마지막 주
- 1 시리아 — 3월 31일~10월 30일
- 1 대만 — 대만은 일광 절약 시간제를 실시하지 않습니다.
- 1 터키 — 3월 마지막 주~10월 마지막 주
- 1 영국 — 3월 마지막 주~10월 마지막 주
- 1 미국 — 4월 첫 번째 일요일 오전 2시~10월 마지막 일요일 오전 2시

SNTP에 대한 자세한 정보는 [SNTP 설정 구성](#)을 참조하십시오.

[Time Synchronization](#) 페이지를 열려면 트리 뷰에서 System → General → Time Synchronization을 클릭하십시오.

### 그림 6-3. 시간 동기화



[Time Synchronization](#) 페이지에는 다음 필드가 들어 있습니다.

### Clock Source

**클럭 소스** — 시스템 클럭을 설정할 때 사용하는 소스입니다. 가능한 필드 값은 다음과 같습니다.

**SNTP** — 시스템 시간이 SNTP 서버를 통해 설정되었음을 표시합니다. 자세한 정보는 [SNTP 설정 구성](#)을 참조하십시오.

**None** — 시스템 시간이 외부 소스에 의해 설정되지 않았음을 표시합니다.

### Local Settings

**Date** — 시스템 날짜를 정의합니다. 필드 형식은 DD/MMM/YY입니다. 예를 들면 04/May/50과 같습니다.

**Local Time** — 시스템 시간을 정의합니다. 필드 형식은 HH/MM/SS입니다. 예를 들면 21/15/03과 같습니다.

**Time Zone Offset** — 그리니치 표준시(GMT)와 로컬 시간의 시차입니다. 예를 들면 파리의 시간대 오프셋은 GMT +1.00이고, 뉴욕의 로컬 시간은 GMT -5:00입니다.

특정 연도의 특정 날짜 또는 연도와는 무관하게 반복되는 설정을 따르는 두 가지 종류의 일광 설정이 있습니다. 특정 연도의 특정 설정인 경우 **Daylight Savings** 영역을, 반복 설정인 경우 **Recurring** 영역을 채우십시오.

**Daylight Savings** — 장치 위치에 맞는 장치의 일광 절약 시간제(DST)를 사용하도록 설정합니다. 가능한 필드 값은 다음과 같습니다.

**USA** — 장치에서 4월 첫 번째 일요일 오전 2시에 DST로 전환하고, 10월 마지막 일요일 오전 2시에 표준 시간으로 다시 전환합니다.

**European** — 장치에서 3월 마지막 일요일 오전 1시에 DST로 전환하고, 10월 마지막 일요일 오전 1시에 표준 시간으로 다시 전환합니다. 유럽 옵션은 EU 회원국 및 EU 표준을 사용하는 기타 유럽 국가에 적용됩니다.

**Other** — DST 정의는 장치의 위치에 따라 사용자 정의됩니다. **Other**를 선택하면 **From** 및 **To** 필드를 반드시 정의해야 합니다.

**Time Set Offset(1 - 1440)** — 유럽 및 미국 이외의 국가에서는 DST의 시간을 분 단위로 설정할 수 있습니다. 기본 시간은 60분입니다.

**From** — 미국 또는 유럽 이외의 국가에서 DST가 시작되는 시간을 정의합니다. 한 필드에는 DD/MMM/YY 형식의 날짜를, 다른 필드에는 시간을 정의합니다. 예를 들면, DST가 2007년 10월 25일 오전 5시 00분에 시작되는 경우 두 필드는 각각 25/Oct/07 및 05:00으로 정의됩니다. 가능한 필드 값은 다음과 같습니다.

**Date** — DST가 시작되는 날짜입니다. 가능한 필드 범위는 1~31입니다.

**Month** — DST가 시작되는 달입니다. 가능한 필드 범위는 1월~12월입니다.

**Year** — 구성된 DST가 시작되는 연도입니다.

**Time** — DST가 시작되는 시간입니다. 시간 형식은 시:분입니다. 예를 들면 05:30:00과 같습니다.

**To** — 미국 또는 유럽 이외의 국가에서 DST가 끝나는 시간을 정의합니다. 한 필드에는 DD/MMM/YY 형식의 날짜를, 다른 필드에는 시간을 정의합니다. 예를 들면, DST가 2008년 3월 23일 오전 12시 00분에 끝나는 경우 두 필드는 각각 23/Mar/08 및 12:00으로 정의됩니다. 가능한 필드 값은 다음과 같습니다.

**Date** — DST가 끝나는 날짜입니다. 가능한 필드 범위는 1~31입니다.

**Month** — DST가 끝나는 달입니다. 가능한 필드 범위는 1월~12월입니다.

**Year** — 구성된 DST가 끝나는 연도입니다.

**Time** — DST가 끝나는 시간입니다. 시간 형식은 시:분입니다. 예를 들면 05:30과 같습니다.

**Recurring** — 미국 또는 유럽 이외의 DST가 매년 일정한 국가에서 DST가 시작되는 시간을 정의합니다. 가능한 필드 값은 다음과 같습니다.

**From** — 해마다 DST가 시작되는 시간을 정의합니다. 예를 들면, DST는 현지 시간으로 항상 4월 두 번째 일요일 오전 5시 00분에 시작됩니다. 가능한 필드 값은 다음과 같습니다.

**Day** — 매년 DST가 시작되는 요일입니다. 가능한 필드 범위는 일요일~토요일입니다.

**Week** — 매년 DST가 시작되는 주입니다. 가능한 필드 범위는 1~5입니다.

**Month** — 매년 DST가 시작되는 달입니다. 가능한 필드 범위는 1월~12월입니다.

**Time** — 매년 DST가 시작되는 시간입니다. 시간 형식은 시:분입니다. 예를 들면 02:10과 같습니다.

**To** — 매년 DST가 끝나는 반복 시간을 정의합니다. 예를 들면 DST는 현지 시간으로 항상 10월 네 번째 금요일 오전 5시 00분에 끝납니다. 가능한 필드 값은 다음과 같습니다.

**Day** — 매년 DST가 끝나는 요일입니다. 가능한 필드 범위는 일요일-토요일입니다.

**Week** — 매년 DST가 끝나는 주입니다. 가능한 필드 범위는 1-5입니다.

**Month** — 매년 DST가 끝나는 달입니다. 가능한 필드 범위는 1월~12월입니다.

**Time** — 매년 DST가 끝나는 시간입니다. 시간 형식은 시:분입니다. 예를 들면 05:30과 같습니다.

### 클럭 소스 선택

1. [Time Synchronization](#) 페이지를 여십시오.
2. **Clock Source** 필드를 정의하십시오.
3. Apply Changes를 클릭하십시오.

클럭 소스가 선택되고 장치가 업데이트됩니다.


### 로컬 클럭 설정 정의

1. [Time Synchronization](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. Apply Changes를 클릭하십시오.

로컬 클럭 설정이 적용됩니다.

### CLI 명령을 사용하여 클럭 설정 정의

다음 표에서는 [Time Synchronization](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

 **주:** 일광 절약 시간제를 설정하기 전에 다음 단계를 수행해야 합니다.

1. 일광 절약 시간제를 구성하십시오.
2. 시간대를 정의하십시오.
3. 클럭을 설정하십시오.

예를 들면 다음과 같습니다.

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

표 6-13. 클럭 설정 CLI 명령

CLI	설명
clock source sntp	시스템 클럭의 외부 시간 소스를 구성합니다.
clock time zone 시간 오프셋 [minutes 분 오프셋][zone 약자]	표시할 시간대를 설정합니다.
clock summer-time	자동으로 서머 타임(일광 절약 시간제)으로 전환하도록 시스템을 구성합니다.
clock summer-time recurring {usa   eu   주 일 월 시:분 주 일 월 시:분} [offset 오프셋] [zone 약자]	자동으로 미국 및 유럽 표준에 따라 일광 절약 시간제로 전환하도록 시스템을 구성합니다.

clock summer-time date 날짜 달 연도 시:분 날짜 달 연도 시:분[offset 오프셋]  
[zone 약자]

자동으로 특정 기간(일/월/연도 형식)에 대해 구성된 서머 타임(일광 절약 시간제)으로 전환하도록 시스템을 구성합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# clock
timezone -6 zone CST

console(config)# clock
summer-time recurring
first sun apr 2:00 last
sun oct 2:00

console(config)# clock
source sntp

console(config)# interface
ethernet e14

console(config-if)# sntp
client enable

console(config-if)# exit

console(config)# sntp
broadcast client enable
```

## 시스템 상태 정보 보기

[System Health](#) 페이지에서는 장치의 전원 및 환기 설비 정보가 포함된 물리적 장치 정보를 표시합니다. [System Health](#) 페이지를 열려면 트리 뷰에서 **System** → **General** → **Health**를 클릭하십시오.

그림 6-4. 시스템 상태

Dell OpenManage Switch Administrator

176.210.11.22 General - Health

System Health


Unit No.	Power Supply Status	Fan Status
1 1	PS1:  RPS:	Fan1:  Fan2:  Fan3:
1 3	PS1:  RPS:	Fan1:  Fan2:  Fan3:




[System Health](#) 페이지에는 다음 필드가 들어 있습니다.

**Unit No.** — 장치 자산 정보가 표시되는 단원의 번호입니다.


**Power Supply Status** — 장치에는 2개의 전원 공급 장치가 있습니다. 전원 공급 장치 1은 인터페이스에서 **PS1**로 표시되고, 예비 전원 공급 장치는 **RPS**로 표시됩니다. 가능한 필드 값은 다음과 같습니다.


 — 전원 공급 장치가 정상적으로 작동합니다.

 — 전원 공급 장치가 정상적으로 작동하지 않습니다.

**Not Present** — 전원 공급 장치가 없습니다.

**Fan Status** — 비 PoE 장치에는 2개의 팬이 있지만 PoE 장치에는 5개의 팬이 있습니다. 각 팬은 인터페이스에서 팬과 팬 번호로 표시됩니다. 가능한 필드 값은 다음과 같습니다.

 — 팬이 정상적으로 작동합니다.

 — 팬이 정상적으로 작동하지 않습니다.

**Not Present** — 팬이 없습니다.

**Temperature** — 장치가 작동되는 온도입니다. 장치 온도는 섭씨로 표시됩니다. 장치 온도의 일계값은 0~40C(32~104F)입니다. 다음 표에서는 5도를 증분으로 화씨 온도를 표시합니다.

표 6-14. 섭씨의 화씨 변환표

섭씨	화씨
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

## CLI 명령을 사용하여 시스템 상태 정보 보기

다음 표에서는 [System Health](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-15. 시스템 상태 CLI 명령

CLI 명령	설명
--------	----

<code>show system [unit 단위]</code>	시스템 정보를 표시합니다.
------------------------------------	----------------

다음은 시스템 상태 CLI 명령의 예입니다.

console# <b>show system</b>				
System Description: Ethernet switch				
System Up Time (days, hour:min:sec): 1,22:38:21				
System Contact:				
System Name: RS1				
System location:				
System MAC Address: 00.10.B5.F4.00.01				
Sys Object ID: 1.3.6.1.4.1.674.10895.3004				
Type: PowerConnect 3424				
Temperature Sensors:				
Unit	Sensor	Temperature (Celsius)		Status
----	-----	-----		-----
1	1		41	OK
1	2		41	OK
2	1		42	OK
2	2		42	OK
Unit	Power Supply	Source	Status	
----	-----	-----	-----	
1	Main	AC	OK	

2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	-----		
1	CPU	OK		
2	CPU	OK		

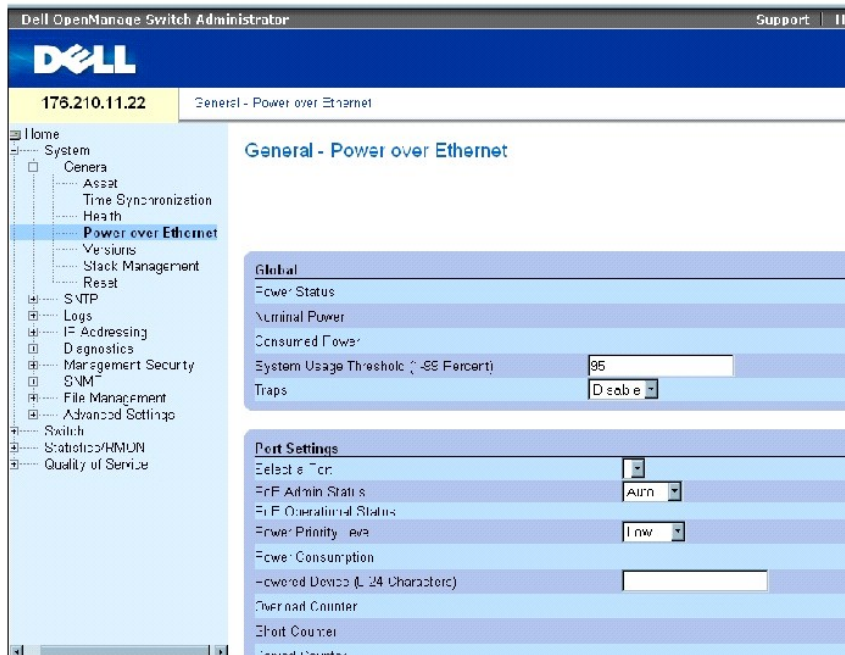
## PoE(이더넷상의 전원) 관리

PoE(이더넷상의 전원)에서는 네트워크 인프라를 업데이트하거나 수정하지 않고 기존 LAN 케이블을 통해 장치에 전원을 공급합니다. PoE를 사용하면 전원 가까이에 네트워크 장치를 놓지 않아도 됩니다.

전원 사용 장치(PD)는 IP 전화처럼 PowerConnect 전원 공급 장치에서 전원을 공급 받는 장치입니다. PD는 이더넷 포트를 통해 PowerConnect에 연결됩니다. PD는 모든 PowerConnect 3424P의 24 FE 포트 또는 모든 PowerConnect 3448P의 48 FE 포트를 통해 연결되었습니다.

[Power Over Ethernet](#) 페이지를 열려면 트리 뷰에서 **System**→**General**→**Power over Ethernet**을 클릭하십시오.

그림 6-5. 이더넷상의 전원



[Power Over Ethernet](#) 페이지에는 다음 필드가 들어 있습니다.

- 1 Global
- 1 Port Settings

## Global

PoE 전역 설정 항목에는 다음 필드가 들어 있습니다.

**Power Status** — 인라인 전원 상태를 표시합니다.

**On** — 전원 공급 장치가 작동 중임을 표시합니다.

**Off** — 전원 공급 장치가 작동하지 않음을 표시합니다.

**Faulty** — 전원 공급 장치가 작동 중지지만 오류가 발생했음을 표시합니다. 예를 들면 전원 과부하나 단락이 발생한 경우입니다.

**Nominal Power** — 장치에서 공급할 수 있는 전원의 실제 양을 표시합니다. 필드 값은 와트(W) 단위로 표시됩니다.

**Consumed Power** — 장치에서 소비한 전원의 양을 표시합니다. 필드 값은 와트(W) 단위로 표시됩니다.

**System Usage Threshold(1-99%)** — 경보가 생성되기 전에 사용한 전원(%)을 표시합니다. 필드 값은 1~99 % 단위로 표시됩니다. 기본값은 95%입니다.

**Traps** — PoE 장치 트랩의 수신을 활성화하거나 비활성화합니다. 기본값은 비활성화입니다.

## Port Settings

**Select a Port** — PoE 매개변수가 정의되고, 선택한 포트에 연결된 전원 사용 인터페이스에 할당된 특정 인터페이스를 표시합니다.

**PoE Admin Status** — 장치 PoE 모드를 표시합니다. 가능한 필드 값은 다음과 같습니다.

**Auto** — DDP(장치 복구 프로토콜)를 활성화하고, PoE 모드를 사용하는 장치에 전원을 공급합니다. DDP를 사용하면 장치에서 장치 인터페이스에 연결된 전원 장치를 감지하고 해당 분류를 확인할 수 있습니다. 이는 기본 설정입니다.

**Never** — DDP(장치 복구 프로토콜)를 비활성화하고, PoE 모드를 사용하여 장치에 전원 공급을 중단합니다.

**PoE Operational Status** — 포트가 PoE에 활성화되어 있는지를 표시합니다. 가능한 필드 값은 다음과 같습니다.

**On** — 장치가 인터페이스에 전원을 전달함을 표시합니다.

**Off** — 장치가 인터페이스에 전원을 전달하지 않음을 표시합니다.

**Test Fail** — 전원 장치 테스트에 실패했음을 표시합니다. 예를 들면, 포트를 활성화할 수 없거나 전원 장치에 전원을 전달할 때 포트를 사용할 수 없는 경우입니다.

**Testing** — 전원 장치가 테스트 중임을 표시합니다. 예를 들면, 전원 장치에 대해 전원 공급 장치를 통해 전원을 공급 받고 있는지 확인하는 테스트를 수행 중입니다.

**Searching** — 현재 PowerConnect 장치에서 전원 장치를 검색 중임을 표시합니다. 검색은 PoE 작동의 기본 상태입니다.

**Fault** — PowerConnect 장치가 전원 장치에서 오류를 탐지했음을 표시합니다. 예를 들면 전원 장치 메모리를 읽을 수 없는 경우입니다.

**Power Priority Level** — 전원 공급 수준이 낮은 경우 포트 우선순위를 결정합니다. 전원 공급 수준이 낮은 경우 포트 전원 우선순위가 사용됩니다. 필드 기본값은 낮음입니다. 예를 들면 전원 공급 장치가 99% 사용되는 상태에서 포트 1의 우선순위는 높음이지만 포트 3의 우선순위는 낮음인 경우 포트 1은 우선순위에 따라 먼저 전원을 공급 받고 포트 3은 전원 공급을 받지 못할 수 있습니다.

**Critical** — 가장 높은 전원 우선순위를 지정합니다.

**High** — 두 번째로 높은 전원 우선순위를 지정합니다.

**Low** — 가장 낮은 전원 우선순위를 지정합니다.

**Power Consumption** — 선택한 인터페이스에 연결된 전원 장치에 할당된 전원의 양을 표시합니다. 장치가 전원 장치 별로 분류되고, PowerConnect 장치에서 이 분류 정보를 사용합니다. 필드 값은 W(와트) 단위로 표시됩니다. 가능한 필드 값은 다음과 같습니다.

**0.44 – 12.95** — 포트에 전원 소비 수준이 0.44~12.95W로 할당되었음을 표시합니다.

**0.44 – 3.8** — 포트에 전원 소비 수준이 0.44~3.8W로 할당되었음을 표시합니다.

**3.84 – 6.49** — 포트에 전원 소비 수준이 3.84~6.49W로 할당되었음을 표시합니다.

**6.49 – 12.95** — 포트에 전원 소비 수준이 6.49~12.95W로 할당되었음을 표시합니다.

**Power Device (0-24 characters)** — 사용자 정의된 전원 장치 설명을 제공합니다. 필드에는 최대 24자를 입력할 수 있습니다.

**Overload Counter** — 총 전원의 과부하 발생 횟수를 표시합니다.

**Short Counter** — 총 전원의 단락 발생 횟수를 표시합니다.

**Denied Counter** — 전원 장치에서 전원 공급을 취소했음을 표시합니다.

**Absent Counter** — 더 이상 전원 장치가 감지되지 않음으로 전원 장치에 전원 공급이 중단된 횟수를 표시합니다.

**Invalid Signature Counter** — 유효하지 않은 서명을 수신한 횟수를 표시합니다. 서명은 전원 장치가 PSE에 자체를 식별하는 수단입니다. 서명은 전원 장치 감지, 분류 또는 유지 관리 중에 생성됩니다.

## PoE 설정 정의

1. [Power Over Ethernet](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

PoE 설정이 정의되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 PoE 관리

다음 표에서는 [Power Over Ethernet](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-16. POE 설정

CLI 명령	설명
<code>power inline {auto   never}</code>	인터페이스에서 인라인 전원의 관리 모드를 구성합니다.
<code>power inline powered-device 전원 장치종류</code>	전원 장치 종류에 대한 설명을 추가합니다.
<code>power inline priority {critical   high   low}</code>	인라인 전원 관리 측면에서 인터페이스의 우선순위를 구성합니다.
<code>power inline usage-threshold</code>	경보를 시작하는 임계값을 구성합니다.
<code>power inline traps enable</code>	PoE 장치 트랩을 활성화합니다.
<code>show power inline [ethernet interface ]</code>	PoE 구성 정보를 표시합니다.

다음은 PoE CLI 명령의 예입니다.

Console# <code>show power inline</code>					
Power: On					
Nominal Power: 150 Watts					
Consumed Power: 120 Watts (80%)					
Usage Threshold: 95%					
Traps: Enabled					
Port	Powered Device	State	Priority	Status	Classification [W]
----	-----	----	-----	-----	-----
1/e1	IP Phone Model A	Auto	High	On	0.44 - 12.95
2/e1	Wireless AP Model	Auto	Low	On	0.44 - 3.84
3/e1		Auto	Low	Off	N/A

Port	Powered Device	State	Priority	Status	Classification [W]
1/1e	IP Phone Model A	Auto	High	On	0.44 - 12.95
Overload Counter: 1					
Short Counter: 0					
Denied Counter: 0					
Absent Counter: 0					
Invalid Signature Counter: 0					

## 버전 정보 보기

[Versions](#) 페이지에는 현재 실행 중인 하드웨어 및 소프트웨어 버전에 대한 정보가 들어 있습니다. [Versions](#) 페이지를 열려면 트리 뷰에서 **System** → **General** → **Version**을 클릭하십시오.

그림 6-6. 버전

Dell OpenManage Switch Administrator

176.210.11.22    General - Versions

Home

- System
  - General
    - Asset
    - Time Synchronization
    - Health
    - Power over Ethernet
    - Versions**
    - Stack Management
    - Reset
  - SNTP
  - Logs
  - IP Addressing
  - Diagnostics
  - Management Security
  - SNMP
  - File Management
  - Advanced Settings
- Switch
  - Statistics/RMON
  - Quality of Service

**General - Versions**

Unit No.	Software Version	Root Version
1	7.00	
2	7.31	

[Versions](#) 페이지에는 다음 필드가 들어 있습니다.

**Unit No.** — 장치 버전이 표시되는 단원의 번호입니다.

**Software Version** — 현재 장치에서 실행 중인 소프트웨어 버전입니다.

**Boot Version** — 현재 장치에서 실행 중인 부팅 버전입니다.

**Hardware Version** — 현재 장치의 하드웨어 버전입니다.

## CLI를 사용하여 장치 버전 표시

다음 표에서는 [Versions](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-17. 버전 CLI 명령

CLI 명령	설명
<code>show version</code>	시스템 버전 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console> show version

SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)

Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)

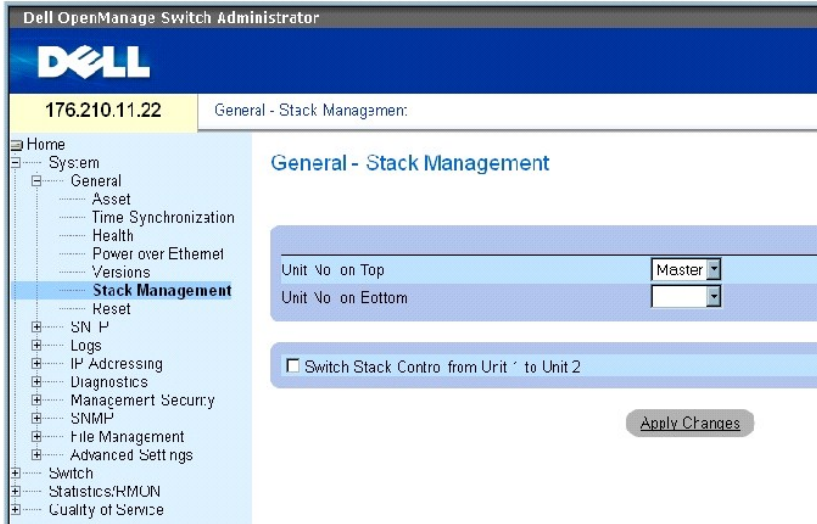
HW version 1.0.0
```

## 스택 멤버 관리

[Stack Management](#) 페이지를 통해 네트워크 관리자가 전체 스택 또는 특정 장치를 재설정할 수 있습니다. [Stack Management](#) 페이지를 열려면 트리 뷰에서 **System** → **General** → **Stack Management**를 클릭하십시오.

그림 6-7. 스택 관리





**주:** 장치를 재설정하기 전에 실행 구성 파일에서 변경한 사항을 모두 저장하십시오. 그러면 현재 장치 구성을 잃어버리지 않습니다. 구성 파일 저장에 대한 자세한 정보는 [파일 관리](#)를 참조하십시오.

**Unit No. on Top** — 첫 번째 스택 멤버 번호입니다. 가능한 값은 마스터 및 1-6 사이의 수입니다.

**Unit No. on Bottom** — 두 번째 스택 멤버 번호입니다. 가능한 값은 마스터 및 1-6 사이의 수입니다.

**Switch Stack Control from Unit 1 to Unit 2** — 현재 스택 마스터를 백업 마스터 단원으로 전환할 수 있습니다.

**주:** 마스터 단원을 재설정하면 전체 스택이 재설정됩니다.

### 스택 마스터 간 전환

1. [Stack Management](#) 페이지를 여십시오.
2. Switch Stack Control from Unit 1 to Unit 2 확인란을 선택하십시오.
3. [Apply Changes](#)를 클릭하십시오.

확인 메시지가 표시됩니다.

4. OK를 클릭하십시오.

장치가 재설정됩니다. 장치가 재설정된 후, 사용자 이름과 암호를 입력하는 프롬프트가 표시됩니다.

### 스택 표시 순서 구성

1. [Stack Management](#) 페이지를 여십시오.
2. 상위 및 하위 단원을 정의하여 스택 위상을 정의합니다. 이 두 단원은 서로 이웃해야 합니다.
3. [Apply Changes](#)를 클릭하십시오.

표시 순서는 System 페이지에서 재구성됩니다.

### CLI 명령을 사용한 스택 관리

다음 표에서는 [Stack Management](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-18. 스택 관리 CLI 명령

CLI 명령	설명
reload	운영 체제를 다시 로드합니다.
stack reload	스택 멤버를 다시 로드합니다.
stack master	스택 마스터를 선택하도록 합니다.

다음은 CLI 명령의 예입니다.


```
console# reload
Are you sure you want to erase running configuration (y/n) [n]
```

## 장치 재설정

Reset 페이지를 통해 장치를 원격 위치에서 재설정할 수 있습니다. Reset 페이지를 열려면 트리 뷰에서 **System**→**General**→**Reset**을 클릭하십시오.

Reset 페이지에는 다음 필드가 들어 있습니다.

**Reset Unit No.** — 선택한 스택 멤버를 재설정합니다.

 **주:** 장치를 재설정하기 전에 시작 구성 파일에서 변경한 사항을 모두 저장하십시오. 그러면 현재 장치 구성을 잃어버리지 않습니다. 구성 파일 저장에 대한 자세한 정보는 "[파일 관리](#)"를 참조하십시오.

## 장치 재설정

1. Reset 페이지를 여십시오.
2. **Reset Unit Number** 필드에서 단원을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

확인 메시지가 표시됩니다.

4. **OK**를 클릭하십시오.

장치가 재설정됩니다. 장치가 재설정된 후, 사용자 이름과 암호를 입력하는 프롬프트가 표시됩니다.

5. 사용자 이름과 암호를 입력하여 웹 인터페이스에 다시 연결하십시오.

## CLI를 사용하여 장치 재설정

다음 표에서는 CLI를 통해 장치를 재설정하는 CLI 명령을 요약합니다.

표 6-19. 재설정 CLI 명령

CLI 명령	설명
--------	----

reload	운영 체제를 다시 로드합니다.
--------	------------------

다음은 CLI 명령의 예입니다.

```
console >reload

This command will reset
the whole system and
disconnect your current
session. Do you want to
continue (y/n) [n] ?
```

## SNTP 설정 구성

스위치에서는 **SNTP(Simple Network Time Protocol)**를 지원합니다. **SNTP**를 사용하면 밀리초 단위까지 네트워크 스위치 클럭 시간 동기화를 정확하게 지정할 수 있습니다. 시간 동기화는 네트워크 **SNTP** 서버에서 수행됩니다. **SNTP**는 클라이언트로서만 작동하며, 다른 시스템에 시간 서비스를 제공할 수 없습니다.

스위치에서는 서버 시간에 대한 다음 서버 종류를 풀링할 수 있습니다.

- 1 유니캐스트
- 1 애니캐스트
- 1 브로드캐스트

시간 소스는 계층으로 설정되어 있습니다. 계층은 참조 클럭의 정확도를 정의합니다. 계층이 높을수록(0이 가장 높음) 클럭이 더욱 정확해집니다. 스위치는 계층 1 이상의 시간을 수신합니다. 다음은 계층의 예입니다.

- 1 **Stratum 0** — 실제 시간 클럭이 시간 소스로 사용됨을 표시합니다(예: **GPS** 시스템).
- 1 **Stratum 1** — 계층 0 시간 소스에 직접 연결된 서버가 사용됨을 표시합니다. 계층 1 서버에서는 주 네트워크 시간 표준을 제공합니다.
- 1 **Stratum 2** — 시간 소스가 네트워크 경로에서 계층 1 서버와 떨어져 있음을 표시합니다. 예를 들면 계층 2 서버는 계층 1 서버에서 **NTP**를 통해 네트워크 링크의 시간을 수신합니다.

**SNTP** 서버에서 수신한 정보는 시간 레벨 및 서버 종류를 기준으로 평가됩니다. **SNTP** 시간 정의가 평가되고 다음 시간 레벨을 기준으로 해당 정의가 결정됩니다.

- 1 **T1** — 클라이언트에서 원래 요청을 전송한 시간입니다.
- 1 **T2** — 서버에서 원래 요청을 수신한 시간입니다.
- 1 **T3** — 서버가 클라이언트에 응답을 보낸 시간입니다.
- 1 **T4** — 클라이언트가 서버의 응답을 수신한 시간입니다.

장치에서는 서버 시간에 대한 서버 종류를 풀링할 수 있습니다. 유니캐스트, 애니캐스트, 브로드캐스트가 이에 해당합니다.

**IP** 주소가 알려진 서버를 풀링할 경우 유니캐스트 정보 풀링이 사용됩니다. 장치에 구성된 **SNTP** 서버는 동기화 정보에 대해 풀링된 유일한 서버입니다. **T1 - T4**를 사용하여 서버 시간이 결정됩니다. 보안 설정이 가장 강력하기 때문에 장치 시간을 동기화할 때 선호되는 방법입니다. 이 방법을 선택한 경우 **SNTP** 정보는 [SNTP Servers](#) 페이지를 사용하여 장치에 정의된 **SNTP** 서버에서만 수신됩니다.

서버 **IP** 주소가 알려지지 않은 경우 애니캐스트 풀링 정보가 사용됩니다. 이 방법을 선택한 경우 네트워크의 모든 **SNTP** 서버에서 동기화 정보를 전송할 수 있습니다. 사전에 동기화 정보를 요청하는 경우 장치가 동기화됩니다. 동기화 정보 요청에 응답하기 위해 첫 **SNTP** 서버 3대가 전송한 가장 완전한 응답(최하위 계층)이 시간 값을 설정하는 데 사용됩니다. 시간 레벨 **T3** 및 **T4**가 서버 시간을 결정하는 데 사용됩니다.

장치 시간을 동기화할 때 시간 정보를 얻기 위해 애니캐스트 풀링을 사용하는 방법이 브로드캐스트 풀링보다 선호됩니다. 그러나 이 방법은 장치에 구성되지 않은 **SNTP** 서버에서도 **SNTP** 패킷이 수신되기 때문에 유니캐스트 풀링보다 보안성이 떨어집니다.

서버 IP 주소가 알려지지 않은 경우 브로드캐스트 정보가 사용됩니다. 브로드캐스트 메시지가 SNMP 서버에서 전송되면 SNMP 클라이언트가 이 메시지를 수신하기 위해 대기합니다. 브로드캐스트 폴링이 활성화된 경우 장치에서 요청하지 않은 경우에도 모든 동기화 정보가 수신됩니다. 이 방법이 최소한의 보안 방법입니다.

장치는 적극적으로 정보를 요청하거나 각 폴링 간격을 기준으로 동기화 정보를 검색합니다. 유니캐스트, 애니캐스트 및 브로드캐스트 폴링이 활성화된 경우 정보는 다음 순서로 검색됩니다.

- 1 장치에 정의된 서버의 정보가 우선됩니다. 유니캐스트 폴링이 활성화되지 않았거나 장치에 정의된 서버가 없는 경우 장치는 응답하는 모든 SNMP 서버의 시간 정보를 수신합니다.
- 1 둘 이상의 유니캐스트 장치가 응답한 경우 최하위 계층에 해당하는 장치의 동기화 정보가 우선됩니다.
- 1 여러 서버의 계층이 동일한 경우 제일 먼저 응답하는 SNMP 서버의 동기화 정보가 수신됩니다.

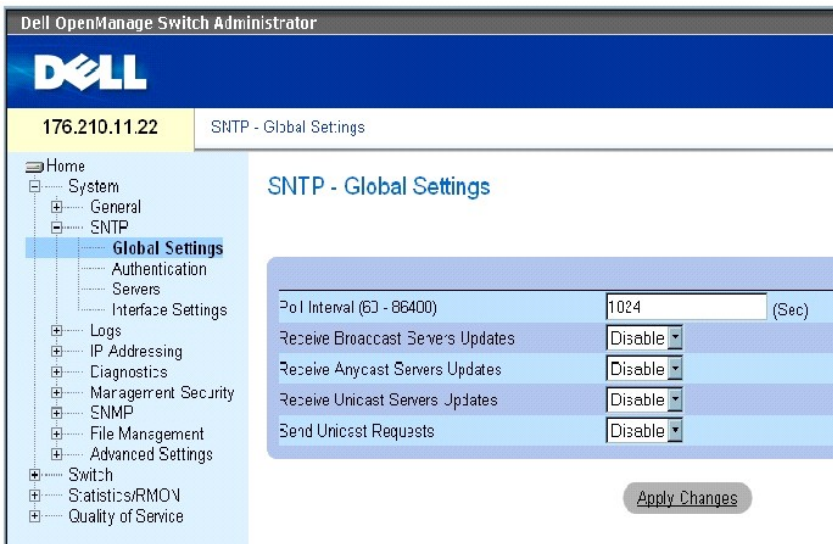
MD5(Message Digest 5) 인 증은 SNMP 서버로 가는 장치 동기화 경로를 보호합니다. MD5는 128비트 해시를 생성하는 알고리즘입니다. MD5는 MD4가 변형된 것으로 MD4보다 보안을 더욱 강화하였습니다. MD5는 통신의 무결성을 확인하고 통신의 시작을 인증합니다.

SNMP 페이지를 열려면 트리 뷰에서 **System**→ **SNTP**를 클릭하여 **SNTP** 페이지를 여십시오.

## SNTP 전역 매개변수 정의

[SNTP Global Settings](#) 페이지에서는 SNTP 매개변수를 전역로 정의하는 데 필요한 정보를 제공합니다. [SNTP Global Settings](#) 페이지를 열려면 트리 뷰에서 **System**→ **SNTP**→ **Global Settings**를 클릭하십시오.

그림 6-8. SNTP 전역 설정



[SNTP Global Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**Poll Interval(60-86400)** — SNMP 서버에서 유니캐스트 정보를 폴링하는 간격(초 단위)을 정의합니다. 기본적으로 폴링 간격은 1024초입니다.

**Receive Broadcast Servers Updates** — 활성화된 경우 SNMP 서버의 선택한 인터페이스의 브로드캐스트 서버 시간 정보를 수신하기 위해 대기합니다.

**Receive Anycast Servers Updates** — 활성화된 경우 SNMP 서버에 애니캐스트 서버 시간 정보를 폴링합니다. **Receive Anycast Servers Update**와 **Receive Broadcast Servers Update** 필드가 모두 활성화된 경우 시스템 시간은 애니캐스트 서버 시간 정보에 따라 설정됩니다.

**Receive Unicast Servers Updates** — 활성화된 경우 SNMP 서버에 애니캐스트 서버 시간 정보를 폴링합니다. **Receive Broadcast Servers Update**, **Receive Anycast Servers Update** 및 **Receive Unicast Servers Update** 필드가 모두 활성화된 경우 시스템 시간은 유니캐스트 서버 시간 정보에 따라 설정됩니다.

**Send Unicast Requests** — 활성화된 경우 SNMP 유니캐스트 서버 시간 정보 요청을 SNMP 서버에 전송합니다.

## 클럭 소스 선택

1. [Time Synchronization](#) 페이지를 여십시오.
2. **Clock Source** 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

클럭 소스가 선택되고 장치가 업데이트됩니다.

## 로컬 클럭 설정 정의

1. [Time Synchronization](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

로컬 클럭 설정이 적용됩니다.

## CLI 명령을 사용하여 SNMP 전역 매개변수 정의

다음 표에서는 **SNMP Global Settings** 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-20. SNMP 전역 매개변수 CLI 명령

CLI 명령	설명
<code>sntp broadcast client enable</code>	SNMP 브로드캐스트 클라이언트를 활성화합니다.
<code>sntp anycast client enable</code>	SNMP 애니캐스트 클라이언트를 활성화합니다.
<code>sntp unicast client enable</code>	미리 정의된 SNMP 유니캐스트 클라이언트를 활성화합니다.

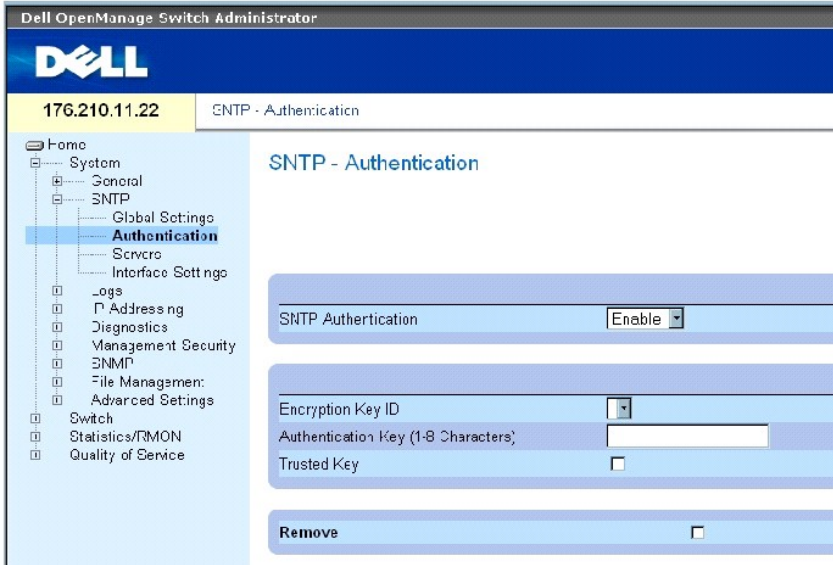
다음은 CLI 명령의 예입니다.

```
console(config)# sntp  
anycast client enable
```

## SNMP 인증 방법 정의

[SNMP Authentication](#) 페이지에서는 장치와 SNMP 서버 간의 SNMP 인증을 활성화합니다. SNMP 서버를 인증하는 방법은 [SNMP Authentication](#) 페이지에서도 선택됩니다. 트리 뷰에서 **System** → **SNMP** → **Authentication**를 클릭하여 [SNMP Authentication](#) 페이지를 여십시오.

그림 6-9. SNMP 인증



[SNTP Authentication](#) 페이지에는 다음 필드가 들어 있습니다.

**SNTP Authentication** — 활성화된 경우 장치와 SNTP 서버 간의 SNTP 세션 인증을 활성화합니다.

**Encryption Key ID** — SNTP 서버 및 장치를 인증할 때 사용되는 키 ID를 정의합니다. 필드의 최대값은 4294967295입니다.

**Authentication Key (1-8 Characters)** — 인증 시 사용되는 키입니다.

**Trusted Key** — SNTP 서버를 인증할 때 사용되는 암호화 키를 표시합니다(유니캐스트).

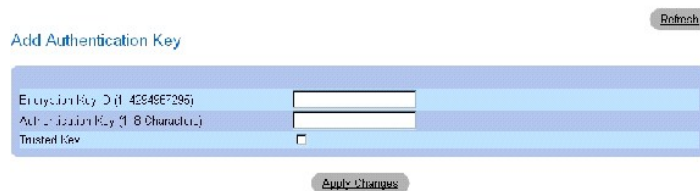
**Remove** — 이 필드를 선택하면 선택한 인증 키가 제거됩니다.

## SNTP 인증 키 추가

1. [SNTP Authentication](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

페이지가 열립니다.

그림 6-10. 인증 키 추가



3. 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

SNTP 인증 키가 추가되고 장치가 업데이트됩니다.

### 인증 키 표 표시

1. [SNTP Authentication](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Authentication Key Table](#)이 열립니다.

그림 6-11. 인증 키 표

Authentication Key Table Refresh

Encryption Key ID	Authentication Key	Trusted Key	Remove
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Changes

### 인증 키 삭제

1. [SNTP Authentication](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Authentication Key Table](#)이 열립니다.

3. **Authentication Key Table**의 항목을 선택하십시오.
4. Remove 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

항목이 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 SNTP 인증 설정 정의

다음 표에서는 [SNTP Authentication](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-21. SNTP 인증 CLI 명령

CLI 명령	설명
sntp authenticate	서버에서 수신된 SNTP(Simple Network Time Protocol) 처리량의 인증을 정의합니다.
sntp trusted key	SNTP에서 동기화할 대상 시스템의 ID를 인증합니다.
sntp authentication-key 번호 md5 값	SNTP의 인증 키를 정의합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# sntp
authentication-key 8 md5
Calked
```

```

console(config)# snmp
trusted-key 8

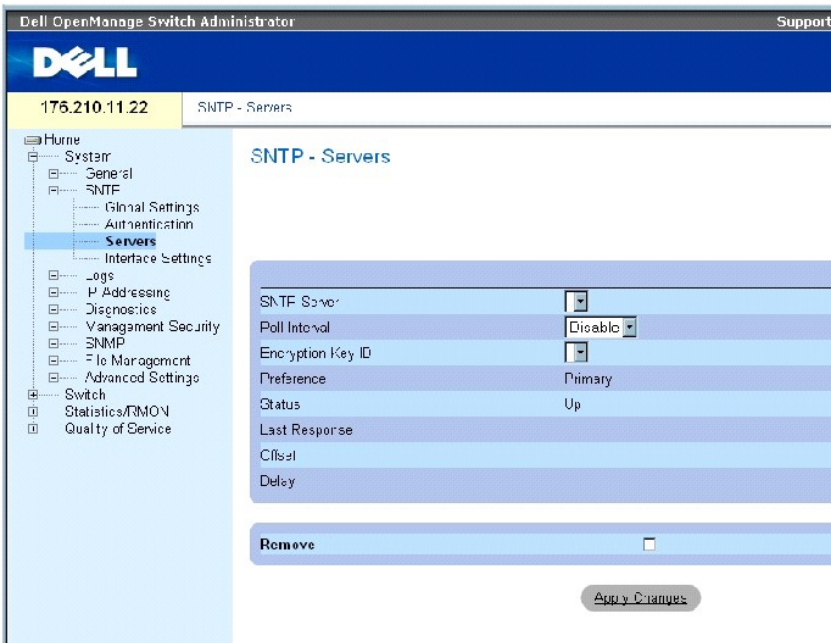
Console(config)# snmp
authenticate

```

## SNTP 서버 정의

[SNTP Servers](#) 페이지에서 SNTP 서버를 활성화하고 새 SNTP 서버를 추가할 수 있습니다. [SNTP Servers](#) 페이지를 열려면 트리 뷰에서 System→SNTP→Servers를 클릭하십시오.

그림 6-12. SNTP 서버



[SNTP Servers](#) 페이지에는 다음 필드가 들어 있습니다.

**SNTP Server** — 사용자 정의된 SNTP 서버 IP 주소를 선택합니다. 최대 8개의 SNTP 서버를 정의할 수 있습니다.

**Poll Interval** — 활성화된 경우 시스템 시간 정보를 확인하도록 선택한 SNTP 서버 폴링을 활성화합니다.

**Encryption Key ID** — SNTP 서버와 장치의 통신에 사용되는 키 ID를 표시합니다. 값의 범위는 1~4294967295입니다.

**Preference** — SNTP 시스템 시간 정보를 제공하는 SNTP 서버입니다. 가능한 필드 값은 다음과 같습니다.

**Primary** — SNTP 정보를 제공하는 1차 서버입니다.

**Secondary** — SNTP 정보를 제공하는 백업 서버입니다.



**Status** — 작동하는 SNTP 서버의 상태입니다. 가능한 필드 값은 다음과 같습니다.

**Up** — 현재 SNTP 서버가 정상적으로 작동합니다.

**Down** — 현재 SNTP 서버를 사용할 수 없음을 표시합니다. 예를 들면, 현재 SNTP 서버가 연결되지 않았거나 작동이 중지된 상태입니다.

**In progress** — 현재 SNTP 서버에서 SNTP 정보를 전송 또는 수신 중입니다.

**Unknown** — 현재 전송된 SNTP 정보의 진행 상태를 알 수 없습니다. 예를 들면, 현재 장치에서 인터페이스를 찾는 중입니다.

**Last Response** — SNTP 서버로부터 마지막으로 응답을 수신한 시간입니다.

**Offset** — 장치 로컬 클럭과 SNTP 서버에서 받은 시간 사이의 시간 소인 차이입니다.

**Delay** — SNTP 서버에 도달하는 데 걸리는 총 시간입니다.

**Remove** — 이 필드를 선택하면 **Sntp Servers** 목록에서 특정 SNTP 서버가 제거됩니다.

## SNTP 서버 추가

1. [SNTP Servers](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

[Add SNTP Server](#) 페이지가 열립니다.

그림 6-13. SNTP 서버 추가

The screenshot shows a web interface for adding a new SNTP server. The form is titled "Add SNTP Server" and includes a "Refresh" button in the top right corner. The form itself is a light blue box with three rows of input fields. The first row is "SNTP Server" with a text input field and a "0x.X.XX" label. The second row is "Poll Interval" with a dropdown menu showing "10000" and a "10000" label. The third row is "Encryption Key ID" with a dropdown menu. Below the form is an "Apply Changes" button.

3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

SNTP 서버가 추가되고 장치가 업데이트됩니다.

## SNTP 서버 표 표시

1. [SNTP Servers](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[SNTP Servers Table](#)이 열립니다.

그림 6-14. SNTP 서버 표

### SNTP Servers Table

SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Remove
1	Disable		Primary	Up				<input type="checkbox"/>

[Apply Changes](#)

### SNTP 서버 수정

1. [SNTP Servers](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[SNTP Servers Table](#)이 열립니다.

3. SNTP Server 항목을 선택하십시오.
4. 관련 필드를 수정하십시오.
5. **Apply Changes**를 클릭하십시오.

SNTP Server 정보가 업데이트됩니다.

### SNTP 서버 삭제

1. [SNTP Servers](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[SNTP Servers Table](#)이 열립니다.

3. SNTP Server 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

항목이 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 SNTP 서버 설정 정의

다음 표에서는 SNTP Server 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-22. SNTP 서버 CLI 명령

CLI 명령	설명
sntp server ip-address hostname [poll] [key keyid]	서버로부터 SNTP 트래픽을 요청 및 수신할 때 SNTP를 사용하도록 장치를 구성합니다.

다음은 CLI 명령의 예입니다.

```

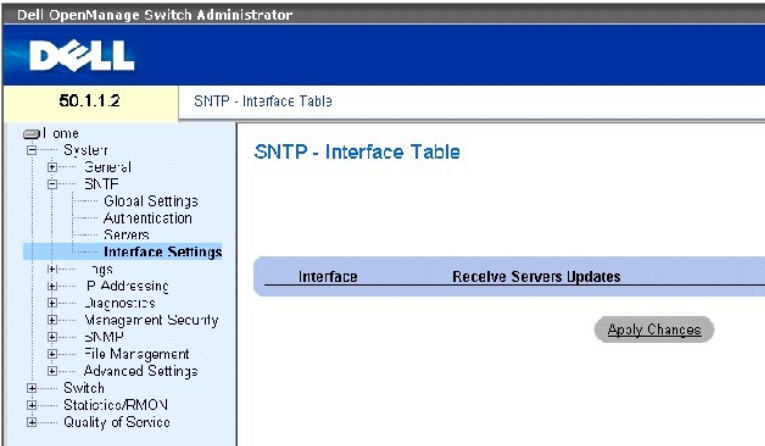
Console(config)# snmp
server 100.1.1.1 poll key
10

```

## SNTP 인터페이스 정의

[SNTP Interface Settings](#) 페이지에는 SNTP 인터페이스 정보가 들어 있습니다. [SNTP Interface Settings](#) 페이지를 열려면 System→SNTP→Interface Settings를 클릭하십시오.

그림 6-15. SNTP 인터페이스 설정



[SNTP Interface Settings](#) 페이지는 다음 필드를 포함합니다.

**Unit No.** — SNTP 인터페이스가 활성화된 스왑 멤버를 표시합니다.

**Interface** — SNTP를 활성화할 수 있는 인터페이스의 목록을 포함합니다.

**Receive Servers Updates** — 특정 인터페이스에서 SNTP를 활성화 또는 비활성화합니다.

**Remove** — 이 필드를 선택하면 특정 인터페이스에서 SNTP가 제거됩니다.

## SNTP 인터페이스 추가

1. [SNTP Interface Settings](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

Add SNTP Interface 페이지가 열립니다.

그림 6-16. SNTP 인터페이스 추가

## Add SNTP Interface

[Refresh](#)

Interface	<input type="radio"/> Port	<input type="radio"/> LAG	<input type="radio"/> VLAN
State	<input type="checkbox"/> Disable		

[Apply Changes](#)

3. 관련 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

SNTP 인터페이스가 추가되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 SNTP 인터페이스 설정 정의

다음 표에서는 [SNTP Interface Settings](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

**주:** 애니캐스트 또는 브로드캐스트 인터페이스로 정의할 인터페이스에 IP 주소를 정의해야 합니다.

**표 6-23. SNTP 인터페이스 설정 CLI 명령**

CLI 명령	설명
<code>sntp client enable</code>	인터페이스에서 SNTP(Simple Network Time Protocol) 클라이언트를 활성화합니다.
<code>show sntp configuration</code>	SNTP(Simple Network Time Protocol) 구성을 표시합니다.

다음은 SNTP 인터페이스를 표시하는 CLI 명령의 예입니다.

```

console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server          Polling      Encryption Key
-----
176.1.1.8      Enabled     9
    
```

176.1.8.179	Disabled	Disabled
Broadcast Clients: Enabled		
Broadcast Clients Poll: Enabled		
Broadcast Interfaces:1/e1, 1/e3		

## 로그 관리

Logs 페이지에는 여러 로그 페이지에 대한 링크가 있습니다. Logs 페이지를 열려면 트리 뷰에서 **System** → **Logs**를 클릭하십시오.

### 전역 로그 매개변수 정의

시스템 로그를 사용하면 실시간으로 장치 이벤트를 보고 나중에 사용하도록 이벤트를 기록할 수 있습니다. 시스템 로그에서는 이벤트를 기록 및 관리하고, 오류 또는 정보용 메시지를 보고합니다.

모든 오류 보고 시 시스템 로그 프로토콜의 권장되는 메시지 형식별로 고유한 이벤트 메시지 형식이 있습니다. 예를 들면, Syslog 및 로컬 장치 보고 메시지에 심각도 코드가 지정되고, 이러한 메시지에는 메시지 간락기호가 포함되어 있어서 메시지를 생성하는 소스 응용프로그램을 식별합니다. 이를 통해 긴급한 정도 또는 관련된 정도에 따라 메시지를 필터링할 수 있습니다. 다양한 목적으로 로깅 메시지를 분배하는 프로세스(예: 로깅 버퍼, 로깅 파일 또는 Syslog 서버)는 Syslog 구성 매개변수에서 관리합니다. 사용자는 최대 8개의 Syslog 서버를 정의할 수 있습니다.

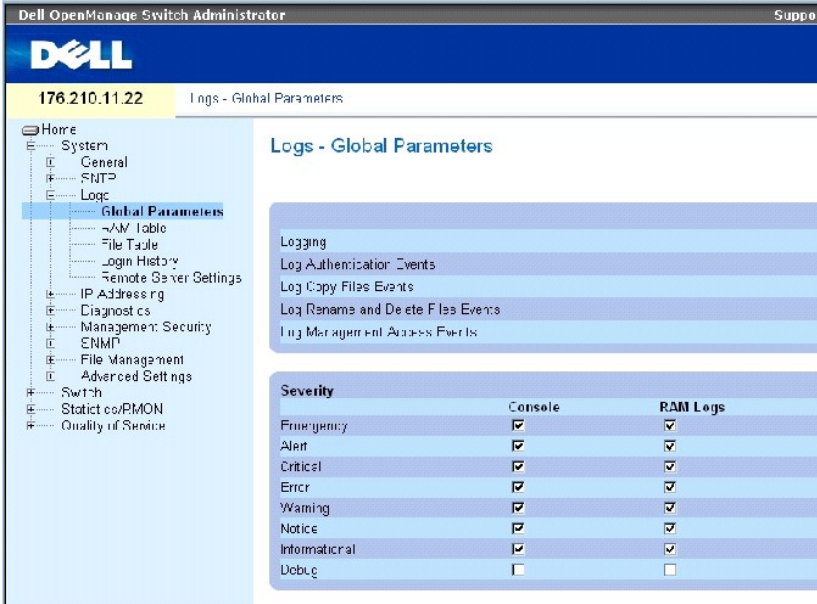
다음 표에는 로그 심각도 레벨이 들어 있습니다.

표 6-24. 로그 심각도 레벨

심각도 종류	심각도 레벨	설명
Emergency	0	시스템이 작동하지 않습니다.
Alert	1	시스템을 즉시 검사해야 합니다.
Critical	2	시스템이 심각한 상태입니다.
Error	3	시스템 오류가 발생했습니다.
Warning	4	시스템 경고가 발생했습니다.
Notice	5	시스템이 제대로 작동하지만 시스템 주의사항이 발생했습니다.
Informational	6	시스템 정보를 제공합니다.
Debug	7	로그에 대한 자세한 정보를 제공합니다. 디버그 오류가 발생하면 Dell 온라인 기술 지원부에 문의하십시오.

[Global Log Parameters](#) 페이지에는 어떤 로그에 어떤 이벤트를 기록할 것인지를 정의하는 필드가 들어 있습니다. 여기에는 로그를 전역로 활성화할 수 있는 필드 및 로그 매개변수를 정의하는 필드가 들어 있습니다. 심각도 로그 메시지는 심각도의 내림차순으로 나열됩니다. [Global Log Parameters](#) 페이지를 열려면 트리 뷰에서 **System** → **Logs** → **Global Parameters**를 클릭하십시오.

그림 6-17. 전역 로그 매개변수



[Global Log Parameters](#) 페이지에는 다음 매개변수가 들어 있습니다.

**Logging** — 캐쉬, 파일 및 서버 로그에 대한 장치 전역 로그를 활성화합니다. 콘솔 로그는 기본적으로 사용 가능합니다.

**Log Authentication Events** — 사용자가 인증된 경우 로그를 생성합니다.

**Log Copy Files Events** — 파일을 복사할 때 로그를 생성합니다.

**Log Rename and Delete Files Events** — 백업 구성 파일의 이름을 변경하거나 해당 파일을 삭제할 때 로그를 생성합니다.

**Log Management Access Events** — 관리 메소드를 사용하여 장치에 액세스할 때 로그를 생성합니다. 예를 들면 SSH를 사용하여 장치에 액세스할 때마다 장치 로그가 생성됩니다.

**Severity** — 사용 가능한 심각도 로그는 다음과 같습니다.

**Emergency** — 최상위 경고 레벨입니다. 장치 작동이 중단되거나 제대로 작동하지 않는 경우 긴급 로그 메시지가 지정된 로깅 위치에 저장됩니다.

**Alert** — 두 번째로 높은 경고 레벨입니다. 심각한 장치 오작동이 발생하는 경우(예: 존재하지 않는 구성 파일을 다운로드하려고 시도한 경우) 경고 로그가 저장됩니다.

**Critical** — 세 번째로 높은 경고 레벨입니다. 중대한 장치 오작동이 발생한 경우(예: 2개의 장치 포트는 작동하지 않지만 나머지 장치 포트는 작동하는 경우) 심각 로그가 저장됩니다.


**Error** — 장치 오류가 발생한 경우입니다(예: 복사에 실패한 경우).

**Warning** — 최하위 장치 경고 레벨입니다. 예를 들면, 장치가 작동 중이지만 현재 포트 링크가 중지된 상태입니다.

**Notice** — 중요한 장치 정보를 제공합니다.

**Informational** — 장치 정보를 제공합니다. 예를 들면, 현재 포트가 작동 중인 경우입니다.

**Debug** — 디버깅 메시지를 제공합니다.

 **주:** 심각도 레벨을 선택하면 선택한 레벨 이상의 모든 심각도 레벨 선택 항목이 자동으로 선택됩니다.

**Global Log Parameters** 페이지는 다른 로깅 시스템에 해당하는 확인란도 포함합니다.

**Console** — 콘솔에 로그를 전송하는 최저 심각도 레벨입니다.

**RAM Logs** — RMA에 보관된 로그 파일(캐시)에 로그를 전송하는 최저 심각도 레벨입니다.

**Log File** — FLASH 메모리에 보관된 로그 파일에 로그를 전송하는 최저 심각도 레벨입니다.

## 로그 사용

1. **Global Log Parameters** 페이지를 여십시오.
2. **Logging** 드롭다운 목록에서 **Enable**를 선택하십시오.
3. **Global Log Parameters** 확인란에서 로그 종류 및 로그 심각도를 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

로그 설정이 저장되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 로그 활성화

다음 표에서는 **Global Log Parameters** 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-25. 전역 로그 매개변수 CLI 명령

CLI 명령	설명
<b>logging on</b>	오류 메시지 로깅을 활성화합니다.
<b>logging</b> { ip-address   hostname } [port port] [severity level] [facility facility] [description text]	Syslog 서버에 메시지를 로그합니다. 심각도 레벨에 대한 목록은 " <a href="#">로그 심각도 레벨</a> "을 참조하십시오.
logging console level	심각도를 기반으로 콘솔에 로그할 메시지를 제한합니다.
logging buffered level	심각도를 기준으로 내부 버퍼(RAM)로부터 표시할 syslog 메시지를 제한합니다.
logging file level	심각도를 기준으로 로깅 파일에 전송할 syslog 메시지를 제한합니다.
<b>clear logging</b>	로그를 지웁니다.
<b>clear logging file</b>	로깅 파일에서 메시지를 지웁니다.

다음은 CLI 명령의 예입니다.

```
console(config)# logging
on

console(config)# logging
console errors
```

```

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

Clear Logging File [y/n]y

```

## RAM 로그 표 보기

[RAM Log Table](#)에는 로그가 입력된 시간, 로그 심각도 및 로그에 대한 설명을 포함하여 RAM에 보관된 로그 항목에 대한 정보가 들어 있습니다. [RAM Log Table](#)를 열려면 트리 뷰에서 **System** → **Logs** → **RAM Table**를 클릭하십시오.

그림 6-18. RAM 로그 표

The screenshot shows the Dell OpenManage Switch Administrator web interface. The top navigation bar includes the Dell logo and the text 'Dell OpenManage Switch Administrator' and 'Support'. Below the navigation bar, the IP address '176.210.11.22' and the page title 'Logs - RAM Table' are displayed. The left sidebar contains a tree view of system settings, with 'RAM Table' highlighted. The main content area displays a table with the following data:

Log Index	Log Time	Severity
1	1AUG12003 1C:12:56	Informational

Below the table, there is a 'Clear Log' button.

[RAM Log Table](#)에는 다음 필드가 들어 있습니다.

**Log Index** — RAM Log Table에 있는 로그 번호입니다.

**Log Time** — RAM Log Table에 로그를 입력한 시간을 표시합니다.

**Severity** — 로그 심각도를 표시합니다.

**Description** — 로그 항목에 대한 설명입니다.



## 로그 정보 제거

1. [RAM Log Table](#)을 여십시오.
2. Clear Log를 클릭하십시오.

**RAM Log Table**에서 로그 정보가 제거되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 RAM 로그 표 보기 및 지우기

다음 표에서는 [RAM Log Table](#)에 표시된 필드를 보거나 지우는 CLI 명령을 요약합니다.

표 6-26. RAM 로그 표 CLI 명령

CLI 명령	설명
show logging	내부 버퍼에 저장된 syslog 메시지 및 로깅 상태를 표시합니다.
clear logging	로그를 지웁니다.

다음은 CLI 명령의 예입니다.

```
console# show logging

Logging is enabled.

Console Logging: Level
info. Console Messages: 0
Dropped.

Buffer Logging: Level
info. Buffer Messages: 26
Logged, 26 Displayed, 200
Max.

File Logging: Level error.
File Messages: 157 Logged,
26 Dropped.

1 messages were not logged

01-Jan-2000 01:03:42 :%
INIT-I-Startup: Cold
Startup

01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e14

01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e13

01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e12
```

```
01-Jan-2000 01:01:36 :%  
LINK-W-Down: 1/e15
```

```
01-Jan-2000 01:01:32 :%  
INIT-I-InitCompleted:  
Initialization task is  
completed
```

```
console# clear logging
```

```
Clear Logging Buffer  
{y/n}?
```

## 로그 파일 표 보기

[Log File Table](#)에는 로그가 입력된 시간, 로그 심각도 및 로그 메시지에 대한 설명을 포함하여 FLASH의 로그 파일에 저장된 로그 항목에 대한 정보가 들어 있습니다. [Log File Table](#)을 열려면 트리 뷰에서 **System** → **Logs** → **File Table**을 클릭하십시오.

그림 6-19. 로그 파일 표

Log Index	Log Time	Severity
1	10:10:11/2003 23:46:37	Warning

[Log File Table](#)에는 다음 필드가 들어 있습니다.

**Log Index** — [Log File Table](#)에 있는 로그 번호입니다.

**Log Time** — [Log File Table](#)에 로그를 입력한 시간을 표시합니다.

**Severity** — 로그 심각도를 표시합니다.

**Description** — 로그 메시지 텍스트입니다.

## CLI 명령을 사용하여 로그 파일 표 표시

다음 표에서는 [Log File Table](#)에 표시된 필드를 보거나 설정하는 CLI 명령을 요약합니다.

표 6-27. 로그 파일 표 CLI 명령

CLI 명령	설명
show logging file	로그 파일에 저장된 syslog 메시지 및 로깅 상태를 표시합니다.
clear logging file	로그 파일에서 메시지를 지웁니다.

다음은 CLI 명령의 예입니다.

```
console# show logging
file

Logging is enabled.

Console Logging:
Level info. Console
Messages: 0 Dropped.

Buffer Logging: Level
info. Buffer
Messages: 62 Logged,
62 Displayed, 200
Max.

File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.

SysLog server
12.1.1.2 Logging:
warning. Messages: 14
Dropped.

SysLog server 1.1.1.1
Logging: info.
Messages: 0 Dropped.

01-Jan-2000
01:12:01 :%COPY-W-
TRAP: The copy
operation was
completed
successfully

01-Jan-2000
01:11:49 :%LINK-I-Up:
1/e11

01-Jan-2000
01:11:46 :%LINK-I-Up:
1/e12

01-Jan-2000
01:11:42 :%LINK-W-
Down: 1/e13
```

```

01-Jan-2000
01:11:35 :%LINK-I-Up:
1/e14

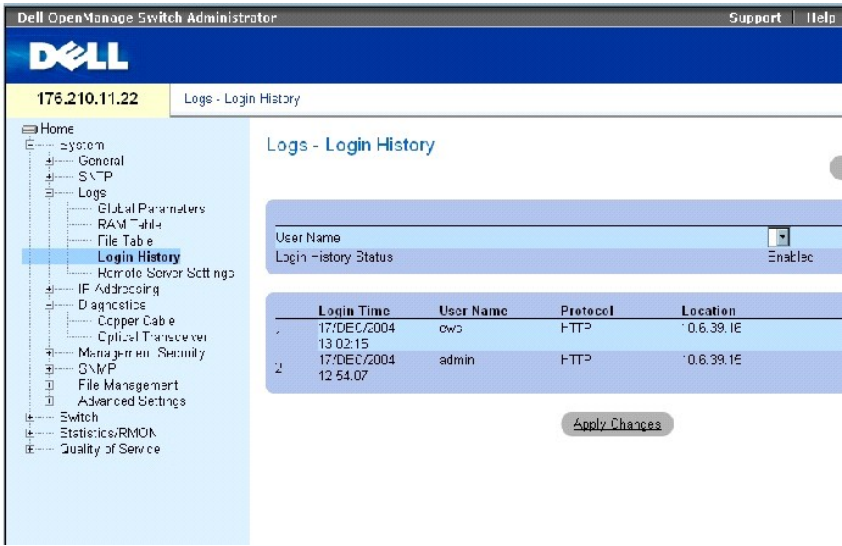
```

**장치 로그인 내역 보기**

[Login History](#) 페이지에는 사용자가 로그인한 시간 및 장치에 로그인할 때 사용된 프로토콜을 포함하여 장치 이용 내역을 보고 모니터링하는 정보가 들어 있습니다.

[Login History](#) 페이지를 열려면 트리 뷰에서 **System** → **Logs** → **Login History**를 클릭하십시오.

그림 6-20. 로그인 내역



[Login History](#) 페이지에는 다음 필드가 들어 있습니다.

**User Name** — 사용자 정의 장치의 사용자 이름 목록이 들어 있습니다.

**Login History Status** — 장치에 암호 내역 로그가 활성화되었는지 여부를 표시합니다.

**Login Time** — 선택한 사용자가 장치에 로그인한 시간을 표시합니다.

**User Name** — 장치에 로그인한 사용자를 표시합니다.

**Protocol** — 사용자가 장치에 로그인한 방법을 표시합니다.

**Location** — 장치에 액세스한 스테이션의 IP 주소를 표시합니다.

**로그인 내역 보기**

1. [Login History](#) 페이지를 여십시오.
2. **User Name** 필드에서 사용자를 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

선택한 사용자의 로그인 정보가 표시됩니다.

## CLI 명령을 사용하여 장치 로그인 내역 표시

다음 표에서는 [Login History](#) 페이지에 표시된 필드를 보고 설정하는 CLI 명령을 요약합니다.

표 6-28. 장치 로그인 사용 내역 CLI 명령

CLI 명령	설명
<code>show users login-history</code>	암호 관리 내역 정보를 표시합니다.

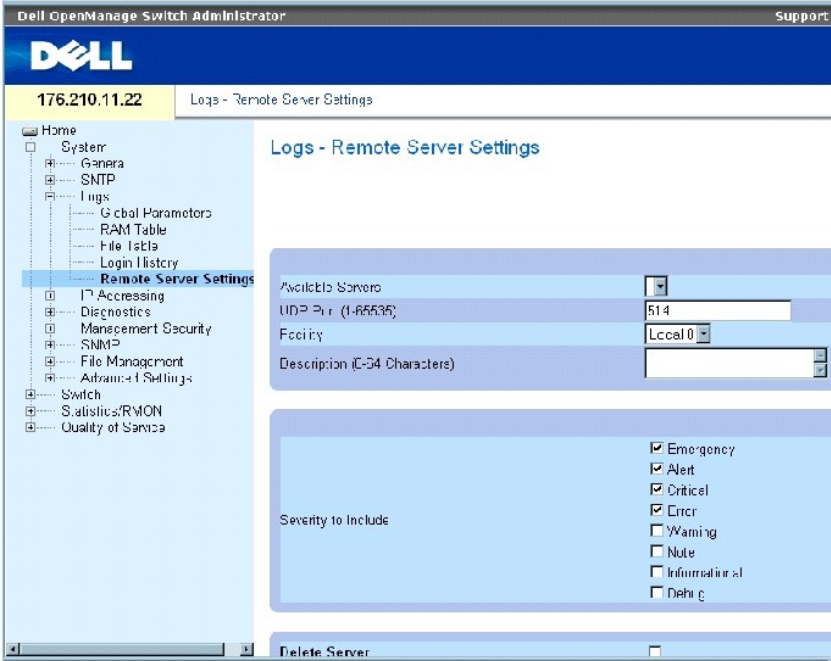
다음은 CLI 명령의 예입니다.

console# show users login-history			
Login Time	Username	Protocol	Location
-----	-----	-----	-----
Jan 1. 2005 23:58:17	Anna	HTTP	172.16.1.8
Jan 1. 2005 07:59:23	Errol	HTTP	172.16.0.8
Jan 1. 2005 08:23:48	Amy	Serial	
Jan 1. 2005 08:29:29	Alan	SSH	172.16.0.8
Jan 1. 2005 08:42:31	Bob	HTTP	172.16.0.1
Jan 1. 2005 08:49:52	Cindy	Telnet	172.16.1.7

## 원격 로그 서버 정의 수정

[Remote Log Server Settings](#) 페이지에는 사용 가능한 로그 서버를 보고 구성하는 데 필요한 필드가 들어 있습니다. 또한 새 로그 서버 및 각 서버에 전송한 로그 심각도를 정의할 수 있습니다. [Remote Log Server Settings](#) 페이지를 열려면 트리 뷰에서 **System**→**Logs**→**Remote Server Settings**를 클릭하십시오.

그림 6-21. 원격 로그 서버 설정



[Remote Log Server Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**Available Servers** — 로그를 전송할 수 있는 대상 서버 목록이 들어 있습니다.

**UDP Port (1-65535)** — 선택한 서버에 대한 로그를 전송할 대상 UDP 포트입니다. 가능한 값의 범위는 1-65535입니다. 기본값은 514입니다.

**Facility** — 시스템 로그를 원격 서버로 전송하는 사용자 정의 응용프로그램을 정의합니다. 단일 서버에 하나의 시설만 지정할 수 있습니다. 2차 시설 레벨을 지정하면 1차 시설 레벨을 덮어 씁니다. 장치에 정의된 모든 응용프로그램은 서버의 동일한 시설을 활용합니다. 필드의 기본값은 Local 7입니다. 가능한 필드 값은 다음과 같습니다.

Local 0-Local 7.

**Description(설명) (0-64 Characters)** — 사용자 정의 서버에 대한 설명입니다.

**Delete Server** — 이 필드를 선택하면 사용 가능한 서버 목록에서 현재 선택한 서버가 삭제됩니다.

[Remote Log Server Settings](#) 페이지에는 심각도 목록도 들어 있습니다. 심각도 정의는 [Global Log Parameters](#) 페이지의 심각도 정의와 동일합니다.

## 서버에 로그 전송

1. [Remote Log Server Settings](#) 페이지를 여십시오.
2. **Available Servers** 드롭다운 목록에서 서버를 선택하십시오.
3. 필드를 정의하십시오.
4. **Severity to Include** 확인란에서 로그 심각도를 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

로그 설정이 저장되고 장치가 업데이트됩니다.

## 새 서버 정의

1. [Remote Log Server Settings](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

[Add a Log Server](#) 페이지가 열립니다.

그림 6-22. 로그 서버 추가

Refresh

Add a Log Server

New Log Server IP Address (X.X.X)

UDP Port (65535) 514

Facility Local0

Description (1-34 Characters)

Severity To Include

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

Apply Changes

[Add a Log Server](#) 페이지에는 다음의 추가 필드가 들어 있습니다.

New Log Server IP Address(새 로그 서버 IP 주소) — 새 로그 서버의 IP 주소를 정의합니다.

3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

서버가 정의되고 **Available Servers** 목록에 추가됩니다.

## 원격 로그 서버 표 표시

1. [Remote Log Server Settings](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

[Log Servers Table](#) 페이지가 열립니다.

그림 6-23. 로그 서버 표

## Log Server Table

Refresh

Server	UDP Port	Facility	Description	Minimum Severity	Remove
1					<input type="checkbox"/>

Apply Changes

### Log Servers Table 페이지에서 로그 서버 제거

1. [Remote Log Server Settings](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[Log Servers Table](#) 페이지가 열립니다.

3. [Log Servers Table](#)의 항목을 선택하십시오.
4. **Remove** 확인란을 선택하여 서버를 제거하십시오.
5. **Apply Changes**를 클릭하십시오.

[Log Servers Table](#)의 항목이 제거되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 원격 로그 서버 사용

다음 표에서는 원격 로그 서버를 사용하기 위한 CLI 명령을 요약합니다.

표 6-29. 원격 로그 서버 CLI 명령

CLI 명령	설명
logging (ip 주소   호스트 이름) [port 포트] [severity 레벨] [facility 시설] [description 문자]	원격 서버에 메시지를 로그합니다.
no logging	Syslog 서버를 삭제합니다.
show logging	syslog 메시지 및 로깅 상태를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console> enable

console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.
```



```
Console Logging: Level
debug. Console Messages: 5
Dropped.

Buffer Logging: Level
debug. Buffer Messages: 16
Logged, 16 Displayed, 200
Max.

File Logging: Level error.
File Messages: 0 Logged,
209 Dropped.

SysLog server 31.1.1.2
Logging: error. Messages:
22 Dropped.

SysLog server 5.2.2.2
Logging: info. Messages: 0
Dropped.

SysLog server 10.2.2.2
Logging: critical.
Messages: 21 Dropped.

SysLog server 10.1.1.1
Logging: critical.
Messages: 0 Dropped.

1 messages were not logged

03-Mar-2004 12:02:03 :%
LINK-I-Up: 1/e11

03-Mar-2004 12:02:01 :%
LINK-W-Down: 1/e12

03-Mar-2004 12:02:01 :%
LINK-I-Up: 1/e13
```

---

## IP Addressing 정의

IP Addressing 페이지에는 인터페이스 및 기본 게이트웨이 IP 주소를 지정하고 인터페이스의 ARP 및 DHCP 매개변수를 정의하는 연결이 들어 있습니다. IP Addressing 페이지를 열려면 트리 뷰에서 System→ IP Addressing을 클릭하십시오.

## 기본 게이트웨이 정의

**Default Gateway** 페이지에는 장치에 게이트웨이를 지정하는 데 필요한 필드가 들어 있습니다. 원격 네트워크로 전송될 때 패킷은 기본 IP로 전달됩니다. 구성된 IP 주소는 IP 인터페이스 중 하나와 동일한 IP 주소 서브넷에 속해야 합니다. **Default Gateway** 페이지를 열려면 트리 뷰에서 System→ IP Addressing→ Default Gateway를 클릭하십시오.

**Default Gateway** 페이지에는 다음 필드가 들어 있습니다.

**User Defined** — 장치의 게이트웨이 IP 주소입니다.

**Active** — 게이트웨이가 활성화된지 여부를 표시합니다.

**Remove User Defined** — 이 필드를 선택하면 **Default Gateway** 드롭다운 목록에서 장치의 게이트웨이가 제거됩니다.

### 장치 게이트웨이 선택:

1. **Default Gateway** 페이지를 여십시오.
2. **Default Gateway** 드롭다운 목록에서 IP 주소를 선택하십시오.
3. Active 확인란을 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

장치의 기본 게이트웨이가 선택되고 장치가 업데이트됩니다.

### 장치의 기본 게이트웨이 장치 제거

1. **Default Gateway** 페이지를 여십시오.
2. **Remove** 확인란을 선택하여 기본 게이트웨이를 제거하십시오.
3. **Apply Changes**를 클릭하십시오.

기본 게이트웨이 항목이 제거되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 장치의 게이트웨이 정의

다음 표에서는 **Default Gateway** 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-30. 기본 게이트웨이 CLI 명령

CLI 명령	설명
<code>ip default-gateway ip-address</code>	기본 게이트웨이를 정의합니다.
<code>no ip default-gateway</code>	기본 게이트웨이를 제거합니다.

다음은 CLI 명령의 예입니다.

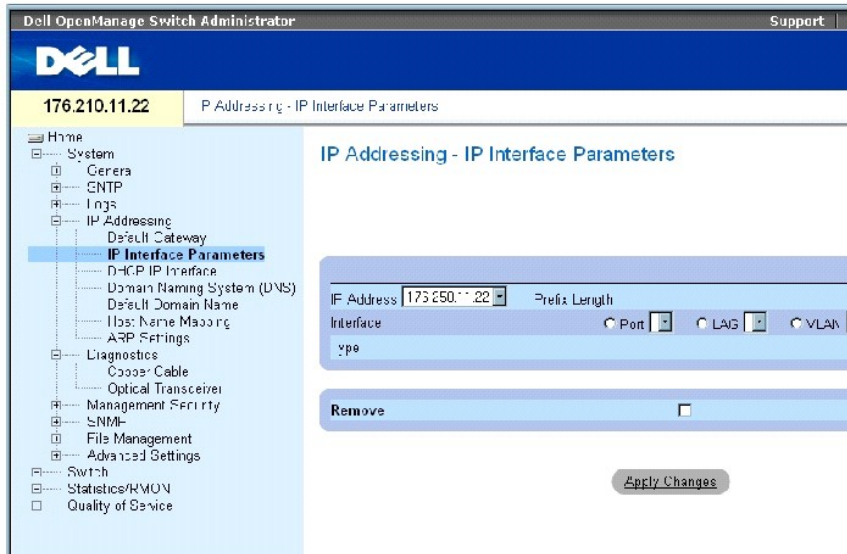
```
console(config)# ip
default-gateway
196.210.10.1

console(config)# no ip
default-gateway
```

### IP 인터페이스 정의

[IP Interfaces Parameters](#) 페이지에는 인터페이스에 IP 매개변수를 지정하는 필드가 들어 있습니다. [IP Interfaces Parameters](#) 페이지를 열려면 트리 뷰에서 **System** → **IP Addressing** → **IP Interface Parameters**를 클릭하십시오.

그림 6-24. IP 인터페이스 매개변수



[IP Interfaces Parameters](#) 페이지에는 다음 매개변수가 들어 있습니다.

**IP Address** — 인터페이스 IP 주소입니다.

**Prefix Length** — 소스 IP 주소 접두어 또는 소스 IP 주소의 네트워크 마스크를 구성하는 비트 수입니다.

**Source Interface** — IP 주소가 정의된 인터페이스 종류입니다. **Port**, **LAG** 또는 **VLAN**을 선택하십시오.

**Type** — IP 주소가 고정으로 구성되었는지 아닌지를 표시합니다.

**Remove** — 이 필드를 선택하면 **IP Address** 드롭다운 메뉴에서 인터페이스가 제거됩니다.

## IP 인터페이스 추가

1. [IP Interfaces Parameters](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

[Add a Static IP Interface](#) 페이지가 열립니다.

그림 6-25. 고정 IP 인터페이스 추가

## Add a Static IP Interface

[Refresh](#)

IP Address	<input type="text" value=""/>	(X.X.X.X)	<input type="radio"/> Network Mask	<input type="text" value=""/>	(X.X.X.X)
			<input type="radio"/> Prefix Length	<input type="text" value=""/>	(/XX)
Interface	<input type="text" value=""/>	<input type="radio"/> Port	<input type="radio"/> LAC	<input type="radio"/> V_LAN	

[Apply Changes](#)

**Network Mask** — 소스 IP 주소의 서브네트워크 마스크를 표시합니다.

3. 페이지의 필드를 채우십시오.
4. **Apply Changes**를 클릭하십시오.

새 IP 주소가 인터페이스에 추가되고 장치가 업데이트됩니다.

## IP 주소 매개변수 수정

1. [IP Interfaces Parameters](#) 페이지를 여십시오.
2. **IP Address** 드롭다운 메뉴에서 IP 주소를 선택하십시오.
3. 인터페이스 종류를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

매개변수가 수정되고 장치가 업데이트됩니다.

## IP 주소 삭제

1. [IP Interfaces Parameters](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

**IP Interface Parameters Table** 페이지가 열립니다.

그림 6-26. IP 인터페이스 매개변수 표

### IP Interface Parameter Table

[Refresh](#)

IP Address	Prefix Length	Interface	Type	Remove
1			Static	<input type="checkbox"/>

[Apply Changes](#)

3. IP 주소를 선택한 후 **Remove** 확인란을 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

선택한 IP 주소가 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 IP 인터페이스 정의

다음 표에서는 [IP Interfaces Parameters](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-31. IP 인터페이스 매개변수 CLI 명령

CLI 명령	설명
ip address ip-address {mask   prefix-length}	IP 주소를 설정합니다.
no ip address [ip-address]	IP 주소를 제거합니다.
show ip interface [ethernet interface-number   vlan vlan-id   port-channel number]	IP에 구성된 인터페이스의 사용 상태를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# interface
vlan 1

console(config-if)# ip
address 92.168.1.123
255.255.255.0

console(config-if)# no ip
address 92.168.1.123

console(config-if)# end

console# show ip interface
vlan 1

Gateway IP Address
Activity status

-----

192.168.1.1 Active

IP address Interface Type

-----
-----

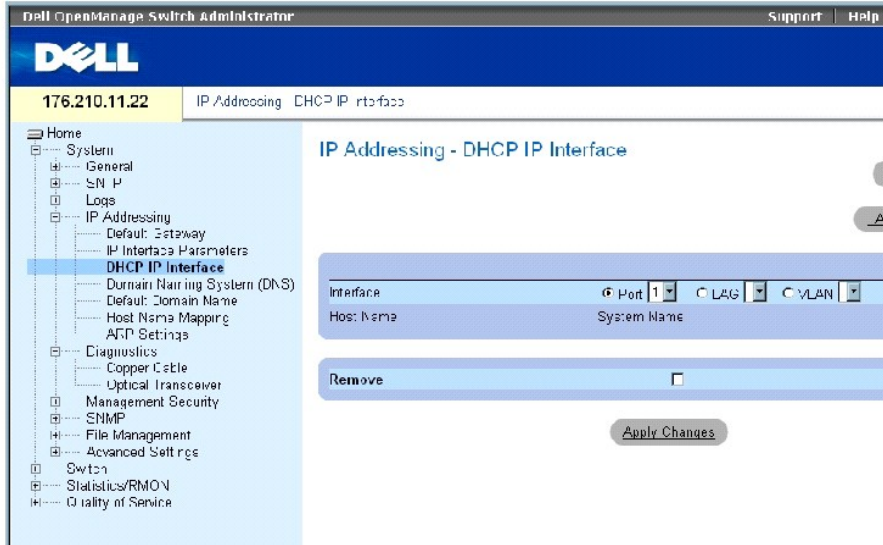
192.168.1.123/24 VLAN 1
Static

```

## DHCP IP 인터페이스 매개변수 정의

[DHCP IP Interface](#) 페이지에는 장치에 연결된 DHCP 클라이언트를 정의하는 매개변수가 들어 있습니다. [DHCP IP Interface](#) 페이지를 열려면 트리 뷰에서 System→IP Addressing→DHCP IP Interface를 클릭하십시오.

그림 6-27. DHCP IP 인터페이스



[DHCP IP Interface](#) 페이지에는 다음 필드가 들어 있습니다.

**Interface** — 장치에 연결된 특정 인터페이스입니다. **Port**, **LAG** 또는 **VLAN** 옆의 옵션 단추를 클릭하여 장치에 연결된 인터페이스를 선택하십시오.

**Host Name** — 호스트 이름입니다.

**Remove** — 이 필드를 선택하면 DHCP 클라이언트가 제거됩니다.

### DHCP 클라이언트 추가

1. [DHCP IP Interface](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add DHCP IP Interface** 페이지가 열립니다.

3. 페이지에 정보를 입력하십시오.
4. **Apply Changes**를 클릭하십시오.

DHCP 인터페이스가 추가되고 장치가 업데이트됩니다.

### DHCP IP 인터페이스 수정

1. [DHCP IP Interface](#) 페이지를 여십시오.
2. 필드를 수정하십시오.
3. **Apply Changes**를 클릭하십시오.

항목이 수정되고 장치가 업데이트됩니다.

## DHCP IP 인터페이스 삭제

1. [DHCP IP Interface](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

DHCP Client Table이 열립니다.

3. DHCP 클라이언트 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

선택한 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 DHCP IP 인터페이스 정의

다음 표에서는 DHCP 클라이언트를 정의하는 CLI 명령을 요약합니다.

표 6-32. DHCP IP 인터페이스 CLI 명령

CLI 명령	설명
ip address dhcp [hostname 호스트 이름]	DHCP(동적 호스트 구성 프로토콜)의 이더넷 인터페이스에서 IP 주소를 가져옵니다.

다음은 CLI 명령의 예입니다.

```
console(config)# interface
ethernet 1/e11

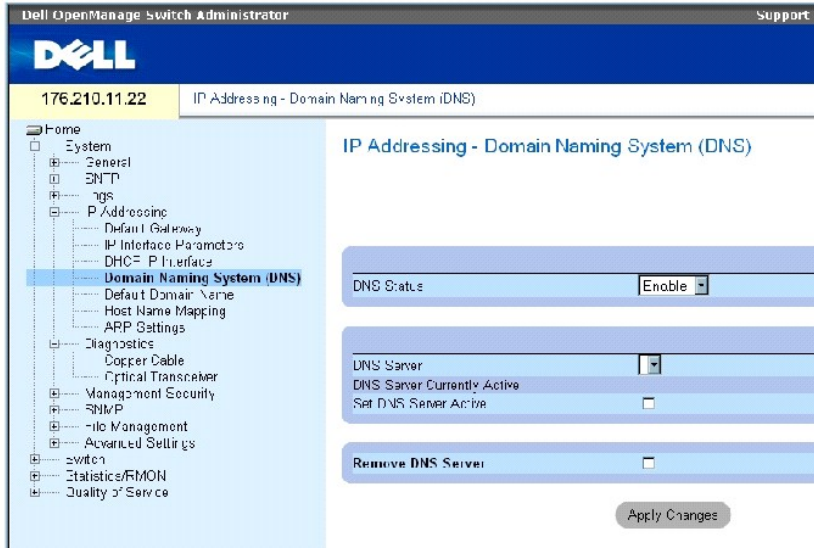
console(config-if)# ip
address dhcp
```

## DNS(도메인 이름 시스템) 구성

DNS(도메인 이름 시스템)는 사용자 정의 도메인 이름을 IP 주소로 변환합니다. 도메인 이름을 지정할 때마다 DNS 서비스는 이름을 숫자 IP 주소로 변환합니다. 예를 들면, www.ipexample.com은 192.87.56.2로 변환됩니다. DNS 서버는 도메인 이름 데이터베이스 및 해당 IP 주소를 유지관리합니다.

[Domain Naming System \(DNS\)](#) 페이지에는 특정 DNS 서버를 사용 설정 및 활성화하는 필드가 들어 있습니다. [Domain Naming System \(DNS\)](#) 페이지를 열려면 트리 뷰에서 **System**→**IP Addressing**→**Domain Naming System(DNS)**을 클릭하십시오.

그림 6-28. DNS(도메인 이름 시스템)



[Domain Naming System \(DNS\)](#) 페이지에는 다음 필드가 들어 있습니다.

**DNS Status** — DNS 이름의 IP 주소 변환을 활성화 또는 비활성화합니다.

**DNS Server** — DNS 서버 목록이 들어 있습니다. DNS 서버가 **Add DNS Server** 페이지에 추가됩니다.

**DNS Server Currently Active** — 현재 활성 상태인 DNS 서버입니다.

**Set DNS Server Active** — 선택한 DNS 서버를 활성화합니다.

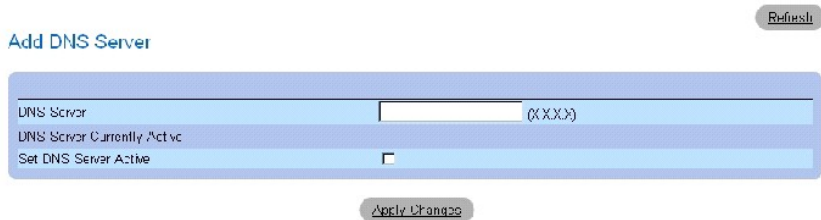
**Remove DNS Server** — 이 필드를 선택하면 선택한 DNS 서버가 제거됩니다.

## DNS 서버 추가

1. [Domain Naming System \(DNS\)](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add DNS Server** 페이지가 열립니다.

그림 6-29. DNS 서버 추가





DNS Server — DNS 서버 IP 주소입니다.

3. 관련 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

새 DNS 서버가 정의되고 장치가 업데이트됩니다.

## DNS 서버 표 표시

1. [Domain Naming System \(DNS\)](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

DNS Server Table이 열립니다.

그림 6-30. DNS 서버 표

### DNS Servers Table

	DNS Server	Active Server	Remove <a href="#">Select All</a>
1		<input checked="" type="radio"/>	<input type="checkbox"/>
2		<input checked="" type="radio"/>	<input type="checkbox"/>

## DNS 서버 제거

1. [Domain Naming System \(DNS\)](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

DNS Server Table 페이지가 열립니다.

3. DNS Server Table의 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

선택한 DNS 서버가 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 DNS 서버 구성

다음 표에서는 DNS 서버를 구성하는 CLI 명령을 요약합니다.

표 6-33. DNS 서버 CLI 명령

CLI 명령	설명
ip name-server 서버 주소	사용 가능한 이름 서버를 설정합니다. 최대 8개의 이름 서버를 정의할 수 있습니다.
no ip name-server 서버 주소	이름 서버를 제거합니다.
ip domain-name 이름	정식이 아닌 호스트 이름을 입력할 때 소프트웨어에서 사용하는 기본 도메인 이름을 정의합니다.
clear host {name *}	호스트 이름 대 주소 간 캐시에서 항목을 삭제합니다.

<b>show hosts</b> [이름]	기본 도메인 이름, 이름 서버 호스트의 목록, 정적 및 캐쉬된 호스트 이름과 주소 목록을 표시합니다.
<b>ip domain-lookup</b>	호스트 이름을 IP 주소로 변환할 때 DNS 시스템을 활성화합니다.

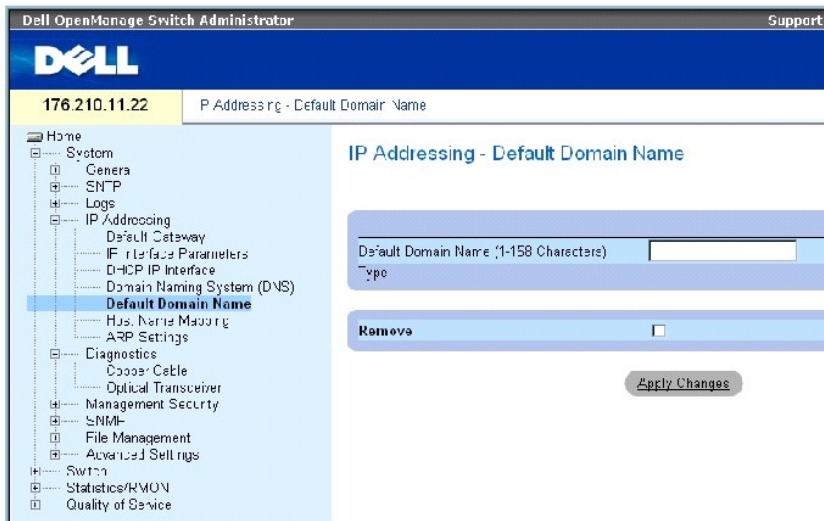
다음은 CLI 명령의 예입니다.

```
console(config)# ip name-
server 176.16.1.18
```

## 기본 도메인 정의

[Default Domain Name](#) 페이지에서는 기본 DNS 도메인 이름을 정의하는 데 필요한 정보를 제공합니다. [Default Domain Name](#) 페이지를 열려면 **System** → **IP Addressing** → **Default Domain Name**를 클릭하십시오.

그림 6-31. 기본 도메인 이름



[Default Domain Name](#) 페이지에는 다음 필드가 들어 있습니다.

**Default Domain Name (1-158 characters)** — 사용자 정의 기본 도메인 이름이 들어 있습니다. 이 필드를 정의하면 기본 도메인 이름이 모든 정식이 아닌 호스트 이름에 적용됩니다.

**Type** — IP 주소의 종류입니다. 가능한 필드 값은 다음과 같습니다.

**Dynamic** — 유동 IP 주소가 작성됩니다.

**Static** — 고정 IP 주소가 지정됩니다.

**Remove** — 이 필드를 선택하면 기본 도메인 이름이 제거됩니다.

## CLI 명령을 사용하여 DNS 도메인 이름 정의

다음 표에서는 DNS 도메인 이름을 구성하는 CLI 명령을 요약합니다.

표 6-34. DNS 도메인 이름 CLI 명령

CLI 명령	설명
ip domain-name name	정식이 아닌 호스트 이름을 입력할 때 소프트웨어에서 사용하는 기본 도메인 이름을 정의합니다.
no ip domain-name	DNS(도메인 이름 시스템)를 사용할 수 없도록 비활성화합니다.
show hosts [이름]	기본 도메인 이름, 이름 서버 호스트의 목록, 정적 및 캐쉬된 호스트 이름과 주소 목록을 표시합니다.

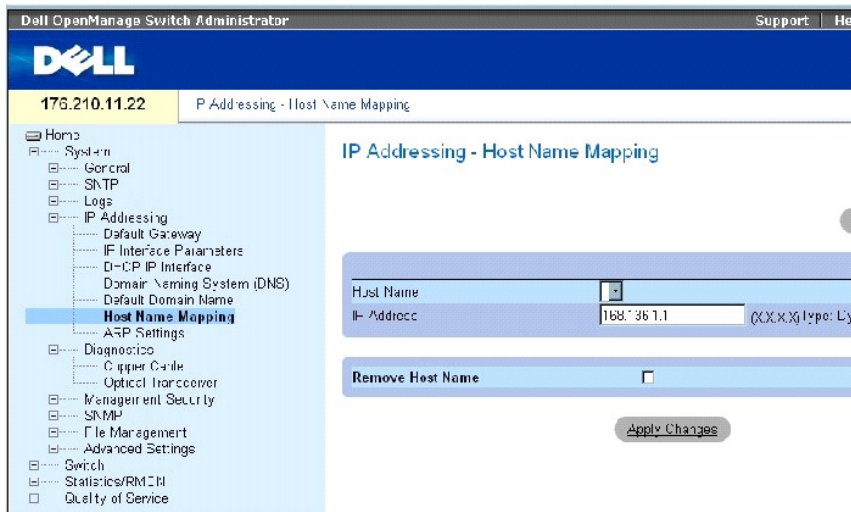
다음은 CLI 명령의 예입니다.

```
console(config)# ip
domain-name dell.com
```

## 도메인 호스트 매핑

[Host Name Mapping](#) 페이지에서는 IP 주소를 정적 호스트 이름에 지정하는 데 필요한 매개변수를 제공합니다. 이 페이지에서 하나의 호스트에 하나의 IP 주소를 지정할 수 있습니다. **Host Name Mapping** 페이지를 열려면 트리 뷰에서 **System** → **IP Addressing** → **Host Name Mapping**을 클릭하십시오.

그림 6-32. 호스트 이름 매핑



[Host Name Mapping](#) 페이지에는 다음 필드가 들어 있습니다.

**Host Name** — 호스트 이름 목록이 들어 있습니다. 호스트 이름은 **Add Host Name Mapping** 페이지에서 정의됩니다. 각 호스트에서는 하나의 IP 주소를 제공합니다.

**IP Address(X.X.X.X)** — 특정 호스트 이름에 지정된 IP 주소를 제공합니다.

**Type** — IP 주소의 종류입니다. 가능한 필드 값은 다음과 같습니다.

**Dynamic** — 유동 IP 주소가 작성됩니다.

Static — 고정 IP 주소가 지정됩니다.

Remove Host Name — 이 필드를 선택하면 DNS 호스트 매핑이 제거됩니다.

### 호스트 도메인 이름 추가

1. [Host Name Mapping](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

Add Host Name Mapping 페이지가 열립니다.

그림 6-33. 호스트 이름 매핑 추가

Refresh

Add Host Name Mapping

Host Name (C-1E8 Characters)

IP Address  (X.XXX.X.XXX)

Apply Changes

3. 관련 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

IP 주소가 호스트 이름에 매핑되고 장치가 업데이트됩니다.

### 호스트 이름 매핑 표 표시

1. [Host Name Mapping](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

Hosts Name Mapping Table 페이지가 열립니다.

그림 6-34. 호스트 이름 매핑 표

Refresh

	Host Name	IP Address	Remove Select: All
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Apply Changes

### IP 주소 매핑에서 호스트 이름 제거

1. [Host Name Mapping](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.
3. Host Name Mapping Table 페이지가 열립니다.

4. **Host Name Mapping Table**의 항목을 선택하십시오.
5. **Remove** 확인란을 선택하십시오.
6. **Apply Changes**를 클릭하십시오.

**Host Mapping Table**의 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 IP 주소를 도메인 호스트 이름에 매핑

다음 표에서는 도메인 호스트 이름을 IP 주소로 매핑하는 CLI 명령을 요약합니다.

표 6-35. 도메인 호스트 이름 CLI 명령

CLI 명령	설명
<b>ip host 이름 주소</b>	호스트 캐쉬에 정적 호스트 이름 대 주소 간 매핑을 정의합니다.
<b>no ip host name</b>	이름 대 주소 간 매핑을 제거합니다.
<b>clear host {name   *}</b>	호스트 이름 대 주소 간 캐쉬에서 항목을 삭제합니다.
<b>show hosts [name]</b>	기본 도메인 이름, 이름 서버 호스트의 목록, 정적 및 캐쉬된 호스트 이름과 주소 목록을 표시합니다.

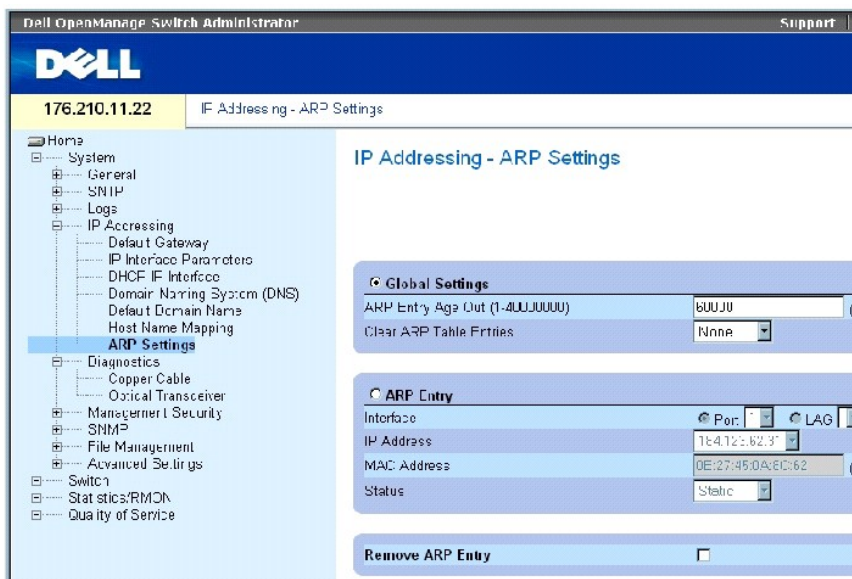
다음은 CLI 명령의 예입니다.

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

## ARP 설정 정의

ARP(주소 결정 프로토콜)는 IP 주소를 실제 주소로 변환하고 IP 주소를 MAC 주소에 매핑합니다. ARP는 이웃한 IP 주소가 알려진 경우에만 호스트가 다른 호스트와 통신할 수 있도록 합니다. [ARP Settings](#) 페이지를 열려면 트리 뷰에서 **System** → **IP Addressing** → **ARP**를 클릭하십시오.

그림 6-35. ARP 설정



[ARP Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**Global Settings** — ARP 전역 설정의 필드를 활성화할 경우 이 옵션을 선택하십시오.

**ARP Entry Age Out (1-4000000)** — 모든 장치에서 ARP 표 항목에 대한 ARP 요청을 전달하는 데 걸리는 시간(초)입니다. 이 시간이 지나면 항목이 표에서 삭제됩니다. 값의 범위는 1~4000000입니다. 기본값은 60000초입니다.

**Clear ARP Table Entries** — 모든 장치에서 지워진 ARP 항목의 종류입니다. 가능한 값은 다음과 같습니다.

**None** — ARP 항목을 지우지 않습니다.

**All** — 모든 ARP 항목을 지웁니다.

**Dynamic** — 동적 ARP 항목만 지웁니다.

**Static** — 정적 ARP 항목만 지웁니다.

**ARP Entry** — 단일 이더넷 장치에서 ARP 설정의 필드를 활성화할 경우 이 옵션을 선택하십시오.

**Interface** — 장치에 연결된 포트, LAG 또는 VLAM의 인터페이스 번호입니다.

**IP Address** — 스테이션 IP 주소로서 아래에 입력된 MAC 주소와 연관됩니다.

**MAC Address** — 스테이션 MAC 주소로서 ARP 표에서 IP 주소와 연관됩니다.

**Status** — ARP 표 항목의 상태입니다. 가능한 필드 값은 다음과 같습니다.

**Dynamic** — ARP 항목이 동적으로 확인됩니다.

**Static** — ARP 항목이 정적 항목입니다.

**Remove ARP Entry** — 이 필드를 선택하면 ARP 항목이 제거됩니다.

## 정적 ARP 표 항목 추가

1. [ARP Settings 페이지](#)를 여십시오.
2. **Add**를 클릭하십시오.

**Add ARP Entry** 페이지가 열립니다.

3. 인터페이스를 선택하십시오.
4. 필드를 정의하십시오.
5. **Apply Changes**를 클릭하십시오.

ARP Table의 항목이 추가되고 장치가 업데이트됩니다.

### ARP 표 표시

1. [ARP Settings 페이지](#)를 여십시오.
2. **Show All**을 클릭하십시오.

ARP Table 페이지가 열립니다.

### ARP 표 항목 삭제

1. [ARP Settings 페이지](#)를 여십시오.
2. **Show All**을 클릭하십시오.

ARP Table 페이지가 열립니다.

3. 표 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

ARP Table의 항목이 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 ARP 구성

다음 표에서는 [ARP Settings](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-36. ARP 설정 CLI 명령

CLI 명령	설명
arp ip_addr hw_addr {ethernet interface-number   vlan vlan-id   port-channel number}	ARP 캐시에서 영구적인 항목을 추가합니다.
arp timeout seconds	ARP 캐시에 항목의 보관 기간을 구성합니다.
clear arp-cache	ARP 캐시에서 모든 동적 항목을 삭제합니다.
show arp	ARP 표에 항목을 표시합니다.
no arp	ARP 표에서 ARP 항목을 제거합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp
```

ARP timeout: 12000 Seconds			
Interface	IP address	HW address	Status
-----	-----	-----	-----
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

## 케이블 진단 실행

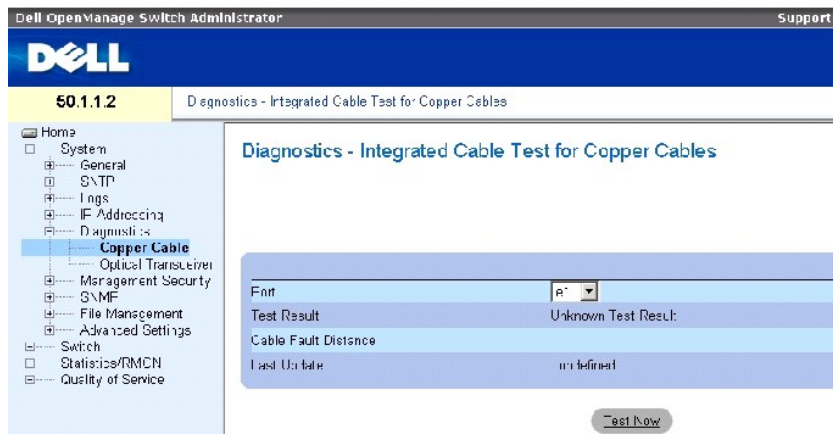
**Diagnostics** 페이지에는 구리 케이블에서 가장 케이블 테스트를 수행하는 페이지에 대한 링크가 들어 있습니다. **Diagnostics** 페이지를 열려면 트리 뷰에서 **System** → **Diagnostics**를 클릭하십시오.

## 구리 케이블 진단 보기

**Copper Cables** 페이지에는 구리 케이블에서 테스트를 수행하는 데 필요한 필드가 들어 있습니다. 케이블 테스트는 케이블에서 오류가 발생한 위치, 케이블 테스트를 수행한 마지막 시간 그리고 발생한 케이블 오류 종류에 대한 정보를 제공합니다. 테스트에서는 TDR(시간 영역 반사 측정법) 기술을 사용하여 포트에 연결된 구리 케이블의 품질 및 특성을 테스트합니다. 최대 120 미터의 케이블을 검사할 수 있습니다. 근사 케이블 길이 테스트를 제외하고는 포트가 중단 상태일 때 케이블이 테스트됩니다.

**Copper Cables** 페이지를 열려면 트리 뷰에서 **System** → **Diagnostics** → **Copper Cable**을 클릭하십시오.

그림 6-36. 구리 케이블 통합 케이블 테스트



**Copper Cables** 페이지에는 다음 필드가 들어 있습니다.

**Port** — 케이블이 연결된 포트입니다.

**Test Result** — 케이블 테스트 결과입니다. 가능한 필드 값은 다음과 같습니다.

**No Cable** — 포트에 연결된 케이블이 없습니다.



**Open Cable** — 케이블이 한쪽만 연결된 상태입니다.

**Short Cable** — 케이블에서 단락이 발생했습니다.

**OK** — 케이블이 테스트를 통과했습니다.

**Cable Fault Distance** — 케이블 오류가 발생한 포트와의 거리입니다.

**Last Update** — 포트를 마지막으로 테스트한 시간입니다.

**Approximate Cable Length** — 대략적인 케이블 길이입니다. 이 테스트는 포트가 1Gbps로 작동 중인 경우에만 수행할 수 있습니다.

## 케이블 테스트 수행


1. 구리 케이블의 양쪽이 모두 장치에 연결되었는지 확인하십시오.
2. [Copper Cables](#) 페이지를 여십시오.
3. 테스트할 인터페이스를 선택하십시오.
4. **Test Now**를 클릭하십시오.

구리 케이블 테스트가 수행되고 그 결과가 [Copper Cables](#) 페이지에 표시됩니다.

## 가상 케이블 테스트 결과 표 표시

1. [Copper Cables](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

**Integrated Cable Test Results Table** 페이지가 열립니다.

 **주:** 이 화면에서는 이전에 실행한 테스트 결과를 표시하지만 지금 모든 포트에서 실제로 테스트를 수행하지는 않습니다.

[Copper Cables](#) 페이지의 필드 이외에도 **Integrated Cable Test Results Table**에는 다음 필드가 들어 있습니다.

**Unit No.** — 케이블이 표시되는 단원의 번호입니다.

## CLI 명령을 사용하여 구리 케이블 테스트 수행

다음 표에는 구리 케이블 테스트를 수행하는 CLI 명령이 들어 있습니다.


표 6-37. 구리 케이블 테스트 CLI 명령

CLI 명령	설명
<code>test copper-port tdr</code> 인터페이스	VCT 테스트를 수행합니다.
	포트에서 마지막으로 수행한 VCT 테스트 결과를 표시합니다.

show copper-port tdr 인터페이스	
	포트에 연결된 구리 케이블의 예상 길이를 표시합니다.
show copper-port cable-length 인터페이스	

다음은 CLI 명령의 예입니다.

console> enable	
Console# test copper-port tdr 1/e3	
Cable is open at 100 meters.	
Console# show copper-port cable-length	
Port	Length (meters)
----	-----
1/e3	110-140
1/e4	Fiber

 **주:** ICT(Integrated Cable Tester)의 테스트 결과에 있는 케이블 길이는 최대 50m, 50m-80m, 80m-110m, 110m-120m 또는 120m 초과 간격으로 측정된 대략치입니다. 편차는 최대 20m입니다. 10Mbps 링크에는 케이블 길이 측정이 작동하지 않습니다.

## 광 송수신기 진단 보기

[Optical Transceiver](#) 페이지를 사용하여 광섬유 케이블에서 테스트를 수행합니다. [Optical Transceiver](#) 페이지를 열려면 트리 뷰에서 **System**→**Diagnostics**→**Optical Transceiver**를 클릭하십시오.


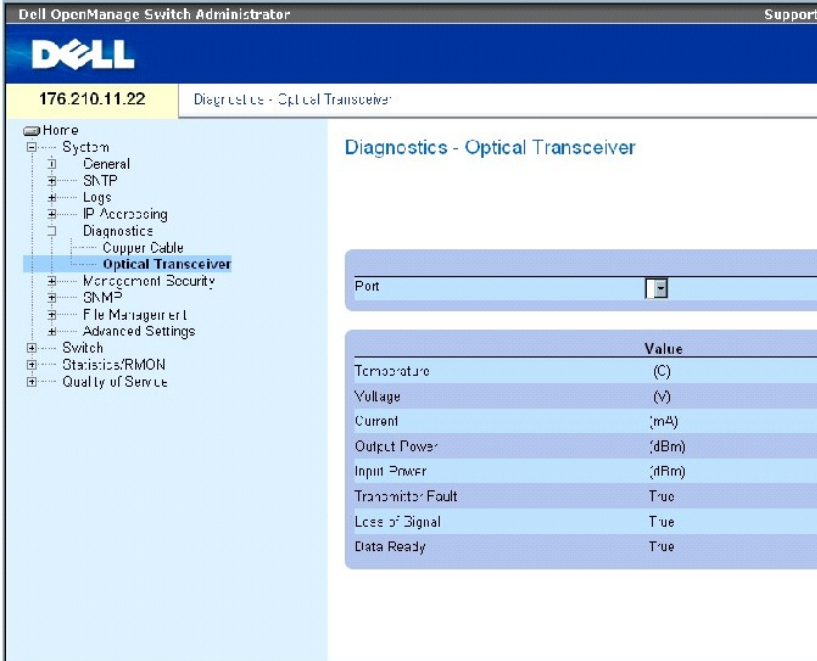
 **주:** 광 송수신기 진단은 링크가 존재하는 경우에만 수행할 수 있습니다.

그림 6-37. 광 송수신기



[Optical Transceiver](#) 페이지에는 다음 필드가 들어 있습니다.

**Port** — 케이블을 테스트하는 포트 IP 주소입니다.

**Temperature** — 케이블의 작동 온도(C)입니다.

**Voltage** — 케이블의 작동 전압입니다.

**Current** — 케이블의 작동 전류입니다.

**Output Power** — 출력을 송신하는 비율입니다.

**Input Power** — 입력을 송신하는 비율입니다.

**Transmitter Fault** — 송신 시 오류가 발생했는지 여부를 표시합니다.

**Loss of Signal** — 케이블에 신호 손실이 발생했는지 여부를 표시합니다.

**Data Ready** — 송수신기에 전원이 공급되어 데이터 준비가 완료된 상태입니다.

### 광 송수신기 진단 테스트 결과 표 표시

1. [Optical Transceiver](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.


테스트가 실행되고 **Optical Transceiver Diagnostics Table** 페이지가 열립니다.

[Optical Transceiver](#) 페이지의 필드 이외에도 **Optical Transceiver Diagnostics Table**에는 다음 필드가 들어 있습니다.

**Unit No.** — 케이블이 표시되는 단원의 번호입니다.

1 N/A — 해당 사항 없음, N/S - 지원되지 않음, W - 경고, E - 오류

 **주:** Finisar 송수신기는 송신기 오류 진단 테스트를 지원하지 않습니다.

 **주:** 광섬유 분석 기능은 디지털 진단 표준 SFF-872를 지원하는 SFP에서만 작동합니다.

## CLI 명령을 사용하여 광섬유 케이블 테스트 수행

다음 표에는 광섬유 케이블 테스트를 수행하는 CLI 명령이 들어 있습니다.

표 6-38. 광섬유 케이블 테스트 CLI 명령

CLI 명령	설명
<code>show fiber-ports optical-transceiver [인터페이스] [세부 정보]</code>	광 송수신기 진단을 표시합니다.

다음은 CLI 명령의 예입니다.

```
Console# show fiber-ports optical-transceiver detailed
```

Port	Temp [C]	Voltage	Current [Volt]	Output [mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
---	---	-----	-----	-----	-----	-----	-----
1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

## 스위치 보안 관리

**Management Security** 페이지에서는 포트의 보안 매개변수, 장치 관리 메소드, 사용자 및 서버 보안을 설정하는 데 필요한 필드가 들어 있는 보안 페이지에 액세스할 수 있습니다. **Management Security** 페이지를 열려면 트리 뷰에서 System→Management Security를 클릭하십시오.

## 액세스 프로파일 정의

**Access Profiles** 페이지에는 장치에 액세스하는 규칙 및 프로파일을 정의하는 필드가 들어 있습니다. 관리 기능에 대한 액세스는 수신 인터페이스 및 소스 IP 주소나 소스 IP 서브넷에 의해 정의된 사용자 그룹으로 제한될 수 있습니다.

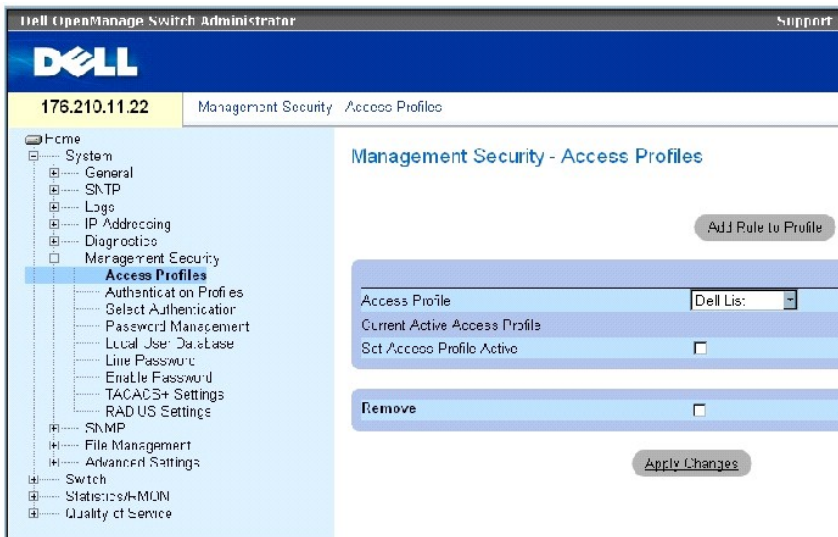
관리 액세스는 웹(HTTP), 보안 웹(HTTPS), 텔넷 및 보안 텔넷을 포함하여 관리 액세스 메소드의 종류마다 별도로 정의할 수 있습니다.

다른 관리 메소드에 대한 액세스는 사용자 그룹마다 다를 수 있습니다. 예를 들면, 사용자 그룹 1은 HTTPS 세션을 통해서만 장치에 액세스할 수 있지만 사용자 그룹 2는 HTTPS 및 텔넷 세션 모두를 통해 장치에 액세스할 수 있습니다.

관리 액세스 목록에는 장치를 관리할 수 있는 사용자를 결정하는 규칙이 메소드별로 최대 256개가 있습니다. 사용자의 장치에 대한 액세스를 차단할 수도 있습니다.

Access Profiles 페이지에는 관리 목록을 구성하여 특정 인터페이스에 적용하는 데 필요한 필드가 들어 있습니다. Access Profiles 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Access Profiles**를 클릭하십시오.

그림 6-38. 액세스 프로파일



Access Profiles 페이지에는 다음 필드가 들어 있습니다.

**Access Profile** — 사용자 정의된 액세스 프로파일 목록입니다. 액세스 프로파일 목록에는 **Console Only**가 기본값으로 들어 있습니다. 이 액세스 프로파일을 선택하면 콘솔 연결만 사용하여 장치의 활성 관리가 수행됩니다.

**Current Active Access Profile** — 현재 활성 상태인 액세스 프로파일입니다.

**Set Access Profile Active** — 액세스 프로파일을 활성화합니다.

**Remove** — 이 필드를 선택하면 **Access Profile Name** 목록에서 액세스 프로파일이 제거됩니다.

## 프로파일 활성화

1. [Access Profiles](#) 페이지를 여십시오.
2. **Access Profile** 필드에서 액세스 프로파일을 선택하십시오.
3. **Set Access Profile Active** 확인란을 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

액세스 프로파일이 활성화됩니다.

## 액세스 프로파일 추가

규칙 우선순위, 장치 관리 메소드, 인터페이스 종류, 소스 IP 주소 및 네트워크 마스크, 장치 관리 액세스 조치를 결정할 때 규칙은 필터 역할을 합니다. 사용자의 관리 액세스를 차단하거나 허용할 수도 있습니다. 규칙 우선순위는 규칙을 구현하는 순서를 설정합니다.

## 액세스 프로파일의 규칙 정의

1. **Access Profiles** 페이지를 여십시오.
2. **Add Profile**을 클릭하십시오.

**Add an Access Profile** 페이지가 열립니다.

그림 6-39. 액세스 프로파일 추가

Refresh

Add an Access Profile

Access Profile Name (1-32 Characters)

Rule Priority (1-65535)

Management Method

Interface  Port  LAG  VLAN

Source IP Address   Network Mask

Prefix Length

Action

Apply Changes


[Add an Access Profile](#) 페이지에는 다음의 추가 필드가 들어 있습니다.

**Access Profile Name (1-32 Characters)** — 액세스 프로파일의 사용자 정의 이름입니다. 액세스 프로파일 이름의 최대값은 32자입니다.

**Rule Priority (1-65535)** — 규칙 우선순위입니다. 패킷이 규칙과 일치하면 사용자 그룹에게 장치 관리에 대한 액세스 권한이 부여되거나 액세스가 거부됩니다. 규칙 순서는 이 필드를 통해 규칙 우선순위를 정의하여 설정됩니다. 패킷이 최초 일치율 기준으로 일치되므로 규칙 번호는 패킷과 규칙을 일치시킬 때 필수적입니다. 규칙 우선순위는 **Profile Rules Table**에서 확인할 수 있습니다.

**Management Method** — 액세스 프로파일의 정의되는 관리 메소드입니다. 이 액세스 프로파일의 사용자는 선택한 관리 메소드(라인)를 통해 장치에 대한 액세스가 거부되거나 허용됩니다.

**Interface** — 규칙이 적용되는 인터페이스 종류입니다. 이 필드는 선택 사항입니다. 이 규칙은 확인란을 선택한 후 해당 옵션 단추 및 인터페이스를 선택하여 선택한 포트, LAG 또는 VLAN에 적용됩니다.

 **주:** 인터페이스에 액세스 프로파일을 지정하면 다른 인터페이스를 통한 액세스는 거부됩니다. 액세스 프로파일을 인터페이스에 지정하지 않은 경우 모든 인터페이스를 통해 장치에 액세스할 수 있습니다.

**Source IP Address(X.X.X.X)** — 규칙이 적용되는 인터페이스 소스 IP 주소입니다. 이 필드는 선택 사항이며, 규칙이 서브네트워크에 유효한지를 표시합니다.

**Network Mask(X.X.X.X)** — IP 서브네트워크 마스크입니다.

**Prefix Length(XX)** — 소스 IP 주소 접두어 또는 소스 IP 주소의 네트워크 마스크를 구성하는 비트 개수입니다.

**Action** — 정의된 인터페이스에 대한 관리 액세스를 허용할 것인지 거부할 것인지 여부를 정의합니다.

3. **Access Profile Name** 필드를 정의하십시오.
4. 관련 필드를 정의하십시오.
5. **Apply Changes**를 클릭하십시오.

새 액세스 프로파일이 추가되고 장치가 업데이트됩니다.

## 액세스 프로파일에 규칙 추가

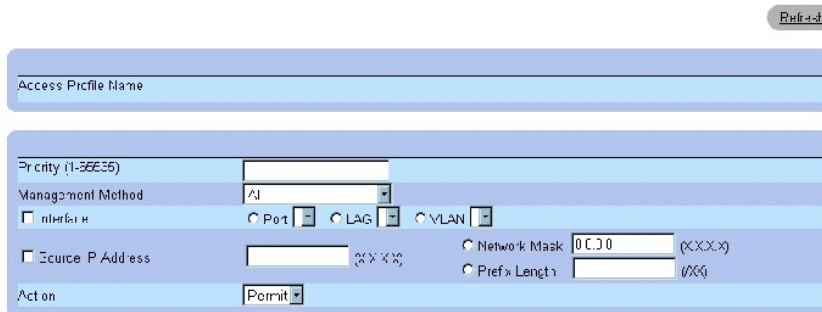
**주:** 첫 번째 규칙은 액세스 프로파일과 처음 일치하는 처리량에 정의해야 합니다.

1. **Access Profile** 페이지를 여십시오.
2. **Add Rule to Profile**을 클릭하십시오.

**Add an Access Profile Rule** 페이지가 열립니다.

그림 6-40. 액세스 프로파일 규칙 추가

### Add an Access Profile Rule



3. 필드를 채우십시오.
4. **Apply Changes**를 클릭하십시오.

액세스 프로파일에 규칙이 추가되고 장치가 업데이트됩니다.

## 프로파일 규칙 표 보기

**주:** 규칙이 프로파일 규칙 표에 표시되는 순서가 중요합니다. 패킷이 규칙 기준을 충족시키는 첫 번째 규칙과 일치합니다.

1. [Access Profiles](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

**Profile Rules Table** 페이지가 열립니다.

그림 6-41. 프로파일 규칙 표

## Profile Rules Table

Refresh

Access Profile Name

Priority	Interface	Management Method	Source IP Address	Prefix Length	Action	R
1		All			Permit	

Apply Changes

## 규칙 제거

1. **Access Profiles** 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

**Profile Rules Table** 페이지가 열립니다.

3. 규칙을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

선택한 규칙이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 액세스 프로파일 정의

다음 표에서는 [Access Profiles](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-39. 액세스 프로파일 CLI 명령

CLI 명령	설명
management access-list name	관리에 대한 액세스 목록을 정의하고 구성에 대한 액세스 목록 컨텍스트를 입력합니다.
permit [ethernet interface-number   vlan vlan-id   port-channel number] [service service]	관리 액세스 목록에 대한 포트 허용 조건을 설정합니다.
permit ip-source ip-address [mask mask   prefix-length] [ethernet interface-number   vlan vlan-id   port-channel number] [service service]	선택한 관리 메소드 및 관리 액세스 목록에 대한 포트 허용 조건을 설정합니다.
deny [ethernet interface-number   vlan vlan-id   port-channel number] [service service]	선택한 관리 메소드 및 관리 액세스 목록에 대한 포트 거부 조건을 설정합니다.
deny ip-source ip-address [mask mask   prefix-length] [ethernet interface-number   vlan vlan-id   port-channel number] [service service]	선택한 관리 메소드 및 관리 액세스 목록에 대한 포트 거부 조건을 설정합니다.
management access-class {console-only   name}	활성 관리 연결로 사용되는 액세스 목록을 정의합니다.
show management access-list [name]	활성 관리 액세스 목록을 표시합니다.
show management access-class	관리 액세스 클래스에 대한 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)#
management access-list
m1ist

console(config-macl)#
permit ethernet 1/e1
    
```



```
console(config-macl)#
permit ethernet 1/e2

console(config-macl)# deny
ethernet 1/e3

console(config-macl)# deny
ethernet 1/e4

console(config-macl)# exit

console(config)#
management access-class
m1ist

console(config)# exit

console# show management
access-list

m1ist

-----

permit ethernet 1/e1

permit ethernet 1/e2

deny ethernet 1/e3

deny ethernet 1/e4

! (Note: all other access
implicitly denied)

Console# show management
access-class

Management access-class is
enabled, using access list
m1ist
```

## 인증 프로파일 정의

[Authentication Profile](#) 페이지에는 장치에서 사용자 인증 메소드를 선택하는 데 필요한 필드가 들어 있습니다. 사용자 인증은 다음과 같은 방법으로 진행됩니다.

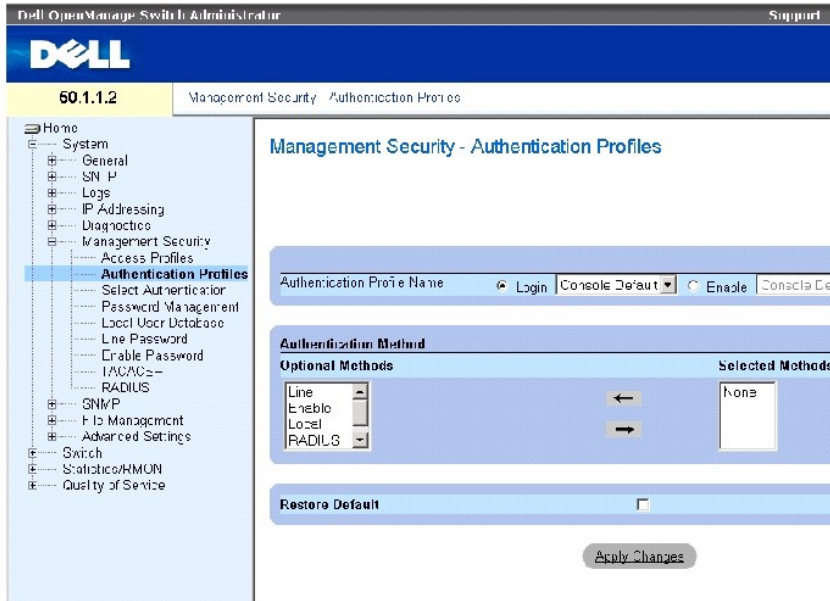
1 외부 서버를 통해

사용자 인증은 None으로도 설정할 수 있습니다.

사용자 인증은 메소드를 선택한 순서대로 수행됩니다. 예를 들면, 로컬 및 RADIUS 옵션을 모두 선택하면 사용자는 로컬로 먼저 인증됩니다. 로컬 사용자 데이터베이스가 비어 있는 경우 사용자는 RADIUS 서버를 통해 인증됩니다. 첫 번째 메소드를 사용하여 인증에 실패한 경우 인증 프로세스는 종료됩니다.

인증 도중 오류가 발생한 경우 다음에 선택한 메소드가 사용됩니다. [Authentication Profiles](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Authentication Profiles**를 클릭하십시오.

그림 6-42. 인증 프로파일



[Authentication Profiles](#) 페이지에는 다음 필드가 들어 있습니다.

**Authentication Profile Name** — 사용자 정의 인증 프로파일이 추가된 사용자 정의 인증 프로파일 목록입니다. 기본값은 **Network Default** 및 **Console Default**입니다.

- **Login** — 로그인 암호의 사용자 정의 인증 프로파일 목록을 지정합니다.
- **Enable** — 활성 암호의 사용자 정의 인증 프로파일 목록을 지정합니다.

**Optional Methods** — 사용자 인증 메소드입니다. 가능한 선택 사항은 다음과 같습니다.

**None** — 사용자 인증이 발생하지 않습니다.

**Local** — 사용자 인증이 장치 레벨로 수행됩니다. 장치에서는 인증 시 사용자 이름과 암호를 확인합니다.

**RADIUS** — RADIUS 서버에서 사용자 인증이 수행됩니다. 자세한 정보는 [RADIUS 설정 구성](#)을 참조하십시오.

**Line** — 라인 암호는 사용자 인증에 사용됩니다.

**Enable** — 활성화된 암호는 인증에 사용됩니다.

**TACACS+** — TACACS+ 서버에서 사용자 인증이 수행됩니다.

**Restore Default**— 장치의 기본 사용자 인증 메소드를 복구합니다. 기본 프로파일에만 사용 가능합니다.

**Remove** — 이 필드를 선택하면 선택한 프로파일이 제거됩니다. 활성 프로파일은 삭제할 수 없습니다. 사용자 정의 프로파일에만 사용 가능합니다.

### 인증 프로파일 선택

1. [Authentication Profiles](#) 페이지를 여십시오.
2. **Authentication Profile Name** 필드에서 프로파일을 선택하십시오.
3. 탐색 화살표를 사용하여 인증 메소드를 선택하십시오. 인증 메소드가 나열된 순서대로 인증이 수행됩니다.
4. **Apply Changes**를 클릭하십시오.

사용자 인증 프로파일이 장치에 업데이트됩니다.

### 인증 프로파일 추가:

1. [Authentication Profiles](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add Authentication Profile** 페이지가 열립니다.

그림 6-43. 인증 프로파일 추가

### Add Authentication Profile

Refresh

Login  Erable

Profile Name

Authentication Method	
Optional Methods	Selected Methods
None	
Erable	
_local	
FACIOS	

3. 프로파일을 구성하십시오.

**주:** 새 프로파일 이름에 공백을 넣지 마십시오.

4. **Apply Changes**를 클릭하십시오.

인증 프로파일이 장치에 업데이트됩니다.

### 인증 프로파일 표 표시:

1. [Authentication Profiles](#) 페이지를 여십시오.

2. **Show All**을 클릭하십시오.

Authentication Profiles Table 페이지가 열립니다.

## 인증 프로파일 삭제

1. [Authentication Profiles](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

Authentication Profile Table 페이지가 열립니다.

3. 인증 프로파일을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

선택한 인증 프로파일이 삭제됩니다.

## CLI 명령을 사용하여 인증 프로파일 구성

다음 표에서는 [Authentication Profiles](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-40. 인증 프로파일 CLI 명령

CLI 명령	설명
aaa authentication login {default   list-name} method1 [method2.]	로그인 인증을 구성합니다.
no aaa authentication login {default   list-name}	로그인 인증 프로파일을 제거합니다.

다음은 CLI 명령의 예입니다.

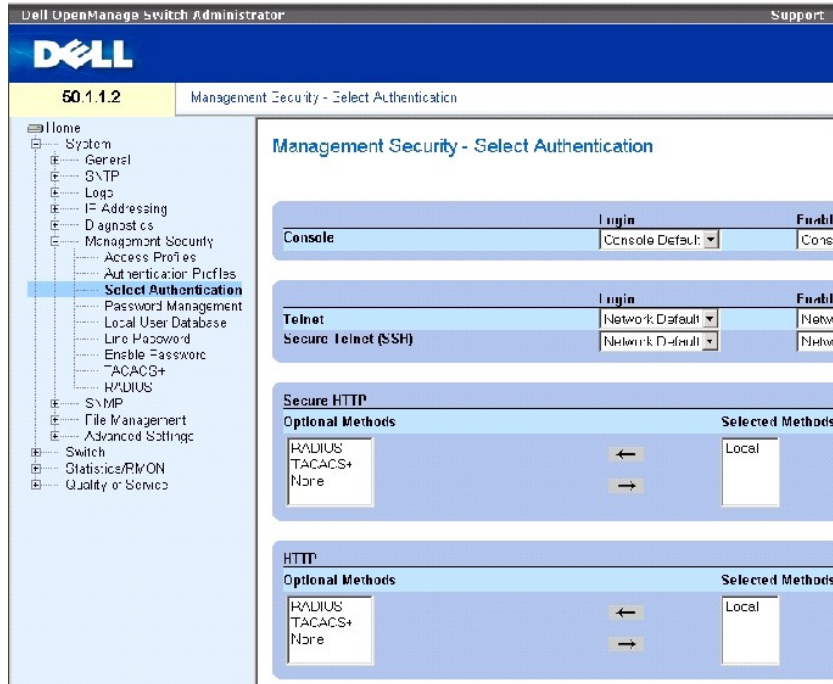
```
console(config)# aaa
authentication login
default radius local
enable none

console(config)# no aaa
authentication login
default
```

## 인증 프로파일 선택

인증 프로파일을 정의한 후 인증 프로파일을 관리 액세스 메소드에 적용할 수 있습니다. 예를 들면, 콘솔 사용자는 인증 메소드 목록 1로 인증될 수 있지만 텔넷 사용자는 인증 메소드 목록 2로 인증됩니다. [Select Authentication](#) 페이지를 열려면 트리 뷰에서 **System**→**Management Security**→**Select Authentication**을 클릭하십시오.

그림 6-44. 인증 선택



[Select Authentication](#) 페이지에는 다음 필드가 들어 있습니다.

**Console** — 콘솔 사용자를 인증할 때 사용하는 인증 프로파일입니다.

**Login** — 콘솔 인터페이스로 로그인하는 사용자가 사용할 인증 프로파일을 지정합니다.

**Enable** — 콘솔 인터페이스에서 권한 부여된 EXEC 모드를 활성화하는 사용자가 사용할 인증 프로파일을 지정합니다.

**Telnet** — 텔넷 사용자를 인증할 때 사용하는 인증 프로파일입니다.

**(Secure Telnet)(SSH)** — 보안 셸(SSH) 사용자를 인증할 때 사용하는 인증 프로파일입니다. SSH는 클라이언트에게 장치에 대한 암호화된 보안 원격 연결을 제공합니다.

**HTTP 및 Secure HTTP** — HTTP 액세스 및 보안 HTTP 액세스에서 각각 사용하는 인증 메소드입니다. 가능한 필드 값은 다음과 같습니다.

**None** — 액세스할 때 인증 메소드를 사용하지 않습니다.

**Local** — 로컬로 인증이 수행됩니다.

**RADIUS** — RADIUS 서버에서 인증이 수행됩니다.

**TACACS+** — TACACS+ 서버에서 인증이 수행됩니다.

## 콘솔 세션에 인증 목록 적용

1. [Select Authentication](#) 페이지를 여십시오.
2. **Console** 필드에서 인증 프로파일을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

콘솔 세션에 인증 목록이 지정됩니다.

### 텔넷 세션에 인증 프로파일 적용

1. [Select Authentication](#) 페이지를 여십시오.
2. **Telnet** 필드에서 인증 프로파일을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

텔넷 세션에 인증 목록이 지정됩니다.

### 보안 텔넷(SSH) 세션에 인증 프로파일 적용

1. [Select Authentication](#) 페이지를 여십시오.
2. **Secure Telnet (SSH)** 필드에서 인증 프로파일을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

보안 텔넷(SSH) 세션에 인증 프로파일 지정됩니다.

### HTTP 세션에 인증 순서 지정

1. [Select Authentication](#) 페이지를 여십시오.
2. **HTTP** 필드에서 인증 순서를 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

HTTP 세션에 인증 순서가 지정됩니다.

### 보안 HTTP 세션에 인증 순서 지정

1. [Select Authentication](#) 페이지를 여십시오.
2. **Secure HTTP** 필드에서 인증 순서를 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

보안 HTTP 세션에 인증 순서가 지정됩니다.

### CLI 명령을 사용하여 액세스 인증 프로파일 또는 순서 지정

다음 표에서는 [Select Authentication](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-41. 인증 선택 CLI 명령

CLI 명령	설명
enable authentication [default   list-name]	원격 텔넷, 콘솔 또는 SSH의 더 높은 권한 레벨에 액세스하는 경우 인증 메소드 목록을 표시합니다.
login authentication [default   list-name]	원격 텔넷, 콘솔 또는 SSH의 로그인 인증 메소드 목록을 표시합니다.

ip http authentication method1 [method2.]	HTTP 서버의 인증 메소드를 표시합니다.
ip https authentication method1 [method2.]	HTTPS 서버의 인증 메소드를 표시합니다.
show authentication methods	인증 메소드에 대한 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

console(config-line)# enable authentication default		
console(config-line)# login authentication default		
console(config-line)# exit		
console(config)# ip http authentication radius local		
console(config)# ip https authentication radius local		
console(config)# exit		
console# show authentication methods		
Login Authentication Method Lists		
-----		
Console_Default	: None	
Network_Default	: Local	
Enable Authentication Method Lists		
-----		
Console_Default	: Enable None	
Network_Default	: Enable	
Line	Login Method List	Enable Method List
----	----- ----	----- ----- ----

Console	Default	Default
Telnet	Default	Default
SSH	Default	Default
http	: Local	
https	: Local	
dot1x	:	

## 암호 관리

암호 관리를 통해 네트워크 보안이 강화되고 암호 제어 기능이 개선됩니다. SSH, 텔넷, HTTP, HTTPS 및 SNMP 액세스의 암호에 다음을 포함하는 보안 기능이 지정됩니다.

- 1 최소 암호 길이 정의
- 1 암호 만기
- 1 암호 재사용 횟수 제한
- 1 로그인 실패 후 사용자 잠금

암호 관리를 활성화하는 즉시 암호 사용 기간이 시작됩니다. 암호는 사용자 정의 시간/일 정의 만기에 따라 만료됩니다. 암호 만료 10일 전에 장치에서 암호 만료에 관한 경고 메시지를 표시합니다.

암호가 만료된 후 사용자는 추가로 3번 더 로그인할 수 있습니다. 이 3번의 로그인 동안에 즉시 암호를 변경해야 함을 사용자에게 알리는 추가 경고 메시지가 표시됩니다. 암호를 변경하지 않으면 사용자는 시스템에서 잠기고 콘솔을 사용해야만 로그인할 수 있습니다. 암호 경고는 Syslog 파일에 로그됩니다.

권한 레벨을 재정의한 경우 사용자도 재정의해야 합니다. 그러나 암호 사용 기간은 첫 번째 사용자 정의에 따라 만료됩니다.

[Password Management](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Password Management**를 클릭하십시오.

**그림 6-45. 암호 관리**





[Password Management](#) 페이지에는 다음 필드가 들어 있습니다.

**Password Minimum Length (8-54)** — 이 필드를 선택하면 최소 암호 길이가 표시됩니다. 예를 들면, 관리자는 모든 암호 길이의 최소값을 10자로 정의할 수 있습니다.

**Consecutive Passwords Before Re-use** — 암호를 재사용하기 위해 암호를 변경한 횟수를 표시합니다. 가능한 필드 값 범위는 1~10입니다.

**주:** 암호가 만료되기 전에 암호를 변경해야 한다는 경고가 사용자에게 전송됩니다. 그러나 이 알람은 웹 사용자에게 표시되지 않습니다.

**Enable Login Attempts** — 이 필드를 선택하면 잘못된 암호를 사용자 정의 횟수 이상 사용한 경우 장치에서 사용자를 장치 외부에 잠글 수 있습니다. 예를 들면, 이 필드를 선택하고 잘못된 암호로 로그인 하는 횟수를 5로 입력하면 여섯 번째 시도에서 사용자를 잠급니다. 가능한 필드 값 범위는 1~5입니다.

## 암호 관리 정의

1. [Password Management](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. Apply Changes를 클릭하십시오.

암호 관리가 정의되고 장치가 업데이트됩니다.

## CLI 명령을 사용한 암호 관리

다음 표에서는 [Password Management](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-42. CLI 명령을 사용한 암호 관리

CLI 명령	설명
password min-length 길이	최소 암호 길이를 정의합니다.
password history number	암호를 재사용하기 위해 암호를 변경하는 횟수를 표시합니다.
password lock-out 횟수	장치에서 사용자를 잠그기 전에 먼저 잘못된 암호를 입력하는 횟수를 정의합니다.
show password configuration	암호 관리 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

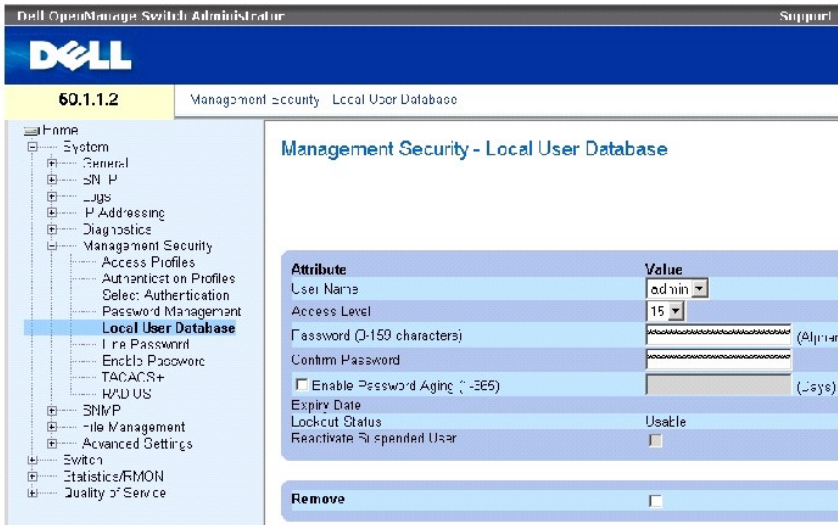
console # show passwords configuration				
Minimal length: 0				
History: Disabled				
History hold time: no limit				
Lockout control: disabled				
Enable Passwords				
Level	Password Aging	Password Expiry date	Lockout	
----	-----	-----	-----	
		---		
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-----	-----	-----	-----	
		---		
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	

console # show users accounts				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
-----	-----	-----	-----	-----
nim	15	39	18-Feb-2005	

### 로컬 사용자 데이터베이스 정의

[Local User Database](#) 페이지에는 사용자, 암호 및 액세스 레벨을 정의하는 필드가 들어 있습니다. [Local User Database](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Local User Database**를 클릭하십시오.

그림 6-46. 로컬 사용자 데이터베이스



[Local User Database](#) 페이지에는 다음 필드가 들어 있습니다.

**User Name** — 사용자 목록입니다.

**Access Level** — 사용자 액세스 레벨입니다. 최하위 사용자 액세스 레벨은 1이고 최상위 사용자 액세스 레벨은 15입니다. 액세스 레벨이 15인 사용자는 권한 사용자이고 이 사용자만 OpenManage 스위치 관리자에 액세스하여 해당 관리자를 사용할 수 있습니다.

**Password (0-159 Characters)** — 사용자 정의 암호입니다.

**Confirm Password** — 사용자 정의 암호를 확인합니다.

**Enable Password Aging (1 - 365)** — 이 필드를 선택하면 암호의 사용 기간을 초과하기 전의 경과된 기간(일 단위)이 표시됩니다.

**Expiry Date** — 사용자 정의 암호의 만기일을 표시합니다.

**Lockout Status** — [Password Management](#) 페이지에서 **Enable Login Attempts** 확인란을 선택한 경우 사용자가 마지막으로 로그인에 성공한 이후로 실패한 인증 시도의 수를 지정합니다. 사용자 계정이 잠긴 경우 **LOCKOUT**을 지정합니다.

**Reactivate Suspended User** — 이 필드를 선택하면 지정된 사용자의 액세스 권한이 재활성화됩니다. 로그인에 실패한 후 액세스 권한은 일시 중지될 수 있습니다.

**Remove** — 이 필드를 선택하면 **User Name** 목록에서 사용자가 제거됩니다.

## 사용자에게 액세스 권한 지정

1. [Local User Database](#) 페이지를 여십시오.
2. **User Name** 필드에서 사용자를 선택하십시오.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

사용자 액세스 권한 및 암호가 정의되고 장치가 업데이트됩니다.

## 새 사용자 정의

1. [Local User Database](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add User** 페이지가 열립니다.

그림 6-47. 사용자 추가

### Add a User Name

[Refresh](#)

Attribute	Value
User Name (1-20 characters)	<input type="text"/> (Alphanumeric)
Access Level (1-15)	1 <input type="text"/>
Password (0-159 characters)	<input type="text"/> (Alphanumeric)
Confirm Password	<input type="text"/>
<input type="checkbox"/> Enable Password Aging (1-365)	<input type="text"/> (Days)

[Apply Changes](#)

3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

새 사용자가 정의되고 장치가 업데이트됩니다.

## 로컬 사용자 표 표시

1. [Local User Database](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

Local User Table이 열립니다.

그림 6-48. 로컬 사용자 표

User Name	Access Level	Aging	Expiry Date	Lockout Status	Reactivate Suspended User	Remove
1					<input type="checkbox"/>	<input type="checkbox"/>

### 일시 중지된 사용자 재활성화

1. [Local User Database\(로컬 사용자 데이터베이스\)](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

Local User Table이 열립니다.

3. **User Name**의 항목을 선택하십시오.
4. **Reactivate Suspended User** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

사용자 액세스 권한이 재활성화되고 장치가 업데이트됩니다.

### 사용자 삭제

1. [Local User Database](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[Local User Table](#)이 열립니다.

3. **User Name**을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. **Apply Changes**를 클릭하십시오.

선택한 사용자가 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 사용자 지정

다음 표에서는 [Local User Database](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-43. 로컬 사용자 데이터베이스 CLI 명령

CLI 명령	설명
username name [password password] [level level] [encrypted]	사용자 이름 기반 인증 시스템을 설정합니다.

set username name active	일시 중지된 사용자 액세스 권한을 재활성화합니다.
--------------------------	-----------------------------

다음은 CLI 명령의 예입니다.

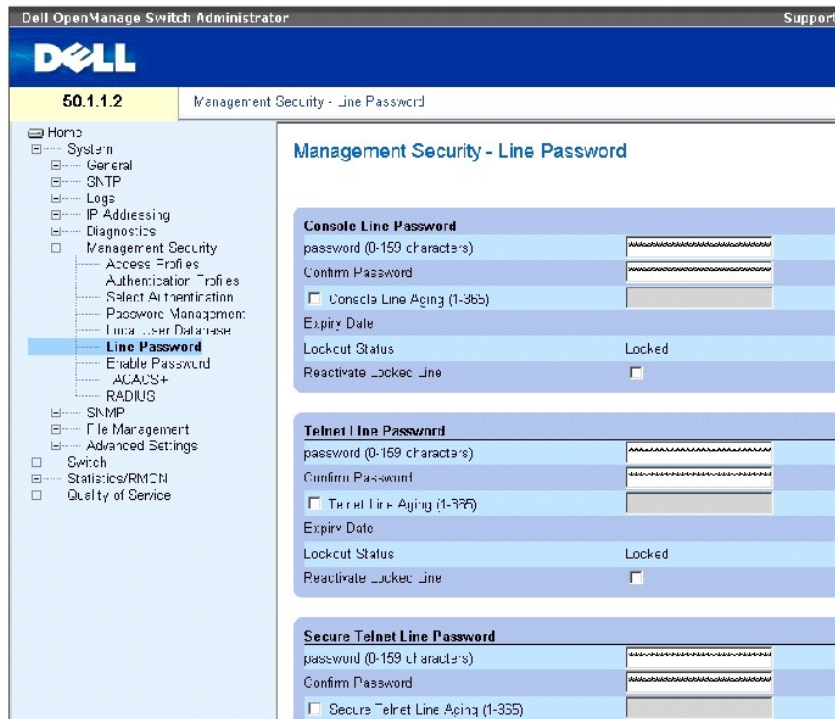
```
console(config)# username
bob password lee level 15

console# set username bob
active
```

## 라인 암호 정의

[Line Password](#) 페이지에는 관리 메소드의 라인 암호를 정의하는 데 필요한 필드가 들어 있습니다. [Line Password](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Line Passwords**를 클릭하십시오.

그림 6-49. 라인 암호



[Line Password](#) 페이지에는 다음 필드가 들어 있습니다.

**Line Password for Console/Telnet/Secure Telnet** — 콘솔, 텔넷 또는 보안 텔넷 세션을 통해 장치에 액세스하는 경우 사용하는 라인 암호입니다.

**Confirm Password for Console/Telnet/Secure Telnet** — 새 라인 암호를 확인합니다. 암호는 \*\*\*\*\* 형식으로 표시됩니다.

**Line Aging (1-365) for Console/Telnet/Secure Telnet** — 이 필드를 선택하면 라인 암호 사용 기간이 만료되기 전에 경과한 기간(일 단위)이 표시됩니다.

**Expiry Date for Console/Telnet/Secure Telnet** — 라인 암호의 만기일을 표시합니다.

**Lockout Status for Console/Telnet/Secure Telnet** — [Password Management](#) 페이지에서 **Enable Login Attempts** 확인란을 선택한 경우 사용자가 마지막으로 로그인에 성공한 이후로 실패한 인증 시도의 수를 지정합니다. 사용자 계정이 잠긴 경우 **LOCKOUT**을 지정합니다.

**Reactivate Locked Line for Console/Telnet/Secure Telnet** — 이 필드를 선택하면 콘솔/텔넷/보안 텔넷 세션의 라인 암호가 재활성화됩니다. 로그인에 실패한 후 액세스 권한은 일시 중지될 수 있습니다.

## 콘솔 세션의 라인 암호 정의

1. [Line Password](#) 페이지를 여십시오.
2. **Console Line Password** 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

콘솔 세션의 라인 암호가 정의되고 장치가 업데이트됩니다.

## 텔넷 세션의 라인 암호 정의

1. [Line Password](#) 페이지를 여십시오.
2. **Telnet Line Password** 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

텔넷 세션의 라인 암호가 정의되고 장치가 업데이트됩니다.

## 보안 텔넷 세션의 라인 암호 정의

1. [Line Password](#) 페이지를 여십시오.
2. **Secure Telnet Line Password** 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

보안 텔넷 세션의 라인 암호가 정의되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 라인 암호 지정

다음 표에서는 [Line Password](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

**표 6-44. 라인 암호 CLI 명령**

CLI 명령	설명
password password [encrypted]	라인의 암호를 표시합니다.

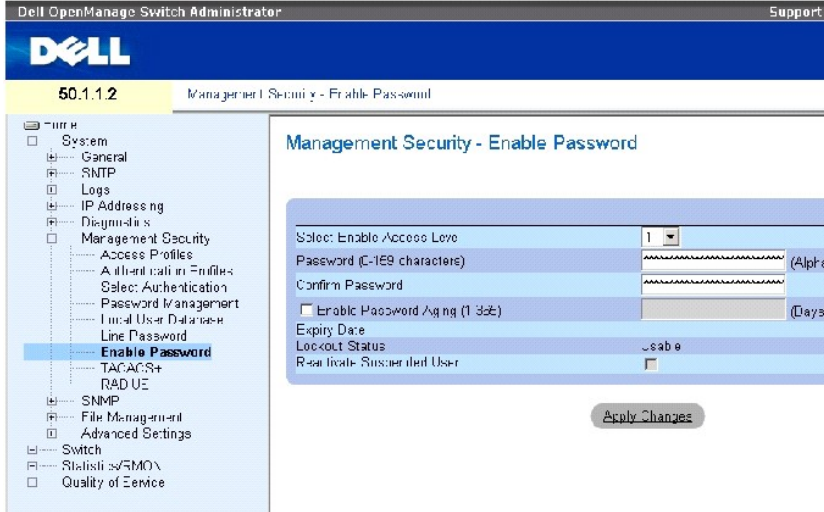
다음은 CLI 명령의 예입니다.

```
console(config-line)#  
password dell
```

## 활성 암호 정의

[Enable Password](#) 페이지에서는 로컬 암호를 설정하여 일반 및 권한 레벨에 대한 액세스를 제어합니다. [Enable Password](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **Enable Passwords**를 클릭하십시오.

그림 6-50. 활성 암호



[Enable Password](#) 페이지에는 다음 필드가 들어 있습니다.

**Select Enable Access Level** — 활성 암호와 연관된 액세스 레벨입니다. 가능한 필드 값 범위는 1~15입니다.

**Password (0-159 characters)** — 현재 활성 암호입니다.

**Confirm Password** — 새 활성 암호를 확인합니다. 암호는 \*\*\*\*\* 형식으로 표시됩니다.

**Enable Password Aging (1 - 365)** — 이 필드를 선택하면 암호의 사용 기간을 초과하기 전의 경과된 기간(일 단위)이 표시됩니다.

**Expiry Date** — 활성 암호의 만기일을 표시합니다.

**Lockout Status** — [Password Management](#) 페이지에서 **Enable Login Attempts** 확인란을 선택한 경우 사용자가 마지막으로 로그인에 성공한 이후로 실패한 인증 시도의 수를 지정합니다. 사용자 계정이 잠긴 경우 **LOCKOUT**을 지정합니다.

**Reactivate Suspended User** — 이 필드를 선택하면 지정된 사용자의 액세스 권한이 재활성화됩니다. 로그인에 실패한 후 액세스 권한은 일시 중지될 수 있습니다.

## 새 활성 암호 정의

1. [Enable Password](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. Apply Changes를 클릭하십시오.

새 활성 암호가 정의되고 장치가 업데이트됩니다.



## CLI 명령을 사용하여 활성화 암호 지정

다음 표에서는 [Enable Password](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-45. 활성화 암호 CLI 명령

CLI 명령	설명
enable password [level level] password [encrypted]	로컬 암호를 설정하여 사용자 및 권한 레벨에 대한 액세스를 제어합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# enable
password level 15 secret
```

## TACACS+ 설정 정의

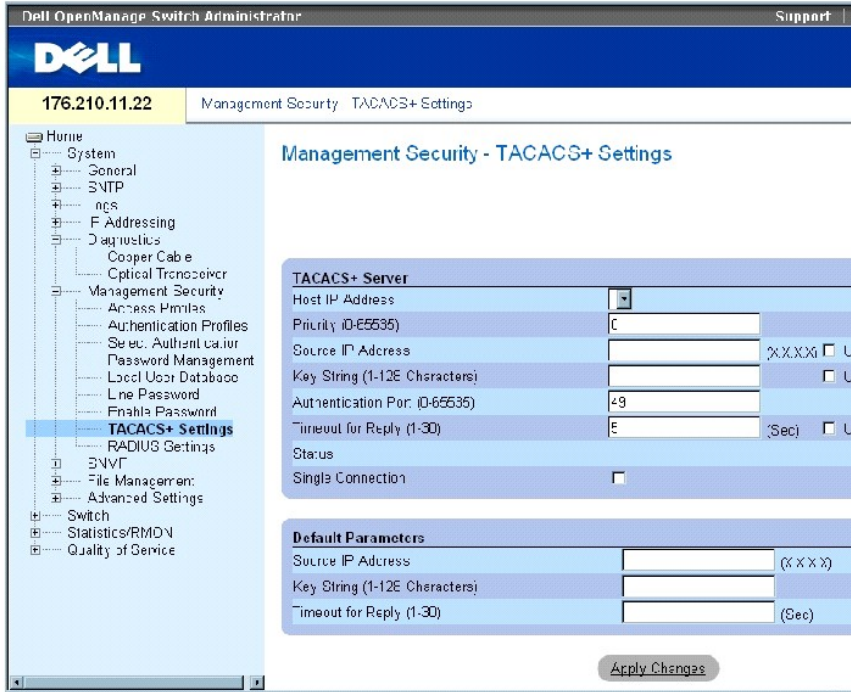
장치에서는 TACACS+(터미널 액세스 컨트롤러 액세스 제어 시스템) 클라이언트 지원을 제공합니다. TACACS+에서는 장치에 액세스하는 사용자를 검증하는 중앙 집중식 보안을 제공합니다.

TACACS+는 중앙 집중식 사용자 관리 시스템을 제공하는 동시에 RADIUS 및 기타 인증 프로세스와 일관성을 계속 유지합니다. TACACS+에서는 다음 서비스를 제공합니다.

- 1 Authentication — 사용자 이름 및 사용자 정의 암호를 통해 로그인 시 인증을 제공합니다.
- 1 Authorization — 로그인 시 수행됩니다. 인증 세션을 마치면 인증된 사용자 이름을 사용하여 승인 세션이 시작됩니다. TACACS+ 서버는 사용자 권한을 확인합니다.

TACACS+ 프로토콜은 장치와 TACACS+ 서버 간 암호화된 프로토콜 교환을 통해 네트워크 무결성을 보장합니다. [TACACS+ Settings](#) 페이지를 열려면 트리 뷰에서 **System** → **Management Security** → **TACACS+**를 클릭하십시오.

그림 6-51. TACACS+ 설정



[TACACS+ Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**Host IP Address** — TACACS+ 서버 IP 주소를 표시합니다.

**Priority (0 - 65535)** — TACACS+ 서버가 사용되는 순서를 표시합니다. 기본값은 0입니다.

**Source IP Address** — 장치와 TACACS+ 서버 간 TACACS+ 세션에 사용되는 장치 소스 IP 주소입니다.

**Key String (0-128 Characters)** — 장치와 TACACS+ 서버 간 TACACS+ 통신에 사용되는 인증 및 암호화 키를 정의합니다. 이 키는 TACACS+ 서버에서 사용하는 암호화 키와 일치해야 합니다. 이 키는 암호화되어 있습니다.

**Authentication Port (0 - 65535)** — TACACS+ 세션이 발생하는 포트 번호입니다. 기본값은 포트 49입니다.

**Timeout for Reply (1 - 30)** — 장치와 TACACS+ 서버 간 연결이 시간 종료되기 전에 경과된 시간입니다. 필드 범위는 1-30초입니다.

**Status** — 장치와 TACACS+ 서버 간 연결의 상태입니다. 가능한 필드 값은 다음과 같습니다.

**Connected** — 현재 장치와 TACACS+ 서버가 서로 연결되어 있습니다.

**Not Connected** — 현재 장치와 TACACS+ 서버가 서로 연결되어 있지 않습니다.

**Single Connection** — 이 필드를 선택하면 장치와 TACACS+ 서버 간에 하나의 열린 연결이 유지됩니다.

TACACS+ 기본 매개변수는 사용자 정의된 기본값입니다. 기본 설정이 새로 정의된 TACACS+ 서버에 적용됩니다. 기본값을 정의하지 않으면 시스템 기본값이 새 TACACS+ 서버에 적용됩니다.

다음은 TACACS+ 기본값입니다.

**Source IP Address** — 장치와 TACACS+ 서버 간 TACACS+ 세션에 사용되는 기본 장치 소스 IP 주소입니다. 기본 소스 IP 주소는 0.0.0.0입니다.

**Key String (0-128 Characters)** — 장치와 TACACS+ 서버 간 모든 통신을 인증하고 암호화할 때 사용하는 기본 키 문자열입니다. 이 키는 암호화되어 있습니다.

**Timeout for Reply (1 - 30)** — 장치와 TACACS+ 서버 간 연결 시간이 종료되기 전에 경과된 기본 시간입니다. 기본값은 5초입니다.

## TACACS+ 서버 추가

1. [TACACS+ Settings](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

[Add TACACS+ Host](#) 페이지가 열립니다.

그림 6-52. TACACS+ 호스트 추가

### Add TACACS+ Host

Refresh

Host IP Address	<input type="text"/>	(X.X.X.X)
Priority (1-255)	<input type="text"/>	0
Source IP Address	<input type="text"/>	(X.X.X.X) <input type="checkbox"/> Use Default
Key String (0-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Authentication Port (0-65535)	<input type="text"/>	49
Timeout for Reply (1-30)	<input type="text"/>	(Sec) <input type="checkbox"/> Use Default
Single Connection	<input type="checkbox"/>	

3. 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

TACACS+ 서버가 추가되고 장치가 업데이트됩니다.

## TACACS+ Table 표시

1. [TACACS+ Settings](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[TACACS+ Table](#)이 열립니다.

그림 6-53. TACACS+ 표

Refresh

### TACACS+ Table

Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Remove
1					<input type="checkbox"/>		<input type="checkbox"/>

Apply Changes

### TACACS+ 서버 제거

1. [TACACS+ Table](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[TACACS+ Table](#)이 열립니다.

3. [TACACS+ Table](#)의 항목을 선택하십시오.
4. Remove 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

TACACS+ 서버가 제거되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 TACACS+ 설정 정의

다음 표에서는 [TACACS+ Settings](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-46. TACACS+ CLI 명령

CLI 명령	설명
tacacs-server host [IP 주소   호스트 이름] [single-connection] [port 포트 번호] [timeout 타임 아웃] [key 키 문자열] [source 소스] [priority 우선 순위]	TACACS+ 호스트를 표시합니다.
tacacs-server key key-string	장치와 TACACS+ 서버 간의 모든 TACACS+ 통신에서 사용하는 인증 및 암호화 키를 표시합니다. 이 키는 TACACS+ 디먼에서 사용하는 암호화와 일치해야 합니다. (범위: 0-128자)
tacacs-server timeout timeout	타임 아웃 값(초 단위)을 표시합니다. (범위: 1 - 30.)
tacacs-server source-ip source	소스 IP 주소를 표시합니다. (범위: 유효한 IP 주소)
show tacacs [ip 주소]	TACACS+ 서버의 구성 및 통계를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console# show tacacs
Device Configuration

```

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	----	-----	-----	-----	-----
--				-	-	-

12.1.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						
-----						
TimeOut :						
5						
Device Configuration						
-----						
Source IP : 0.0.0.0						
console#						

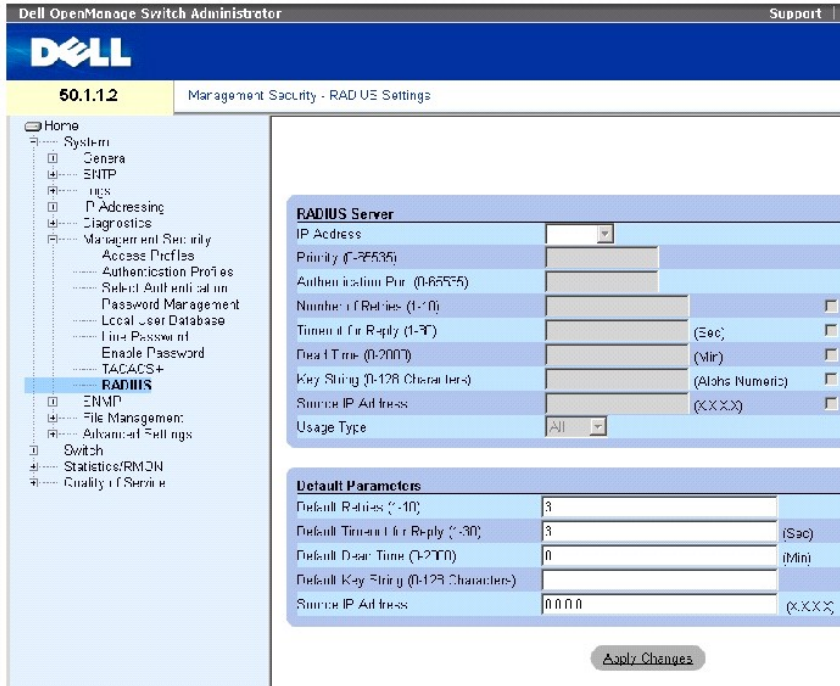
## RADIUS 설정 구성

RADIUS(Remote Authorization Dial-In User Service) 서버는 네트워크에 대한 추가 보안을 제공합니다. 최대 4개의 RADIUS 서버를 정의할 수 있습니다. RADIUS 서버에서는 다음 경우에 중앙 집중식 인증 메소드를 제공합니다.

- 1 텔넷 액세스
- 1 보안 셸 액세스
- 1 웹 액세스
- 1 콘솔 액세스

[RADIUS Settings](#) 페이지를 열려면 트리 뷰에서 **System**→**Management Security**→**RADIUS**를 클릭하십시오.

그림 6-54. RADIUS 설정



[RADIUS Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**IP Address** — 인증 서버 IP 주소 목록입니다.

**Priority (0-65535)** — 서버 우선순위입니다. 가능한 값의 범위는 0-65535입니다. 여기에서 0이 최대값입니다. 이 필드를 사용하여 서버 조회 순서를 구성합니다.

**Authentication Port** — 인증 포트를 식별합니다. 인증 포트는 RADIUS 서버 인증을 검증하는 데 사용됩니다.

**(Number of Retries) (1-10)** — 오류가 발생하기 전에 RADIUS 서버에 전송한 요청의 수를 표시합니다. 가능한 필드 값 범위는 1-10입니다.

**Timeout for Reply(1-30)** — 조회를 재시도하거나 다음 서버로 전환하기 전에 장치에서 RADIUS 서버의 응답을 기다리는 시간(초 단위)를 표시합니다. 가능한 필드 값 범위는 1-30입니다.


**Dead Time (0-2000)** — 서비스 요청에 대해 RADIUS 서버가 무시되는 시간(분 단위)을 표시합니다. 값의 범위는 0-2000입니다.

**Key String (0-128 Characters)** — 장치와 RADIUS 서버 간 모든 RADIUS 통신을 인증하고 암호화할 때 사용하는 키 문자열입니다. 이 키는 암호화되어 있습니다.

**Source IP Address** — RADIUS 서버와 통신할 때 사용하는 소스 IP 주소를 표시합니다.

**Usage Type** — 서버의 사용 종류를 표시합니다. 가능한 값은 login, 802.1x 또는 all입니다. 지정하지 않은 경우 기본값은 모두 all입니다.

다음 필드에서는 RADIUS 기본값을 설정합니다.

 **주:** 호스트별 타임 아웃, 재시도 또는 불량 시간 값을 지정하지 않으면 전역 값(기본값)이 모든 호스트에 적용됩니다.

**Default Retries (1-10)** — 오류가 발생하기 전에 RADIUS 서버에 전송한 요청의 기본 횟수를 표시합니다.

**Timeout for Reply(1-30)** — 시간이 종료되기 전에 장치에서 RADIUS 서버의 응답을 기다리는 기본 시간(초 단위)을 표시합니다. 기본값은 5초입니다.

**Default Dead Time(0-2000)** — 서비스 요청에 대해 RADIUS 서버가 무시되는 기본 시간(분 단위)을 표시합니다. 값의 범위는 0~2000입니다.

**Default Key String (1-128 Characters)** — 장치와 RADIUS 서버 간의 모든 RADIUS 통신을 인증하고 암호화할 때 사용하는 기본 키 문자열입니다. 이 키는 암호화되어 있습니다.

**Source IP Address** — RADIUS 서버와 통신할 때 사용하는 기본 소스 IP 주소를 표시합니다. 기본 소스 IP 주소는 0.0.0.0입니다.

## RADIUS 매개변수 정의

1. [RADIUS Settings](#) 페이지를 여십시오.
2. 필드를 정의하십시오.
3. **Apply Changes**를 클릭하십시오.

RADIUS 설정이 장치에 업데이트됩니다.

## RADIUS 서버 추가

1. [RADIUS Settings](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add RADIUS Server** 페이지가 열립니다.

그림 6-55. RADIUS 서버 추가

**Add RADIUS Server** Refresh

IP Address	<input type="text"/>	(X.X.X.X)
Primary (1-89935)	<input type="text"/>	
Authentication Port (1-65535)	<input type="text" value="1645"/>	
Number of Retries (1-10)	<input type="text" value="3"/>	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text" value="5"/>	(Sec) <input type="checkbox"/> Use Default
Dead Time (0-2000)	<input type="text" value="0"/>	(Min) <input type="checkbox"/> Use Default
Key String (1-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Source IP Address	<input type="text"/>	(X.X.X.X) <input type="checkbox"/> Use Default
Usage Type	<input type="text" value="_cgit"/>	

**Apply Changes**

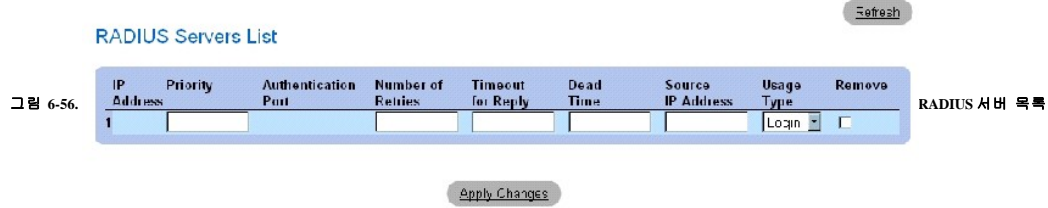
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

새 RADIUS 서버가 추가되고 장치가 업데이트됩니다.

## RADIUS 서버 목록 표시

1. [RADIUS Settings](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[RADIUS Servers List](#)가 열립니다.



### RADIUS 서버 제거

1. [RADIUS Settings](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[RADIUS Servers List](#)가 열립니다.

3. [RADIUS Servers List](#)의 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

RADIUS 서버가 제거되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 RADIUS 서버 정의

다음 표에서는 [RADIUS Settings](#) 페이지에 표시된 필드를 정의하는 CLI 명령을 요약합니다.

표 6-47. RADIUS 서버 CLI 명령

CLI 명령	설명
<code>radius-server timeout</code> 타임 아웃	라우터에서 서버 호스트의 응답을 기다리는 간격을 설정합니다.
<code>radius-server retransmit</code> 재시도 횟수	소프트웨어에서 RADIUS 서버 호스트 목록을 검색하는 횟수를 지정합니다.
<code>radius-server deadtime</code> deadtime	사용할 수 없는 서버를 건너뛰도록 구성합니다.
<code>radius-server key</code> 키 문자열	라우터와 RADIUS 환경 간의 모든 RADIUS 통신에서 사용하는 인증 및 암호화 키를 설정합니다.
<code>radius-server host</code> IP 주소 [auth-port 인증 포트 번호] [timeout 타임아웃] [retransmit 재시도 횟수] [deadtime 불감 시간] [key 키 문자열] [source 소스] [priority 우선권]	RADIUS 서버 호스트를 지정합니다.
<code>show radius-servers</code>	RADIUS 서버 설정을 표시합니다.

다음은 CLI 명령의 예입니다. \_\_\_\_\_



```
Console(config)# radius-  
server timeout 5  
  
Console(config)# radius-  
server retransmit 5  
  
Console(config)# radius-  
server deadtime 10  
  
Console(config)# radius-  
server key dell-server  
  
Console(config)# radius-  
server host 196.210.100.1  
auth-port 127timeout 20  
  
Console# show radius-  
servers  
  
IP address Auth Acct  
TimeOut Retransmit  
Deadtime Source IP  
Priority  
  
-----  
-----  
-----  
  
172.16.1.1 164 51646 3 3 0  
01 172.16.1.2 164 51646 3  
3 0 02
```

---

## SNMP 매개변수 정의

SNMP(Simple Network Management Protocol)에서는 네트워크 장치를 관리하는 메소드를 제공합니다. 스위치에서 지원하는 SNMP 버전은 다음과 같습니다.

- 1 SNMPv1(버전 1)
- 1 SNMPv2(버전 2)
- 1 SNMPv3(버전 3)

### SNMP v1 및 v2

SNMP 에이전트에서는 스위치를 관리할 때 사용되는 변수 목록을 유지 관리합니다. 변수는 관리 정보 베이스(MIB)에 정의됩니다. MIB에는 에이전트에서 제어하는 변수가 들어 있습니다. SNMP 에이전트는 MIB 사양 형식 및 네트워크의 정보에 액세스할 때 사용되는 형식을 정의합니다. SNMP 에이전트에 대한 액세스 권한은 액세스 문자열로 제어됩니다.

기본적으로 SNMPv1 및 v2가 활성화됩니다.

### SNMP v3

SNMP v3도 SNMPv1 및 SNMPv2 PDU에 액세스 제어 및 새 트랩 메커니즘을 적용합니다. 또한 사용자 보안 모델(USM)이 SNMPv3에 정의됩니다. 이 버전에는 다음 필드가 들어 있습니다.

- 1 **Authentication** — 데이터 무결성 및 데이터 원본 인증을 제공합니다.
- 1 **Privacy** — 메시지 내용이 유출되지 않게 합니다. 암호 블록 체인(CBC)이 암호화에 사용됩니다. 인증이 SNMP 메시지에서 활성화되거나 인증 및 개인 정보 보호 모두가 SNMP 메시지에 활성화됩니다. 그러나 개인 정보 보호는 인증없이 사용할 수 없습니다.
- 1 **Timeliness** — 메시지 지연 또는 메시지 중복을 방지합니다. SNMP 에이전트는 수신 메시지를 메시지 시간 정보와 비교합니다.
- 1 **Key Management** — 키 생성, 키 업데이트 및 키 사용을 정의합니다.

스위치에서는 개체 ID(OID)별로 SNMP 알림 필터를 지원합니다. OID는 시스템에서 스위치 기능을 관리할 때 사용됩니다. SNMP v3은 다음 기능을 지원합니다.

- 1 보안
- 1 기능 액세스 제어
- 1 트랩

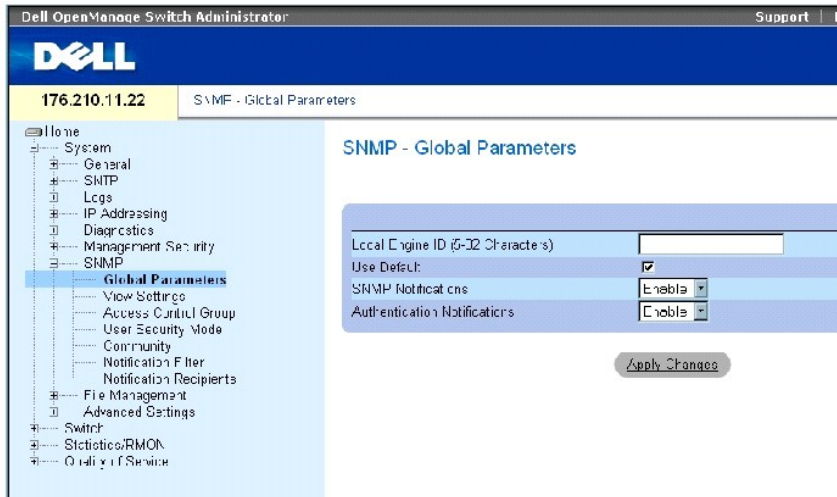
인증 또는 개인 정보 보호 키는 사용자 보안 모델(USM)에서 수정됩니다.

SNMPv3은 로컬 엔진 ID가 활성화된 경우에 활성화됩니다.

## SNMP 전역 매개변수 정의

[SNMP Global Parameters](#) 페이지에서 SNMP 및 인증 알림을 모두 활성화할 수 있습니다. [SNMP Global Parameters](#) 페이지를 열려면 트리 뷰에서 **System** → **SNMP** → **Global Parameters**를 클릭하십시오.

그림 6-57. SNMP 전역 매개변수



[SNMP Global Parameters](#) 페이지에는 다음 필드가 들어 있습니다.

**Local Engine ID** — 로컬 장치 엔진 ID를 표시합니다. 필드 값은 16진 문자열입니다. 16진 문자열의 각 바이트는 2개의 16진수로 구성됩니다. 각 바이트는 마침표 또는 쉼표로 구분할 수 있습니다. 엔진 ID는 SNMPv3을 활성화하기 전에 먼저 정의되어야 합니다.

독립형 장치의 경우 엔터프라이즈 번호 및 기본 MAC 주소로 구성된 기본 엔진 ID를 선택하십시오.

스택 가능 시스템의 경우 엔진 ID를 구성하고 엔진 ID가 관리 도메인에서 고유한지 확인하십시오. 이는 네트워크에 있는 두 장치의 엔진 ID가 같게 되는 것을 방지합니다.

**Use Defaults** — 장치 생성 엔진 ID를 사용합니다. 기본 엔진 ID는 장치 MAC 주소를 기반으로 다음 표준에 따라 정의됩니다.

**First 4 octets** — 첫 번째 비트는 1이고 나머지는 IANA 엔터프라이즈 번호인 674입니다.

**Fifth octet** — 3으로 설정하면 뒤에 오는 MAC 주소를 표시합니다.

**Last 6 octets** — 장치의 MAC 주소입니다.

**SNMP Notifications** — 라우터 전송 SNMP 알람을 활성화 또는 비활성화합니다.

**Authentication Notifications** — 인증에 실패한 경우 라우터 전송 SNMP 트랩을 활성화 또는 비활성화합니다.

### SNMP 알람 활성화

1. [SNMP Global Parameters](#) 페이지를 여십시오.
2. **SNMP Notifications** 필드에서 **Enable**를 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

SNMP 알람이 활성화되고 장치가 업데이트됩니다.

### 인증 알람 활성화

1. [SNMP Global Parameters](#) 페이지를 여십시오.
2. **Authentication Notifications** 필드에서 **Enable**를 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

### CLI 명령을 사용하여 SNMP 알람 활성화

다음 표에서는 SNMP Global Parameters(SNMP 전역 매개변수) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-48. SNMP 알람 CLI 명령

CLI 명령	설명
<code>snmp-server enable traps</code>	라우터에서 SNMP 트랩을 전송할 수 있도록 설정합니다.
<code>snmp-server trap authentication</code>	인증에 실패한 경우 라우터에서 SNMP 트랩을 전송할 수 있도록 설정합니다.
<code>show snmp</code>	SNMP 통신 상태를 확인합니다.
<code>snmp-server engine ID local (엔진 ID 문자열   default)</code>	로컬 장치 엔진 ID를 표시합니다. 필드 값은 16진 문자열입니다. 16진 문자열의 각 바이트는 2개의 16진수로 구성됩니다. 각 바이트는 마침표 또는 쉼표로 구분할 수 있습니다. 엔진 ID는 SNMPv3를 활성화하기 전에 먼저 정의되어야 합니다.

다음은 CLI 명령의 예입니다.

--	--

Console(config)# snmp-server enable traps							
Console(config)# snmp-server trap authentication							
Console# show snmp							
Community-String	Community-Access		View name		IP address		
-----	-----		-----		-----		
public	read only		view-1		All		
Community-String	Group name		IP address		Type		
-----	-----		-----		----		
Traps are enabled.							
Authentication-failure trap is enabled.							
Version 1,2 notifications							
Target Address	Type	Community	Version	Udp Port	Filter name	To Sec	Retries
-----	----	-----	-----	----	-----	---	-----
Version 3 notifications							
Target Address	Type	Username	Security Level	Udp Port	Filter name	To Sec	Retries
-----	----	-----	-----	----	-----	---	-----
System Contact: Robert							
System Location: Marketing							

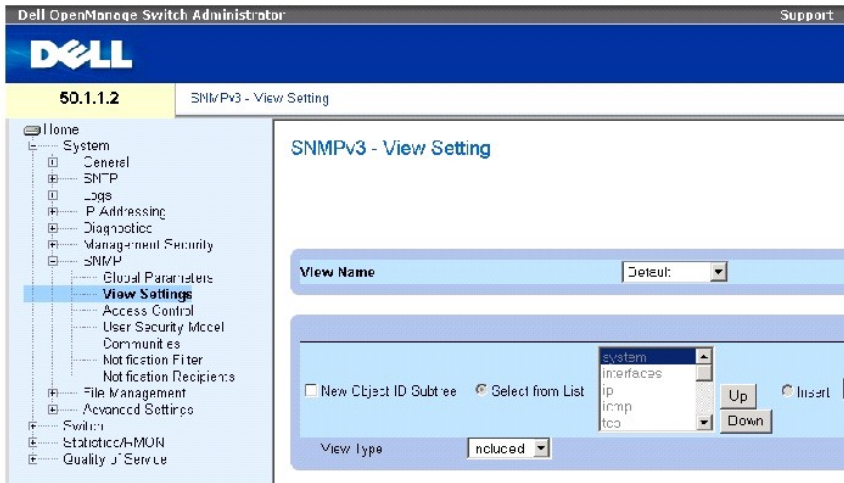
## SNMP 보기 설정 정의

SNMP 보기에서는 장치 기능 또는 기능 측면에 대한 액세스를 제공하거나 차단합니다. 예를 들면, SNMP 그룹 A에는 멀티캐스트 그룹에 대한 읽기 전용(R/O) 액세스를 부여하지만 SNMP 그룹 B에는 멀티캐스트 그룹에 대한 읽기/쓰기(R/W) 액세스를 부여하도록 보기를 정의할 수 있습니다. 기능 액세스 권한은 MIB 이름 또는 MIB 객체 ID를 통해 부여됩니다.

위/아래 화살표를 사용하여 MIB 트리 및 MIB 분기를 살펴볼 수 있습니다.

[SNMPv3 View Settings](#) 페이지를 열려면 트리 뷰에서 **System** → **SNMP** → **View Settings**를 클릭하십시오.

그림 6-58. SNMPv3 보기 설정



[SNMPv3 View Settings](#) 페이지에는 다음 필드가 들어 있습니다.

**View Name** — 사용자 정의 보기 목록이 들어 있습니다. 보기 이름의 최대 길이는 알파벳과 문자로 된 30자입니다.

**New Object ID Subtree** — 선택한 SNMP 보기에서 포함 또는 제외할 장치 기능 OID를 표시합니다.

**Selected from List** — **Up** 및 **Down** 단추를 눌러서 모든 장치 OID 목록으로 이동하면서 장치 기능 OID를 선택합니다.

**Insert** — 장치 기능 OID를 지정합니다.

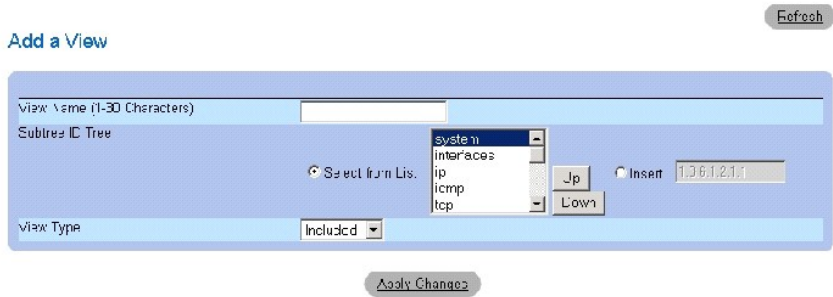
**View Type(보기 종류)** — 선택한 SNMP 보기에 정의된 OID 분기를 포함할 것인지 또는 제외할 것인지를 표시합니다.

## 보기 추가

1. [SNMPv3 View Settings](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

[Add A View](#) 페이지가 열립니다.

그림 6-59. 보기 추가



3. 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

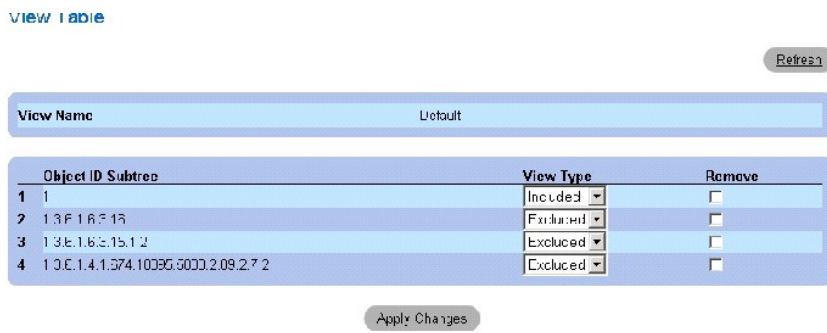
SNMP 보기가 추가되고 장치가 업데이트됩니다.

### 보기 표 표시

1. [SNMPv3 View Settings](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[View Table](#) 페이지가 열립니다.

그림 6-60. 보기 표



### CLI 명령을 사용하여 SNMPv3 보기 정의

다음 표에서는 [SNMPv3 View Settings](#) 페이지에 표시된 필드를 정의하는 CLI 명령을 요약합니다.

표 6-49. SNMP 보기 CLI 명령

CLI 명령	설명
<code>snmp-server view 보기 이름 OID 트리 {included   excluded}</code>	보기 항목을 작성하거나 업데이트합니다.
	보기 구성을 표시합니다.

```
show snmp views[보기 이름]
```

다음은 CLI 명령의 예입니다.

```
Console(config)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views
```

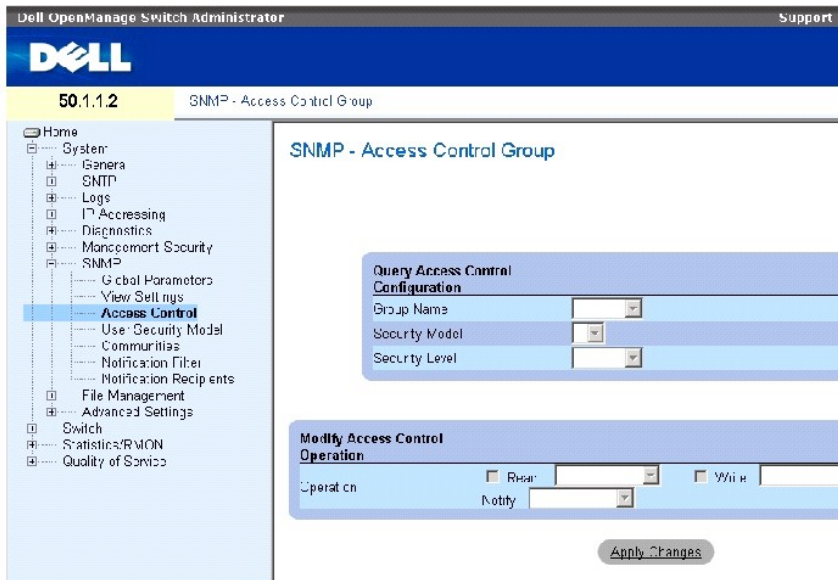
Name	OID Tree	Type
-----	-----	-----
-		
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

## SNMP 액세스 제어 정의

Access Control 페이지에서는 SNMP 그룹 작성, SNMP 그룹에 SNMP 액세스 제어 권한 지정 등에 대한 정보를 제공합니다. 이러한 그룹을 통해 네트워크 관리자는 특정 장치 기능 또는 기능 측면에 대한 액세스 권한을 지정할 수 있습니다.

[Access Control Group](#) 페이지를 열려면 트리 뷰에서 System→SNMP→Access Control을 클릭하십시오.

그림 6-61. 액세스 제어 그룹



[Access Control Group](#)에는 다음 필드가 들어 있습니다.

**Group Name** — 액세스 제어 규칙을 적용할 사용자 정의 그룹입니다. 필드에는 최대 30자를 입력할 수 있습니다.

**SNMP Version** — 그룹에 연결된 SNMP 버전을 정의합니다. 가능한 필드 값은 다음과 같습니다.

**SNMPv1** — 그룹에 SNMPv1이 정의됩니다.

**SNMPv2** — 그룹에 SNMPv2가 정의됩니다.

**SNMPv3** — 그룹에 SNMPv3이 정의됩니다.

**Security Level** — 그룹에 연결된 보안 레벨입니다. 보안 레벨은 SNMPv3에만 적용됩니다. 가능한 필드 값은 다음과 같습니다.

**No Authentication** — 인증 및 개인 정보 보호가 그룹에 지정되어 있지 않습니다.

**Authentication** — SNMP 메시지를 인증하고 SNMP 메시지 원본이 인증되었는지 확인합니다.

**Privacy** — SNMP 메시지를 암호화합니다.

**Operation** — 그룹 액세스 권한을 정의합니다. 가능한 필드 값은 다음과 같습니다.

**Read** — 관리 액세스는 읽기 전용으로 제한되며, 지정된 SNMP 보기는 변경할 수 없습니다.

**Write** — 관리 액세스는 읽기 및 쓰기이며, 지정된 SNMP 보기를 변경할 수 있습니다.



Notify — 지정된 SNMP 보기의 트랩을 전송합니다.

## SNMP 그룹 정의

1. [Access Control Group](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

Add an Access Control Group 페이지가 열립니다.

그림 6-62. 액세스 제어 그룹 추가

Refresh

Add an Access Control Group

Group Name (1-30 Characters)

Security Model

Security Level

Operation  Read  Write  Notify

Apply Changes

3. [Add an Access Control Group](#) 페이지의 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

그룹이 추가되고 장치가 업데이트됩니다.

## 액세스 표 표시

1. [Access Control Group](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Access Table](#)이 열립니다.

그림 6-63. 액세스 표

Refresh

Group Name	Security Model	Security Level	Operation			Remove
			Read	Write	Notify	
1	SNMPv1	No Authentication	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Changes

## SNMP 그룹 제거

1. [Access Control Group](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Access Table](#)이 열립니다.

3. SNMP 그룹을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

SNTP 그룹이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 SNMP 액세스 제어 정의

다음 표에서는 **Access Control Group** 페이지에 표시된 필드를 정의하는 CLI 명령을 요약합니다.

표 6-50. SNMP 액세스 제어 CLI 명령

CLI 명령	설명
<code>snmp-server group 그룹 이름 {v1   v2   v3 {noauth   auth   priv}} [read 읽기 보기] [write 쓰기 보기] [notify 알림 보기]</code>	새 SNMP(Simple Network Management Protocol) 그룹을 구성하거나 SNMP 사용자를 SNMP 보기에 매핑하는 표를 구성합니다.
<code>show snmp groups [그룹 이름]</code>	그룹 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

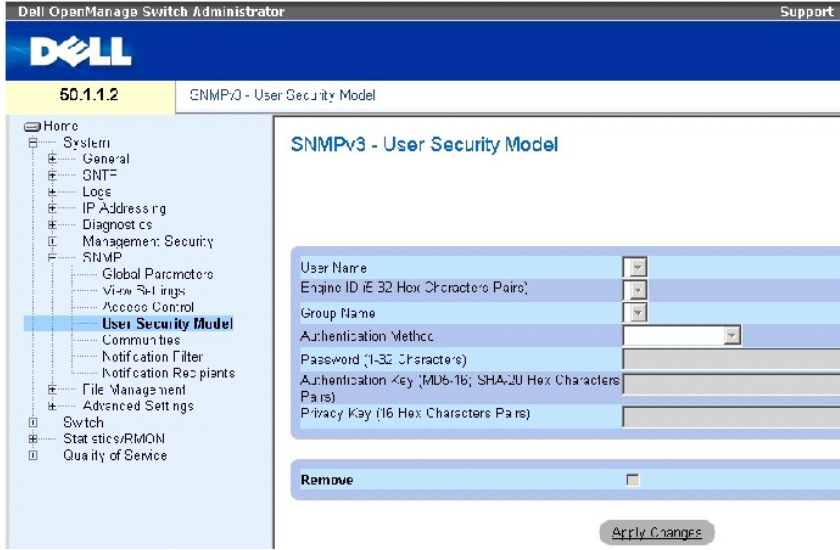
```
console (config)# snmp-server group user-group v3
priv read user- view
```

## SNMP 사용자 보안 지정

[SNMPv3 User Security Model \(USM\)](#) 페이지에서는 SNMP 그룹에 시스템 사용자를 지정하고 사용자 인증 메소드를 정의할 수 있습니다.

[SNMPv3 User Security Model \(USM\)\(SNMPv3 사용자 보안 모델\(USM\)\)](#) 페이지를 열려면 트리 뷰에서 **System(시스템)→SNMP→User Security Model**을 클릭하십시오.

그림 6-64. SNMPv3 사용자 보안 모델(USM)



[SNMPv3 User Security Model \(USM\)](#) 페이지에는 다음 필드가 들어 있습니다.

**User Name** — 사용자 정의 사용자 이름 목록이 들어 있습니다. 필드의 최대 길이는 문자와 숫자를 포함한 30자입니다.

**Engine ID** — 사용자가 연결된 로컬 또는 원격 SNMP 항목을 표시합니다. 로컬 SNMP 엔진 ID를 변경하거나 제거하면 SNMPv3 사용자 데이터베이스가 삭제됩니다.

**Local** — 사용자가 로컬 SNMP 항목에 연결되었음을 표시합니다.

**Remote** — 사용자가 원격 SNMP 항목에 연결되었음을 표시합니다. 엔진 ID가 정의된 경우 원격 장치에서 알림 메시지를 수신합니다.

**Group Name** — 사용자 정의 SNMP 그룹 목록이 들어 있습니다. SNMP 그룹은 [Access Control Group](#) 페이지에서 정의됩니다.

**Authentication Method** — 사용자 인증에 사용되는 인증 메소드입니다. 가능한 필드 값은 다음과 같습니다.

**MD5 Key** — HMAC-MD5 알고리즘을 사용하여 사용자를 인증합니다.

**SHA Key** — HMAC-SHA-96 인증 레벨을 사용하여 사용자를 인증합니다.

**MD5 Password** — 인증에 HMAC-MD5-96 암호가 사용됨을 표시합니다. 사용자는 암호를 입력해야 합니다.

**SHA Password** — HMAC-SHA-96 인증 레벨을 사용하여 사용자를 인증합니다. 사용자는 암호를 입력해야 합니다.

**None** — 사용자 인증이 사용되지 않습니다.

**Password(0-32 Characters)** — 그룹의 사용자 정의 암호를 수정합니다. 암호의 최대 길이는 알파벳과 숫자로 된 32자입니다.

**Authentication Key (MD5-16; SHA-20 hexa chars)** — HMAC-MD5-96 또는 HMAC-SHA-96 인증 레벨을 정의합니다. 인증 및 개인 정보 보호 키를 입력하여 인증 키를 정의합니다. 인증만 필

요한 경우 MD5에 16바이트를 정의합니다. 개인 정보 보호 및 인증이 모두 필요한 경우 MD5에 32바이트를 정의합니다. 16진 문자열의 각 바이트는 2개의 16진수로 구성됩니다. 각 바이트는 마침표 또는 쉼표로 구분할 수 있습니다.

**Privacy Key (16 hexa characters)** — 인증만 필요한 경우 20바이트를 정의합니다. 개인 정보 보호 및 인증이 모두 필요한 경우 16바이트를 정의합니다. 16진 문자열의 각 바이트는 2개의 16진수로 구성됩니다. 각 바이트는 마침표 또는 쉼표로 구분할 수 있습니다.

**Remove** — 이 필드를 선택하면 지정된 그룹의 사용자가 제거됩니다.

## 그룹에 사용자 추가

1. [SNMPv3 User Security Model \(USM\)](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

[Add SNMPv3 User Name](#) 페이지가 열립니다.

그림 6-65. SNMPv3 사용자 이름 추가

**Refresh**

**Add User Name**

User Name (1-32 Characters)

Engine ID  Local  Remote

Group Name

Authentication Method

Password (1-32 Characters)

Authentication Key (MD5-1E; SHA-20 Hex Characters pairs)

Privacy Key (1E -ex Characters pairs)

**Apply Changes**

3. 관련 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

그룹에 사용자가 추가되고 장치가 업데이트됩니다.

## 사용자 보안 모델 표 표시

1. [SNMPv3 User Security Model \(USM\)](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[User Security Model Table](#)이 열립니다.

그림 6-66. 사용자 보안 모델 표

**Refresh**

User Name	Group Name	Remote Engine ID	Authentication	Remove
1				<input type="checkbox"/>

**Apply Changes**

## 사용자 보안 모델 표의 항목 삭제

1. [SNMPv3 User Security Model \(USM\)](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[User Security Model Table](#)이 열립니다.

3. [User Security Model Table](#)의 항목을 선택하십시오.
4. Remove 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

[User Security Model Table](#)의 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 SNMPv3 사용자 정의

다음 표에서는 [SNMPv3 User Security Model \(USM\)](#) 페이지에 표시된 필드를 정의하는 CLI 명령을 요약합니다.

표 6-51. SNMPv3 사용자 CLI 명령

CLI 명령	설명
<code>snmp-server user 사용자 이름 그룹 이름 [remote engineid- string][auth-md5 password   auth-sha password   auth- md5-key md5-des-키   auth- sha-key sha-des-키]</code>	새 SNMP V3 사용자를 구성합니다.
<code>show snmp users [사용자 이름]</code>	사용자 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console (config)# snmp-
server user John user-
group auth-md5 1234

console(config)# end

console# show snmp users

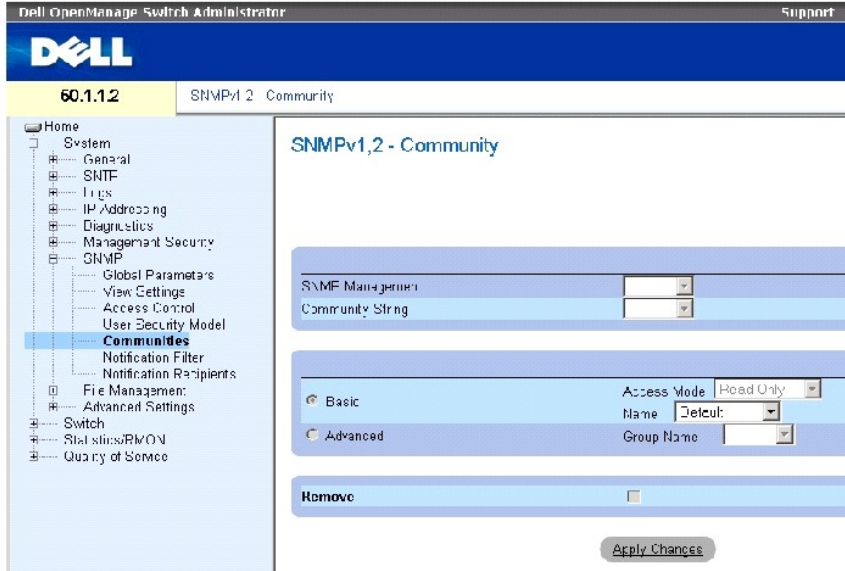
```

Name	Group Name	Auth Method	Remote
----	-----	-----	-----
John	user- group	md5	

## SNMP 커뮤니티 정의

액세스 권한은 [SNMPv1,2 Community](#) 페이지에서 커뮤니티를 정의하여 관리됩니다. 커뮤니티 이름을 변경하면 액세스 권한도 변경됩니다. SNMP 커뮤니티는 SNMP v1 및 SNMP v2에만 정의됩니다. [SNMPv1,2 Community](#) 페이지를 열려면 트리 뷰에서 **System**→ **SNMP**→ **Communities**를 클릭하십시오.

그림 6-67. SNMPv1, 2 커뮤니티



[SNMPv1,2 Community](#) 페이지에는 다음 필드가 들어 있습니다.

**SNMP Management Station** — SNMP 커뮤니티가 정의된 관리 스테이션 IP 주소입니다.

**Community String** — 장치에 관리 스테이션을 인증할 때 사용하는 암호 역할을 합니다.

**Basic** — 선택한 커뮤니티에 SNMP 기본 모드를 활성화합니다. 가능한 필드 값은 다음과 같습니다.

**Access Mode** — 커뮤니티의 액세스 권한을 정의합니다. 가능한 필드 값은 다음과 같습니다.

**Read Only** — 관리 액세스는 읽기 전용으로 제한되며, 커뮤니티는 변경할 수 없습니다.

**Read-Write** — 관리 액세스는 읽기/쓰기로 제한되며, 장치 구성은 변경할 수 있지만 커뮤니티는 변경할 수 없습니다.

**SNMP-Admin** — 사용자는 모든 장치 구성 옵션에 대한 액세스 권한 및 커뮤니티 수정 권한을 가집니다.

**View Name** — 사용자 정의 SNMP 보기 목록이 들어 있습니다.

**Name** — SNMPv1, v2에 사용되는 커뮤니티 이름을 지정합니다.

**Advanced** — 사용자 정의 그룹 목록이 들어 있습니다. SNMP 고급 모드를 선택하면 그룹을 구성하는 SNMP 액세스 제어 규칙이 선택한 커뮤니티에 활성화됩니다. 또한 고급 모드에서는 특정 SNMP 커뮤니티의 SNMP 그룹도 활성화합니다. SNMP 고급 모드는 SNMPv3에서만 정의됩니다. 가능한 필드 값은 다음과 같습니다.

**Group Name** — SNMP 고급 모드에서 사용할 그룹 이름을 지정합니다.

**Remove** — 이 필드를 선택하면 커뮤니티가 제거됩니다.

## 새 커뮤니티 정의

1. [SNMPv1.2 Community](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

Add SNMP Community 페이지가 열립니다.

그림 6-68. SNMP 커뮤니티 추가

Add SNMPv1,2 SNMP Community Refresh

SNMP Management: Station  (XXX)  
 All (D.O.C.)

Community String (1-20 Characters)

Basic  Access Mode   View Name   
 Advanced

Apply Changes

3. 관련 필드를 채우십시오.
4. **Apply Changes**를 클릭하십시오.

새 커뮤니티가 저장되고 장치가 업데이트됩니다.

## 커뮤니티 삭제

1. [SNMPv1.2 Community](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

Community Table 페이지가 열립니다.

3. 커뮤니티를 선택하고 **Remove** 확인란을 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

커뮤니티 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 커뮤니티 구성

다음 표에서는 [SNMPv1.2 Community](#)에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-52. SNMP 커뮤니티 CLI 명령

CLI 명령	설명
<code>snmp-server community 커뮤니티 [ro   rw   su] [IP 주소][view 보기 이름]</code>	SNMP 프로토콜에 대한 액세스를 허용하도록 커뮤니티 액세스 문자열을 설정합니다.
<code>snmp-server community-group 커뮤니티 그룹 이름 [IP 주소]</code>	그룹 액세스 권한에 따라 SNMP 프로토콜에 대한 제한된 액세스를 허용하도록 커뮤니티 액세스 문자열을 설정합니다.
<code>show snmp</code>	현재 SNMP 장치 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

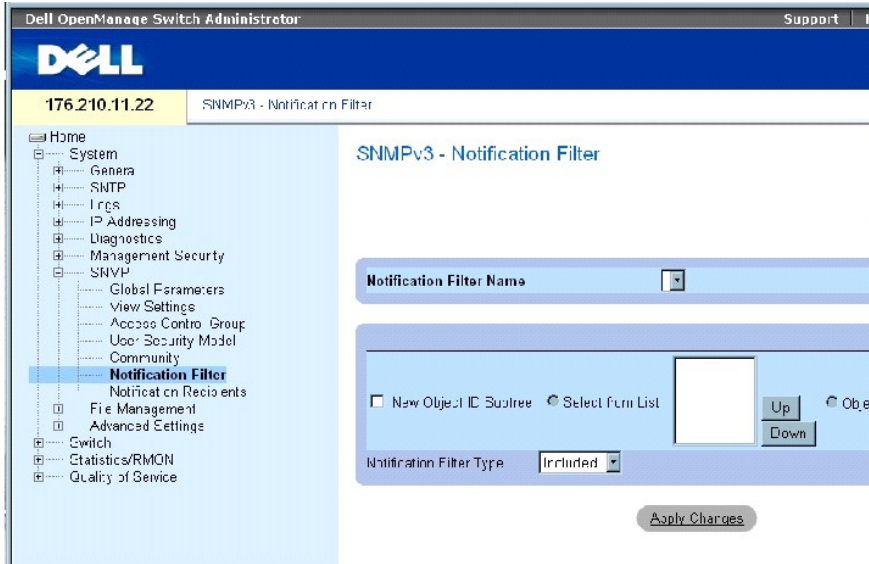
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

## SNMP 알림 필터 정의

[Notification Filter](#) 페이지에서는 OID를 기준으로 필터링 트랩을 허용합니다. 각 OID는 장치 기능 또는 기능 측면에 연결되어 있습니다. [Notification Filter](#) 페이지에서는 네트워크 관리자가 알림을 필터링할 수도 있습니다.

[Notification Filter](#) 페이지를 열려면 트리 뷰에서 System → SNMP → Notification Filters를 클릭하십시오.

그림 6-69. 알림 필터



[Notification Filter](#) 페이지에는 다음 필드가 들어 있습니다.

**Notification Filter Name** — 사용자 정의 알림 필터입니다.

**New Object Identifier Tree** — 알림이 전송되거나 차단되는 OID입니다. 필터가 OID에 연결된 경우 트랩 또는 정보용 메시지가 생성되어 트랩 수신자에게 전송됩니다. 개체 ID는 **Select from List** 또는 **Object ID List**에서 선택됩니다.



**Notification Filter Type** — OID와 관련하여 정보용 메시지 또는 트랩을 트랩 수신자에게 전송할지 여부를 표시합니다.

**Excluded** — OID 트랩 또는 정보용 메시지 전송을 제한합니다.

**Included** — OID 트랩 또는 정보용 메시지를 전송합니다.

## SNMP 필터 추가

1. [Notification Filter](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

[Add Filter](#) 페이지가 열립니다.

그림 6-70. 필터 추가

Refresh

Add Filter

Filter Name (1-63 Characters)

New Object Identifier Tree  Search from List  Object ID: 1.3.6.1.2.1.1

Filter Type: Included

Apply Changes

3. 관련 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

새 필터가 추가되고 장치가 업데이트됩니다.

## 필터 표 표시

1. [Notification Filter](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Filter Table](#)이 열립니다.

그림 6-71. 필터 표

Refresh

Object Identifier Subtree	Filter Type	Remove
1	Included	<input type="checkbox"/>

Apply Changes

## 필터 제거

1. [Notification Filter](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Filter Table](#)이 열립니다.

3. [Filter Table](#)의 항목을 선택하십시오.
4. **Remove** 확인란을 선택하십시오.

필터 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 알림 필터 구성

다음 표에서는 [Notification Filter](#) 페이지에 표시된 필드를 정의하는 CLI 명령을 요약합니다.

표 6-53. SNMP 알림 필터 CLI 명령

CLI 명령	설명
<code>snmp-server filter filter-name oid-tree {included   excluded}</code>	SNMP 알림 필터를 작성하거나 업데이트합니다.
<code>show snmp filters[filtername]</code>	SNMP 알림 필터 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

Console (config)# <code>snmp-server filter user1 iso included</code>		
Console(config)# end		
Console # <code>show snmp filters</code>		
Name	OID Tree	Type
-----	-----	-----
user1	iso	Included

## SNMP 알림 수신자 정의

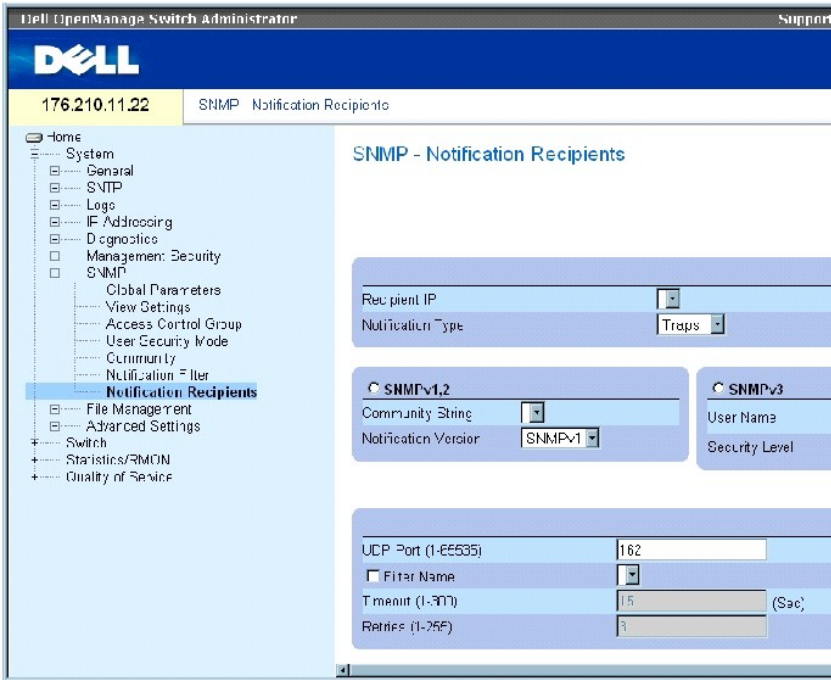
[Notification Recipients](#) 페이지에는 특정 사용자에게 트랩을 전송할 것인지 여부 및 전송한 트랩 종류를 결정하는 필터를 정의하는 데 필요한 정보가 들어 있습니다. SNMP 알림 필터에서는 다음 서비스를 제공합니다.

1. 관리 트랩 대상 식별
1. 트랩 필터링

- 1 트랩 생성 매개변수 선택
- 1 액세스 제어 확인

[Notification Recipients](#) 페이지를 열려면 트리 뷰에서 **System** → **SNMP** → **Notification Recipient**를 클릭하십시오.

그림 6-72. 알림 수신자



[Notification Recipients](#) 페이지에는 다음 필드가 들어 있습니다.

**Recipient IP** — 트랩을 전송할 IP 주소를 표시합니다.

**Notification Type** — 전송할 알림입니다. 가능한 필드 값은 다음과 같습니다.

**Trap** — 트랩을 전송합니다.

**Inform** — 정보용 메시지를 전송합니다.

**SNMPv1, 2** — 선택한 수신자에게 SNMP 버전 1 및 2가 활성화됩니다. SNMPv1 및 SNMPv2의 다음 필드를 정의하십시오.

**Community String (1-20 Characters)** — 트랩 관리자의 커뮤니티 문자열을 식별합니다.

**Notification Version** — 트랩 종류를 결정합니다. 가능한 필드 값은 다음과 같습니다.

**SNMP V1** — SNMP 버전 1 트랩을 전송합니다.

**SNMP V2** — SNMP 버전 2 트랩을 전송합니다.

**SNMPv3** — SNMPv3을 사용하여 트랩을 송수신합니다. SNMPv3의 다음 필드를 정의하십시오.

**User Name** — SNMP 알람을 수신할 사용자입니다.

**Security Level** — 패킷 인증 방법을 정의합니다. 가능한 필드 값은 다음과 같습니다.

**No Authentication** — 패킷을 인증하거나 암호화하지 않습니다.

**Authentication** — 패킷을 인증합니다.

**Privacy** — 패킷을 인증하고 암호화합니다.

**UDP Port (1-65535)** — 알람을 전송할 때 사용된 UDP 포트입니다. 기본값은 162입니다.

**Filter Name** — SNMP 필터를 포함하거나 제외합니다.

**Timeout(1-300)** — 정보용 메시지를 재전송하기 전에 장치가 기다리는 시간(초)입니다. 기본값은 15초입니다.

**Retries (1-255)** — 장치에서 정보용 메시지 요청을 재전송하는 횟수입니다. 기본값은 3입니다.

**Remove Notification Recipient** — 이 필드를 선택하면 선택한 알람 수신자가 제거됩니다.

## 새 트랩 수신자 추가

1. [Notification Recipients](#) 페이지를 여십시오.
2. Add를 클릭하십시오.

[Add Notification Recipients](#) 페이지가 열립니다.

그림 6-73. 알람 수신자 추가

Refresh

### Add Notification Recipient

Recipient IP  (X.X.X.X)

Notification Type

---

**SNMPv1,2**

Community String (1-20 Characters)

Notification Version

---

**SNMPv3**

User Name (1-20 Characters)

Security Level

---

UDP Port (1-65535)

Filter Name

Timeout (1-300)  (sec)

Retries (1-255)

**Apply Changes**

3. 관련 필드를 정의하십시오.
4. Apply Changes를 클릭하십시오.

알림 수신자가 추가되고 장치가 업데이트됩니다.

### 알림 수신자 표 표시

1. [Notification Recipients](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Notification Recipients Tables](#) 페이지가 열립니다.

그림 6-74. 알림 수신자 표

### Notification Recipient Tables

Refresh

#### SNMPv1,2 Notification Recipient

Recipients IP	Notification Type	Community String	Via OOB	Notification Version	UDP Port	Filter Name	Timeout	Retries	Remove
---------------	-------------------	------------------	---------	----------------------	----------	-------------	---------	---------	--------

#### SNMPv3 Notification Recipient

Recipients IP	Notification Type	User Name	Via OOB	Security Level	UDP Port	Filter Name	Timeout	Retries	Remove
---------------	-------------------	-----------	---------	----------------	----------	-------------	---------	---------	--------

Apply Changes

### 알림 수신자 삭제

1. [Notification Recipients](#) 페이지를 여십시오.

2. Show All을 클릭하십시오.

[Notification Recipients Tables](#) 페이지가 열립니다.

3. SNMPV1.2 Notification Recipient 또는 SNMPv3 Notification Recipient Tables에서 알람 수신자를 선택하십시오.
4. Remove 확인란을 선택하십시오.
5. Apply Changes를 클릭하십시오.

수신자가 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 SNMP 알람 수신자 구성

다음 표에서는 [Notification Recipients](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-54. SNMP 커뮤니티 CLI 명령

CLI 명령	설명
<code>snmp-server host {ipaddress   hostname} 커뮤니티 문자열 [traps   informs] [1   2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]</code>	SNMP 버전 1 또는 2에서 알람을 수신하는 알람 수신자를 작성하거나 업데이트합니다.
<code>snmp-server v3-host {ip-address   hostname} 사용자 이름 [traps   informs] [noauth   auth   priv] [udp-port 포트] [filter filtername] [timeout seconds] [retries retries]</code>	SNMP 버전 3에서 알람을 수신하는 알람 수신자를 작성하거나 업데이트합니다.
<code>show snmp</code>	현재 SNMP 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# snmp-server host 172.16.1.1
private

console(config)# end

console# show snmp

```

Community-String	Community-Access	View name	IP address
-----	-----	-----	-----
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

## 파일 관리

**File Management** 페이지를 사용하여 장치 소프트웨어, 이미지 파일 및 구성 파일을 관리하십시오. 파일은 TFTP 서버를 통해 다운로드 또는 업로드할 수 있습니다.

## 파일 관리 개요

파일 관리 구조는 다음 파일로 구성됩니다.

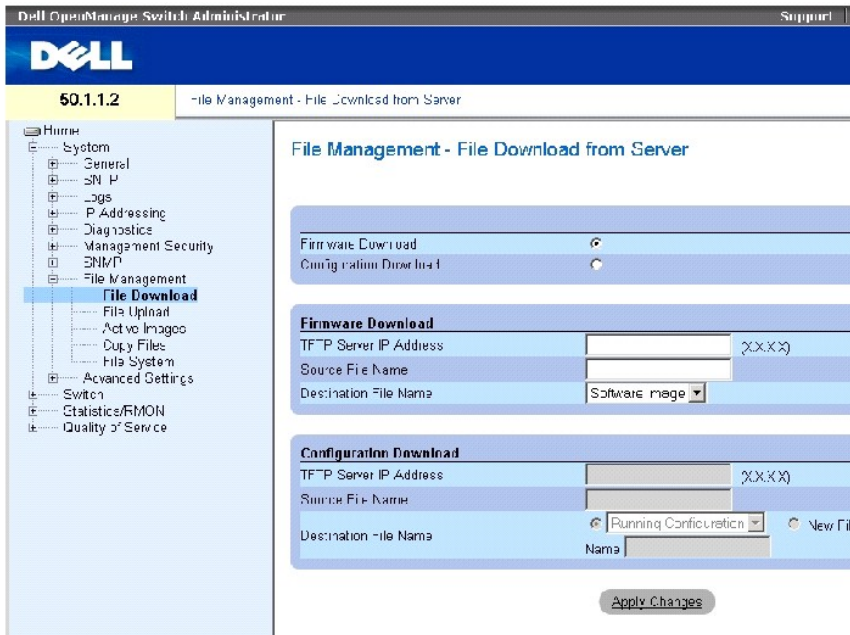
- 1 시작 구성 파일 — 시작 시 또는 재부팅 후 장치를 구성하는 데 필요한 명령이 들어 있습니다. 시작 구성 파일은 실행 구성 파일 또는 백업 구성 파일의 구성 명령을 시작 구성 파일에 복사하여 작성됩니다.
- 1 실행 구성 파일 — 모든 시작 구성 파일의 명령 및 현재 세션에서 입력한 모든 명령이 들어 있습니다. 장치의 전원을 끄거나 재부팅하면 실행 구성 파일에 저장된 모든 명령이 지워집니다. 시작 프로세스 시 시작 구성 파일에 있는 모든 명령이 실행 구성 파일에 복사되어 장치에 적용됩니다. 이 세션에서 모든 새 명령이 실행 구성 파일에 있는 명령에 추가됩니다. 시작 구성 파일을 업데이트하려면 장치 전원을 끄기 전에 실행 구성 파일을 시동 구성 파일에 복사해야 합니다.
- 1 백업 구성 파일 — 장치 구성의 백업 사본이 들어 있습니다. 최대 5개의 백업 구성 파일을 사용자 구성 이름을 지정하여 장치에 저장할 수 있습니다. 이러한 파일은 사용자가 실행 구성 파일 또는 시작 구성 파일을 사용자가 이름을 지정한 파일에 복사할 때 생성됩니다. 백업 구성 파일의 내용은 실행 구성 파일 또는 시작 구성 파일에 복사할 수 있습니다.
- 1 이미지 파일 — 시스템 파일 이미지는 2개의 Flash 파일(이미지 1 및 이미지 2)에 저장됩니다. 활성 이미지는 활성 사본으로 저장되지만 나머지 이미지는 2차 사본으로 저장됩니다. 장치가 부팅되고 활성 이미지로 실행됩니다. 활성 이미지가 손상된 경우 시스템은 자동으로 비활성 이미지로 부팅됩니다. 이것은 소프트웨어 업그레이드 프로세스에서 발생할 수 있는 오류를 예방하는 안전 기능입니다.

File Management 페이지를 열려면 트리 뷰에서 System→File Management를 클릭하십시오.

## 파일 다운로드

[File Download from Server](#) 페이지에는 TFTP 서버의 구성 파일 및 시스템 이미지를 장치에 다운로드하는 데 필요한 필드가 들어 있습니다. [File Download from Server](#) 페이지를 열려면 트리 뷰에서 System→File Management→File Download를 클릭하십시오.

그림 6-75. 서버에서 파일 다운로드



[File Download from Server](#) 페이지에는 다음 필드가 들어 있습니다.

**Firmware Download** — 펌웨어 파일을 다운로드합니다. **Firmware Download**를 선택하면 **Configuration Download** 필드가 비활성화됩니다.

**Configuration Download** — 구성 파일을 다운로드합니다. **Configuration Download**를 선택하면 **Firmware Download** 필드가 비활성화됩니다.

#### Firmware Download

**TFTP Server IP Address** — 펌웨어 파일을 다운로드하는 원본 TFTP 서버 IP 주소입니다.

**Source File Name** — 다운로드할 파일을 표시합니다.

**Destination File Name** — 파일을 다운로드할 대상 파일 종류입니다. 가능한 필드 값은 다음과 같습니다.

**Software Image** — 이미지 파일을 다운로드합니다.

**Boot Code** — 부팅 파일을 다운로드합니다.

#### Configuration Download

**TFTP Server IP Address** — 구성 파일을 다운로드하는 TFTP 서버 IP 주소입니다.

**Source File Name** — 다운로드할 구성 파일을 표시합니다.


**Destination File Name** — 구성 파일을 다운로드할 대상 파일입니다. 가능한 필드 값은 다음과 같습니다.

**Running Configuration** — 실행 구성 파일의 명령을 다운로드합니다.

**Startup Configuration** — 시작 구성 파일을 다운로드하여 덮어씁니다.

**User Defined Backup Configuration** — 사용자 정의 백업 구성 파일을 다운로드하여 덮어씁니다.

**New File Name** — 대상 파일로 지정할 수 있는 새 백업 구성 파일을 다운로드합니다.

 **주:** 이미지 파일은 비활성 이미지를 덮어씁니다. 비활성 이미지를 재설정하여 활성 이미지로 설정한 후, 장치를 재설정하고 다운로드를 수행하도록 지정하는 것이 좋습니다.


이미지 파일을 다운로드하는 중에 다운로드 진행을 표시하는 대화상자가 열립니다. 다운로드가 끝나면 자동으로 창이 닫힙니다.

## 파일 다운로드

1. [File Download from Server](#) 페이지를 여십시오.
2. 다운로드할 파일 종류를 정의하십시오.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.



소프트웨어가 장치에 다운로드됩니다.

 **주:** 선택한 이미지 파일을 활성화하려면 장치를 재설정하십시오. 장치 재설정에 대한 정보는 [스택 마스터 간 전환](#)을 참조하십시오.

## CLI 명령을 사용하여 파일 다운로드

다음 표에서는 [File Download from Server](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-55. 파일 다운로드 CLI 명령

CLI 명령	설명
copy source-url destination-url	소스의 파일을 대상에 복사합니다.


다음은 CLI 명령의 예입니다.

```
console# copy
tftp://10.6.6.64/pp.txt
startup-config

....!

Copy: 575 bytes copied in
00:00:06 [hh:mm:ss]

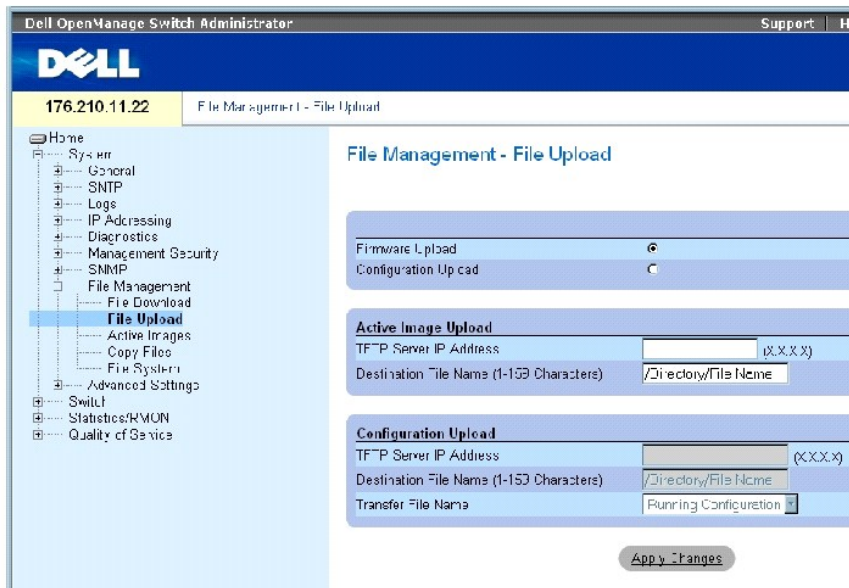
01-Jan-2000 06:41:55 %
COPY-W-TRAP: The copy
operation was completed
successfully
```

 **주:** 각각의 느낌표(!)는 10개의 패킷을 전송했음을 표시합니다.

## 파일 업로드

[File Upload to Server](#) 페이지에는 장치에서 TFTP 서버로 소프트웨어를 업로드하는 데 필요한 필드가 들어 있습니다. 이미지 파일도 [File Upload to Server](#) 페이지에서 업로드할 수 있습니다. [File Upload to Server](#) 페이지를 열려면 트리 뷰에서 **System** → **File Management** → **File Upload**를 클릭하십시오.

그림 6-76. 서버에 파일 업로드



[File Upload to Server](#) 페이지에는 다음 필드가 들어 있습니다.

**Firmware Upload** — 펌웨어 파일을 업로드합니다. **Firmware Upload**를 선택하면 **Configuration Upload** 필드가 비활성화됩니다.

**Configuration Upload** — 구성 파일을 업로드합니다. **Configuration Upload**를 선택하면 **Active Image Upload** 필드가 비활성화됩니다.

#### Active Image Upload

**TFTP Server IP Address** — 소프트웨어 이미지를 업로드하는 대상 TFTP 서버 IP 주소입니다.

**Destination File Name (1-159 Characters)** — Indicates the Software Image file path to which the file is uploaded.

#### Configuration Upload

**TFTP Server IP Address** — 구성 파일을 업로드하는 대상 TFTP 서버 IP 주소입니다.


**Destination File Name (1-159 Characters)** — 파일을 업로드하는 구성 파일의 대상 경로를 표시합니다.

**Transfer File Name** — 구성이 업로드되는 대상 소프트웨어 파일입니다. 가능한 필드 값은 다음과 같습니다.

**Running Configuration** — 실행 구성 파일을 업로드합니다.

**Startup Configuration** — 시작 구성 파일을 업로드합니다.

**List of User Defined Configuration Files** — 사용자 정의 구성 파일을 업로드합니다.

 **주:** 사용자 정의 구성 파일 목록은 사용자가 백업 구성 파일을 작성한 경우에만 표시됩니다. 예를 들면, 사용자가 실행 구성 파일을 사용자 정의 구성 파일(BACKUP-SITE-1)에 복사한 경우 이 목록은 [File Upload to Server](#) 페이지에 표시되고 BACKUP-SITE-1 구성 파일이 목록에 표시됩니다.

## 파일 업로드

1. [File Upload to Server](#) 페이지를 여십시오.
2. 업로드할 파일 종류를 정의하십시오.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

소프트웨어가 TFTP 서버에 업로드됩니다.

## CLI 명령을 사용하여 파일 업로드

다음 표에서는 [File Upload to Server](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

**표 6-56. 파일 업로드 CLI 명령**

CLI 명령	설명
copy source-url destination-url	소스의 파일을 대상에 복사합니다.

다음은 CLI 명령의 예입니다.

```

console# copy image tftp://10.6.6.64/uploaded.ros

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully

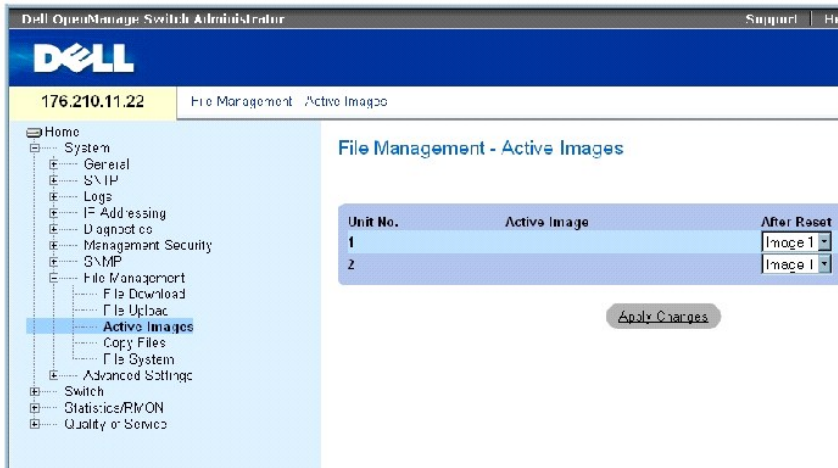
```

## 이미지 파일 활성화

[Active Images](#) 페이지에서는 네트워크 관리자가 이미지 파일을 선택한 후 재설정할 수 있습니다. 스택 구성에 있는 각 단원의 활성 이미지 파일은 개별적으로 선택할 수 있습니다. [Active](#)

[Images](#) 페이지를 열려면 트리 뷰에서 **System** → **File Management** → **Active Images**를 클릭하십시오.

그림 6-77. 활성 이미지



[Active Images](#) 페이지에는 다음 필드가 들어 있습니다.

**Unit No.** — 선택되는 이미지 파일의 단원 번호입니다.

**Active Image** — 현재 단원에서 활성인 이미지 파일입니다.

**After Reset** — 장치를 재설정 후 단원에서 활성인 이미지 파일입니다. 가능한 필드 값은 다음과 같습니다.

**Image 1** — 장치를 재설정 후 이미지 파일 1을 활성화합니다.

**Image 2** — 장치를 재설정 후 이미지 파일 2를 활성화합니다.

### 이미지 파일 선택

1. [Active Images](#) 페이지를 여십시오.
2. **After Reset** 필드에서 특정 단원의 이미지 파일을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

이미지 파일이 선택됩니다. 이미지 파일은 다음 재설정 이후에만 다시 로드됩니다. 현재 선택한 이미지 파일은 다음에 장치를 재설정할 때까지 계속 실행됩니다.

### CLI 명령을 사용하여 활성 이미지 파일 사용

다음 표에서는 [Active Images](#) 페이지에 표시된 필드를 보는 CLI 명령을 요약합니다.

표 6-57. 파일 업로드 CLI 명령

CLI 명령	설명
--------	----

boot system [unit   <b>단원</b> ] (image-1   image-2)	시작 시 장치에서 로드하는 시스템 이미지를 표시합니다.
show version [unit <b>단원</b> ]	시스템의 버전 정보를 표시합니다.

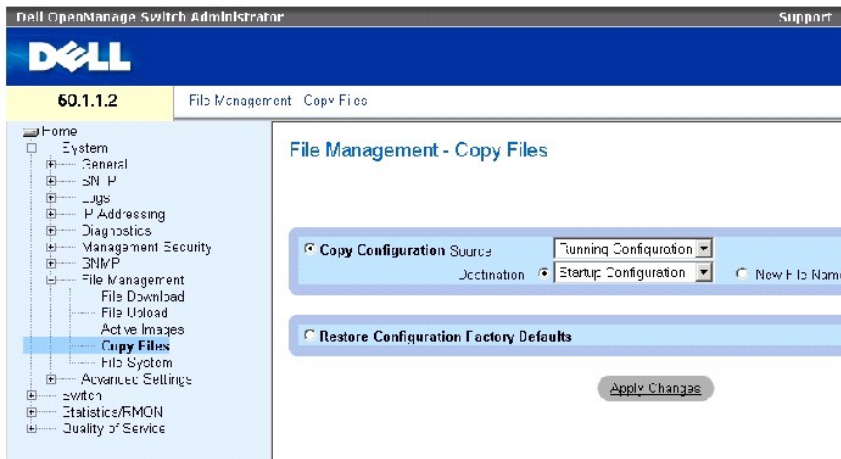
다음은 CLI 명령의 예입니다.

```
Console# boot system
image-1
```

## 파일 복사

[Copy Files](#) 페이지에서 파일을 복사 및 삭제할 수 있습니다. [Copy Files](#) 페이지를 열려면 트리 뷰에서 **System** → **File Management** → **Copy Files**를 클릭하십시오.

그림 6-78. 파일 복사



[Copy Files](#) 페이지에는 다음 필드가 들어 있습니다.

**Copy Configuration** — 이 필드를 선택하면 마스터 파일의 실행, 시작 또는 백업 구성 파일이 대상 파일에 복사됩니다.

**Source** — 대상 파일에 복사할 파일 종류를 표시합니다. 실행 구성, 시작 구성 또는 사용자 정의 백업 구성 파일 중 하나를 선택하십시오.

**Destination** — 소스 파일이 복사되는 대상 구성 파일을 표시합니다. 파일을 백업 마스터의 백업 파일에 복사할 수 없습니다. 백업 파일은 백업 파일을 정의한 경우에만 **Destination Unit** 필드에 표시됩니다. **New File Name** 확인란을 선택하고 새 파일 이름을 지정하여 소스 파일을 새 백업 구성 파일에 복사하십시오.

**New File Name** — 새로 작성한 백업 구성 파일 이름을 표시합니다.

**Restore Configuration Factory Defaults** — 이 필드를 선택하면 현재 구성 설정이 출하 시 구성 기본 설정으로 대체되도록 지정됩니다. 이 필드를 선택하지 않으면 현재 구성 설정이 유지됩니다.

## 파일 복사

1. [Copy Files](#) 페이지를 여십시오.
2. **Source** 및 **Destination** 필드를 정의하십시오.

3. **Apply Changes**를 클릭하십시오.

파일이 복사되고 장치가 업데이트됩니다.

### 출하 시 기본 설정 복구

1. [Copy Files](#) 페이지를 여십시오.
2. **Restore Configuration Factory Defaults**를 클릭하십시오.
3. **Apply Changes**를 클릭하십시오.

출하 시 기본 설정이 복구되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 파일 복사 및 삭제

다음 표에서는 [Copy Files](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-58. 파일 복사 CLI 명령

CLI 명령	설명
copy 소스-url 대상-url	소스의 파일을 대상에 복사합니다.
delete startup-config	시작 구성 파일을 삭제합니다.

다음은 CLI 명령의 예입니다.

```
console# delete startup-
config

Startup file was deleted

console#

console# copy running-
config startup-config

01-Jan-2000 06:55:32 %
COPY-W-TRAP: The copy
operation was completed
successfully

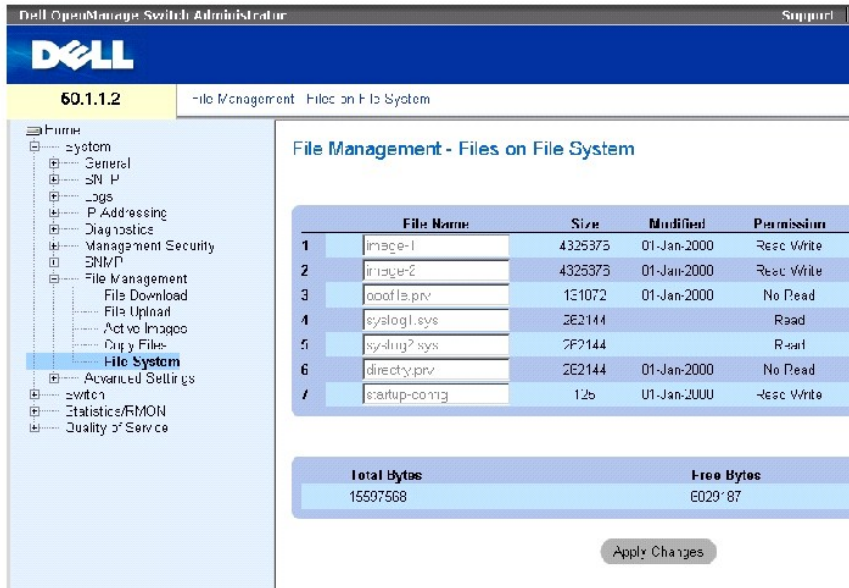
Copy succeeded

console#
```

### 장치 파일 관리

[Files on File System](#) 페이지에서는 파일 이름, 파일 크기, 파일 수정 사항 및 파일 권한을 포함하여 현재 시스템에 저장된 파일에 대한 정보를 제공합니다. 파일 시스템에서는 총 3MB까지 최 대 5개 파일의 관리가 가능합니다. [Files on File System](#) 페이지를 열려면 트리 뷰에서 **System**→**File Management**→**File System**를 클릭하십시오.

그림 6-79. 파일 시스템의 파일



[Files on File System](#) 페이지에는 다음 필드가 들어 있습니다.

**File Name** — 현재 파일 관리 시스템에 저장된 파일을 표시합니다.

**Size** — 파일 크기를 표시합니다.

**Modified** — 파일을 마지막으로 수정한 날짜를 표시합니다.

**Permission** — 파일에 지정된 권한 종류를 표시합니다. 가능한 필드 값은 다음과 같습니다.

**Read Only** — 읽기 전용 파일을 표시합니다.

**Read Write** — 읽기 및 쓰기 파일을 표시합니다.

**Remove** — 이 필드를 선택하면 파일이 삭제됩니다.

**Rename** — 파일 이름을 변경할 수 있습니다. 파일 이름은 **File Name** 필드에서 변경합니다.

**Total Bytes** — 현재 사용 중인 공간의 전체 크기를 표시합니다.

**Free Bytes** — 현재 사용 가능한 여유 공간의 크기를 표시합니다.

## CLI 명령을 사용하여 파일 관리

다음 표에서는 시스템 파일을 관리하는 CLI 명령을 요약합니다.

**표 6-59. 파일 복사 CLI 명령**

CLI 명령	설명
dir	플래쉬 파일 시스템에서 파일 목록을 표시합니다.

다음은 CLI 명령의 예입니다.

console# <b>dir</b>				
Directory of flash:				
File Name	Permis- sion	Flash Size	Data Size	Modified
----- -	-----	-----	-----	----- ----- ----
3.txt	rw	524288	523776	22-Feb- 2005 18:49:27
setup	rw	524288	95	22-Feb- 2005 15:58:19
setup2	rw	524288	95	22-Feb- 2005 15:58:35
image-1	rw	4325376	4325376	06-Feb- 2005 17:55:32
image-2	rw	4325376	4325376	06-Feb- 2005 17:55:31
test.txt	rw	524288	95	22-Feb- 2005 12:16:44
aaafile.prv	--	131072	--	06-Feb- 2005 19:09:02
syslog1.sys	r-	262144	--	22-Feb- 2005 18:49:27
syslog2.sys	r-	262144	--	22-Feb- 2005 18:49:27



directory.prv	--	262144	--	06-Feb-2005 17:55:31
startup-config	rw	524288	347	22-Feb-2005 11:56:03
Total size of flash: 16646144 bytes				
Free size of flash: 4456448 bytes				

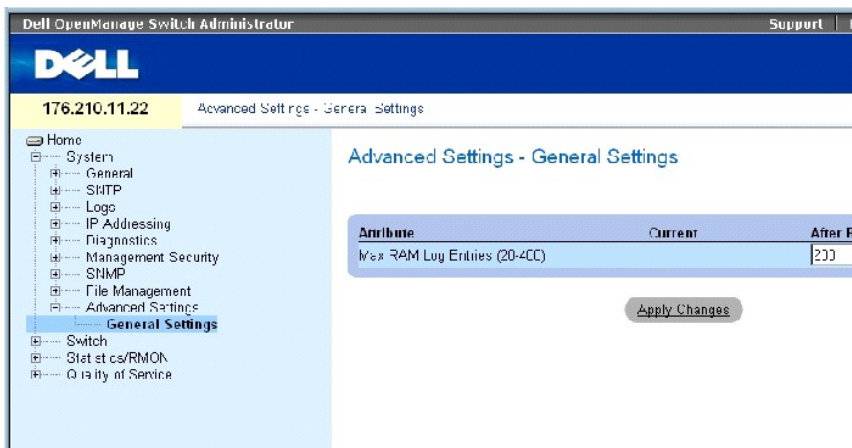
## 일반 설정 구성

고급 설정을 사용하여 스위치의 다른 전역 속성을 설정하십시오. 이러한 특성의 변경사항은 스위치를 재설정된 후에만 적용됩니다. 트리 뷰에서 **System** → **Advanced Settings**를 클릭하여 **Advanced Settings** 페이지를 여십시오.

**Advanced Settings** 페이지에는 일반 설정을 구성하는 데 필요한 링크가 들어 있습니다.

**General Settings** 페이지에서는 일반 장치 매개변수를 정의하는 데 필요한 정보를 제공합니다. **General Settings** 페이지를 열려면 트리 뷰에서 **System** → **Advanced Settings** → **General Settings**를 클릭하십시오.

그림 6-80. 일반 설정



**General Settings** 페이지에는 다음 정보가 들어 있습니다.

**Attribute** — 일반 설정 특성입니다.

**Current** — 현재 구성된 값입니다.

**After Reset** — 재설정 후(나중)의 값입니다. **After Reset** 옆에 값을 입력하면 필드 테이블에 메모리가 할당됩니다.

**Max RAM Log Entries** — RAM 로그 항목의 최대 수입니다. 로그 항목이 가득 차면 로그가 지워지고 로그 파일이 다시 시작됩니다.

## CLI 명령을 사용하여 RAM 로그 항목 수 보기

다음 표에서는 [General Settings](#) 페이지에 표시된 필드를 설정하는 CLI 명령을 요약합니다.

표 6-60. 일반 설정 CLI 명령

CLI 명령	설명
logging buffered size number	내부 버퍼(RAM)에 저장된 syslog 메시지 수를 설정합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# logging
buffered size 300
```

---

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

## 스위치 정보 구성

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [네트워크 보안 구성](#)
- [포트 기반 인증 구성](#)
- [포트 구성](#)
- [주소 표 구성](#)
- [GARP 구성](#)
- [스패닝 트리 프로토콜 구성](#)
- [VLAN 구성](#)
- [포트 결합](#)
- [멀티캐스트 전달 지원](#)

본 항목에서는 네트워크 보안, 포트, 주소 표, GARP, VLAN, 스패닝 트리, 포트 결합 및 멀티캐스트 지원에 대한 모든 시스템 작동 및 일반 정보를 제공합니다.

## 네트워크 보안 구성

네트워크 보안 페이지를 사용하여 액세스 제어 목록과 잠긴 포트를 통해 네트워크 보안을 설정합니다. **네트워크 보안** 페이지를 열려면 **Switch** → **Network Security**를 선택합니다.

## 포트 기반 인증

포트 기반 인증은 외부 서버를 통해 포트별로 시스템 사용자를 인증할 수 있게 합니다. 인증되고 승인된 시스템 사용자만이 데이터를 전송하고 수신할 수 있습니다. 포트는 RADIUS 서버에서 확장 가능 인증 프로토콜(EAP)을 사용하여 인증됩니다. 포트 인증에는 다음과 같은 항목이 포함됩니다.

- 1 **인증자** — 시스템 액세스를 허용하기 전에 인증된 장치 포트를 지정합니다.
- 1 **요청자** — 인증된 포트에 연결되어 시스템 서비스에 대한 액세스를 요청하는 호스트를 지정합니다.
- 1 **인증 서버** — RADIUS 서버와 같이 인증자를 대표하여 인증을 수행하는 외부 서버를 지정하고 요청자가 시스템 서비스에 액세스하도록 인증되었는지를 표시합니다.

포트 기반 인증은 두 가지 액세스 상태를 생성합니다.

- 1 **제어 액세스** — 요청자가 인증된 경우 요청자와 시스템 사이의 통신을 허용합니다.
- 1 **비제어 액세스** — 포트 상태에 상관없이 제어되지 않는 통신을 허용합니다.

본 장치는 현재 RADIUS 서버를 통한 포트 기반 인증을 지원합니다.

## 고급 포트 기반 인증

고급 포트 기반 인증으로 다음과 같은 기능을 수행할 수 있습니다.

- 1 단일 포트에 다중 호스트가 연결될 수 있도록 합니다.
- 1 하나의 호스트만 승인을 받으면 모든 호스트가 시스템에 액세스할 수 있습니다. 포트가 승인되지 않은 경우, 연결된 모든 호스트의 네트워크 액세스가 거부됩니다.
- 1 사용자 기반 인증을 사용합니다. 장치의 특정 VLAN은 VLAN에 연결된 특정 포트가 승인되지 않았더라도 항상 사용할 수 있습니다.
  - 1 예를 들면, 데이터 처리량에는 인증이 필요하지만 VoIP에는 인증이 필요하지 않습니다. 승인이 필요 없는 VLAN을 정의할 수 있습니다. 인증되지 않은 VLAN은 VLAN에 연결된 포트가 승인된 것으로 정의되어 있어도 사용자가 사용할 수 있습니다.

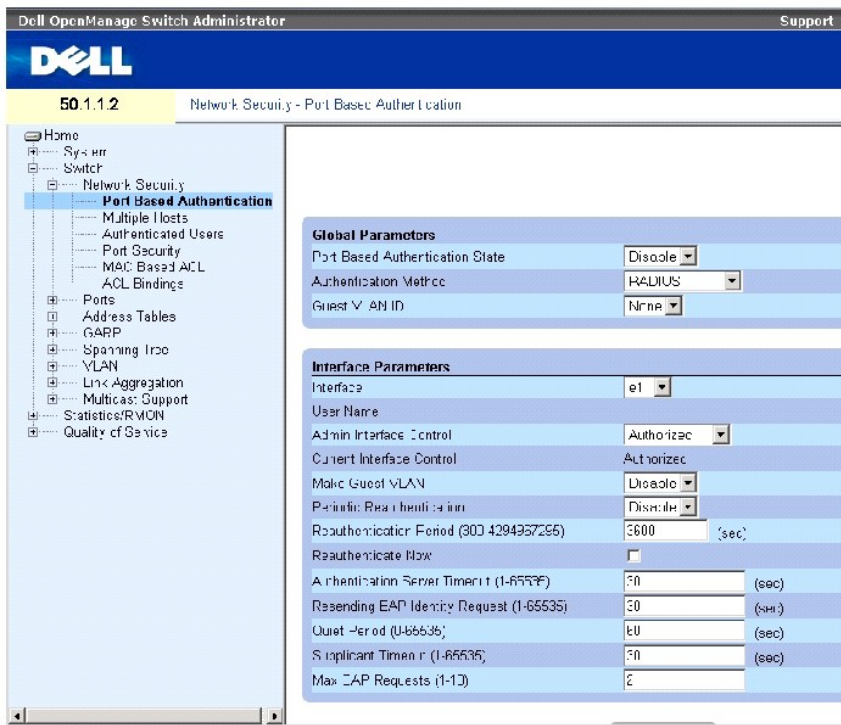
고급 포트 기반 인증은 다음과 같은 모드에서 구현됩니다.

- 1 **단일 호스트 모드** — 승인된 호스트만 포트에 액세스할 수 있습니다.
- 1 **다중 호스트 모드** — 단일 포트에 다중 호스트를 연결할 수 있습니다. 하나의 호스트만 승인을 받으면 모든 호스트가 네트워크에 액세스할 수 있습니다. 호스트 인증이 실패하거나 EAPOL-logout 메시지를 수신한 경우, 연결된 모든 클라이언트의 네트워크 액세스가 거부됩니다.
- 1 **게스트 VLAN** — 포트에 승인된 제한된 네트워크 액세스를 제공합니다. 포트가 포트 기반 승인을 통한 네트워크 액세스가 거부되었지만 게스트 VLAN이 활성화된 경우 해당 포트는 제한된 네트워크 액세스를 받습니다. 예를 들면, 네트워크 관리자는 게스트 VLAN을 사용하여 포트 기반 인증을 통한 네트워크 액세스를 거부하지만 승인되지 않은 사용자에게 대한 인터넷 액세스를 허용할 수 있습니다.

## 포트 기반 인증 구성

[포트 기반 인증](#) 페이지에서 네트워크 관리자가 포트 기반 인증을 구성할 수 있습니다. [포트 기반 인증](#) 페이지를 열려면 **Switch** → **Network Security** → **Port Based Authentication**을 클릭하십시오.

그림 7-1. 포트 기반 인증



[포트 기반 인증](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Port Based Authentication State** — 장치에 포트 기반 인증을 허용합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Enable** — 장치에 포트 기반 인증을 사용합니다.

**Disable** — 장치에 포트 기반 인증을 사용하지 않습니다.

**Authentication Method** — 사용되는 인증 방식을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**None** — 포트 인증에 사용되는 인증 방식이 없음을 표시합니다.

**RADIUS** — RADIUS 서버를 통해 포트 인증을 수행함을 표시합니다.

**RADIUS, None** — 먼저 RADIUS 서버를 통해 포트 인증을 수행함을 표시합니다. 포트가 인증되지 않은 경우, 인증 방식이 사용되지 않으며 세션이 허용됩니다.

**Guest VLAN** — 승인되지 않은 포트에 게스트 VLAN을 사용하도록 합니다. 게스트 VLAN이 활성화된 경우 비승인 포트는 자동으로 **VLAN List** 필드에서 선택된 VLAN에 연결됩니다. 필드 기본값은 비활성화입니다.

**Interface** — 포트 기반 인증이 활성화된 인터페이스 목록을 포함합니다.

**User Name** — 요청자 사용자 이름을 표시합니다.

**Admin Interface Control** — 포트 승인 상태를 정의합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Auto** — 장치에 포트 기반 인증을 사용합니다. 인터페이스는 장치와 클라이언트 사이의 인증 교환에 기반하여 승인 또는 비승인 상태 사이를 전환합니다.

**Authorized** — 인증이 없이 인터페이스를 승인 상태에 둡니다. 인터페이스는 클라이언트 포트 기반 인증이 없이 일반 처리량을 재전송하고 수신합니다.

**Unauthorized** — 인터페이스를 비승인 상태로 이동시켜 선택된 인터페이스의 시스템 액세스를 거부합니다. 장치는 클라이언트에게 이 인터페이스를 통해 인증 서비스를 제공할 수 없습니다.

**Current Interface Control** — 현재 포트 승인 상태입니다.

**Make Guest VLAN** — 활성화된 경우, 이 인터페이스에 연결된 비승인 사용자가 게스트 VLAN에 액세스할 수 있음을 표시합니다.

**Periodic Reauthentication** — 즉시 포트 재인증을 허용합니다.

**Reauthentication Period (300-4294967295)** — 선택된 포트가 재인증되는 기간을 표시합니다. 필드 값은 초를 단위로 합니다. 필드 기본값은 3600초입니다.

**Reauthenticate Now** — 이 항목이 선택되면 즉시 포트 재인증을 허용합니다.

**Authentication Server Timeout (1-65535)** — 장치가 인증 서버에 요청을 다시 전송하기 전까지 기다릴 시간을 정의합니다. 필드 값은 초 단위로 지정됩니다. 필드 기본값은 30초입니다.

**Resending EAP Identity Request (1-65535)** — EAP 요청이 다시 전송되기 전까지 기다릴 시간을 정의합니다. 필드 기본값은 30초입니다.

**Quiet Period (0-65535)** — 인증 교환에 실패한 후 장치가 정숙 상태를 유지할 시간(초)을 표시합니다. 가능한 필드 범위는 0-65535입니다. 필드 기본값은 60초입니다.

**Supplicant Timeout (1-65535)** — EAP 요청이 요청자에게 다시 전송되기 전까지 기다릴 시간을 표시합니다. 필드 값은 초를 단위로 합니다. 필드 기본값은 30초입니다.

**Max EAP Requests (1-10)** — 전송된 EAP 요청 횟수를 표시합니다. 정의된 기간 동안 응답이 없는 경우, 인증 프로세스가 재시작됩니다. 필드 기본값은 2회입니다.

## 포트 기반 인증 표 표시

1. [Port Based Authentication](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Port Based Authentication Table](#)이 열립니다.

그림 7-2. 포트 기반 인증 표

### Port-based Authentication Table

Port	User Name	Admin Port Control	Current Port Control	Periodic Reauthentication	Reauthentication Period	Reauthenticate Now <small>Select All</small>
1	e1	Authorized	Authorized	Disable	3600	<input type="checkbox"/>
2	e2	Authorized	*	Disable	3600	<input type="checkbox"/>
3	e3	Authorized	*	Disable	3600	<input type="checkbox"/>
4	e4	Authorized	*	Disable	3600	<input type="checkbox"/>
5	e5	Authorized	*	Disable	3600	<input type="checkbox"/>
6	e6	Authorized	*	Disable	3600	<input type="checkbox"/>

[Port Based Authentication](#) 페이지의 필드 외에도 [Port Based Authentication Table](#)에는 다음과 같은 필드가 표시됩니다.

**Unit No.** — 스택 구성요소를 선택합니다.

**Copy Parameters from Port No.** — 선택된 포트의 매개변수를 복사합니다.

### [Port Based Authentication Table](#)의 매개변수 복사

1. 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Port Based Authentication Table](#)가 열립니다.

3. **Copy Parameters from Port No.** 필드에서 인터페이스를 선택합니다.
4. [Port Based Authentication Table](#)에서 인터페이스를 선택합니다.
5. **Copy to** 확인란을 선택하여 포트 기반 인증 매개변수가 복사될 인터페이스를 정의합니다.
6. **Apply Changes**를 클릭하십시오.

### CLI 명령을 사용하여 포트 기반 인증 활성화

다음 표는 [Port Based Authentication table](#)에 표시된 것과 같이 포트 기반 인증을 활성화하는 해당 CLI 명령을 요약합니다.

표 7-61. 포트 인증 CLI 명령

CLI 명령	설명
aaa authentication dot1x default 메서드1 [메서드2]	IEEE 802.1X가 실행되는 인터페이스에 사용할 하나 이상의 인증, 승인 및 계정(AAA) 방식을 지정합니다.

dot1x max-req 횟수	인증 프로세스를 재시작하기 전에 장치가 클라이언트에 EAP를 전송할 수 있는 최대 횟수를 설정합니다.
dot1x re-authenticate [ethernet 인터페이스]	모든 802.1X 활성화 포트 또는 지정된 802.1X 활성화 포트의 재인증을 수동으로 시작합니다.
dot1x re-authentication	클라이언트의 주기적인 재인증을 활성화합니다.
dot1x timeout quiet-period 초	인증 교환에 실패한 후 장치가 정숙 상태를 유지할 시간(초)을 설정합니다.
dot1x timeout re-authperiod 초	재인증 시도 사이의 시간(초)을 설정합니다.
dot1x timeout server-timeout 초	인증 서버에 패킷을 재전송할 시간을 설정합니다.
dot1x timeout supp-timeout 초	클라이언트에 EAP 요청 프레임의 재전송할 시간을 설정합니다.
dot1x timeout tx-period 초	장치가 EAP 요청을 재전송하기 전에 EAP - 요청/식별 프레임에 대한 클라이언트의 응답을 기다릴 시간(초)을 설정합니다.
show dot1x [ethernet 인터페이스]	장치 또는 지정된 인터페이스의 802.1X 상태를 표시합니다.
show dot1x users [username username]	장치의 802.1X 사용자를 표시합니다.
dot1x guest-vlan enable	비승인 포트에 게스트 VLAN 사용을 활성화합니다. 게스트 VLAN이 활성화된 경우 비승인 포트는 자동으로 VLAN List 필드에서 선택된 VLAN에 연결됩니다. 필드 기본값은 비활성화입니다.
dot1x guest-vlan	VLAN 목록을 포함합니다. 게스트 VLAN은 VLAN List에서 선택됩니다.

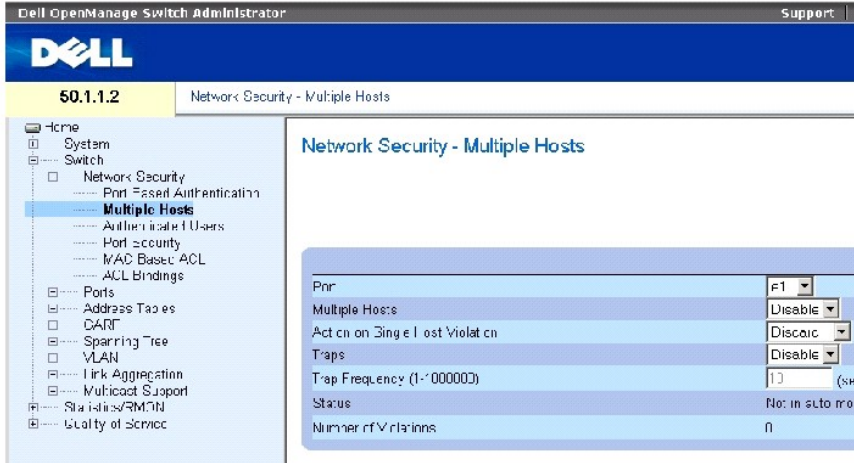
다음은 CLI 명령의 예입니다.

Console# show dot1x					
-----					
Interface	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
-----	-----	-----	-----	-----	-----
1/e1	Auto	Authorized	Ena	3600	Bob
1/e2	Auto	Authorized	Ena	3600	John
1/e3	Auto	Unauthorized	Ena	3600	Clark
1/e4	Force-auth	Authorized	Dis	3600	n/a

## 고급 포트 기반 인증 구성

[Multiple Hosts](#) 페이지는 특정 포트와 VLAN의 고급 포트 기반 인증 설정에 대한 정보를 제공합니다. 고급 포트 기반 인증에 대한 자세한 내용은 [고급 포트 기반 인증](#)을 참조하십시오. [Multiple Hosts](#)를 열려면 **Switch**→**Network Security**→**Multiple Hosts**를 클릭하십시오.

그림 7-3. 다중 호스트



[Multiple Hosts](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Port** — 고급 포트 기반 인증이 활성화된 포트 번호입니다.

**Multiple Hosts** — 다중 호스트의 시스템 액세스를 승인하도록 단일 호스트를 활성화 또는 비활성화합니다. 진입 필터를 비활성화하거나 선택한 포트에 포트 잠금 보안을 사용하려면 이 설정을 활성화해야 합니다.

**Action on Single Host Violation** — MAC 주소가 클라이언트(요청자) MAC 주소가 아닌 호스트에서 보내어 단일 호스트 모드에 도착하는 패킷에 적용될 동작을 정의합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Forward** — Forwards the packets from an unknown source, however, the MAC address is not learned.

**Discard** — 모든 습득되지 않은 소스의 패킷을 폐기합니다. 이 값은 기본값입니다.

**Shutdown** — 모든 습득되지 않은 소스의 패킷을 폐기하고 포트를 닫습니다. 포트는 활성화되거나 스위치가 재설정될 때까지 닫힌 상태를 유지합니다.

**Traps** — 위반이 발생한 경우 호스트에 트랩을 전송하거나 전송할 수 없게 합니다.

**Trap Frequency (1-1000000) (Sec)** — 호스트에 트랩을 보내는 주기를 정의합니다. **Trap Frequency (1-1000000)** 필드는 **Multiple Hosts** 필드가 **Disable**로 정의된 경우에만 정의할 수 있습니다. 기본값은 10초입니다.

**Status** — 호스트 상태입니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Unauthorized** — 포트 제어가 **강제로 비승인**되었거나 포트 링크가 끊겼거나 포트 제어가 자동이지만 클라이언트가 포트를 통해 승인되었음을 표시합니다.

**Not in Auto Mode** — 포트 제어가 **강제로 승인**되었으며 클라이언트가 전체 포트 액세스를 가짐을 표시합니다.

**Single-host Lock** — 포트 제어가 **자동**이며 단일 클라이언트가 포트를 통해 인증되었음을 표시합니다.

**No Single Host** — 다중 호스트가 활성화되었음을 표시합니다.



**Number of Violations** — MAC 주소가 클라이언트(요청자) MAC 주소가 아닌 호스트에서 단일 호스트 모드의 인터페이스에 도착한 패킷의 수입니다.

### 다중 호스트 표 표시

1. [Multiple Hosts](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[Multiple Hosts Table](#)가 열립니다.

그림 7-4. 다중 호스트 표

### Multiple Hosts Table

Refresh

	Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	e1	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
2	e2	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
3	e3	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
4	e4	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
5	e5	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
6	e6	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0
7	e7	<input type="checkbox"/>	Discard	<input type="checkbox"/>	10	Unauthorized	0

### CLI 명령을 사용하여 다중 호스트 활성화

다음 표는 [Multiple Hosts](#) 페이지에 표시된 것과 같이 고급 포트 기반 인증을 활성화하는 해당 CLI 명령을 요약합니다.

표 7-62. 다중 호스트 CLI 명령

CLI 명령	설명
<code>dot1x multiple-hosts</code>	dot1x 포트 제어 인터페이스 구성 명령이 auto로 설정된 802.1X 승인 포트에 다중 호스트(클라이언트)를 허용합니다.
<code>dot1x single-host-violation {forward  discard  discard-shutdown}[trap seconds]</code>	MAC 주소가 클라이언트(요청자) MAC 주소가 아닌 스테이션이 인터페이스에 액세스를 시도할 때 수행할 동작을 구성합니다.

다음은 CLI 명령의 예입니다.

```

Console(config)# interface
ethernet 1/e1

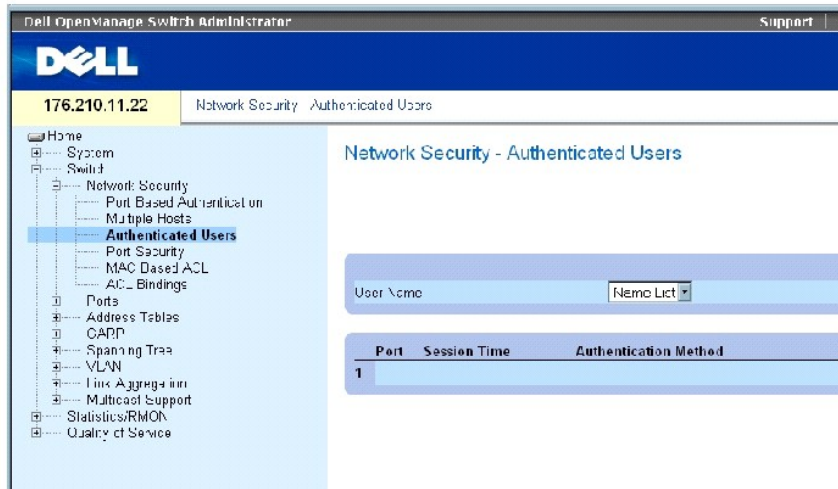
Console(config-if)# dot1x
multiple-hosts
    
```

### 사용자 인증

[Authenticated Users](#) 페이지는 사용자 포트 액세스 목록을 표시합니다. 사용자 액세스 목록은 사용자 이름 추가 페이지에서 정의됩니다. [Authenticated Users](#) 페이지를 열려면 **Switch**→

Network Security → Authenticated Users를 클릭하십시오.

그림 7-5. 인증된 사용자



[Authenticated Users](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**User Name** — RADIUS 서버를 통해 승인된 사용자의 목록입니다.

**Port** — 사용자 이름별로 인증에 사용된 포트 번호입니다.

**Session Time** — 사용자가 장치에 로그인된 상태로 있던 시간입니다. The field format is **Day:Hour:Minute:Seconds**, for example, 3 days: 2 hours: 4 minutes: 39 seconds.

**Authentication Method** — 마지막 세션이 인증될 때 사용된 방식입니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Remote** — 사용자가 원격 서버에서 인증되었습니다.

**None** — 사용자가 인증되지 않았습니다.

**MAC Address** — 요청자 MAC 주소입니다.

### 인증된 사용자 표 표시

1. [Authenticated Users](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

**Authenticated Users Table**이 열립니다.

그림 7-6. 인증된 사용자 표

## Authenticated Users Table

Refresh

User Name	Port	Session Time	Authentication Method	MAC Address
1				

## CLI 명령을 사용하여 사용자 인증

다음 표는 [Authenticated Users](#) 페이지에 표시된 것과 같이 사용자를 인증하는 데 사용하는 해당 CLI 명령을 요약합니다.

표 7-63. 사용자 이름 CLI 명령 추가

CLI 명령	설명
show dot1x users [username username]	장치의 802.1X 사용자를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console# show dot1x users
```

```
Port Username Session Time Auth Method MAC Address
```


```
-----  
1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

## 포트 보안 구성

특정 MAC 주소를 가진 사용자만 특정 포트에 액세스할 수 있도록 제한함으로써 네트워크 보안을 강화할 수 있습니다. MAC 주소는 그 지정까지 동적으로 습득할 수 있으며 정적으로 구성할 수도 있습니다. 잠긴 포트 보안은 특정 포트에서 수신한 수신 패킷과 습득 패킷을 모두 모니터링합니다. 잠긴 포트에 대한 액세스는 특정 MAC 주소를 가진 사용자로 제한됩니다. 이 주소들은 수동으로 포트에서 정의되거나 또는 잠긴 시점까지 포트에서 습득됩니다. 잠긴 포트에서 패킷을 수신하고 패킷의 소스 MAC 주소가 해당 포트에 연관되어 있지 않은 경우(주소가 다른 포트에서 습득되었거나 시스템에 알려지지 않은 경우), 보호 메커니즘이 시동되고 다양한 옵션이 제공될 수 있습니다. 잠긴 포트에 도착한 비승인 패킷은 다음 중 한 가지 방법으로 처리됩니다.

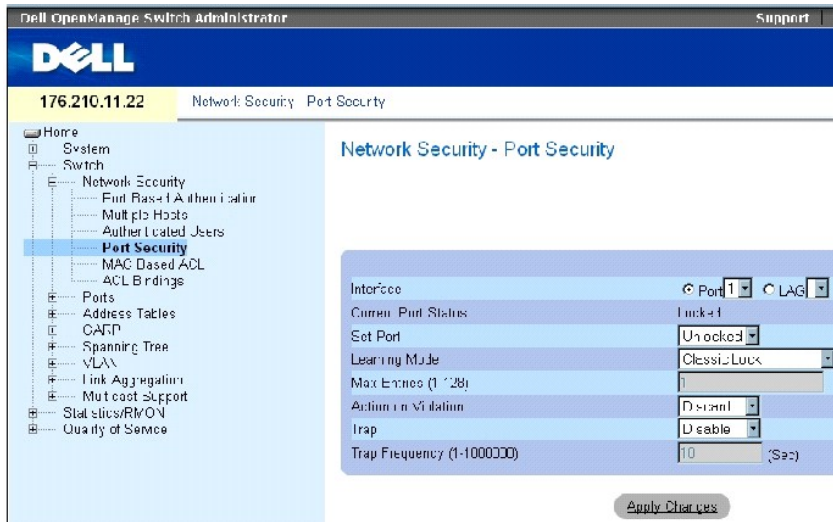
- 1 전달
- 1 트랩 없이 폐기
- 1 트랩과 함께 폐기
- 1 포트 종료

또한, 잠긴 포트 보안은 구성 파일에 MAC 주소 목록을 저장할 수 있게 합니다. MAC 주소 목록은 장치가 재설정된 후 복구할 수 있습니다.

 **주:** 포트 보안을 활성화하려면 필요한 포트에 [다중 호스트](#) 기능을 활성화합니다.

비활성화된 포트는 [Port Security](#) 페이지에서 활성화할 수 있습니다. **포트** 페이지는 스텝 제어 및 포트 미러링과 같은 고급 기능을 포함한 포트 기능을 구성하고 가상 포트 테스트를 수행하는 링크를 제공합니다. [Port Security](#) 페이지를 열려면, **Switch** → **Network Security** → **Port Security**를 클릭하십시오.

그림 7-7. 포트 보안



[Port Security](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Interface** — 잠긴 포트가 활성화된 선택된 인터페이스 종류입니다.

**Port** — 선택된 인터페이스 종류는 포트입니다.

**LAG** — 선택된 인터페이스 종류는 LAG입니다.

**Current Port Status** — 현재 구성된 포트 상태입니다.

**Set Port** — 포트가 잠겨 있거나 잠겨 있지 않습니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Unlocked** — 포트를 잠금 해제합니다. 이 값은 기본값입니다.

**Locked** — 포트를 잠급니다.

**Learning Mode** — 잠긴 포트 종류를 정의합니다. **Learning Mode** 필드는 **Set Port** 필드에 **Locked**가 선택된 경우에만 활성화됩니다. 다음과 같은 필드 값이 가능합니다.

**Classic Lock** — 전형적인 잠금 메커니즘을 사용하여 포트를 잠급니다. 이미 습득한 주소의 개수에 상관없이 포트가 즉시 잠급니다.

**Limited Dynamic Lock** — 포트와 연관된 현재 동적 MAC 주소를 삭제하여 포트를 잠급니다. 포트는 포트에 허용된 최대 개수의 주소까지 습득할 수 있습니다. 재습득된 MAC 주소 및 에이징 MAC 주소 모두가 활성화됩니다.

**Max Entries** — 포트에서 습득할 수 있는 MAC 주소의 개수를 지정합니다. **Max Entries** 필드는 **Set Port** 필드에 **Locked**가 선택된 경우에만 활성화됩니다. 또한 Limited Dynamic Lock 모드가 선택됩니다. 기본값은 1입니다.

**Action on Violation** — 잠긴 포트에 도착한 패킷에 적용될 동작입니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Forward** — 알 수 없는 소스의 패킷을 전달하나, MAC 주소는 숨겨지지 않습니다.

**Discard** — 모든 숨겨지지 않은 소스의 패킷을 폐기합니다. 이 값은 기본값입니다.

**Shutdown** — 모든 숨겨지지 않은 소스의 패킷을 폐기하고 포트를 닫습니다. 포트는 재활성화하거나 장치가 재설정될 때까지 닫힌 상태를 유지합니다.

**Trap** — 잠긴 포트에 패킷이 수신될 때 트랩을 전송하도록 합니다.

**Trap Frequency (1-1000000)** — 트랩 사이의 시간(초)입니다. 기본값은 10초입니다.

### 잠긴 포트 정의

1. [Port Security](#) 페이지를 여십시오.
2. 인터페이스 종류 및 번호를 선택합니다.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

잠긴 포트가 [포트 보안 표](#)에 추가되고 장치가 업데이트됩니다.

### 포트 보안 표 표시

1. [Port Security](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[포트 보안 표](#); 열립니다.

 **주:** 잠긴 포트는 [Port Security Table](#)에서 정의됩니다.

그림 7-8. 포트 보안 표

Port Security Table

[Refresh](#)

Port	Current Port Status	Set Port	Learning Mode	Max Entries (1-120)	Action	Trap	Trap Frequency	
1	e1	Unlocked	Locked	Classic Lock	0	Forward	Disable	0
2	e2	Unlocked	Locked	Classic Lock	0	Shutdown	Disable	0
3	e3	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
4	e4	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
5	e5	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
6	e6	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
7	e7	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
8	e8	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
9	e9	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0
10	e10	Unlocked	Unlocked	Classic Lock	0	Discard	Disable	0

[Port Security Table](#)에는 다음과 같은 추가 필드가 포함되어 있습니다.

**Unit No.** — 잠긴 포트 정보가 표시되는 스테킹 장치를 지정합니다.

**Copy Parameters from** — 매개변수를 선택된 장치 번호에 복사합니다.

## CLI 명령으로 잠긴 포트 보안 구성

다음 표는 Port Security 페이지에 표시된 것과 같이 잠긴 포트 보안을 구성하는 해당 CLI 명령을 요약합니다.

**표 7-64. 포트 보안 CLI 명령**

CLI 명령	설명
shutdown	인터페이스를 비활성화합니다.
set interface active {ethernet interface   port-channel port-channel-number}	포트 보안 원인으로 인해 종료된 인터페이스를 재활성화합니다.
port security learning {disabled   dynamic}	잠긴 포트 종류를 정의합니다.
port security max max-addr	포트에서 습득할 수 있는 MAC 주소의 개수를 지정합니다.
port security [forward   discard   discard-shutdown] [trap seconds]	인터페이스에서 새 주소 습득 기능을 잠급니다.
show ports security {ethernet interface   port-channel port-channel-number}	포트 잠금 상태를 표시합니다.

다음은 CLI 명령의 예입니다.

console # show ports security					
Port	Status	Action	Trap	Frequency	Counter
----	-----	-----	-----	-----	-----
-					-
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

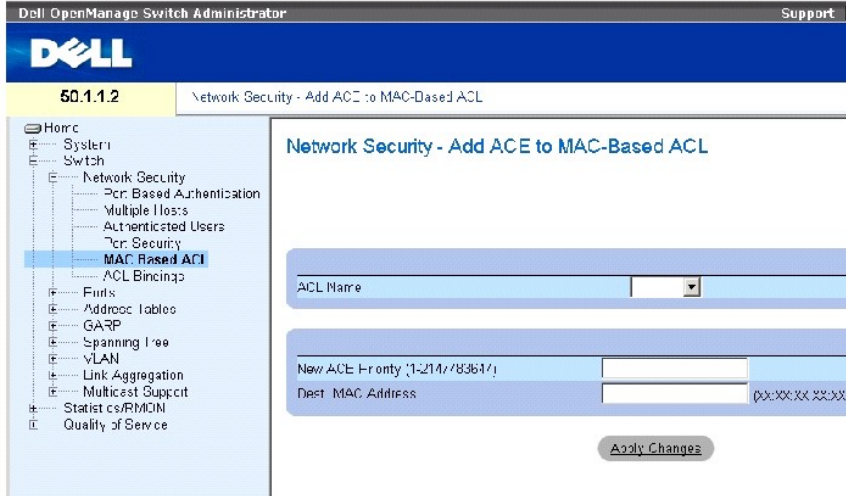
## MAC 기반 ACL 정의

엑세스 제어 목록(ACL)은 네트워크 관리자가 특정 수신 포트에 대한 분류 동작과 규칙을 정의할 수 있게 합니다. ACL은 다중 분류 규칙과 동작을 포함합니다. 각 분류 규칙 및 동작을 액세스 제어 요소(ACE)라고 합니다. ACE는 처리량 분류를 결정하는 필터입니다. MAC 기반 ACL은 비 IP를 포함한 모든 패킷에 적용됩니다. 분류 필드는 L2 필드에만 기반합니다.

[MAC Based ACL](#) 페이지에서 MAC 기반 ACL을 정의할 수 있습니다. ACL에 대한 자세한 설명은 "[MAC 기반 ACL 정의](#)"를 참조하십시오.

[MAC Based ACL](#) 페이지를 열려면, **Switch** → **Network Security** → **MAC based ACL**을 선택합니다.

**그림 7-9. MAC 기반 ACL**



[MAC Based ACL](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**ACL Name** — 사용자 정의된 ACL입니다.

**New ACE Priority (1-2147483647)** — ACL 필드에 있는 ACE 규칙의 색인입니다.

**Destination MAC Address** — 패킷이 ACE에 어드레스되는 대상 MAC 주소를 일치시킵니다.

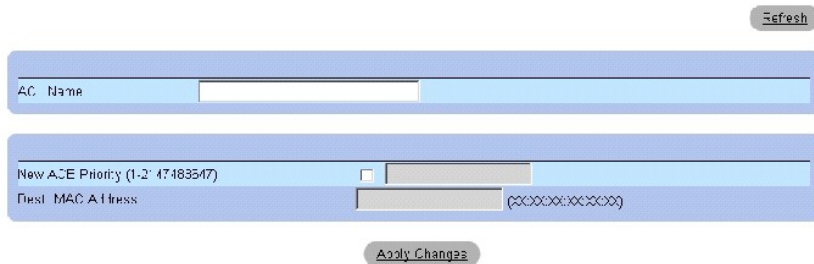
### MAC 기반 ACL 추가:

1. [MAC Based ACL](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

[MAC Based ACL](#) 페이지가 열립니다.

그림 7-10. MAC 기반 ACL 추가

### Add MAC Based ACL



3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

MAC 기반 ACL이 정의되고 장치가 업데이트됩니다.


## ACL 특정 ACE 표시

1. [MAC Based ACL](#) 페이지를 여십시오.
2. ACL을 선택합니다.
3. **Show All**을 클릭하십시오.

ACEs Associated with MAC ACL 페이지가 열립니다.

## ACL 제거

1. [MAC Based ACL](#) 페이지를 여십시오.

 **주:** ACL은 인터페이스에 연관되어 있지 않을 경우에만 제거할 수 있습니다.

2. ACL을 선택합니다.
3. **Show All**을 클릭하십시오.

ACEs Associated with MAC ACL 페이지가 열립니다.

4. **Remove ACL** 확인란을 선택합니다.

## CLI 명령을 사용하여 MAC 기반 ACE를 ACL에 지정

다음 표는 [MAC Based ACL](#) 페이지에 표시된 것과 같이 MAC 기반 ACE를 ACL에 지정하는 해당 CLI 명령을 요약합니다.

표 7-65. MAC 기반 ACE CLI 명령

CLI 명령	설명
<code>mac access-list name</code>	Layer 2 MAC ACL을 생성하고 MAC 액세스 목록 구성 모드에 들어갑니다.
<code>deny 대상</code>	MAC 기반 ACE에 정의된 조건과 일치할 경우 처리량을 거부합니다.
<code>show access-lists [이름]</code>	장치에 구성된 액세스 제어 목록을 표시합니다.

다음은 CLI 명령의 예입니다.

```
console (config)# mac access-list dell
```

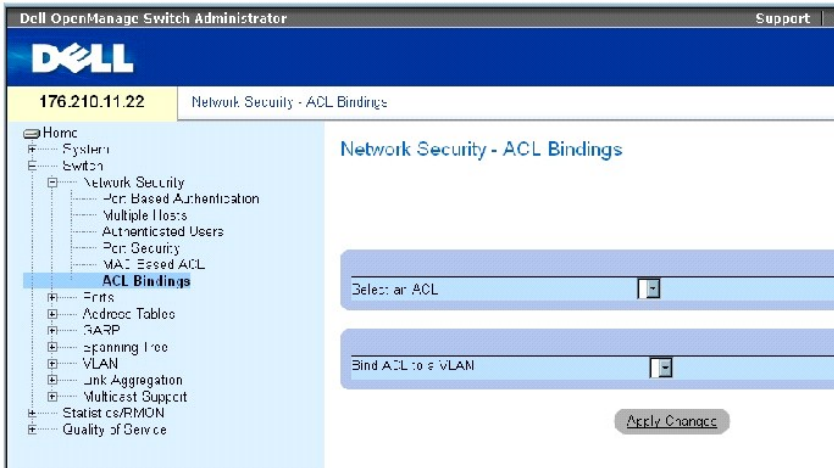
```
console (config-mac-a1)# deny 00-10-B5-F4-00-01
```

## ACL 바인딩 구성

ACL이 인터페이스에 바인딩되면 선택된 인터페이스에 ACL이 적용됩니다. [ACL Bindings](#) 페이지를 사용하여 분류 방식과 인터페이스에 ACL 목록을 지정합니다. [ACL Bindings](#) 페이지를 열려면, **Switch** → **Network Security** → **ACL Binding**을 클릭하십시오.

그림 7-11. ACL 바인딩





[ACL Bindings](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Select an ACL** — 수신 패킷과 일치시킬 ACL 종류입니다.

**Bind ACL to VLAN** — ACL이 연결된 VLAN입니다.

### 인터페이스에 ACL 지정

1. [ACL Bindings](#) 페이지를 여십시오.
2. **Select an ACL** 필드에서 ACL 종류를 선택합니다.
3. **Bind ACL to a VLAN** 필드에서 ACL이 연결된 VLAN을 선택합니다.
4. **Apply Changes**를 클릭하십시오.

ACL이 인터페이스에 연결됩니다.

### ACL 바인딩 표에서 항목 제거

1. [ACL Bindings](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

ACL 바인딩 표가 열립니다.

3. 제거해야 할 항목의 **Remove** 확인란을 선택합니다.
4. **Apply Changes**를 클릭하십시오.

선택한 항목이 표에서 제거되고 장치가 업데이트됩니다.

### ACL 바인딩 표 표시

1. [ACL Bindings](#) 페이지를 여십시오.
2. **Show All**을 클릭하여 **ACL 바인딩 표**를 여십시오.

ACL Bindings Table의 필드는 ACL 바인딩 페이지의 필드와 같습니다.

## ACL 바인딩 표의 매개변수 복사

1. [ACL Bindings](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

ACL 바인딩 표가 열립니다.

3. **Copy Parameters from** 필드에서 인터페이스를 선택합니다.
4. **VLAN** 드롭다운 메뉴에서 VLAN을 선택합니다.

해당 인터페이스에 대한 정의가 선택된 대상 포트/트렁크로 복사됩니다.

5. 편집하거나 모든 사용 가능한 포트/트렁크로 정의를 복사할 항목의 **Copy to** 확인란을 선택합니다.
6. **Select All**을 클릭하십시오.
7. **Apply Changes**를 클릭하십시오.

ACL 바인딩 표의 대상 포트/트렁크에 매개변수가 복사되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 ACL 멤버십 지정

다음 표는 ACL Binding 페이지에 표시된 것과 같이 ACL 멤버십을 지정하는 해당 CLI 명령을 요약합니다.

표 7-66. ACL 바인딩 CLI 명령

CLI 명령	설명
<code>service-acl {input acl 이름}</code>	액세스 목록을 인터페이스 입력에 적용합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# interface vlan 123
```

```
console(config-if)# service-acl input dell
```

## 포트 구성

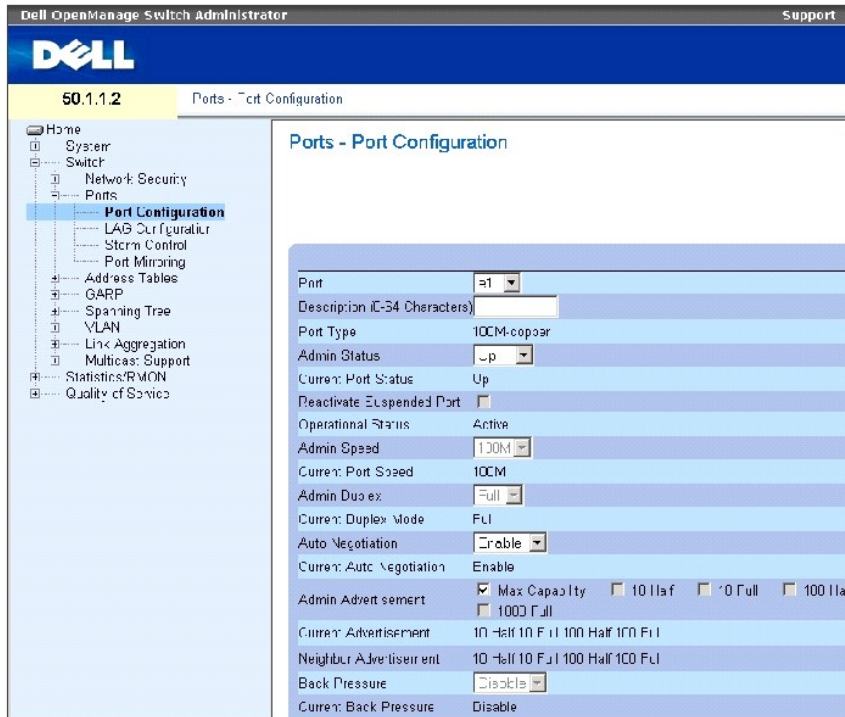
Ports 페이지는 스톱 제어 및 포트 미러링과 같은 고급 기능을 포함한 포트 기능을 구성하고 가상 포트 테스트를 수행하는 링크를 제공합니다. Ports 페이지를 열려면 **Switch** → **Ports**를 선택합니다.

## 포트 구성 정의

[Port Configuration](#) 페이지를 사용하여 포트 매개변수를 정의합니다. 포트가 LAG 구성요소일 때 포트 구성이 수정된 경우 구성 변경사항은 포트가 LAG에서 제거된 후에만 적용됩니다. [Port](#)

[Configuration](#) 페이지를 열려면 트리 보기에서 **Switch** → **Ports** → **Port Configuration**을 클릭하십시오.

그림 7-12. 포트 구성



[Port Configuration](#) 페이지는 다음과 같은 필드가 포함합니다

**Port** — 포트 매개변수가 정의된 포트 번호입니다.

**Description (0 - 64 Characters)** — 이더넷과 같은 간략한 인터페이스 설명입니다.

**Port Type** — 포트의 종류입니다.

**Admin Status** — 포트를 통한 트래픽 전달을 활성화 또는 비활성화합니다.

**Current Port Status** — 포트가 현재 작동 중인지 여부를 지정합니다.

**Reactivate Suspended Port** — 포트가 잠긴 포트 보안 옵션을 통해 비활성화된 경우 포트를 다시 활성화합니다.

**Operational Status** — 포트 작동 상태를 표시합니다. 가능한 필드 값은 다음과 같습니다.

**Suspended** — 포트가 현재 활성 상태이며 트래픽을 수신하거나 전송하고 있지 않습니다.

**Active** — 포트가 현재 활성이며 트래픽을 수신하거나 전송하고 있습니다.

**Disable** — 포트가 현재 비활성이며 트래픽을 수신하거나 전송하고 있지 않습니다.

**Admin Speed** — 포트에 대해 구성된 속도입니다. 어떤 속도 설정 옵션을 사용할 수 있는지는 포트 종류의 의해 결정됩니다. 관리 속도는 포트가 비활성일 때에만 지정할 수 있습니다.

**Current Port Speed** — 실제 동기화된 포트 속도(bps)입니다.

**Admin Duplex** — bps 단위의 포트 이중 모드입니다. **Full**은 인터페이스가 장치와 클라이언트 사이의 동시 쌍방향 전송을 지원함을 표시합니다. **Half**는 인터페이스가 장치와 클라이언트 사이에서 임의의 시점에 단방향 전송만 지원함을 표시합니다.

**Current Duplex Mode** — 동기화된 포트 이중 모드입니다.

**Auto Negotiation** — 포트의 Auto Negotiation을 활성화합니다. Auto Negotiation은 두 연결 파트너 사이의 프로토콜로서 포트가 전송 속도, 이중 모드 및 흐름 제어 능력을 파트너에게 통지할 수 있게 합니다.

**Current Auto Negotiation** — 현재 Auto Negotiation 설정입니다.

**Admin Advertisement** — 포트가 통지하는 Auto Negotiation 설정을 정의합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Max Capability** — 모든 포트 속도와 이중 모드 설정을 수락함을 표시합니다.

**10 Half** — 포트가 10mbps 속도 포트와 반이중 모드 설정을 통지함을 표시합니다.

**10 Full** — 포트가 10mbps 속도 포트와 전이중 모드 설정을 통지함을 표시합니다.

**100 Half** — 포트가 100mbps 속도 포트와 반이중 모드 설정을 통지함을 표시합니다.

**100 Full** — 포트가 100mbps 속도 포트와 전이중 모드 설정을 통지함을 표시합니다.

**1000 Full** — 포트가 1000mbps 속도 포트와 전이중 모드 설정을 통지함을 표시합니다.

**Current Advertisement** — 조정 프로세스를 시작하기 위해 포트가 자체 속도를 주변 포트에 통지합니다. 필드 값으로는 Admin Advertisement 필드에 지정된 값이 가능합니다.

**Neighbor Advertisement** — 주변 포트의 통지 설정을 표시합니다. 필드 값은 Admin Advertisement field values와 동일합니다.

**Back Pressure** — 포트에 배압 모드를 사용합니다. 배압 모드는 반이중 모드와 함께 사용되어 포트가 메시지를 수신할 수 없게 합니다. 배압 기능은 OOB 포트에는 지원되지 않습니다.

**Current Back Pressure** — 현재 배압 설정입니다.

**Flow Control** — 흐름 제어를 활성화 또는 비활성화하거나 포트에서 흐름 제어의 자동 조정을 활성화합니다.

**Current Flow Control** — 현재 흐름 제어 설정입니다.

**MDI/MDIX** — 장치가 교차 케이블 또는 비교차 케이블 여부를 판별하게 합니다. 허브와 스위치는 엔드 스테이션에 연결되었을 때 직선 통과 이더넷 케이블을 사용할 수 있고 배선 쌍이 적절하게 일치하도록 엔드 스테이션의 배선과 의도적으로 반대 방향으로 배선되어 있습니다. 두 개의 허브/스위치가 서로 연결되거나 두 개의 엔드 스테이션이 서로 연결될 때는 올바른 쌍이 연결되도록 교차 케이블이 사용됩니다. **Auto MDIX**는 자동 조정이 비활성인 경우 **FE** 포트에 작동하지 않습니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Auto** — 케이블 종류를 자동으로 감지하는 경우에 사용됩니다.

**MDIX** — 허브 및 스위치에 사용됩니다.


**MDI** — 엔드 스테이션에 사용됩니다.

**Current MDI/MDIX** — 현재 장치 MDIX 설정을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**MDI** — 현재 MDI 설정이 MDI입니다.

**MDIX** — 현재 MDI 설정이 MDIX입니다.

**LAG** — 포트가 LAG의 일부인지 여부를 지정합니다.

 **주:** 포트가 LAG 구성원일 때 포트 구성이 수정된 경우 구성 변경 내용은 포트가 LAG에서 제거된 후에만 적용됩니다.

## 포트 매개변수 정의

1. [Port Configuration](#) 페이지를 여십시오.
2. **Port** 필드에서 포트를 선택하십시오.
3. 대화상자에서 사용 가능한 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

포트 매개변수가 장치에 저장됩니다.

## 포트 표 표시

1. [Port Configuration](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

**Port Configuration Table**이 열립니다.

그림 7-13. 포트 구성 표

Port Configuration Table Refresh

Unit Number:

Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	Auto MDIX	LAG
1/0/1	Ethernet	Up	1000	Full	Enabled	Enabled	Enabled	MDI	

Apply Changes

## CLI 명령으로 포트 구성

다음 표는 [Port Configuration](#) 페이지에 표시된 것과 같이 포트를 구성할 수 있는 해당 CLI 명령을 요약합니다.

표 7-67. 포트 구성 CLI 명령

CLI 명령	설명
<code>interface ethernet 인터페이스</code>	이더넷 종류 인터페이스를 구성하기 위해 인터페이스 구성 모드를 실행합니다.
<code>description 문자열</code>	인터페이스 구성에 설명을 추가합니다.
<code>shutdown</code>	현재 설정된 내용의 일부인 인터페이스를 비활성화합니다.
<code>set interface active {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	보안 이유로 인해 종료된 인터페이스를 다시 활성화합니다.
<code>speed Mbps</code>	자동 조정을 사용하지 않을 경우에 해당 이더넷 인터페이스의 속도를 구성합니다.
<code>duplex {half   full}</code>	자동 조정을 사용하지 않을 경우에 해당 이더넷 인터페이스의 전이중/반이중 작동을 구성합니다.
<code>negotiation [capability1 [capability2...capability5]</code>	주어진 인터페이스의 속도 및 이중 모드 매개변수에 대해 자동 조정 작동을 활성화합니다.
<code>back-pressure</code>	주어진 인터페이스에 배압을 활성화합니다.
<code>flowcontrol {auto   on   off }</code>	해당 인터페이스의 흐름 제어를 구성합니다.
<code>mdix {on   auto}</code>	주어진 인터페이스 또는 포트 채널에 자동 교차를 활성화합니다.
<code>show interfaces configuration [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	모든 구성된 인터페이스에 대한 구성을 표시합니다.
<code>show interface advertise</code>	인터페이스의 조정 통지 설정을 표시합니다.
<code>show interfaces status [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	모든 구성된 인터페이스의 상태를 표시합니다.
<code>show interfaces description [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	모든 구성된 인터페이스의 설명을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# interface ethernet 1/e3

console(config-if)# description "RD SW#3"

console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure

console(config-if)# flowcontrol on

console(config-if)# mdix auto

```

```
console(config-if)# end
```

```
console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

```
Console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

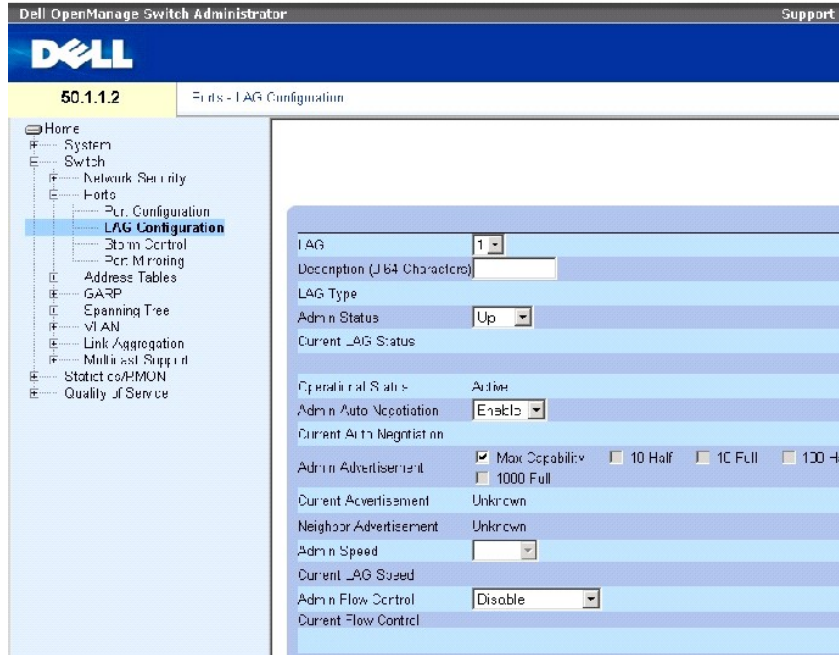
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State
1	1000	Full	1000	Off	Off	Disable	Up

## LAG 매개변수 정의

[LAG 구성](#) 페이지는 구성된 LAG에 대한 매개변수를 구성할 수 있는 필드를 포함합니다. 본 장치는 LAG 당 최대 8개의 포트, 시스템 당 최대 8개의 LAG를 지원합니다. LAG(링크 결함 그룹)에 대한 정보와 포트를 LAG에 지정하는 방법에 대한 자세한 내용은 [포트 결합](#)을 참조하십시오.

[Port Configuration](#) 페이지를 열려면, 트리 보기에서 **Switch**→**Ports**→**LAG Configuration**을 클릭하십시오.

그림 7-14. LAG 구성



[LAG Configuration](#) 페이지는 다음과 같은 필드를 포함합니다.

**LAG** — LAG 번호입니다.

**Description (0 - 64 Characters)** — 구성된 LAG의 사용자 정의된 설명을 제공합니다.

**LAG Type** — LAG를 구성하는 포트 종류입니다.

**Admin Status** — 선택한 LAG를 활성화 또는 비활성화합니다.

**Current LAG Status** — LAG가 현재 작동 중인지 여부를 표시합니다.

**Operational Status** — 선택한 LAG를 통한 트래픽 전달을 활성화 또는 비활성화합니다.

**Admin Auto Negotiation** — LAG의 Auto Negotiation을 활성화 또는 비활성화합니다. Auto Negotiation은 두 연결 파트너 사이의 프로토콜로서 LAG가 전송 속도, 이중 모드 및 흐름 제어(흐름 제어 기본값은 비활성) 능력을 상대 파트너에게 통지할 수 있게 합니다.

**Current Auto Negotiation** — 현재 구성된 Auto Negotiation 설정입니다.

**Admin Advertisement** — LAG가 통지하는 Auto Negotiation 설정을 정의합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Max Capability** — 모든 LAG 속도와 이중 모드 설정을 수락함을 표시합니다.

**10 Half** — LAG가 10Mbps 속도 LAG와 반이중 모드 설정을 통지함을 표시합니다.



**10 Full** — LAG가 10mbps 속도 LAG와 전이중 모드 설정을 통지함을 표시합니다.

**100 Half** — LAG가 100mbps 속도 LAG와 반이중 모드 설정을 통지함을 표시합니다.

**100 Full** — LAG가 100mbps 속도 LAG와 전이중 모드 설정을 통지함을 표시합니다.

**1000 Full** — LAG가 1000mbps 속도 LAG와 전이중 모드 설정을 통지함을 표시합니다.

**Current Advertisement** — 조정 프로세스를 시작하기 위해 LAG가 자체 속도를 주변 LAG에 통지합니다. 필드 값으로는 Admin Advertisement 필드에 지정된 값이 가능합니다.

**Neighbor Advertisement** — 주변 LAG의 통지 설정을 표시합니다. 필드 값은 Admin Advertisement field values와 동일합니다.

**Admin Speed** — LAG가 작동하는 속도입니다.

**Current LAG Speed** — LAG가 작동하는 현재 속도입니다.

**Admin Flow Control** — 흐름 제어를 활성화 또는 비활성화하거나 LAG에서 흐름 제어의 자동 조정을 활성화합니다. 흐름 제어 모드는 LAG에서 전이중으로 작동하는 포트에 효과적입니다.

**Current Flow Control** — 사용자 지정된 흐름 제어 설정입니다.

## LAG 매개변수 정의

1. [LAG Configuration](#) 페이지를 여십시오.
2. LAG 필드에서 LAG를 선택하십시오.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

LAG 매개변수가 장치에 저장됩니다.

## LAG 매개변수 수정

1. [LAG Configuration](#) 페이지를 여십시오.
2. LAG 필드에서 LAG를 선택하십시오.
3. 필드를 수정합니다.
4. **Apply Changes**를 클릭하십시오.

LAG 매개변수가 장치에 저장됩니다.

## LAG 구성 표 표시

1. [LAG Configuration](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

[LAG Configuration Table](#)이 열립니다.

그림 7-15. LAG 구성 표

LAG Configuration Table

[Refresh](#)

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Flow Control
1	1		Up		Enable	Disable
2	2		Up		Enable	Disable
3	3		Up		Enable	Disable
4	4		Up		Enable	Disable
5	5		Up		Enable	Disable
6	6		Up		Enable	Disable
7	7		Up		Enable	Disable
8	8		Up		Enable	Disable

[Apply Changes](#)

CLI 명령으로 LAG 구성

다음 표는 [LAG Configuration](#) 페이지에 표시된 것과 같이 LAG를 구성할 수 있는 해당 CLI 명령을 요약합니다.

표 7-68. LAG 구성 CLI 명령

CLI 명령	설명
<code>interface port-channel 포트-채널-번호</code>	특정 포트 채널의 인터페이스 구성 모드를 실행합니다.
<code>description 문자열</code>	인터페이스 구성에 설명을 추가합니다.
<code>shutdown</code>	현재 설정된 내용의 일부인 인터페이스를 비활성화합니다.
<code>speed bps</code>	자동 조정을 사용하지 않을 경우에 해당 이더넷 인터페이스의 속도를 구성합니다.
<code>negotiation [capability1 [capability2...capability5]</code>	인터페이스 속도 자동 조정 동작을 활성화합니다.
<code>back-pressure</code>	주어진 인터페이스에 배압을 활성화합니다.
<code>flowcontrol {auto   on   off }</code>	해당 인터페이스의 흐름 제어를 구성합니다.
<code>show interfaces configuration [ ethernet 인터페이스   port-channel 포트-채널-번호 ]</code>	모든 구성된 인터페이스에 대한 구성을 표시합니다.
<code>show interfaces status [ ethernet 인터페이스   port-channel 포트-채널-번호 ]</code>	모든 구성된 인터페이스의 상태를 표시합니다.
<code>show interfaces description [ ethernet 인터페이스   port-channel 포트-채널-번호 ]</code>	모든 구성된 인터페이스의 설명을 표시합니다.
<code>show interfaces port-channel [ 포트-채널-번호 ]</code>	포트 채널 정보를 표시합니다(어느 포트가 해당 포트 채널의 구성원인지 및 현재 이 포트들이 활성화 여부).

다음은 CLI 명령의 예입니다.

```
console(config)# interface port-channel 2

console(config-if)# no negotiation
```

```

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel

```

Channel	Ports
-----	-----
ch1	Inactive: 1/e(11-13)
ch2	Active: 1/e14

## 스톡 제어 활성화

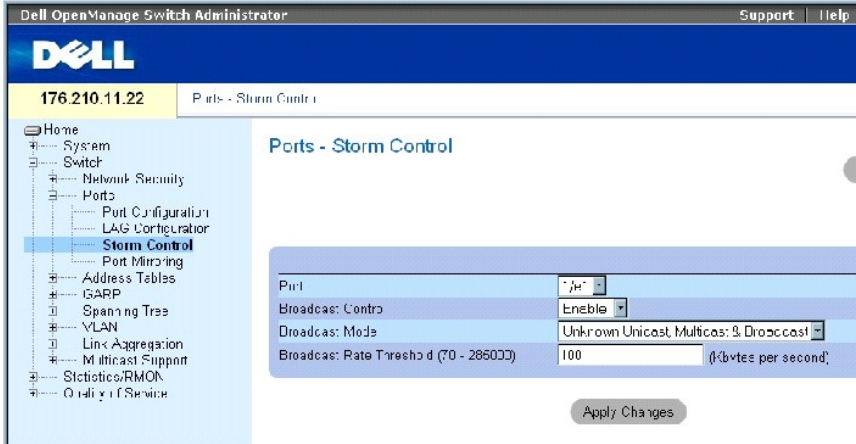
브로드캐스트 스톡은 단일 포트에 의해 네트워크에 과도한 양의 브로드캐스트 메시지가 동시에 전송됨으로써 발생하는 결과입니다. 전달된 메시지 응답은 네트워크에 누적되어 네트워크 자원에 과부하를 가하거나 네트워크 시간 초과를 야기합니다.

스톡 제어는 패킷 종류와 전송되는 패킷 속도를 정의하여 포트 별로 활성화됩니다.

시스템은 수신되는 브로드캐스트, 유니캐스트 및 멀티캐스트 프레임 속도를 포트 별로 개별적으로 측정하고 사용자 정의된 속도를 초과하면 프레임을 폐기합니다.

[Storm Control](#) 페이지는 스톡 제어를 활성화하고 구성할 수 있는 필드를 제공합니다. [Storm Control](#) 페이지를 열려면 트리 뷰에서 **Switch** → **Ports** → **Storm Control**을 클릭하십시오.

그림 7-16. 스톡 제어



[Storm Control](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Port** — 스톰 제어가 활성화된 포트입니다.

**Broadcast Control** — 특정 인터페이스의 브로드캐스트 패킷 종류 전달을 활성화 또는 비활성화합니다.

**Broadcast Mode** — 장치 또는 스왑에 현재 활성화된 브로드캐스트 모드를 지정합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Unknown Unicast, Multicast & Broadcast** — 유니캐스트, 멀티캐스트 및 브로드캐스트 소용량을 계산합니다

**Multicast & Broadcast** — 브로드캐스트 및 멀티캐스트 소용량을 함께 계산합니다.

**Broadcast Only** — 브로드캐스트 소용량만 계산합니다.

**Broadcast Rate Threshold (70-285000)** — 미지의 패킷이 전달되는 최대 속도(킬로바이트/초)입니다. 필드 범위는 초당 70~285000킬로바이트입니다.

## 스톰 제어 활성화

1. [Storm Control](#) 페이지를 여십시오
2. 스톰 제어를 구현할 인터페이스를 선택하십시오.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

스톰 제어가 활성화됩니다.

## 스톰 제어 포트 매개변수 수정

1. [Storm Control](#) 페이지를 여십시오.
2. 필드를 수정합니다.
3. **Apply Changes**를 클릭하십시오.+

스톱 제어 포트 매개변수가 장치에 저장됩니다.

## 포트 매개변수 표 표시

1. [Storm Control](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[Storm Control Settings Table](#)이 열립니다.

그림 7-17. 스톱 제어 설정 표

-refresh

Copy Parameters from Port

Port	Broadcast Control	Broadcast Mode	Broadcast Rate Threshold	Copy to Select All
e1	Disable	Broadcast Only	100	<input type="checkbox"/>
e2	Disable	Broadcast Only	100	<input type="checkbox"/>
e3	Disable	Broadcast Only	100	<input type="checkbox"/>
e4	Disable	Broadcast Only	100	<input type="checkbox"/>
e5	Disable	Broadcast Only	100	<input type="checkbox"/>
e6	Disable	Broadcast Only	100	<input type="checkbox"/>
e7	Disable	Broadcast Only	100	<input type="checkbox"/>
e8	Disable	Broadcast Only	100	<input type="checkbox"/>
e9	Disable	Broadcast Only	100	<input type="checkbox"/>
e10	Disable	Broadcast Only	100	<input type="checkbox"/>
e11	Disable	Broadcast Only	100	<input type="checkbox"/>
e12	Disable	Broadcast Only	100	<input type="checkbox"/>
e13	Disable	Broadcast Only	100	<input type="checkbox"/>
e14	Disable	Broadcast Only	100	<input type="checkbox"/>
e15	Disable	Broadcast Only	100	<input type="checkbox"/>
e16	Disable	Broadcast Only	100	<input type="checkbox"/>

[Storm Control](#) 페이지의 필드 외에 [Storm Control Settings Table](#)는 다음과 같은 추가 필드를 포함합니다.

**Copy Parameters from Port** — 스톱 제어 매개 변수가 복사된 특정 포트를 지정합니다.

## 스톱 제어 설정 표에 매개변수 복사

1. [Storm Control](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

[Storm Control Settings Table](#)이 열립니다.

3. **Copy Parameters from Port** 필드에서 설정이 복사되는 포트를 선택하십시오.
4. **Copy to** 확인란을 선택하여 스톱 제어 정의를 복사할 대상 인터페이스를 정의하거나 **Select All**을 선택하여 모든 포트에 정의를 복사하십시오.
5. **Apply Changes**를 클릭하십시오.

[Storm Control Settings Table](#)의 선택 포트에 매개변수가 복사되고 장치가 업데이트됩니다.

## CLI 명령으로 스톱 제어 구성

다음 표는 [Storm Control](#) 페이지에 표시된 것과 같이 스톰 제어를 구성할 수 있는 해당 CLI 명령을 요약합니다.

표 7-69. 스톰 제어 CLI 명령

CLI 명령	설명
port storm-control include-multicast	장치가 멀티캐스트, 유니캐스트 및 브로드캐스트 패킷을 함께 계산할 수 있게 합니다.
port storm-control broadcast enable	브로드캐스트 스톰 제어를 활성화합니다.
port storm-control broadcast rate	최대 브로드캐스트 속도를 구성합니다.
show ports storm-control <b>포트</b>	스톰 제어 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# port
storm-control include-
multicast

console(config)# interface
ethernet 1/e1

console(config-if)# port
storm-control broadcast
enable

console(config-if)# port
storm-control broadcast
rate 100000

console(config-if)# end

console# show ports storm-
control

```

Port	Broadcast Storm control [kbytes/sec]
----	-----
-	-----
1/e1	8000
2/e1	Disabled
3/e2	Disabled

## 포트 미러링 세션 정의

포트 미러링으로 다음과 같은 기능을 수행할 수 있습니다.

- 1 일정 포트에서 보내고 받은 패킷의 사본을 모니터링 포트에 전달하여 네트워크 트래픽을 모니터링하고 미러링합니다.
- 1 진단 도구 및/또는 디버깅 기능으로 사용할 수 있습니다.
- 1 장치 성능 및 모니터링을 활성화합니다.

포트 미러링은 모든 패킷을 복사할 대상 특정 포트와 패킷이 복사될 다른 포트를 선택하여 구성됩니다.

포트 미러링을 구성하기 전에 다음과 같은 사항을 참고하십시오.

- 1 포트 미러링은 모니터링된 포트에서 보내고 받은 패킷의 사본을 모니터링 포트로 전달하여 네트워크 처리량을 모니터링하고 미러링합니다.
- 1 모니터링된 포트는 모니터링하는 포트보다 더 빨리 작동할 수 없습니다.
- 1 모든 RX/TX 패킷은 같은 포트에서 모니터링되어야 합니다.

대상 포트로 구성된 포트에는 다음과 같은 제한 사항이 적용됩니다.

- 1 포트는 원본 포트로 구성될 수 없습니다.
- 1 포트는 LAG 구성원이 될 수 없습니다.
- 1 포트에 IP 인터페이스가 구성되지 않았습니다.
- 1 포트에 GVRP가 활성화되지 않았습니다.
- 1 포트가 VLAN 구성원이 아닙니다.
- 1 하나의 대상 포트만 정의할 수 있습니다.

원본 포트로 구성된 포트에는 다음과 같은 제한 사항이 적용됩니다.

- 1 원본 포트는 LAG 구성원이 될 수 없습니다.
- 1 포트는 대상 포트로 구성될 수 없습니다.
- 1 최대 8개의 원본 포트가 지원됩니다.

[Port Mirroring](#) 페이지를 열려면, 트리 보기에서 **Switch**→**Ports**→**Port Mirroring**을 클릭하십시오.


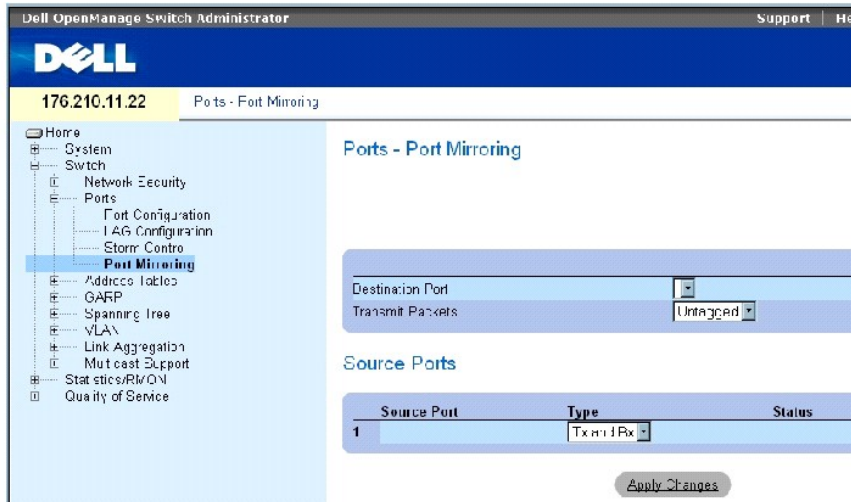
 **주:** 포트가 포트 미러링 세션을 위한 대상 포트로 설정되면 해당 포트의 모든 정상 작동은 중지됩니다. 여기에는 스페닝 트리 및 LACP가 포함됩니다.

그림 7-18. 포트 미러링



[Port Mirroring](#) 페이지는 다음과 같은 필드를 포함합니다.

**Destination Port** — 포트 트래픽이 복사될 대상 포트 번호입니다.

**Transmit Packets** — 패킷이 미러링되는 방식을 정의합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Untagged** — 패킷을 태그 없는 vlan 패킷으로 미러링합니다. 이 값은 기본값입니다.

**Tagged** — 패킷을 태그 있는 vlan 패킷으로 미러링합니다.

**Type** — 미러링된 패킷이 RX, TX 또는 RX 및 TX 모두인지 여부를 표시합니다.

**Status** — 포트가 현재 모니터링되는지(**Active**) 또는 모니터링 되지 않는지(**Ready**) 여부를 표시합니다.

**Remove** — 이 항목을 선택하면 포트 미러링 세션이 제거됩니다.

## 포트 미러링 세션 추가

1. [Port Mirroring](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

원본 포트 추가 페이지가 열립니다.

3. **Source Port**와 **Type** 필드를 정의합니다.
4. **Apply Changes**를 클릭하십시오.
5. **Destination Port** 드롭다운 메뉴에서 대상 포트를 선택합니다.
6. [포트 미러링](#) 페이지에서 **Refresh** 단추를 클릭하십시오.
7. **Tagged Packets** 필드를 정의합니다.
8. **Type** 필드를 정의합니다.
9. **Apply Changes**를 클릭하십시오.



새 원본 포트가 정의되고 장치가 업데이트됩니다.

### 포트 미러링 세션에서 사본 포트 삭제

1. [Port Mirroring](#) 페이지를 여십시오.
2. **Remove** 확인란을 선택합니다.
3. **Apply Changes**를 클릭하십시오.

선택한 포트 미러링 세션이 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 포트 미러링 세션 구성

다음 표는 [Port Mirroring](#) 페이지에 표시된 것과 같이 포트 미러링 세션을 구성하는 동등한 CLI 명령을 요약합니다.

표 7-70. 포트 미러링 CLI 명령

CLI 명령	설명
<code>port monitor src-interface [rx   tx]</code>	포트 모니터링 세션을 시작합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# interface ethernet
1/e1

console(config-if)# port monitor 1/e2

console(config-if)# end

console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
-----	-----	----	-	-----
1/e2	1/e1	RX, TX	Active	No

---

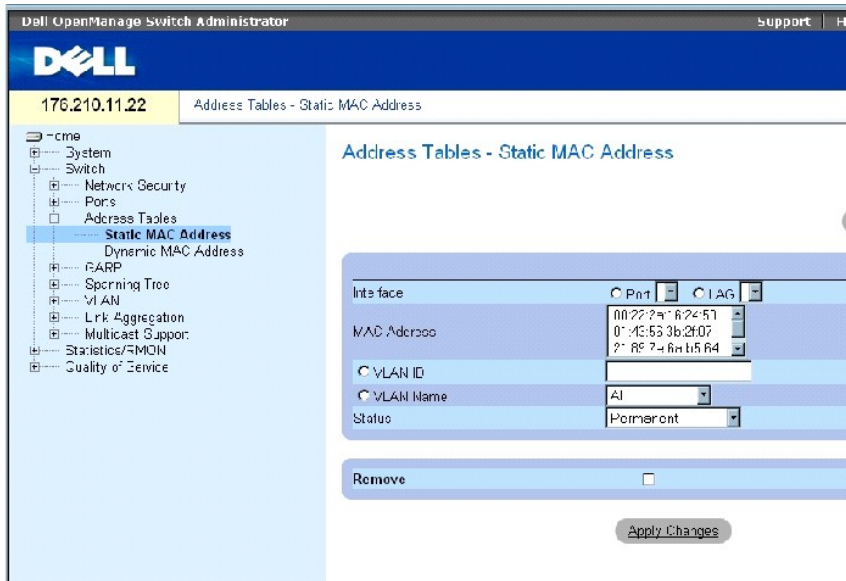
### 주소 표 구성

MAC 주소는 정적 주소 또는 동적 주소 데이터베이스에 저장되어 있습니다. 데이터베이스 중 하나에 저장된 대상에 주소 지정된 패킷은 포트에 즉시 전달됩니다. 동적 주소 표는 인터페이스, VLAN 및 MAC 주소별로 저장될 수 있습니다. MAC 주소는 원본으로부터의 패킷이 장치에 전송되면 동적으로 습득됩니다. 프레임 원본 주소에서 포트를 습득함으로써 주소는 포트와 연결됩니다. 포트와 연결되지 않은 대상 MAC 주소에 전송된 프레임은 관련 VLAN의 모든 포트에 새도합니다. 정적 주소는 수동으로 구성합니다. 브리지 표에 오버플로우되는 것을 방지하기 위해 일정 기간 동안 처리량이 없는 동적 MAC 주소가 지워집니다. 주소 표 페이지를 열려면 트리 뷰에서 Switch → Address Tables를 클릭하십시오.

## 정적 주소 정의

[Static MAC Address Table](#) 페이지는 정적 MAC 주소 목록을 포함합니다. 정적 주소는 [Static MAC Address Table](#) 페이지에서 추가하거나 제거할 수 있습니다. 또한, 여러 MAC 주소를 단일 포트에 정의할 수 있습니다. [Static MAC Address Table](#) 페이지를 열려면 트리 뷰에서 Switch → Address Tables → Static Address Table을 차례로 클릭하십시오.

그림 7-19. 정적 MAC 주소 표



[Static MAC Address Table](#) 페이지에는 다음과 같은 필드가 포함됩니다.

**Interface** — 정적 MAC 주소가 적용된 특정 포트 또는 LAG입니다.

**MAC Address** — 현재 정적 주소 목록에 나열된 MAC 주소입니다.

**VLAN ID** — MAC에 연결된 VLAN ID입니다.

**VLAN Name** — 사용자 정의된 VLAN 이름입니다.


**Status** — MAC 주소 상태입니다. 다음과 같은 값을 가질 수 있습니다.

**Secure** — 잠긴 포트에 정적 MAC 주소를 정의하는 데 사용됩니다.

**Permanent** — MAC 주소가 영구적입니다.

**Delete on Reset** — 장치를 재설정하면 MAC 주소가 삭제됩니다.

**Delete on Timeout** — 시간 초과가 발생하면 MAC 주소가 삭제됩니다.

 **주:** 이더넷 장치를 재설정할 때 정적 MAC 주소가 삭제되는 것을 방지하려면 MAC 주소에 연결된 포트가 잠겨있는지 확인하십시오.

**Remove** — 이 항목을 선택하면 선택한 MAC 주소를 MAC 주소 표에서 제거합니다.

## 정적 MAC 주소 추가

1. [정적 MAC 주소 표](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

정적 MAC 주소 추가 페이지가 열립니다.

3. 필드를 작성합니다.
4. **Apply Changes**를 클릭하십시오.

정적 MAC 주소 표에 새 정적 주소가 추가되며 장치가 업데이트됩니다.

## 정적 주소 표의 정적 주소 설정 수정

1. [Static MAC Address Table](#) 페이지를 여십시오.
2. 인터페이스를 선택합니다.
3. 필드를 수정합니다.
4. **Apply Changes**를 클릭하십시오.

정적 MAC 주소가 수정되고 장치가 업데이트됩니다.

## 정적 주소 표에서 정적 주소 제거

1. [Static MAC Address Table](#) 페이지를 여십시오.
2. 인터페이스를 선택합니다.
3. **Show All**를 클릭하십시오.

정적 MAC 주소 표가 열립니다.

4. 표 항목을 선택합니다.
5. **Remove** 확인란을 선택합니다.
6. **Apply Changes**를 클릭하십시오.

선택한 정적 주소가 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 정적 주소 매개변수 구성

다음 표는 [Static MAC Address Table](#) 페이지에 표시된 것과 같이 정적 주소 매개변수를 구성하는 동등 CLI 명령을 요약합니다.

표 7-71. 정적 주소 CLI 명령

CLI 명령	설명
bridge address mac주소 [permanent   delete-on-reset   delete-on-timeout   secure] [ethernet interface   port-channel 포트-채널-번호]	정적 MAC 층 스테이션 원본 주소를 브리지 표에 추가합니다.
show bridge address-table [vlan vlan] [ethernet 인터페이스   port-channel 포트-채널-번호]	브리지 전달 데이터베이스의 항목을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec


```

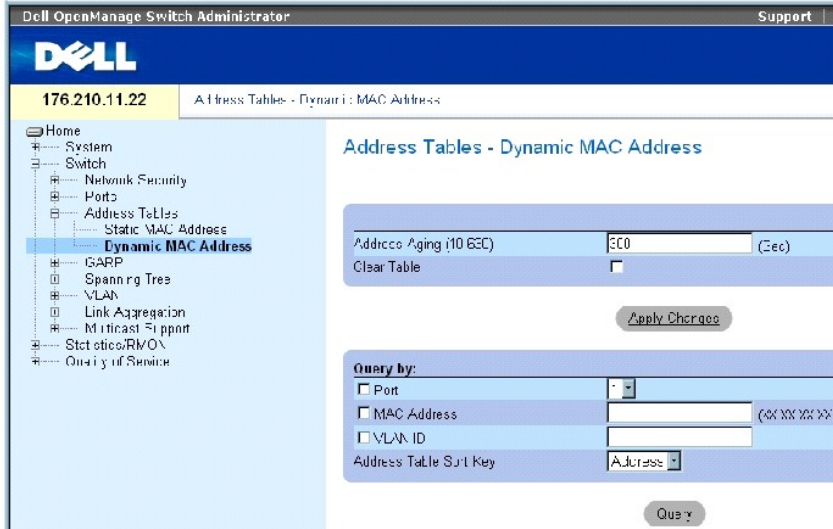
vlan	mac address	port	type
----	-----	----	-----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

### 동적 주소 보기

[Dynamic MAC Address](#)는 인터페이스 종류, MAC 주소, VLAN 및 표 정렬을 포함한 동적 주소 표의 정보를 문의하는 데 대한 정보를 포함합니다. 주소 표에 저장된 주소로 전달된 패킷은 해당 포트로 직접 전달됩니다. 또한, [Dynamic MAC Address](#) 페이지는 동적 MAC 주소가 지워지기 전까지의 수명 시간에 대한 정보를 포함하고 동적 주소 목록을 문의하여 보기 위한 매개변수를 포함합니다. 현재 주소 표는 패킷이 포트에 직접 전달되는 동적 주소 매개변수를 포함합니다.

[Dynamic MAC Address](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **Address Tables** → **Dynamic MAC Address**를 클릭하십시오.

그림 7-20. 동적 MAC 주소



[Dynamic MAC Address](#) 페이지에는 다음과 같은 필드가 포함됩니다.

**Address Aging(10-630)** — 원본으로부터의 처리량이 감지되지 않을 경우 MAC 주소가 시간 초과될 때까지 [Dynamic MAC Address](#)에 유지되는 시간을 지정합니다. 기본값은 300초입니다.

**Clear Table** — 이 항목을 선택하면 동적 주소 표가 지워집니다.

**Port** — 표가 문의되는 인터페이스를 지정합니다. 두 가지 인터페이스 종류 중에서 선택할 수 있습니다.

**MAC Address** — 표가 문의되는 MAC 주소를 지정합니다.

**VLAN ID** — 표가 문의되는 VLAN ID입니다.

**Address Table Sort Key** — 동적 주소 표가 정렬되는 방식을 지정합니다. 주소 표는 주소, VLAN 또는 인터페이스별로 정렬할 수 있습니다.

## 수명 시간 재지정

1. [Dynamic MAC Address](#)를 여십시오.
2. **Aging Time** 필드를 정의합니다.
3. **Apply Changes**를 클릭하십시오.

수명 시간이 수정되고 장치가 업데이트됩니다.

## 동적 주소 표 문의

1. [Dynamic MAC Address](#)를 여십시오.
2. **동적 주소 표**를 문의할 매개변수를 정의합니다.

항목은 **포트**, **MAC 주소** 또는 **VLAN ID**별로 문의될 수 있습니다.

3. **Query**를 클릭하십시오.

[동적 MAC 주소](#)가 문의됩니다.

### 동적 주소 표 정렬

1. [동적 MAC 주소](#)를 여십시오.
2. **Address Table Sort Key** 드롭다운 메뉴에서 주소를 주소, VLAN ID 또는 인터페이스별로 정렬할지 선택합니다.
3. **Query**를 클릭하십시오.

[동적 MAC 주소](#)가 정렬됩니다.

### CLI 명령을 사용하여 동적 주소 문의 및 정렬

다음 표는 [동적 MAC 주소](#)에 표시된 것과 같이 동적 주소를 수명 지정, 문의 및 정렬하는 동등한 CLI 명령을 요약합니다.

표 7-72. 문의 및 정렬 CLI 명령

CLI 명령	설명
bridge aging-time 초	주소 표 수명 시간을 설정합니다.
show bridge address-table [vlan vlan] [ethernet 인터페이스   port-channel 포트-채널-번호]	브리지 전달 데이터베이스의 동적으로 작성된 항목의 등급을 표시합니다.

다음은 CLI 명령의 예입니다.

```
console (config)# bridge aging-time 250

console (config)# end

console# show bridge address-table
```

Aging time is 250 sec			
vlan	mac address	port	type
----	-----	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

---

## GARP 구성

GARP(일반 특정 등록 프로토콜)은 모든 네트워크 연결 또는 멤버십 스타일 정보를 등록하는 범용 프로토콜입니다. GARP는 VLAN 또는 멀티캐스트 주소와 같은 주어진 네트워크 특성에 관한 장치 집합을 정의합니다.

GARP를 구성할 때 다음과 같은 사항을 확인합니다.

1. 나가기 시간은 참가 시간의 3배 이상이어야 합니다.
1. 전체 나가기 시간은 나가기 시간보다 커야 합니다.
1. 모든 총 2 연결 장치에 같은 GARP 타이머 값을 설정합니다. GARP 타이머가 총 2 연결 장치에 다르게 설정된 경우 GARP 응용프로그램이 제대로 작동하지 않습니다.

GARP 페이지를 열려면 트리 뷰에서 Switch→GARP를 클릭하십시오.

## GARP 타이머 정의

GARP Timers 페이지는 장치에 GARP를 활성화하기 위한 필드를 포함합니다. [GARP Timers](#) 페이지를 열려면, 트리 뷰에서 Switch→GARP→GARP Timers를 클릭하십시오.

그림 7-21. GARP 타이머



GARP Timers 페이지에는 다음과 같은 필드가 포함됩니다.

Interface — GARP 타이머 편집을 위한 포트 또는 LAG를 선택합니다.

GARP Join Timer(10 - 2147483640) (Msec)— PDU가 전송되는 시간(밀리초)입니다. 기본값은 200밀리초입니다.

GARP Leave Timer(10 - 2147483640) (Msec)— 장치가 GARP 상태에서 나갈 때까지 기다리는 경과 시간(밀리초)입니다. 나가기 시간은 전송/수신된 전체 나가기 시간 메시지에 의해 활성화되며 수신된 참가 메시지에 의해 취소됩니다. 나가기 시간은 참가 시간의 3배 이상이어야 합니다. 기본값은 600밀리초입니다.

GARP Leave All Timer(10 - 2147483640) (Msec) — 모든 장치가 GARP 상태에서 나갈 때까지 기다리는 경과 시간(밀리초)입니다. 전체 나가기 시간은 나가기 시간보다 커야 합니다. 기본값은 10000밀리초입니다.

## GARP 타이머 정의

1. [GARP Timers](#) 페이지를 여십시오.
2. 인터페이스를 선택합니다.

- 필드를 작성합니다.
- Apply Changes**를 클릭하십시오.

GARP 매개변수가 장치에 저장됩니다.

### GARP 타이머 표의 매개변수 복사

- [GARP Timers](#) 페이지를 여십시오.
- Show All**를 클릭하십시오.

GARP 타이머 표가 열립니다.

- Copy Parameters from** 필드에서 인터페이스 종류를 선택합니다.
- Port** 또는 **LAG** 드롭다운 메뉴에서 인터페이스를 선택합니다.

해당 인터페이스의 정의가 선택한 인터페이스로 복사됩니다. 6단계를 참조하십시오.

- Copy to** 확인란을 선택하여 GARP 타이머 정의를 복사할 대상 인터페이스를 정의하거나 **Select All**을 선택하여 모든 포트 또는 LAG에 정의를 복사합니다.
- Apply Changes**를 클릭하십시오.

GARP Timers Table의 선택한 포트 또는 LAG에 매개변수가 복사되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 GARP 타이머 정의

이 표는 [GARP Timers](#) 페이지에 표시된 것과 같이 GARP 타이머를 정의하는 동등한 CLI 명령을 요약합니다.

표 7-73. GARP 타이머 CLI 명령

CLI 명령	설명
<code>garp timer {join   leave   leaveall} 타이머_값</code>	GARP 응용프로그램 참가, 나가기 및 전체 나가기 GARP 타이머 값을 조절합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# interface ethernet 1/e1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11

GVRP Feature is currently Disabled on the device.

```



Maximum VLANs: 223						
Port (s)	GVRP-	Registration	Dynamic VLAN	Timers	(milliseconds)	
	Status		Creation	Join	Leave	Leave All
---	-----	-----	-----	-----	-----	-----
1/e11	Disabled	Normal	Enabled	200	900	10000

## 스패닝 트리 프로토콜 구성

STP(스패닝 트리 프로토콜)은 모든 브리지 배열의 트리 표현 형태를 제공합니다. STP는 네트워크상의 최종 스테이션 사이에 단일 경로를 제공하여 루프를 제거합니다.

루프는 호스트 사이에 대체 루트가 존재할 때 발생합니다. 확장된 네트워크의 루프는 브리지가 처리량을 무한정 전달하게 하여 처리량을 증가시키고 네트워크 효율을 감소시킬 수 있습니다.

본 장치는 다음과 같은 스패닝 트리 버전을 제공합니다.

- 1 Classic STP — 최종 스테이션 사이에 단일 경로를 제공하여 루프를 방지하고 제거합니다. 클래식 STP의 구성에 대한 자세한 내용은 [STP 전역 설정 정의](#)를 참조하십시오.
- 1 Rapid STP — 전달 루프를 작성하지 않고 스패닝 트리의 빠른 수렴을 제공하는 네트워크 위상을 감지하고 사용합니다. 장치에 RSTP가 활성화되었지만 인접 장치에는 STP가 활성화된 경우, 로컬 장치는 STP를 사용합니다.

고속 STP의 구성에 대한 자세한 내용은 [고속 스패닝 트리 정의](#)를 참조하십시오.

- 1 Multiple STP — 임의 VLAN에 할당된 패킷에 완전한 연결을 제공합니다. 다중 STP는 RSTP를 기반으로 합니다. 또한, 다중 STP는 다른 MST 영역을 통해 다른 VLAN에 할당된 패킷을 전송합니다. 장치에 MSTP가 활성화된 경우 MST 영역은 단일 브리지의 역할을 합니다. 그러나, 인접 장치에 RSTP가 활성화되어 있고 로컬 장치가 STP, RSTP 및 MSTP를 사용하는 경우 두 장치는 상호 작동할 수 있습니다.

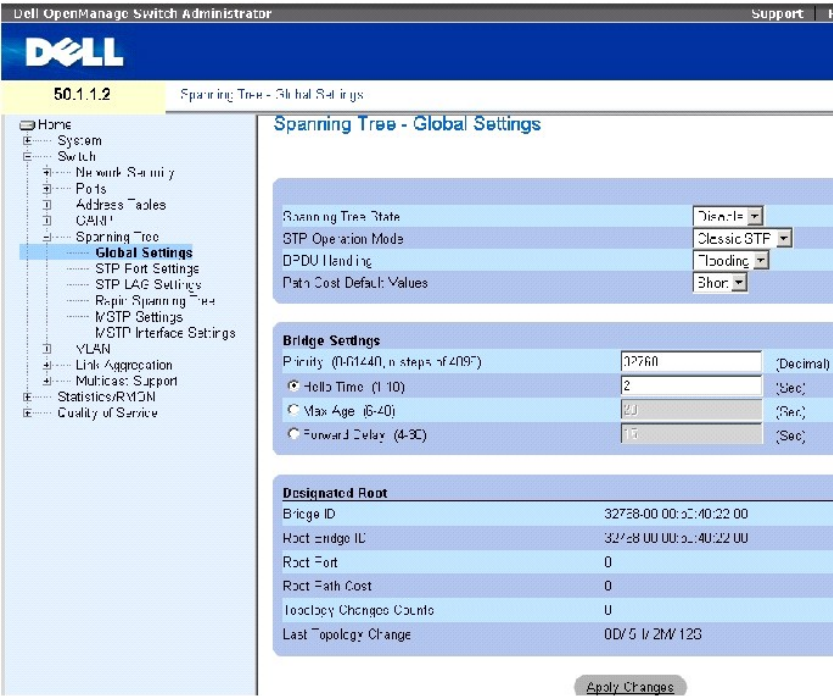
다중 STP의 구성에 대한 자세한 내용은 [다중 스패닝 트리를](#) 참조하십시오.

Spanning Tree 페이지를 열려면 트리 뷰에서 **Switch**→**Spanning Tree**를 클릭하십시오.

## STP 전역 설정 정의

[Spanning Tree Global Settings](#) 페이지는 장치에 STP를 활성화하는 매개변수를 포함합니다. [Spanning Tree Global Settings](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**Spanning Tree**→**Global Settings**를 차례로 클릭하십시오.

그림 7-22. 스패닝 트리 전역 설정



[Spanning Tree Global Settings](#) 페이지에는 다음과 같은 필드가 포함됩니다.

**Spanning Tree State** — 장치에 STP, 고속 STP 또는 MSTP를 활성화 또는 비활성화합니다.

**STP Operation Mode** — 장치에 STP를 활성화하는 STP 모드를 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Classic STP** — 장치에 클래식 STP를 활성화합니다. 이 값은 기본값입니다.

**Rapid STP** — 장치에 고속 STP를 활성화합니다.

**Multiple STP** — 장치에 다중 STP를 활성화합니다.

**BPDU Handling** — 포트/장치에 STP가 비활성화되었을 때 BPDU 패킷 관리 방법을 결정합니다. BPDU는 스페닝 트리 정보를 전송하는 데 사용됩니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Filtering** — 인터페이스에 스페닝 트리 비활성화되었을 때 BPDU 패킷을 필터링합니다. 이 값은 기본값입니다.

**Flooding** — 인터페이스에 스페닝 트리 비활성화되었을 때 BPDU 패킷을 채도합니다.

**Path Cost Default Values** — STP 포트에 기본 경로 비용을 지정하는 데 사용되는 방법을 지정합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Short** — 포트 경로 비용에 1-65,535 범위를 지정합니다. 이 값은 기본값입니다.

**Long** — 포트 경로 비용에 1~200,000,000 범위를 지정합니다.

인터페이스에 지정된 기본 경로 비용은 다음과 같은 선택 방법에 따라 다릅니다.

Interface	Long	Short
LAG	20,000	4
1000Mbps	20,000	4
100Mbps	200,000	19
10Mbps	2,000,000	100

**Priority(0-65535)** — 브리지 우선순위 값을 지정합니다. 스위치 또는 브리지가 STP를 실행할 때 각각에 우선순위가 지정됩니다. BPDU를 교환한 후 가장 낮은 우선순위 값을 가진 장치가 루트 브리지가 됩니다. 기본값은 32768입니다. 포트 우선순위 값은 4096, 8192, 12288 등과 같이 4096의 증분으로 제공됩니다.

**Hello Time(1-10)** — 장치 헬로우 시간을 지정합니다. 헬로우 시간은 루트 브리지가 구성 메시지 사이에 기다리는 시간(초)을 표시합니다. 기본값은 2초입니다.

**Max Age(6-40)** — 장치 최대 수명 시간을 지정합니다. 최대 수명 시간은 브리지가 구성 메시지를 보내기 전에 기다리는 시간(초)을 표시합니다. 기본 최대 수명은 20초입니다.

**Forward Delay(4-30)** — 장치 전달 지연 시간을 지정합니다. 전달 지연 시간은 브리지가 패킷을 전달하기 전에 듣기 또는 스텝 상태를 유지할 시간(초)을 표시합니다. 기본값은 10초입니다.

**Bridge ID** — 브리지 우선순위 및 MAC 주소를 식별합니다.

**Root Bridge ID** — 루트 브리지 우선순위 및 MAC 주소를 식별합니다.

**Root Port** — 해당 브리지에서 루트 브리지까지의 가장 낮은 비용 경로를 제공하는 포트 번호를 표시합니다. 해당 브리지가 루트가 아닐 때 유효합니다.

**Root Path Cost** — 해당 브리지에서 루트까지의 경로 비용입니다.

**Topology Changes Counts** — 발생한 STP 상태 변경의 전체 횟수를 지정합니다.

**Last Topology Change** — 브리지가 초기화되거나 재설정된 후 경과한 시간 및 발생한 마지막 표면 형태 변경을 표시합니다. 시간은 2D/5H/10M/4S와 같이 D/H/M/S 형식으로 표시됩니다.

## STP 전역 매개변수 정의

1. 페이지를 여십시오.
2. **Spanning Tree State** 필드에서 **Enable**를 선택합니다.
3. **STP Operation Mode** 필드에서 **STP** 모드를 선택하고 브리지 설정을 정의합니다.
4. **Apply Changes**를 클릭하십시오.

장치에 STP가 활성화됩니다.

## STP 전역 매개변수 수정

1. 페이지를 여십시오.
2. 대화상자에서 필드를 정의합니다.
3. **Apply Changes**를 클릭하십시오.

STP 매개변수가 수정되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 STP 전역 매개변수 정의

다음 표는 [Spanning Tree Global Settings](#) 페이지에 표시된 것과 같이 STP 전역 매개변수를 정의하는 동등한 CLI 명령을 요약합니다.

표 7-74. STP 전역 매개변수 CLI 명령

CLI 명령	설명
<code>spanning-tree</code>	스패닝 트리 기능을 활성화합니다.
<code>spanning-tree mode {stp   rstp   mstp}</code>	스패닝 트리 프로토콜의 모드를 구성합니다.
<code>spanning-tree prioritypriority</code>	스패닝 트리 우선순위를 구성합니다.
<code>spanning-tree hello-time초</code>	장치가 다른 장치에 헬로우 메시지를 브로드캐스트하는 빈도를 나타내는 스패닝 트리 브리지 헬로우 시간을 구성합니다.
<code>spanning-tree max-age초</code>	스패닝 트리 브리지 최대 수명을 구성합니다.
<code>spanning-tree forward-time seconds</code>	포트가 전달 상태로 들어가기 전에 들기 또는 습득 상태를 유지할 시간을 나타내는 스패닝 트리 브리지 전달 시간을 구성합니다.
<code>show spanning-tree [ethernet 인터페이스   port-channel 포트-채널-번호] [instance 인스턴스_id]</code>	스패닝 트리 구성을 표시합니다.
<code>show spanning-tree [detail] [active   blockedports] [instance 인스턴스_id]</code>	활성 또는 차단된 포트의 자세한 스패닝 트리 정보를 표시합니다.
<code>show spanning-tree mst-configuration</code>	스패닝 트리 MST 구성 식별자를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)# exit

```

console# show spanning-tree

Spanning tree enabled mode MSTP

Default port cost method: short

Gathering information .....

16-4094

##### MST 0 Vlans Mapped:

CST Root ID Priority 20480

00:30:ab:00:00:08

Address

4

Path Cost

ch2

Root Port

This switch is the IST master

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

32768

Bridge ID Priority

00:00:00:16:00:64

Address

Max hops

20

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
------	-------	----------	------	-----	------	----------	------

----	----	-----	----	---	----	-----	----
------	------	-------	------	-----	------	-------	------

1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr
------	---------	-------	-----	------	------	----	----------

1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
------	---------	-------	-----	------	------	----	----------

1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr
------	---------	-------	-----	------	------	----	----------

1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
------	---------	-------	----	-----	------	-----	----------

1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
------	---------	-------	-----	------	------	----	----------

1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
------	---------	-------	-----	------	------	----	----------

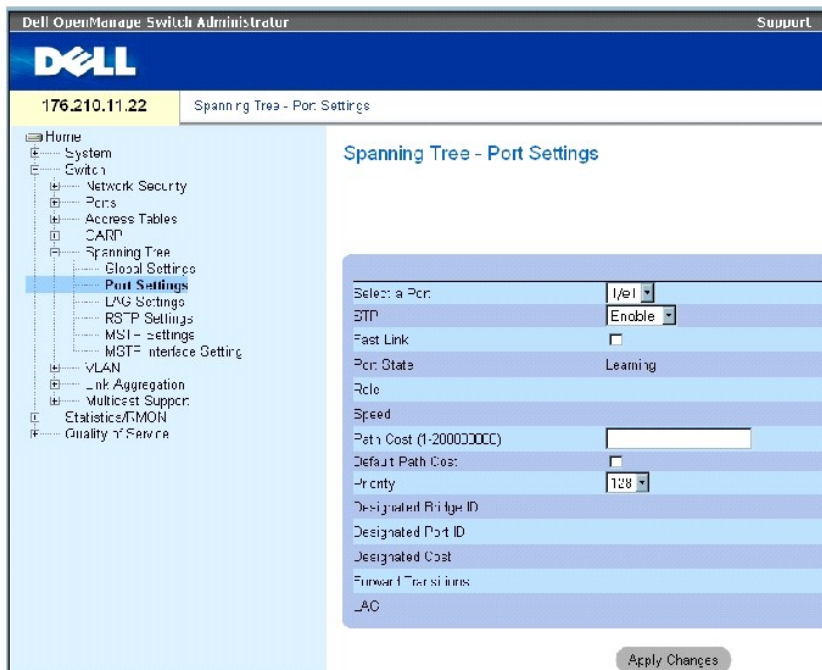
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr
console# show spanning-tree active							
Spanning tree enabled mode MSTP							
Default port cost method: short							
Gathering information .....							
##### MST 0 Vlans Mapped: 16-4094							
CST Root ID Priority 20480							
Address		00:30:ab:00:00:08					
Path Cost		4					
Root Port		ch2					
This switch is the IST master							
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec							
Bridge ID Priority							
Address		00:00:00:16:00:64					
Max hops		20					
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	----	-----	----	---	----	-----	----
1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)

1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

## STP 포트 설정 정의

Spanning Tree Port Settings 페이지를 사용하여 STP 속성을 개별 포트에 지정하십시오. Spanning Tree Port Settings 페이지를 열려면, 트리 뷰에서 **Switch** → **Spanning Tree** → **Port Settings**를 클릭하십시오.

그림 7-23. 스페닝 트리 포트 설정



Spanning Tree Port Settings 페이지는 다음과 같은 필드를 포함합니다.

**Select a Port** — STP 설정을 수정할 포트 번호를 지정합니다.

**STP** — 포트에 STP를 활성화 또는 비활성화합니다.

**Fast Link** — 이 항목을 선택하면 포트에 고속 연결 모드가 활성화됩니다. 포트에 고속 연결 모드가 활성화된 경우 포트 연결이 작동될 때 **Port State**가 자동으로 **Forwarding** 상태로 됩니다. 고속 연결 모드는 STP 프로토콜이 수렴되는 시간을 최적화합니다. STP 수렴은 대형 네트워크의 경우 30-60초가 걸릴 수 있습니다.

**Port State** — 포트의 현재 STP 상태를 표시합니다. 활성화된 경우, 처리량에 수행할 전달 동작은 포트 상태가 결정합니다. 다음과 같은 포트 상태가 가능합니다.

**Disabled** — STP가 포트에서 현재 비활성화되어 있습니다. 포트는 MAC 주소를 학습하는 동안 처리량을 전달합니다.

**Blocking** — 포트가 현재 차단되었으며 처리량을 전달하거나 MAC 주소를 학습하는 데 사용될 수 없습니다. 차단은 클래식 STP가 활성화된 경우에 표시됩니다.

**Listening** — 포트가 현재 듣기 모드에 있습니다. 포트는 처리량을 전달하거나 MAC 주소를 학습할 수 없습니다.

**Learning** — 포트가 현재 학습 모드에 있습니다. 포트는 처리량을 전달할 수 없지만 새 MAC 주소를 학습할 수 있습니다.

**Forwarding** — 포트는 현재 전달 모드에 있습니다. 포트는 처리량을 전달할 수 있으며 새 MAC 주소를 학습할 수 있습니다.

**Role** —STP 경로를 제공하는 STP 알고리즘에 의해 지정된 포트 역할을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Root**—패킷을 루트 스위치에 전달할 수 있는 가장 적은 비용을 소모하는 제공합니다.

**Designated**—지정된 스위치가 LAN에 연결되는 데 사용되는 LAG를 표시합니다.

**Alternate**—루트 인터페이스에서 루트 스위치로의 대체 경로를 제공합니다.

**Backup**—지정된 포트 경로에 대한 스페닝 트리 및 방향의 백업 경로를 제공합니다. 백업 포트는 두 포트가 점 대 점 연결에 의해 루트에 연결되었을 때에만 발생합니다. 또한, 백업 포트는 LAN에서 둘 이상의 연결이 공유 세그먼트에 연결되었을 때에도 발생합니다.

**Disabled**—포트가 스페닝 트리에 참여하지 않음을 표시합니다.

**Speed** — 포트가 작동하는 속도입니다.

**Path Cost (1-200000000)** — 루트 경로 비용에 대해 포트가 분담한 양입니다. 경로 비용은 더 높거나 낮은 값으로 조정되고 경로가 다시 라우팅될 때 처리량을 전달하는 데 사용됩니다.

**Default Path Cost** — 기본 경로 비용입니다. 긴 경로 비용의 기본값은 다음과 같습니다.

이더넷 -2,000,000

고속 이더넷 -200,000

기가비트 이더넷 -20,000

짧은 경로 비용의 기본값은 다음과 같습니다.

이더넷 - 100

고속 이더넷 - 19

기가비트 이더넷 - 4



**Priority (0-240, in steps of 16)** — 포트의 우선 순위 값입니다. 우선 순위 값은 브리지에서 두 개의 포트가 루프에 연결되어 있는 경우에 포트 선택에 영향 줍니다. 우선 순위 값의 범위는 0-240입니다. 우선 순위 값은 16을 증분으로 제공됩니다.

**Designated Bridge ID** — 지정된 브리지의 브리지 우선 순위 및 MAC 주소입니다.

**Designated Port ID** — 지정된 포트의 우선 순위 및 인터페이스입니다.

**Designated Cost** — STP 위상에 참여하는 포트의 비용입니다. 비용이 적은 포트는 STP가 루프를 감지할 때 차단될 가능성이 더 낮습니다.

**Forward Transmission** — 포트가 **Forwarding** 상태에서 **Blocking** 상태로 변경된 횟수입니다.

**LAG** — 포트가 연결된 LAG입니다.

## 포트에 STP 활성화

1. Spanning Tree **Port Settings** 페이지를 여십시오.
2. 포트를 선택하십시오.
3. **STP** 필드에서 **Enabled**를 선택하십시오.
4. **Fast Link, Path Cost** 및 **Priority** 필드를 정의하십시오.
5. **Apply Changes**를 클릭하십시오.

포트에 STP가 활성화됩니다.

## STP 포트 속성 수정

1. Spanning Tree **Port Settings**를 여십시오.
2. 포트를 선택하십시오.
3. 관련 필드를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

STP 포트 매개변수가 수정되고 장치가 업데이트됩니다.

## STP 포트 표 표시

1. Spanning Tree **Port Settings**를 여십시오.
2. **Show All**를 클릭하십시오.

**STP Port Table**이 열립니다.

## CLI 명령을 사용하여 STP 포트 설정 정의

다음 표는 **STP Port Settings** 페이지에 표시된 것과 같이 STP 포트 매개변수를 정의할 수 있는 해당 CLI 명령을 요약합니다.

### 표 7-75. STP STP 포트 설정 CLI 명령

---

CLI 명령	설명
<code>spanning-tree disable</code>	특정 포트의 스페닝 트리를 비활성화합니다.
<code>spanning-tree cost</code> 비용	포트의 스페닝 트리 비용 분담량을 구성합니다.
<code>spanning-tree port-priority</code> 우선 순위	포트 우선 순위를 구성합니다.
<code>show spanning-tree [ethernet인터페이스   port-channel포트-채널-번호][instance 인스턴스-ID]</code>	스페닝 트리 구성을 표시합니다.
<code>spanning-tree portfast</code>	PortFast 모드를 활성화합니다.
<code>show spanning-tree [detail] [active   blockedports] [instance 인스턴스-ID]</code>	활성 또는 차단된 포트의 자세한 스페닝 트리 정보를 표시합니다.
<code>show spanning-tree mst-configuration</code>	스페닝 트리 MST 구성 식별자를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15

```

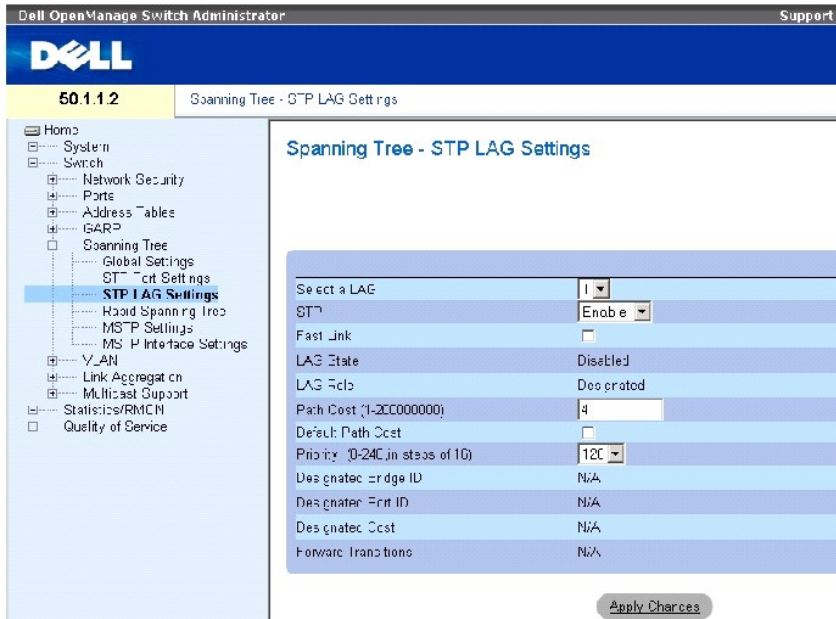
Port 1/e15 enabled					
--------------------	--	--	--	--	--

State: forwarding			Role: designated	
Port id: 128.15			Port cost: 19	
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)				
Designated bridge Priority : 32768			Address: 00:00:00:16:00:64	
Designated port id: 128.15			Designated path cost: 4	
Guard root: Disabled				
Number of transitions to forwarding state: 2				
BPDU: sent 483, received 1037				
console# show spanning-tree ethernet 1/e15 instance 12				
Port 1/e15 enabled				
State: discarding			Role: alternate	
Port id: 128.15			Port cost: 19	
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)				
Designated bridge Priority : 32768			Address: 00:00:b0:07:07:49	
Designated port id: 128.11			Designated path cost: 0	
Guard root: Disabled				
Number of transitions to forwarding state: 3				
BPDU: sent 482, received 1035				

## STP LAG 설정

Spanning Tree LAG Settings 페이지를 사용하여 STP 집합 포트 매개변수를 할당하십시오. Spanning Tree LAG Settings 페이지를 열려면, 트리 보기에서 **Switch** → **Spanning Tree** → **LAG Settings**를 클릭하십시오.

그림 7-24. 스페닝 트리 LAG 설정



Spanning Tree LAG Settings 페이지는 다음과 같은 필드를 포함합니다.

**Select a LAG** — STP 설정을 수정할 LAG 번호입니다.

**STP** — LAG에 STP를 활성화 또는 비활성화합니다.

**Fast Link** — LAG에 대한 고속 연결을 활성화합니다. LAG에 대해 고속 연결 모드가 활성화된 경우, LAG가 연결되면 LAG State는 자동으로 **Forwarding** 상태로 됩니다. 고속 연결 모드는 STP 프로토콜이 수렴되는 시간을 최적화합니다. STP 수렴은 대형 네트워크의 경우 30-60초가 걸릴 수 있습니다.

**LAG State** — LAG의 현재 STP 상태입니다. 활성화된 경우, LAG 상태가 처리량을 수행할 전달 작업을 결정합니다. 브리지에 의해 고장난 LAG가 발견되면 LAG는 **Broken** 상태로 됩니다. 다음과 같은 LAG 상태가 가능합니다.

**Disabled** — STP가 LAG에서 현재 비활성화되어 있습니다. LAG는 MAC 주소를 학습하는 동안 처리량을 전달합니다.

**Blocking** — LAG가 차단되었으며 처리량을 전달하거나 MAC 주소를 학습하는 데 사용될 수 없습니다.

**RSTP Discarding State** — 이 상태에서는 포트가 MAC 주소를 학습하거나 프레임을 전달하지 않습니다.

이 상태는 차단 상태와 STP(802.1D)에 소개된 듣기 상태를 합친 것입니다.

**Listening** — LAG가 듣기 모드에 있으며 처리량을 전달하거나 MAC 주소를 학습할 수 없습니다.

**Learning** — LAG가 듣기 모드에 있으며 처리량을 전달할 수 없지만 새 MAC 주소를 학습할 수 있습니다.

**Forwarding** — LAG가 현재 전달 모드에 있으며, 처리량을 전달할 수 있으며 새 MAC 주소를 학습할 수 있습니다.

**Broken** —LAG가 현재 고장이며 처리량 전달에 사용할 수 없습니다.

**LAG Role** —STP 경로를 제공하는 STP 알고리즘에 의해 지정된 LAG 역할을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Root**—패킷을 루트 스위치에 전달할 수 있는 가장 적은 비용을 소모하는 제공합니다.

**Designated**—지정된 스위치가 LAN에 연결되는 데 사용되는 LAG를 표시합니다.

**Alternate**—루트 인터페이스에서 루트 스위치로의 대체 LAG를 제공합니다.

**Backup**—지정된 포트 경로에 대한 스페닝 트리 일 방향의 백업 경로를 제공합니다. 백업 포트는 두 포트가 정 대 정 연결에 의해 루프에 연결되었을 때에만 발생합니다. 또한, 백업 포트는 LAN에서 둘 이상의 연결이 공유 세그먼트에 연결되었을 때에도 발생합니다.

**Disabled**—LAG가 스페닝 트리에 참여하지 않음을 표시합니다.

**Path Cost (1-200000000)** — 루트 경로 비용에 대해 LAG가 분당한 양입니다. 경로 비용은 더 높거나 낮은 값으로 조정되고 경로가 다시 라우팅될 때 처리량을 전달하는 데 사용됩니다. The path cost has a value of 1 to 200000000.

**Default Path Cost** — 기본 경로 비용이 사용됨을 표시합니다. 다음과 같은 LAG 경로 비용 기본값이 가능합니다.

**LAG에 대한 긴 방식** — 20,000

**LAG에 대한 짧은 방식** — 4

**Priority (0-240, in steps of 16)** — LAG의 우선 순위 값입니다. 우선 순위 값은 브리지에 루프된 포트가 있을 때 LAG 선택에 영향 줍니다. 우선 순위 값은 0-240 사이의 16을 증분으로 하는 값입니다.

**Designated Bridge ID** — 지정된 브리지의 우선 순위 및 MAC 주소입니다.

**Designated Port ID** — 선택한 인터페이스의 ID입니다.

**Designated Cost** — STP 위상에 참여하는 포트의 비용입니다. 비용이 적은 포트는 STP가 루프를 감지할 때 차단될 가능성이 더 낮습니다.

**Forward Transitions** — LAG State가 **Forwarding** 상태에서 **Blocking** 상태로 변경된 횟수입니다.

## LAG STP 매개변수 수정

1. **Spanning Tree LAG Settings** 페이지를 여십시오.
2. **Select a LAG** 드롭다운 메뉴에서 LAG를 선택하십시오
3. 원하는 필드를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

STP LAG 매개변수가 수정되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 STPLAG 설정 정의

다음 표는 STPLAG 설정을 정의하는 CLI 명령을 포함합니다.

표 7-76. STPLAG 설정 CLI 명령

CLI 명령	설명
spanning-tree	스패닝 트리를 활성화합니다.
spanning-tree disable	특정 LAG에 스페닝 트리를 비활성화합니다.
spanning-tree cost 비용	LAG의 스페닝 트리 비용 분당양을 구성합니다.
spanning-tree port-priority 우선 순위	포트 우선 순위를 구성합니다.
show spanning-tree [ethernet인터페이스   port-channel포트 채널 번호][instance 인스턴스- id]	스패닝 트리 구성을 표시합니다.
show spanning-tree [detail] [active   blockedports] [instance 인스턴스-ID]	활성 또는 차단된 포트의 자세한 스페닝 트리 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

console(config-if)#
spanning-tree cost 35000

console(config-if)#
spanning-tree port-
priority 96

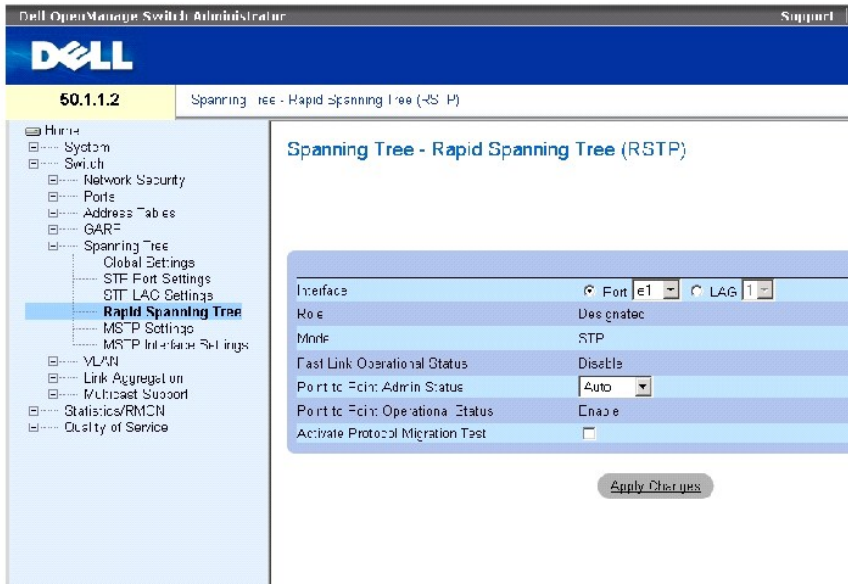
console(config-if)#
spanning-tree portfast
    
```

## 고속 스페닝 트리 정의

클래식 스페닝 트리가 일반 네트워크 위상에서 총 2 전달 루프를 방지하는 수렴에 30-60초가 소요될 수 있습니다. 이 지연 시간은 가능한 루프를 감지하고 상태 변경을 전파할 수 있게 합니다.

RSTP(고속 스페닝 트리 프로토콜)는 전달 루프를 생성하지 않고 스페닝 트리의 빠른 수렴을 허용하는 네트워크 위상을 감지하고 사용합니다. Rapid Spanning Tree (RSTP) settings 페이지를 열려면, 트리 보기에서 **Switch** → **Spanning Tree** → **Rapid Spanning Tree**를 선택하십시오.

그림 7-25. RSTP(고속 스페닝 트리) 설정



Spanning Tree RSTP 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Interface** — RSTP 설정을 보고 편집할 수 있는 포트 또는 LAG입니다.

**State** — 선택한 인터페이스의 RSTP 상태를 비활성화합니다.

**Role** — STP 경로를 제공하기 위해 STP 알고리즘에 의해 지정된 포트 역할을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Root** — 패킷을 루트 스위치에 전달할 수 있는 가장 적은 비용을 소모하는 제공합니다.

**Designated** — 지정된 스위치가 LAN에 연결되는 데 사용되는 포트 또는 LAG를 표시합니다.

**Alternate** — 루트 인터페이스에서 루트 스위치로의 대체 경로를 제공합니다.

**Backup** — 지정된 포트 경로에 대한 스페닝 트리 및 방향의 백업 경로를 제공합니다. 백업 포트는 두 포트가 정대 정 연결에 의해 루프에 연결되었을 때에만 발생합니다. 또한, 백업 포트는 LAN에서 둘 이상의 연결이 공유 세그먼트에 연결되었을 때에도 발생합니다.

**Disabled** — 포트가 스페닝 트리에 참여하지 않음을 표시합니다.

**Mode** — 현재 스페닝 트리 모드를 표시합니다. 스페닝 트리 모드는 [Spanning Tree Global Settings](#) 페이지에서 선택됩니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Classic STP** — 장치에 클래식 STP가 활성화되었음을 표시합니다.

**Rapid STP** — 장치에 고속 STP가 활성화되었음을 표시합니다.

**Multiple STP**—장치가 다중 STP가 활성화되었음을 표시합니다.

**Fast Link Operational Status** — 포트 또는 LAG에 대해 고속 연결이 활성화되었는지 여부를 표시합니다. If Fast Link is enabled for an interface, the interface is automatically placed in the forwarding state.

**Point-to-Point Admin Status** — 장치가 점 대 점 연결을 설정하도록 활성화 또는 비활성화하거나 장치가 자동으로 점 대 점 연결을 설정하도록 지정합니다.

점 대 점 연결을 통해 통신을 설정하기 위해 원본 PPP는 데이터 연결을 구성하고 테스트할 수 있도록 먼저 LCP(연결 제어 프로토콜) 패킷을 전송합니다. 연결이 설정되고 LCP에 필요한 선택적 설비가 조정되면 원본 PPP는 하나 이상의 네트워크 층 프로토콜을 선택할 수 있도록 NCP(네트워크 제어 프로토콜) 패킷을 전송합니다. 각각의 선택된 네트워크 층 프로토콜이 구성된 연결을 통해 해당 네트워크 층 프로토콜의 패킷을 전송할 수 있습니다. 연결은 명시적인 LCP 또는 NCP가 연결을 닫거나 어떤 외부 이벤트가 발생할 때까지 통신 구성을 유지합니다. 이 상태가 실제 스위치 포트 연결 유형입니다. 이 상태는 관리 상태와는 다를 수 있습니다.

**Point-to-Point Operational Status** — 점 대 점 작동 상태입니다.

**Activate Protocol Migration** — 이 항목을 선택하면 데이터 연결을 구성하고 테스트하기 위해 PPO가 LCP(연결 제어 프로토콜) 패킷을 보내는 것을 활성화합니다.

### RSTP 매개변수 정의

1. Spanning Tree RSTP Settings 페이지를 여십시오.
2. 인터페이스를 선택합니다.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

RSTP 매개변수가 정의되고 장치가 업데이트됩니다.

### RSTP(고속 스페닝 트리) 표 표시

1. Rapid Spanning Tree (RSTP) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

**Rapid Spanning Tree (RSTP) Table**이 열립니다.

### CLI 명령을 사용하여 고속 STP 매개변수 정의

다음 표는 고속 스페닝 트리 (RSTP)에 표시된 것과 같이 고속 STP 매개변수를 정의할 수 있는 해당 CLI 명령을 요약합니다.

**표 7-77. RSTP 설정 CLI 명령**

CLI 명령	설명
<code>spanning-tree link-type{point-to-point   shared}</code>	기본 연결 유형 설정을 재지정합니다.
<code>spanning tree mode {stp   rstp   mstp}</code>	현재 실행 중인 스페닝 트리 프로토콜을 구성합니다.
<code>clear spanning-tree detected-protocols [ethernet interface   port-channel port- channel-number]</code>	프로토콜 마이그레이션 프로세스를 다시 시작합니다.
<code>show spanning-tree [ethernet interface   port-channel port- channel-number]</code>	스페닝 트리 구성을 표시합니다.



다음은 CLI 명령의 예입니다.

```
console(config)# interface ethernet 1/e5

console(config-if)# spanning-tree link-type shared

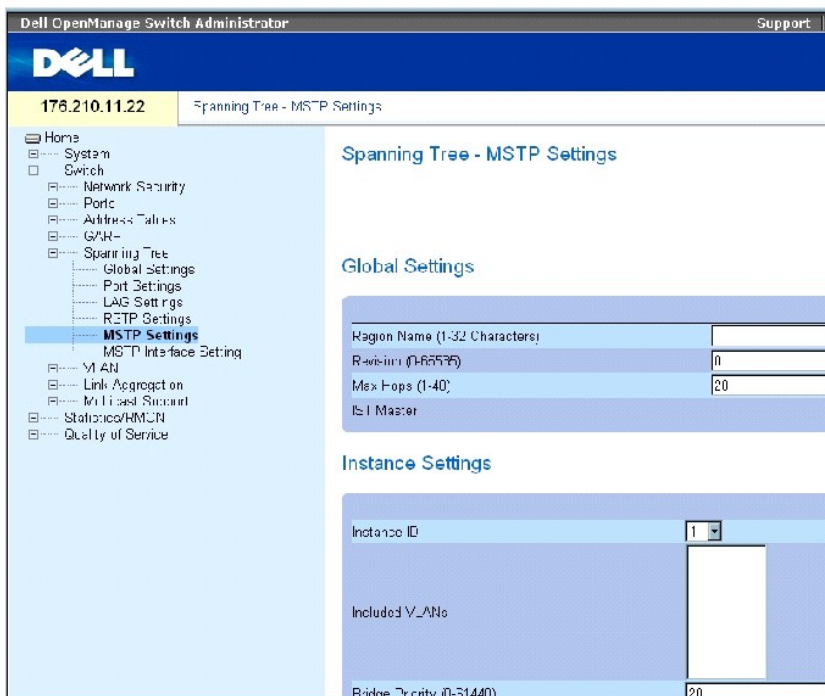
console(config-if)# spanning tree mode rstp
```

## 다중 스페닝 트리 구성

MSTP 작동은 VLAN을 STP 인스턴스에 매핑합니다. 다중 스페닝 트리는 다양한 로드 평형 시나리오를 제공합니다. 예를 들면, 포트 A가 특정 STP 인스턴스에서 차단된 동시에 동일한 포트는 다른 STP 인스턴스에서 전달 상태입니다.

또한, 다양한 VLAN에 지정된 패킷이 다중 스페닝 트리 영역(MST 영역) 내에서 서로 다른 경로를 통해 전송됩니다. 영역은 프레임이 전송될 수 있는 하나 이상의 다중 스페닝 트리 브리지입니다. [MSTP Settings](#) 페이지를 열려면, 트리 보기에서 **Switch** → **Spanning Tree** → **MSTP Settings**를 클릭하십시오.

그림 7-26. MSTP 설정



[MSTP Settings](#) 페이지는 다음과 같은 필드를 포함합니다.

**Region Name (1-32 Characters)** — 사용자 정의된 MSTP 영역 이름을 표시합니다.

**Revision (0-65535)** — 현재 MST 구성 개정을 식별하는 기호 없는 16 비트 수를 정의합니다. 개정 번호는 MST 구성의 일부로 필요합니다. The possible field range is 0-65535.

**Max Hops (1-40)** — 특정 영역에서 BPDU가 폐기되기 전까지 발생하는 홉의 최대 수를 정의합니다. 일단 BPDU가 폐기되면 포트 정보는 수명을 다합니다. 가능한 필드 범위는 1~40입니다. 필

드 기본값은 20입니다.

**IST Master** — 내부 스페닝 트리 마스터 ID를 표시합니다. IST 마스터는 인스턴스 0 루트입니다.

**Instance ID** — MSTP 인스턴스를 정의합니다. 필드 범위는 1~15입니다.

**Included VLANs** — 선택한 인스턴스에 매핑된 VLAN을 표시합니다. Each VLAN belongs to one instance.

**Bridge Priority (0-61440)** — 선택한 스페닝 트리 인스턴스 장치 우선 순위를 지정합니다. 필드 범위는 0-61440이며 4096을 증분으로 합니다.

**Designated Root Bridge ID** — 선택한 인스턴스의 루트인 브리지의 ID를 표시합니다.

**Root Port** — 선택한 인스턴스의 루트 포트를 표시합니다.

**Root Path Cost** — 선택한 인스턴스의 경로 비용을 표시합니다.

**Bridge ID** — 선택한 인스턴스의 브리지 ID를 표시합니다.

**Remaining Hops** — 다음 대상까지 남은 홉의 수를 표시합니다.

### MSTP Instance Table 표시

1. **Spanning Tree** [MSTP Settings](#) 페이지를 여십시오.
2. **Show All**을 클릭하여 [MSTP Instance Table](#)을 여십시오.

그림 7-27. MSTP 인스턴스 표

### MSTP Instance Table

Refresh

	VLAN	Instance ID (0-15)
1	Vlan 1	0
2	Vlan 2	0
3	Vlan 3	0
4	Vlan 4	0
5	Vlan 5	0
6	Vlan 6	0
7	Vlan 7	0
8	Vlan 8	0
9	Vlan 9	0
10	Vlan 10	0
11	Vlan 11	0
12	Vlan 12	0
13	Vlan 13	0
14	Vlan 14	0
15	Vlan 15	0
16	Vlan 16	0
17	Vlan 17	0
18	Vlan 18	0

## CLI 명령을 사용하여 MST 인스턴스 정의

다음 표는 [Spanning Tree MSTP Settings](#) 페이지에 표시된 것과 같이 MST 인스턴스 그룹을 정의할 수 있는 해당 CLI 명령을 요약합니다.

표 7-78. MSTP 인스턴스 CLI 명령

CLI 명령	설명
<code>spanning-tree mst configuration</code>	MST 구성 모드를 시작합니다.
<code>instance instance-id {add   remove} vlan vlan-range</code>	VLAN을 MST 인스턴스에 매핑합니다.
<code>name string</code>	구성 이름을 설정합니다.
<code>revision value</code>	Sets the configuration revision number
<code>spanning-tree mst instance-id port- priority priority</code>	포트의 우선 순위를 설정합니다.
<code>spanning-tree mst instance-id priority priority</code>	지정된 스페닝 트리 인스턴스의 장치 우선 순위를 설정합니다.
<code>spanning-tree mst max- hops hop-count</code>	BPDU가 폐기되고 포트에 있는 정보가 수명을 다하기 전까지 MST 영역의 홉 수를 설정합니다.
<code>spanning-tree mst instance-id cost cost</code>	MST 계산을 위한 포트의 경로 비용을 설정합니다.
<code>exit</code>	MST 영역 구성 모드를 종료하고 구성 변경 내용을 적용합니다.
<code>abort</code>	구성 변경 내용을 적용하지 않고 MST 영역 구성 모드를 종료합니다.
<code>show {current   pending}</code>	현재 또는 대기 중인 MST 영역 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1
    
```

```
console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration

Name: Region1

Revision: 1

Instance Vlans Mapped

-----

0 1-9,31-4094

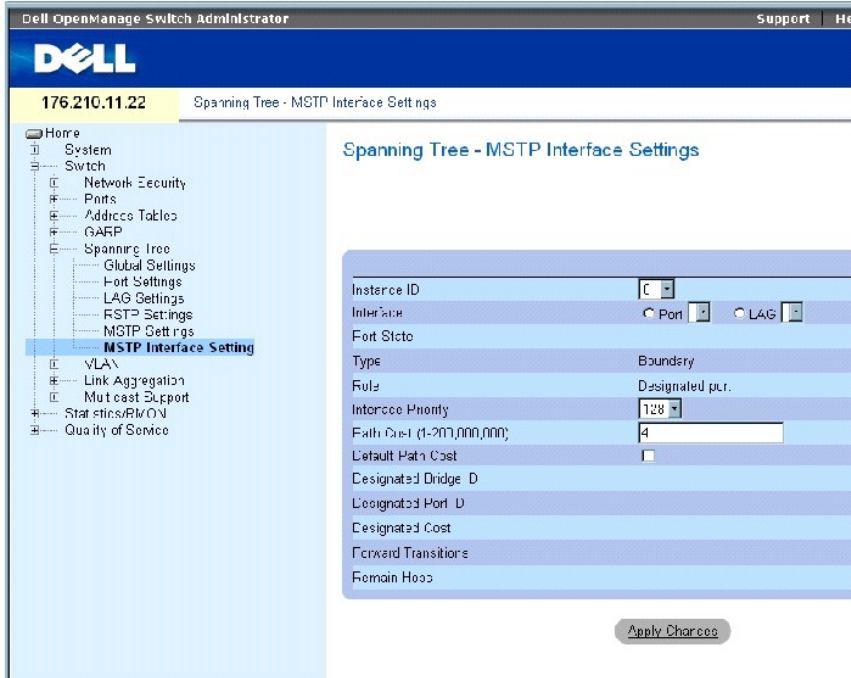
1 10-20

2 21-30
```

### MSTP 인터페이스 설정 정의

[MSTP Interface Settings](#) 페이지는 특정 인터페이스에 MSTP 설정을 지정할 수 있는 매개변수를 포함합니다. [MSTP Interface Settings](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**Spanning Tree**→**MSTP Interface Settings**를 클릭하십시오.

그림 7-28. MSTP 인터페이스 설정



[MSTP Interface Settings](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Instance ID** — 장치에 구성된 MSTP 인스턴스를 나열합니다. 가능한 필드 범위는 1-15입니다.

**Interface** — 선택된 MSTP 인스턴스에 포트 또는 LAG를 지정합니다.

**Port State** — 특정 인스턴스에 포트가 활성화되었는지 비활성화되었는지를 표시합니다.

**Type** — MSTP가 포트를 점 대 점 포트에 취급할지 허브에 연결된 포트에 취급할지와 포트가 MSTP 영역 내부에 있는지 경계 포트인지를 표시합니다. 아스터 포트는 MSTP 영역에서 외부에 있는 CIST 루트로의 연결을 제공합니다. 경계 포트는 MST 브리지를 외부 영역에 있는 LAN에 연결합니다. 포트가 경계 포트일 경우, 링크 반대쪽에 있는 장치가 RSTP 모드로 작동하는지 STP 모드로 작동하는지도 표시합니다.

**Role** — STP 경로에 제공하기 위해 STP 알고리즘에 의해 지정된 포트 역할을 표시합니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Root** — 패킷을 루트 장치에 전달할 수 있는 가장 낮은 비용 경로를 제공합니다.

**Designated** — 지정된 장치가 LAN에 연결되는 데 사용되는 포트 또는 LAG를 표시합니다.

**Alternate** — 루트 인터페이스에서 루트 장치로의 대체 경로를 제공합니다.

**Backup** — 지정된 포트 경로에 스페닝 트리 외 방향의 백업 경로를 제공합니다. 백업 포트는 두 포트가 점 대 점 연결에 의해 루프에 연결되었을 때에만 발생합니다. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

**Disabled** — 포트가 스페닝 트리에 참여하지 않음을 표시합니다.

**Interface Priority (0-240, in steps of 16)** — 특정 인스턴스에 대한 인터페이스 우선순위를 정의합니다. 기본값은 128입니다.

**Path Cost** — 스페닝 트리 인스턴스에 대해 포트가 기여한 부분을 표시합니다. 범위는 항상 1~200,000,000 사이여야 합니다.

**Default Path Cost** — 기본 경로 비용이 [Spanning Tree Global Settings](#) 페이지에 선택된 방식에 따라 지정됨을 표시합니다.

**Designated Bridge ID** — 링크 또는 공유 LAN을 루트에 연결하는 브리지 ID 번호입니다.

**Designated Port ID** — 링크 또는 공유 LAN을 루트에 연결하는 지정된 브리지의 포트 ID 번호입니다.

**Designated Cost** — 링크 또는 공유 LAN에서 루트로의 경로 비용입니다.

**Forward Transitions** — 포트가 **forwarding** 상태로 변경된 횟수입니다.

**Remain Hops** — 다음 대상까지 남은 홉의 수를 표시합니다.

## MSTP 인터페이스 설정 정의

1. [MSTP Interface Settings](#) 페이지를 여십시오.
2. 인터페이스를 선택합니다.
3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

MSTP 매개변수가 정의되고 장치가 업데이트됩니다.

## MSTP 인터페이스 표 보기

1. [MSTP Interface Settings](#) 페이지를 여십시오.
2. Show All을 클릭하십시오.

[MSTP Interface Table](#) 페이지가 열립니다.

그림 7-29. MSTP 인터페이스 표

## MSTP Interface Table

Refresh

Instance		1										
Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Remain Hops		
1	e1	N/A	N/A	N/A	12E	19	N/A	N/A	N/A	N/A	N/A	
2	e2	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
3	e3	N/A	N/A	N/A	12F	100	N/A	N/A	N/A	N/A	N/A	
4	e4	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
5	e5	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
6	e6	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
7	e7	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
8	e8	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
9	e9	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	
10	e10	N/A	N/A	N/A	12E	100	N/A	N/A	N/A	N/A	N/A	

### CLI 명령을 사용하여 MSTP 인터페이스 정의

다음 표는 **Spanning Tree** [MSTP Interface Settings](#) 페이지에 표시된 것과 같이 MSTP 인터페이스를 정의하는 해당 CLI 명령을 요약합니다.

표 7-79. MSTP 인터페이스 CLI 명령

CLI 명령	설명
<code>spanning-tree mst instance-id cost cost</code>	MST 계산을 위한 포트의 경로 비용을 설정합니다.
<code>spanning-tree mst instance-id priority priority</code>	지정된 ST 인스턴스의 장치 우선순위를 설정합니다.
<code>show spanning-tree mst- configuration</code>	MST 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

console# <code>show spanning-tree mst-configuration</code>		
Gathering information .....		
Current MST configuration		
Name: Gili		
Revision: 65000		
Instance	Vlans Mapped	State
-----	-----	-----
	16-4094	enabled

0		enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

---

## VLAN 구성

VLAN은 하드웨어 솔루션을 정의하는 대신 소프트웨어를 통해 LAN을 생성한 논리적 하위그룹입니다. VLAN은 사용자 스테이션과 네트워크 장치를 연결된 물리적 LAN 세그먼트에 상관없이 단일 장치로 결합합니다. VLAN은 네트워크 처리량이 하위그룹 안에서 더 효율적으로 흐르도록 해줍니다. 소프트웨어에 의해 관리되는 VLAN은 네트워크 변경, 추가 또는 이동이 구현되는 시간을 줄여줍니다.

VLAN은 소프트웨어 기반이며 물리적 특성에 의해 정의되지 않기 때문에 포트의 최소 개수가 없으며 장치, 스택 또는 기타 모든 논리적 연결 조합별로 생성될 수 있습니다.

VLAN은 층 2 레벨에서 작동합니다. VLAN은 VLAN 내의 처리량을 격리하기 때문에 VLAN 사이의 처리량 흐름을 허용하는 층 3 프로토콜 레벨에서 작동하는 라우터가 필요합니다. 층 3 라우터는 세그먼트를 식별하고 VLAN을 조율해 줍니다. VLAN은 브로드캐스트 및 멀티캐스트 도메인입니다. 브로드캐스트 및 멀티캐스트 처리량은 처리량이 생성된 VLAN 내에서만 전송됩니다.

VLAN 태그화는 VLAN 그룹 사이에 VLAN 정보를 전송할 수 있는 방법을 제공합니다. VLAN 태그화는 패킷 헤더에 4바이트 태그를 첨부합니다. VLAN 태그는 어느 VLAN에 패킷이 속하는지를 표시합니다. VLAN 태그는 최종 스테이션 또는 네트워크 장치에 의해 VLAN에 첨부됩니다. VLAN 태그는 VLAN 네트워크 우선순위 정보도 포함합니다.



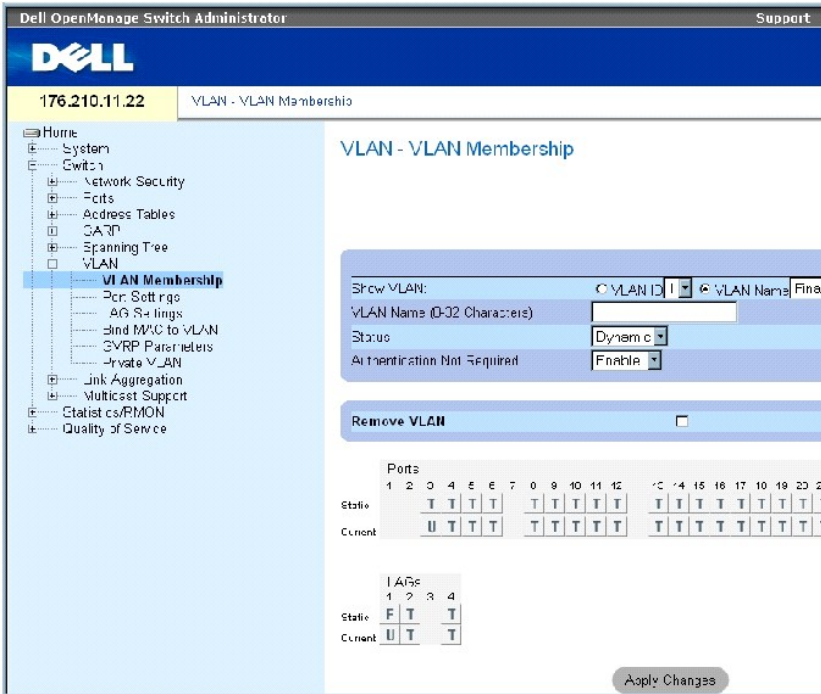
VLAN과 GVRP를 결합하면 네트워크 관리자가 네트워크 노드를 브로드캐스트 도메인에 정의할 수 있습니다. 브로드캐스트 및 멀티캐스트 처리량은 원래 그룹으로 한정됩니다.

VLAN 페이지를 열려면, 트리 뷰에서 **Switch** → **VLAN**을 클릭하십시오.

## VLAN 멤버십 정의

[VLAN Membership](#) 페이지는 VLAN 그룹을 정의하는 필드가 포함됩니다. 본 장치는 4094개의 VLAN ID를 256개의 VLAN에 매핑할 수 있습니다. 모든 포트는 정의된 PVID가 있어야 합니다. 다른 값이 구성되어 있지 않으면 기본 VLAN PVID가 사용됩니다. VLAN ID #1은 기본 VLAN이며 시스템에서 삭제할 수 없습니다. [VLAN Membership](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **VLAN** → **VLAN Membership**을 클릭하십시오.

그림 7-30. VLAN 멤버십



[VLAN Membership](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Show VLAN** — VLAN ID 또는 VLAN 이름에 따라 특정 VLAN 정보를 나열하고 표시합니다.

**VLAN Name (0-32 Characters)** — 사용자 정의된 VLAN 이름입니다.

**Status** — VLAN 종류입니다. 다음과 같은 값을 가질 수 있습니다.

**Dynamic** — VLAN이 GVRP를 통해 동적으로 생성되었습니다.

**Static** — VLAN이 사용자 정의되었습니다.

**Default** — VLAN이 기본 VLAN입니다.

**Authentication Not Required**—비승인 사용자가 VLAN에 액세스하는 것을 허용하거나 허용하지 않습니다.

**Remove VLAN**—이 항목을 선택하면 VLAN이 VLAN 멤버십 표에서 제거됩니다.

## 새 VLAN 추가

1. [VLAN Membership](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Create New VLAN** 페이지가 열립니다.

3. VLAN ID와 이름을 입력합니다.
4. **Apply Changes**를 클릭하십시오.

새 VLAN이 추가되고 장치가 업데이트됩니다.

## VLAN 멤버십 그룹 수정

1. [VLAN Membership](#) 페이지를 여십시오.
2. **Show VLAN** 드롭다운 메뉴에서 VLAN을 선택합니다.
3. 원하는 필드를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

VLAN 멤버십 정보가 수정되고 장치가 업데이트됩니다.

## VLAN 삭제

1. [VLAN Membership](#) 페이지를 여십시오.
2. **Show VLAN** 필드에서 VLAN을 선택합니다.
3. **Remove VLAN** 확인란을 선택합니다.
4. **Apply Changes**를 클릭하십시오.

선택한 VLAN이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 VLAN 멤버십 그룹 정의

다음 표는 VLAN Membership 페이지에 표시된 것과 같이 VLAN 멤버십 그룹을 정의하는 해당 CLI 명령을 요약합니다.

표 7-80. VLAN 멤버십 그룹 CLI 명령

CLI 명령	설명
vlan database	VLAN 구성 모드를 시작합니다.
vlan {vlan-범위}	VLAN을 생성합니다.
name 문자열	VLAN에 이름을 추가합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# vlan
database

console(config-vlan)#vlan
1972

console(config-vlan)# end

console(config)# interface
vlan 1972

console(config-if)# name
Marketing

console(config-if)# end
```

### VLAN 포트 멤버십 표

VLAN Port Membership Table은 포트를 VLAN에 지정하는 Port Table이 포함됩니다. 포트는 Port Control 설정 사이클 전환하여 VLAN에 지정됩니다. 포트는 다음 값을 가질 수 있습니다:

표 7-81. VLAN 포트 멤버십 표

포트 제어	정의
T	인터페이스가 VLAN의 구성요소입니다. 이 인터페이스가 전달하는 모든 패킷은 태그화됩니다. 패킷은 VLAN 정보를 포함합니다.
U	인터페이스가 VLAN 구성요소입니다. 이 인터페이스가 전달하는 패킷은 태그화되지 않습니다.
F	인터페이스가 VLAN에 대한 멤버십 자격이 거부되었습니다.
비어 있음	인터페이스가 VLAN 구성요소가 아닙니다. 이 인터페이스와 연관된 패킷은 전달되지 않습니다.

VLAN Port Membership Table은 LAG뿐만 아니라 포트 및 포트 상태를 표시합니다.

### VLAN 그룹에 포트 지정

1. VLAN Membership 페이지를 여십시오.
2. **VLAN ID** 또는 **VLAN Name** 옵션 단추를 클릭하고 드롭다운 메뉴에서 VLAN을 선택합니다.
3. **Port Membership Table**에서 포트를 선택하고 포트에 값을 지정합니다.
4. **Apply Changes**를 클릭하십시오.

포트가 VLAN 그룹에 지정되고 장치가 업데이트됩니다.

### VLAN 삭제

1. VLAN Membership를 여십시오.
2. **VLAN ID** 또는 **VLAN Name** 옵션 단추를 클릭하고 드롭다운 메뉴에서 VLAN을 선택합니다.
3. **Remove VLAN** 확인란을 선택합니다.

4. **Apply Changes**를 클릭하십시오.

선택한 VLAN이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 VLAN 그룹에 포트 지정

다음 표는 VLAN 그룹에 포트를 지정하는 데 관한 해당 CLI 명령을 요약합니다.

표 7-82. 포트 대 VLAN 그룹 지정 CLI 명령

CLI 명령	설명
switchport general acceptable-frame-types tagged-only	태그화되지 않은 프레임이 수신 시 패기됩니다.
switchport forbidden vlan {add vlan 목록   remove vlan-목록}	특정 VLAN을 포트에 추가하는 것을 금지합니다.
switchport mode {access   trunk   general}	포트의 VLAN 멤버십 모드를 구성합니다.
switchport access vlan vlan-id	인터페이스가 액세스 모드에 있을 때 VLAN ID를 구성합니다.
switchport trunk allowed vlan {add vlan-list   remove vlan-list}	트렁크 포트에서 VLAN을 추가하거나 제거합니다.
switchport trunk native vlan vlan-id	포트를 지정된 VLAN의 구성요소로 정의하고 VLAN ID를 포트 기본 VLAN ID(PVID)로 정의합니다.
switchport general allowed vlan add vlan-list [tagged   untagged]	일반 모드에서 포트에서 VLAN을 추가하거나 제거합니다.
switchport general pvid vlan-id	인터페이스가 일반 모드에 있을 때 PVID를 구성합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# vlan
database

console(config-vlan)# vlan
23-25

console(config-vlan)# end

console(config)#interface
vlan 23

console(config-if)# name
Marketing

console(config-if)# end

console(config)# interface
ethernet 1/e8

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 23
```

```
console(config-if)# end

console(config)# interface
ethernet 1/e9

console(config-if)#
switchport mode trunk

console(config-if)#
switchport mode trunk
allowed vlan add 23-25

console(config-if)# end

console(config)# interface
ethernet 1/e11

console(config-if)#
switchport mode general

console(config-if)#
switchport general allowed
vlan add 23,25 tagged

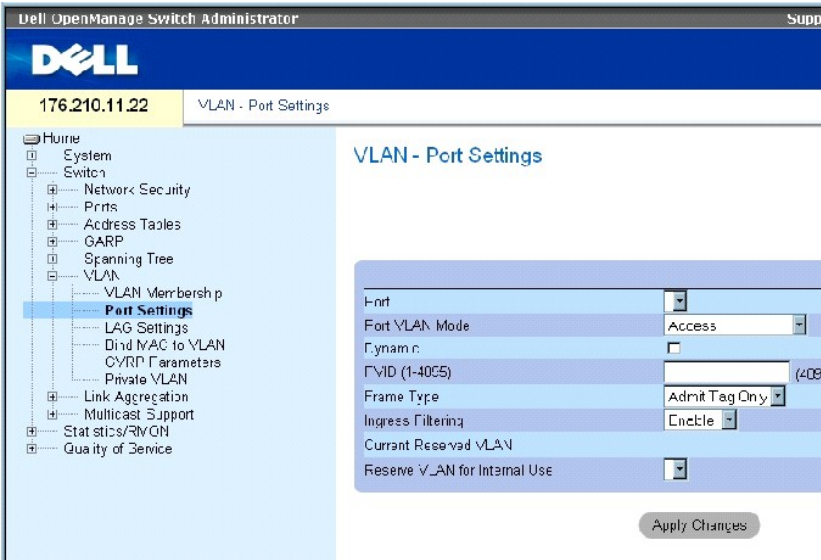
console(config-if)#
switchport general pvid 25
```

## VLAN 포트 설정 정의

[VLAN Port Settings](#) 페이지는 VLAN의 일부인 포트를 관리하는 필드를 포함합니다. 포트 기본 VLAN ID(PVID)는 [VLAN Port Settings](#) 페이지에서 구성됩니다. 장치에 도착하는 태그화되지 않은 모든 패킷은 포트 PVID에 의해 태그화됩니다.

[VLAN Port Settings](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**VLAN**→**Port Settings**를 클릭하십시오.

그림 7-31. VLAN 포트 설정



[VLAN Port Settings](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Port** — VLAN에 포함된 포트 번호입니다.

**Port VLAN Mode** — 포트 모드입니다. 다음과 같은 값을 가질 수 있습니다.

**General** — 포트가 VLAN에 속하며 각 VLAN은 태그화되거나 태그화되지 않음으로 사용자 정의됩니다(전체 802.1Q 모드).

**Access** — 포트가 단일 태그화되지 않은 VLAN에 속합니다. 포트가 액세스 모드에 있으면 포트에서 허용하는 패킷 종류를 지정할 수 없습니다. 수신 필터링은 액세스 포트에서 활성화/비활성화할 수 없습니다.

**Trunk** — 모든 포트가 태그화되는 VLAN에 포트가 속해 있습니다(태그화되지 않을 수 있는 포트 하나 제외).

**PVE Promiscuous** — 포트가 PVE 무차별 VLAN의 일부입니다.

**PVE Community** — 포트가 PVE 커뮤니티 VLAN의 일부입니다.

**PVE Isolated** — 포트가 PVE 격리 VLAN의 일부입니다.

**Dynamic** — Assigns a port to a VLAN based on the host source MAC address connected to the port.

**PVID** — 태그화되지 않은 패킷에 VLAN ID를 지정합니다. 가능한 값은 1~4095입니다. VLAN 4095는 표준 및 업계 관행에 따라 폐기 VLAN으로 정의됩니다. 폐기 VLAN으로 분류된 패킷은 폐기됩니다.

**Frame Type** — 포트에 허용된 패킷 종류입니다. 다음과 같은 값을 가질 수 있습니다.

**Admit Tag Only** — 태그화된 패킷만 포트에 허용됩니다.

**Admit All** — 태그화된 패킷과 태그화되지 않은 패킷 모두가 포트에 허용됩니다.

**Ingress Filtering** — 포트에서 수신 필터링을 활성화 또는 비활성화합니다. 수신 필터링은 특정 포트가 구성요소가 아닌 VLAN을 대상으로 하는 패킷을 폐기합니다.

**Current Reserved VLAN** — 시스템에 의해 예약 VLAN으로 현재 지정된 VLAN입니다.

**Reserve VLAN for Internal Use** — 시스템이 사용하지 않을 경우 예약 VLAN이 되도록 사용자가 선택한 VLAN입니다.

## 포트 설정 지정

1. [VLAN Port Settings](#) 페이지를 여십시오.
2. **Port** 드롭다운 메뉴에서 설정을 지정할 포트를 선택합니다.
3. 페이지의 나머지 필드를 완성합니다.
4. **Apply Changes**를 클릭하십시오.

VLAN 포트 설정이 정의되고 장치가 업데이트됩니다.

## VLAN 포트 표 표시

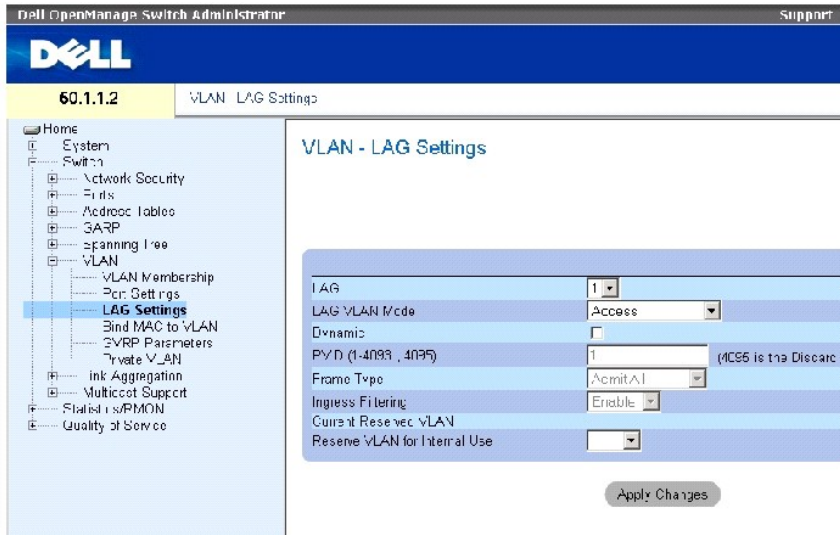
1. [VLAN Port Settings](#) 페이지를 여십시오.
2. **Show All**  
을 클릭하십시오.

VLAN Port Table이 열립니다.

## VLAN LAG 설정 정의

[VLAN LAG Settings](#) 페이지는 VLAN의 일부인 LAG를 관리하는 매개변수를 제공합니다. VLAN은 개별 포트 또는 LAG로 이루어질 수 있습니다. 장치에 들어오는 태그화되지 않은 패킷은 PVID에 의해 지정된 LAG ID와 함께 태그화됩니다. [VLAN LAG Settings](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**VLAN**→**LAG Settings**를 클릭하십시오.

그림 7-32. VLAN LAG 설정



[VLAN LAG Settings](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**LAG** — VLAN에 포함된 LAG 번호입니다.

**LAG VLAN Mode** — LAG VLAN 모드입니다. 다음과 같은 값을 가질 수 있습니다.

**General** — LAG가 VLAN에 속하며 각 VLAN은 태그화되거나 태그화되지 않음으로 사용자 정의됩니다(전체 802.1Q 모드).

**Access** — LAG가 태그화되지 않은 단일 VLAN에 속합니다.

**Trunk** — 모든 포트가 태그화되는 VLAN에 LAG가 속합니다(태그화되지 않을 수 있는 포트 하나 제외).

**PVE Promiscuous** — LAG가 PVE 무차별 VLAN에 속합니다.

**PVE Community** — LAG가 PVE 커뮤니티 VLAN에 속합니다.

**PVE Isolated** — LAG가 PVE 격리 VLAN에 속합니다.

**Dynamic** — Assigns a LAG to a VLAN based on the host source MAC address connected to the LAG.

**PVID (1-4093, 4095)** — 태그화되지 않은 패킷에 VLAN ID를 지정합니다. 가능한 필드 값은 1-4095입니다. VLAN 4095는 표준 및 업계 관행에 따라 폐기 VLAN으로 정의됩니다. 이 VLAN으로 분류된 패킷은 폐기됩니다.

**Frame Type** — LAG에 허용된 패킷 종류입니다. 다음과 같은 값을 가질 수 있습니다.

**Admit Tag Only** — 태그화된 패킷만 LAG에 허용됩니다.

**Admit All** — 태그화된 패킷과 태그화되지 않은 패킷 모두가 LAG에 허용됩니다.



**Ingress Filtering** — LAG에 의해 수신 필터링을 활성화 또는 비활성화합니다. 수신 필터링은 특정 LAG가 구성요소가 아닌 VLAN을 대상으로 하는 패킷을 폐기합니다.

**Current Reserve VLAN** — 예약 VLAN으로 현재 지정된 VLAN입니다.

**Reserve VLAN for Internal Use** — 장치 재설정 후에 예약 VLAN으로 지정된 VLAN입니다.

## VLAN LAG 설정 지정

1. [VLAN LAG Settings](#) 페이지를 여십시오.
2. LAG 드롭다운 메뉴에서 LAG를 선택하고 페이지의 필드를 완성합니다.
3. **Apply Changes**를 클릭하십시오.

VLAN LAG 매개변수가 정의되고 장치가 업데이트됩니다.

## VLAN LAG 표 표시

1. [VLAN LAG Settings](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

VLAN LAG Table 이 열립니다.

## CLI 명령을 사용하여 VLAN 그룹에 LAG 지정

다음 표는 [VLAN LAG Settings](#) 페이지에 표시된 것과 같이 VLAN 그룹에 LAG를 지정하는 해당 CLI 명령을 요약합니다.

표 7-83. LAG VLAN 할당 CLI 명령

CLI 명령	설명
switchport mode {access   trunk   general}	LAG VLAN 멤버십 모드를 구성합니다.
switchport trunk native vlan vlan-ID	포트를 지정한 VLAN의 구성요소로 정의하고 VLAN ID를 LAG 기본 VLAN ID(PVID)로 정의합니다.
switchport general pvid vlan-ID	인터페이스가 일반 모드에 있을 때 LAG VLAN ID(PVID)를 구성합니다.
switchport general allowed vlan add vlan-목록 [tagged   untagged]	일반 LAG에서 VLAN을 추가하거나 제거합니다.
switchport general acceptable-frame-type tagged-only	태그되지 않은 패킷을 수신 시 폐기합니다.
switchport access vlan dynamic	MAC 주소를 VLAN에 바인딩합니다.
switchport general ingress-filtering disable	LAG 수신 필터링을 비활성화합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# interface
port-channel 1

console(config-if)#
switchport mode access
```

```
console(config-if)#
switchport access vlan 2

console(config-if)# exit

console(config)# interface
port-channel 2

console(config-if)#
switchport mode general

console(config-if)#
switchport general allowed
vlan add 2-3 tagged

console(config-if)#
switchport general pvid 2

console(config-if)#
switchport general
acceptable-frame-type
tagged-only

console(config-if)#
switchport general
ingress-filtering disable

console(config-if)# exit

console(config)# interface
port-channel 3

console(config-if)#
switchport mode trunk

console(config-if)#
switchport trunk native
vlan 3

console(config-if)#
switchport trunk allowed
vlan add 2
```

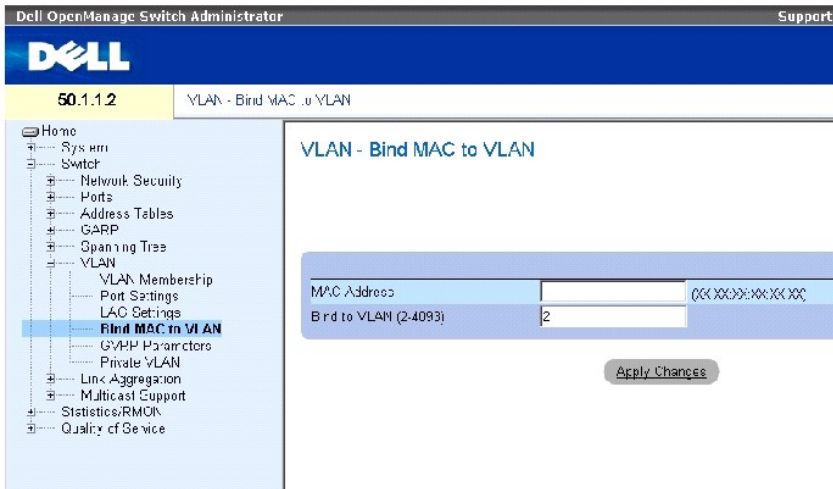
## VLAN에 MAC 주소 바인딩

VLAN에 MAC 주소를 바인딩하면 MAC 주소를 기반으로 VLAN 지정에 포트를 제공할 수 있습니다. 일단 MAC 주소가 VLAN에 지정되고 포트에서 MAC 주소를 습득하면 포트는 바인딩된 VLAN에 연결됩니다. MAC 주소의 수명이 다하면 포트는 VLAN에 연결되지 않습니다. 동적 VLAN만 MAC 주소에 바인딩될 수 있습니다.

VLAN에 MAC 주소를 바인딩하려면 VLAN 포트가 동적으로 추가되었으며 정적 VLAN 포트가 아니어야 합니다.

[Bind MAC to VLAN](#) 페이지를 열려면, **Switch** → **VLAN** → **Bind MAC to VLAN**을 클릭하십시오.

그림 7-33. VLAN에 MAC 바인딩



[Bind MAC to VLAN](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**MAC Address** — VLAN에 바인딩된 MAC 주소를 표시합니다.

**Bind to VLAN (2-4093)** — MAC 주소가 바인딩된 VLAN을 표시합니다.

**MAC 대 VLAN 표 표시:**

1. [Bind MAC to VLAN](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

**MAC to VLAN table**이 열립니다.

**CLI 명령을 사용하여 VLAN에 MAC 주소 바인딩**

다음 표는 VLAN에 MAC 주소를 바인딩하는 해당 CLI 명령을 요약합니다.

표 7-84. VLAN에 MAC 주소 바인딩 CLI 명령

CLI 명령	설명
mac-to-vlan mac-address vlan-id	MAC 주소를 VLAN에 바인딩합니다.
switchport access vlan dynamic	개인용 VLAN을 구성합니다.
show mac-to-vlan	MAC 대 VLAN 데이터베이스를 표시합니다.
no mac-to-vlan mac-address	VLAN에서 MAC 주소 바인딩을 취소합니다.

다음은 CLI 명령의 예입니다.

```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123
```

```
console(config-vlan)# exit
```

```
console(config)# exit
```

```
console# show vlan mac-to-vlan
```

MAC Address VLAN

-----

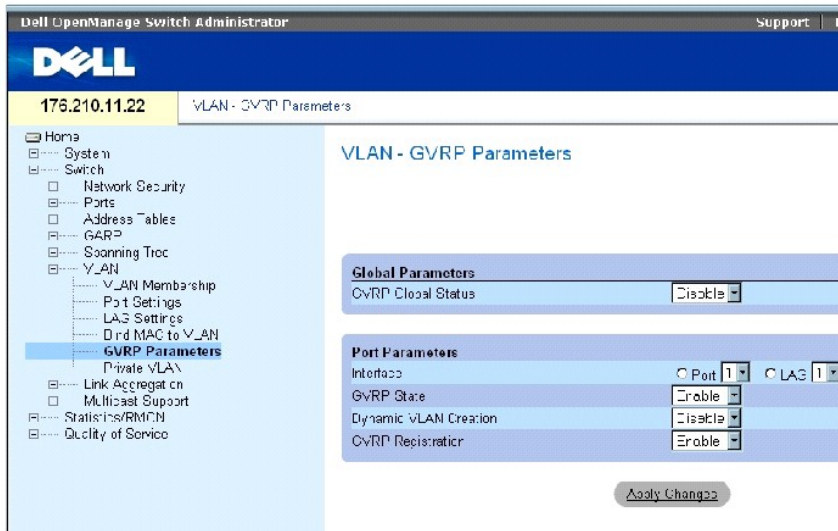
0060.704c.73ff 123

## GVRP 매개변수 구성

GVRP(GARP VLAN 등록 프로토콜)는 VLAN 인식 브리지 사이에 VLAN 멤버십 정보를 자동 배포하기 위해 특별히 제공됩니다. GVRP는 각 브리지의 개별적인 구성 및 VLAN 멤버십 등록 없이 VLAN 인식 브리지가 VLAN 대 브리지 포트 매핑을 자동으로 습득할 수 있게 합니다.

[GVRP Parameters](#) 페이지는 GVRP를 전역적으로 활성화합니다. GVRP는 인터페이스별로 활성화할 수도 있습니다. [GVRP Parameters](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**VLAN**→**GVRP Parameters**를 클릭하십시오.

그림 7-34. GVRP 매개변수



[GVRP Parameters](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**GVRP Global Status** — 장치에 GVRP를 활성화 또는 비활성화합니다. GVRP는 기본적으로 비활성화되어 있습니다.

**Interface** — GVRP 설정을 편집할 포트 또는 LAG를 지정합니다.

**GVRP State** — 인터페이스의 GVRP를 활성화 또는 비활성화합니다.

**Dynamic VLAN Creation** — 인터페이스에서 GVRP를 통한 VLAN 생성을 활성화 또는 비활성화합니다.

**GVRP Registration** — 인터페이스에서 GVRP를 통한 VLAN 등록을 활성화 또는 비활성화합니다.

### 장치에 GVRP 활성화

1. GVRP Global Parameters 페이지를 여십시오.
2. GVRP Global Status 필드에서 **Enable**을 선택합니다.
3. **Apply Changes**를 클릭하십시오.

장치에 GVRP가 활성화됩니다.

### GVRP를 통한 VAN 등록 활성화

1. GVRP Global Parameters 페이지를 여십시오.
2. GVRP Global Status에서 **Enable**을 선택합니다.
3. 원하는 인터페이스의 GVRP State 필드에서 **Enable**을 선택합니다.
4. GVRP Registration 필드에서 **Enable**을 선택합니다.
5. **Apply Changes**를 클릭하십시오.

포트의 GVRP VLAN 등록이 활성화되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 GVRP 구성

다음 표는 GVRP Global Parameters 페이지에 표시된 것과 같이 GVRP를 구성하는 해당 CLI 명령을 요약합니다.

표 7-85. GVRP 전역 매개변수 CLI 명령

CLI 명령	설명
<code>gvrp enable (global)</code>	GVRP를 전역적으로 활성화합니다.
<code>gvrp enable (interface)</code>	인터페이스의 GVRP를 활성화합니다.
<code>gvrp vlan-creation-forbid</code>	동적 VLAN 생성을 활성화 또는 비활성화합니다.
<code>gvrp registration-forbid</code>	모든 VLAN의 등록을 해제하고 포트의 동적 VLAN 등록을 방지합니다.
<code>show gvrp configuration [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	타이머 값, GVRP 또는 동적 VLAN 생성의 활성화 여부 및 어느 포트가 GVRP를 실행하는지를 포함하는 GVRP 구성 정보를 표시합니다.
<code>show gvrp error-statistics [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	GVRP 오류 통계를 표시합니다.
<code>show gvrp statistics [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	GVRP 통계를 표시합니다.
<code>clear gvrp statistics [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	모든 GVRP 통계 정보를 지웁니다.

다음은 CLI 명령의 예입니다.

```
console(config)# gvrp enable
```

```

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device

Maximum VLANs: 223


```


Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
----	-----	-----	-----	-----	-----	-----
--						
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

## 개인용 VLAN 구성

PVLAN(개인용 VLAN)은 VLAN 내의 내부 포트 통신을 제한하여 네트워크 보안을 강화합니다. 개인용 VLAN은 총 2 레벨에서 네트워크 처리량을 제한합니다. 네트워크 관리자가 주 VLAN을 정의합니다. 주 VLAN 내에는 격리 및 커뮤니티 VLAN이 있습니다. 개인용 VLAN 포트는 다음과 같은 상태를 가질 수 있습니다.

- 1 무차별** — 무차별 포트는 PVLAN 내의 모든 포트와 통신할 수 있습니다. 모든 무차별 패킷은 격리 및 커뮤니티 VLAN 모두에 자동으로 지정됩니다.
- 1 격리** — 격리 포트는 같은 PVLAN 내의 다른 포트와 완전히 격리됩니다. 그러나 격리 포트는 무차별 포트와 통신할 수 있습니다. 또한, VLAN과 함께 포트에서 송수신되는 모든 처리량은 무차별 포트로부터의 처리량을 제외하고 모두 차단됩니다. 모든 격리 포트는 자동으로 격리 VLAN에 지정됩니다.
- 1 커뮤니티** — 커뮤니티 포트는 다른 커뮤니티 포트 및 무차별 포트와 통신합니다. 커뮤니티 포트는 다른 커뮤니티의 모든 인터페이스 및 같은 PVLAN의 격리 포트와 분리됩니다. 모든 커뮤니티 포트는 자동으로 커뮤니티 VLAN 및 개인 VLAN에 지정됩니다.

 **주:** 포트가 기존 VLAN의 구성요소이면 무차별 또는 격리 포트로 정의될 수 없습니다.

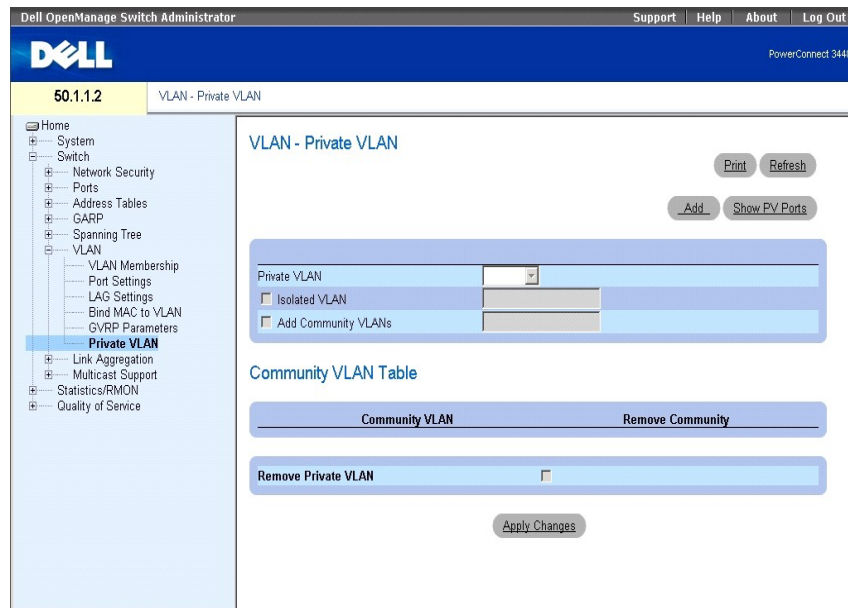
 **주:** 이전에 생성된 VLAN은 격리 또는 커뮤니티 VLAN으로 구성될 수 없습니다.

 **주:** 격리 및 커뮤니티 VLAN은 총 VLAN 수에 포함됩니다.

주 VLAN이 삭제된 경우, 격리 및 커뮤니티 VLAN도 모두 삭제됩니다. 또한, 격리 및 커뮤니티 VLAN은 태그화되지 않은 처리량만 전달합니다.

[Private VLAN](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **VLAN** → **Private VLAN**을 클릭하십시오.

그림 7-35. 개인용 VLAN



[Private VLAN](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Private VLAN** — 사용자 정의된 개인용 VLAN의 목록을 포함합니다. 개인용 VLAN은 [Add Private VLAN](#) 페이지에서 정의됩니다.

**Isolated VLAN** — 어느 VLAN이 어느 격리 포트에 지정되는지를 표시합니다.

**Add Community VLANs** — 커뮤니티 포트가 지정된 커뮤니티 VLAN을 추가합니다.

**Community VLAN** — 커뮤니티 VLAN의 목록을 표시합니다.

**Remove Community** — 이 항목을 선택하면 커뮤니티 VLAN을 제거합니다.

**Remove Private VLAN** — 이 항목을 선택하면 개인용 VLAN을 제거합니다.

### 개인용 VLAN 추가

1. [Private VLAN](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오. [Add Private VLAN](#) 페이지가 열립니다.

그림 7-36. 개인용 VLAN 추가

Refresh

### Add Private VLAN

New Private VLAN

Add Community VLANs

Isolated VLAN

Apply Changes

[Add Private VLAN](#) 페이지에는 다음과 같은 추가 필드가 포함되어 있습니다.

**New Private VLAN** — 개인용 VLAN 목록을 포함합니다. 커뮤니티 VLAN은 개인용 VLAN에 추가됩니다.

**Add Community VLANs** — 커뮤니티 VLAN을 개인용 VLAN에 추가합니다.

**Isolated VLAN** — 격리 VLAN을 개인용 VLAN에 추가합니다.

3. 필드를 정의하십시오.
4. **Apply Changes**를 클릭하십시오.

개인용 VLAN이 정의되고 장치가 업데이트됩니다.

## PV 포트 표 표시

1. [Private VLAN](#) 페이지를 여십시오.
2. **Show PV Ports**를 클릭하십시오.

[PV Ports Table](#)이 열립니다.

그림 7-37. PV 포트 표

Refresh

Interface	Type	VLAN ID
1		<input type="text" value="1"/>

Apply Changes

## CLI 명령을 사용하여 PVLAN 구성

다음 표는 [Private VLAN](#) 페이지에 표시된 것과 같이 PVLAN을 구성하는 해당 CLI 명령을 요약합니다.

표 7-86. 개인용 VLAN CLI 명령

CLI 명령	설명
switchport mode private vlan promiscuous	무차별 포트를 무차별 VLAN에 추가합니다.
switchport mode private vlan community	커뮤니티 포트를 커뮤니티 VLAN에 추가합니다.



<code>switchport mode private-vlan isolated</code>	격리 포트를 격리 VLAN에 추가합니다.
<code>private-vlan primary</code>	주 VLAN을 정의합니다.
<code>private-vlan community {add community-vlan-list   remove community-vlan-list }</code>	주 VLAN의 커뮤니티 VLAN을 정의하거나 제거합니다.
<code>private-vlan isolated</code>	주 VLAN의 격리 VLAN을 정의합니다.
<code>switchport private-vlan 개인 VLAN [community 커뮤니티 VLAN]</code>	개인용 VLAN 포트를 정의합니다.
<code>show vlan private-vlan [primary vlan-id]</code>	개인용 주 VLAN을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# vlan
database

console(config-vlan)#vlan
2

console(config-vlan)#exit

console(config)#interface
vlan 2

console(config-if)#
private-vlan primary

console(config)#interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community add
20

console# show vlan
private-vlan

console(config-if)# end

```

## 포트 결합

링크 결합은 일련의 포트들을 함께 링크하여 하나의 LAG(결합 그룹)를 형성함으로써 포트 사용을 최적화합니다. 포트 결합은 장치 간의 대역폭을 배가하고, 포트 유연성을 높여주며 링크 중복성을 제공합니다.

본 장치는 정적 LAG 및 LACP(링크 결합 제어 프로토콜) LAG를 모두 지원합니다. LACP LAG는 포트의 링크와 다른 장치에 위치한 다른 LACP 포트와의 결합을 협상합니다. 다른 장치 포트도 LACP 포트인 경우 장치는 해당 포트 사이에 LAG를 형성합니다.

포트를 결합할 때는 다음과 같은 사항을 고려해야 합니다.

- 1 LAG 내의 모든 포트가 같은 미디어 종류여야 합니다.
- 1 포트에 VLAN이 구성되어 있지 않습니다.
- 1 포트가 다른 LAG에 지정되어 있지 않습니다.
- 1 포트에 자동 조정 모드가 구성되어 있지 않습니다.
- 1 포트가 전이중 방식 모드에 있습니다.
- 1 LAG의 모든 포트가 같은 수신 필터링 및 태그된 모드를 가지고 있습니다.
- 1 LAG의 모든 포트가 같은 백 프레셔 및 흐름 제어 모드를 가지고 있습니다.
- 1 LAG의 모든 포트가 같은 우선 순위를 가지고 있습니다.
- 1 LAG의 모든 포트가 같은 수신기 종류를 가지고 있습니다.
- 1 본 장치는 최대 8개의 LAG와 각 LAG 당 8개의 포트를 지원합니다.
- 1 Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

LAG에 추가된 포트는 개별 포트 구성을 잃게 됩니다. LAG에서 포트가 제거되면 원래 포트 구성이 포트에 적용됩니다.

본 장치는 해시 기능을 사용하여 어느 결합 링크 구성원이 어느 패킷을 처리할 지를 결정합니다. 해시 기능은 결합 링크 구성원의 부하를 통계적으로 밸런싱합니다. 본 장치는 결합 링크를 단일 논리 포트로 간주합니다.

## LACP 매개변수 정의

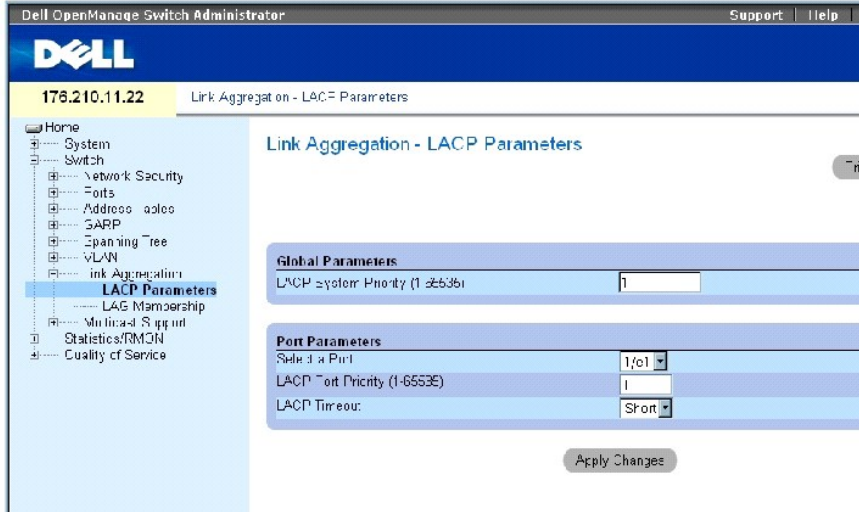
결합 포트는 링크 결합 포트 그룹에 링크될 수 있습니다. 각 그룹은 동일한 속도의 포트에 이루어지며 전이중 방식 작동으로 설정됩니다.

LAG(링크 결합 그룹)의 포트는 포트가 같은 속도에서 작동할 경우 서로 다른 미디어 유형을 포함할 수 있습니다. 결합 링크는 관련 링크에 LACP(링크 결합 제어 프로토콜)을 활성화함으로써 수동 또는 자동으로 구성될 수 있습니다.

## LACP 매개변수 정의

**LACP 매개변수** 페이지는 LACP LAG를 구성할 수 있는 필드를 포함합니다. 결합 포트는 링크 결합 포트 그룹에 링크될 수 있습니다. 각 그룹은 같은 속도의 포트에 이루어져 있습니다. 결합 링크는 관련 링크에 LACP(링크 결합 제어 프로토콜)을 활성화함으로써 수동으로 설치하거나 자동으로 설정할 수 있습니다. [LACP Parameters](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **Link Aggregation** → **LACP Parameters**를 클릭하십시오.

그림 7-38. LACP 매개변수



[LACP Parameters](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**LACP System Priority (1-65535)** — 전역 설정을 위한 LACP 우선 순위 값입니다. 가능한 범위는 1-65535입니다. 기본값은 1입니다.

**Select a Port** — 시간 초과 및 우선 순위 값이 지정된 포트 번호입니다.

**LACP Port Priority (1-65535)** — 포트에 대한 LACP 우선 순위 값입니다.

**LACP Timeout** — 관리 LACP 시간 초과입니다. 다음과 같은 필드 값을 가질 수 있습니다.

**Short** — 짧은 시간 초과 값을 지정합니다.

**Long** — 긴 시간 초과 값을 지정합니다.

### 링크 결합 전역 매개변수 정의

1. [LACP Parameters](#) 페이지를 여십시오.
2. **LACP System Priority** 필드를 작성합니다.
3. **Apply Changes**를 클릭하십시오.

매개변수가 정의되고 장치가 업데이트됩니다.

### 링크 결합 포트 매개변수 정의

1. [LACP Parameters](#) 페이지를 여십시오.
2. **Port Parameters** 영역의 필드를 작성합니다.
3. **Apply Changes**를 클릭하십시오.

매개변수가 정의되고 장치가 업데이트됩니다.

## LACP 매개변수 표 표시

1. [LACP Parameters](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

LACP 매개변수 표가 열립니다.

## CLI 명령을 사용한 LACP 매개변수 구성

다음 표는 [LACP Parameters](#) 페이지에 표시된 것과 같이 LACP 매개변수를 구성할 수 있는 해당 CLI 명령을 요약합니다.

표 7-87. LACP 매개변수 CLI 명령

CLI 명령	설명
lacp system-priority 값	시스템 우선 순위를 구성합니다.
lacp port-priority 값	물리 포트의 우선 순위 값을 구성합니다.
lacp timeout {long   short}	관리 LACP 시간 초과를 지정합니다.
show lacp ethernet 인터페이스 [parameters   statistics   protocol-state]	이더넷 포트에 대한 LACP 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```
Console (config)# lacp
system-priority 120

Console (config)#
interface ethernet 1/e11

Console (config-if)# lacp
port-priority 247

Console (config-if)# lacp
timeout long

Console (config-if)# end

Console# show lacp
ethernet 1/e11 statistics

Port 1/e11 LACP
Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

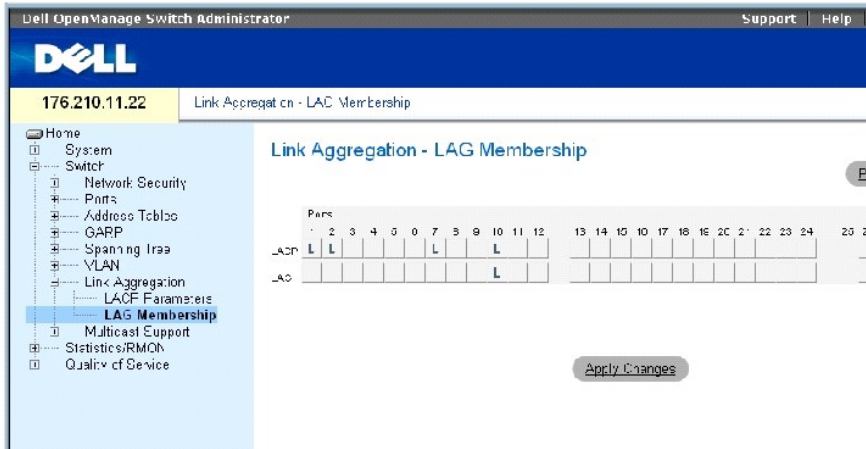
## LAG 구성원 정의

본 장치는 장치가 독립 실행형 장치이든지 스택에 있든지 상관 없이 시스템 당 8개의 LAG 및 LAG 당 8개의 포트를 지원합니다.

포트가 LAG에 추가되면 포트는 LAG의 등록 정보를 획득합니다. 포트가 LAG의 등록 정보로 구성될 수 없는 경우에는 LAG에 추가되지 않습니다. 오류 메시지가 생성됩니다. 그러나, LAG에 추가하는 첫번째 포트가 LAG 설정 내에서 구성될 수 없는 경우에는 포트 기본 설정을 사용하여 포트가 LAG에 추가됩니다. 오류 메시지가 생성됩니다. 그러나, 이 포트가 LAG의 유일한 포트이므로 LAG 전체가 LAG에 정의된 설정 대신 해당 포트의 설정으로 작동합니다.

[LAG Membership](#) 페이지를 사용하여 포트를 LAG에 지정합니다. [LAG Membership](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **Link Aggregation** → **LAG Membership**을 클릭하십시오.

그림 7-39. LAG 구성원



[LAG Membership](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**LACP** — LACP를 사용하여 포트를 LAG에 결합합니다.

**LAG** — 포트를 LAG에 추가하고 포트가 속하는 특정 LAG를 표시합니다.

### LAG 또는 LACP에 포트 추가

1. [LAG Membership](#) 페이지를 여십시오.
2. LAG 행(두번째 행)에서 포트를 결합하거나 제거할 LAG 번호로 단추를 토글합니다.
3. LACP 행(첫번째 행)에서 포트 번호 아래의 단추를 토글하여 LACP 또는 정적 LAG를 지정합니다.
4. **Apply Changes**를 클릭하십시오.

포트가 LAG 또는 LACP에 추가되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 LAG에 포트 추가

다음 표는 [LAG Membership](#) 페이지에 표시된 것과 같이 LAG에 포트를 지정할 수 있는 해당 CLI 명령을 요약합니다.

표 7-88. LAG 구성원 CLI 명령

CLI 명령	설명
<code>channel-group 포트-채널-번호 mode {on   auto}</code>	포트를 포트 채널에 연관시킵니다. 인터페이스에서 채널 그룹 구성을 제거하려면 이 명령의 no 형식을 사용합니다.

<code>show interfaces port-channel [ 포트-채널-번호 ]</code>	포트 채널 번호를 표시합니다.
--	------------------

다음은 CLI 명령의 예입니다.

```
console(config)# interface
ethernet 1/e11

console(config-if)#
channel-group 1 mode on
```

## 멀티캐스트 전달 지원


멀티캐스트 전달은 단일 패킷이 여러 대상에 전달될 수 있게 합니다. 총 2 멀티캐스트 서비스는 특정 멀티캐스트 주소에 어드레스된 단일 패킷을 수신하는 총 2 장치에 기반합니다. 멀티캐스트 전달은 패킷의 사본을 생성하여 관련 포트에 전송합니다.

**등록된 멀티캐스트 처리량** — 등록된 멀티캐스트 그룹에 어드레스된 처리량이 보이면 멀티캐스트 필터링 데이터베이스의 항목에 의해 처리되고 등록된 포트에만 전달됩니다.

**미등록 멀티캐스트 처리량** — 미등록 멀티캐스트 그룹에 어드레스된 처리량이 보이면 멀티캐스트 필터링 데이터베이스에 있는 특별 항목에 의해 처리됩니다. 이 항목의 기본 설정은 그러한 처리량(미등록 멀티캐스트 그룹의 처리량)을 모두 전달하는 것입니다.

본 장치는 다음과 같은 기능을 지원합니다.

- 1. **1:2 멀티캐스트 패킷 전달** — 총 2 멀티캐스트 패킷을 전달합니다. 총 2 멀티캐스트 필터링이 기본으로 활성화되며 사용자가 구성할 수 없습니다.

 **주:** 본 시스템은 256개의 멀티캐스트 그룹에 대한 멀티캐스트 필터링을 지원합니다.

- 1. **1:2 멀티캐스트 패킷 필터링** — 총 2 패킷을 인터페이스에 전달합니다. 멀티캐스트 필터링이 비활성화되어 있는 경우 멀티캐스트 패킷은 모든 관련 포트에 전달됩니다.

**멀티캐스트 지원** 페이지를 열려면, 트리 뷰에서 **Switch** → **Multicast Support**를 클릭하십시오.

## 멀티캐스트 전역 매개변수 정의

총 2 교환은 기본으로 멀티캐스트 패킷을 단일 멀티캐스트 전송으로 관리하여 해당 패킷을 모든 관련 VLAN 포트에 전달합니다. 멀티캐스트 처리량 전달은 효과적이긴 하지만 관련되지 않은 포트도 멀티캐스트 패킷을 수신하므로 최적의 방법은 아닙니다. 과도한 패킷은 네트워크 처리량 증가를 유발합니다. 멀티캐스트 전달 필터는 총 2 패킷을 포트 하위집합에 전달할 수 있게 합니다.

IGMP 스누핑은 전역적으로 활성화되어 모든 IGMP 패킷이 CPU에 전달됩니다. CPU는 수신 패킷을 분석하여 다음과 같은 사항을 결정합니다.

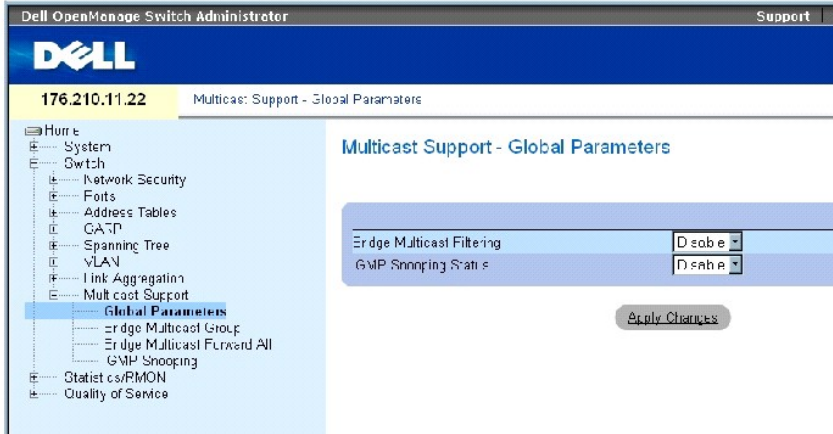
- 1. 어느 포트가 어느 멀티캐스트 그룹에 참여하고자 하는지에 대한 정보
- 1. 어느 포트가 IGMP 질의를 생성하는 멀티캐스트 라우터를 가지고 있는지에 대한 정보
- 1. 어느 라우팅 프로토콜이 패킷과 멀티캐스트 처리량을 전달하는지에 대한 정보

특정 멀티캐스트 그룹에 참여를 요청하는 포트는 멀티캐스트 그룹이 구성원을 수용량을 지정하는 **IGMP** 보고서를 발행합니다. 이에 따른 결과로 멀티캐스트 필터링 데이터베이스가 생성됩니다.

**멀티캐스트 지원** 페이지를 열려면, 트리 뷰에서 **Switch** → **Multicast Support**를 클릭하십시오.

[Global Parameters](#) 페이지는 장치에 IGMP 스누핑을 활성화할 수 있는 필드를 포함합니다. [Global Parameters](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **Multicast Support** → **Global Parameters**를 클릭하십시오.

그림 7-40. 전역 매개변수



[Global Parameters](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**Bridge Multicast Filtering** — 브리지 멀티캐스트 필터링을 활성화 또는 비활성화합니다. 비활성이 기본값입니다.

**IGMP Snooping Status** — 장치에 IGMP 스누핑을 활성화 또는 비활성화합니다. 비활성이 기본값입니다. IGMP 스누핑은 [전역 매개변수](#)가 활성화된 경우에만 활성화할 수 있습니다.

### 장치에 브리지 멀티캐스트 필터링 활성화

1. [Global Parameters](#) 페이지를 여십시오.
2. **Bridge Multicast Filtering** 필드에서 **Enable**를 선택합니다.
3. **Apply Changes**를 클릭하십시오.

장치에 브리지 멀티캐스트 **필터링**이 활성화됩니다.

### 장치에 IGMP 스누핑 활성화

1. [Global Parameters](#) 페이지를 여십시오.
2. **IGMP Snooping Status** 필드에서 **Enable**를 선택합니다.
3. **Apply Changes**를 클릭하십시오.

장치에 IGMP 스누핑이 활성화됩니다.

### CLI 명령을 사용하여 멀티캐스트 필터링 및 IGMP 스누핑 활성화

다음 표는 [Global Parameters](#) 페이지에 표시된 것과 같이 멀티캐스트 필터링 및 IGMP 스누핑을 활성화할 수 있는 해당 CLI 명령을 요약합니다.

표 7-89. 멀티캐스트 필터링 및 스누핑 CLI 명령

CLI 명령	설명
bridge multicast filtering	멀티캐스트 주소의 필터링을 활성화합니다.

**ip igmp snooping** | IGMP(인터넷 그룹 구성원 프로토콜) 스누핑을 활성화합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# bridge
multicast filtering

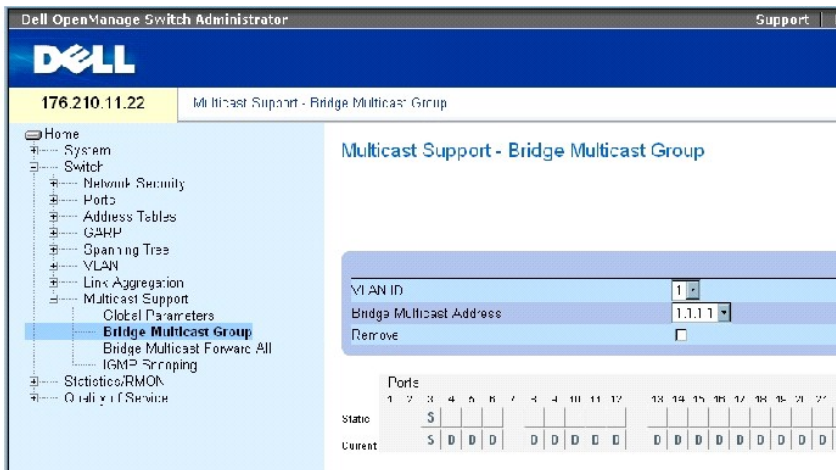
console(config)# ip igmp
snooping
```

## 브리지 멀티캐스트 주소 구성원 추가

[Bridge Multicast Group](#) 페이지는 포트 및 LAG 테이블에 멀티캐스트 서비스 그룹에 연결된 포트 및 LAG를 표시합니다. 또한, 포트 및 LAG 테이블은 포트 또는 LAG가 멀티캐스트 그룹에 참여하는 방식도 반영합니다. 포트는 기존 그룹 또는 새 멀티캐스트 서비스 그룹에 추가될 수 있습니다. [Bridge Multicast Group](#) 페이지는 새 멀티캐스트 서비스 그룹을 생성할 수 있게 합니다. 또한, [Bridge Multicast Group](#) 페이지는 특정 멀티캐스트 서비스 주소 그룹에 포트를 지정합니다.

[Bridge Multicast Group](#) 페이지를 열려면, 트리 뷰에서 **Switch**→**Multicast Support**→**Bridge Multicast Group**를 클릭하십시오.

표 7-41. 브리지 멀티캐스트 그룹



[Bridge Multicast Group](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**VLAN ID** — VLAN을 식별하고 멀티캐스트 그룹 주소에 대한 정보를 포함합니다.

**Bridge Multicast Address** — 멀티캐스트 그룹 MAC 주소/IP 주소를 식별합니다.

**Remove** — 이 항목을 선택하면 브리지 멀티캐스트 주소가 제거됩니다.

**Ports** — 멀티캐스트 서비스에 추가될 수 있는 포트입니다.

**LAGs** — 멀티캐스트 서비스에 추가될 수 있는 LAG입니다.



다음 표는 IGMP 포트 및 LAG 구성원 관리 설정을 포함합니다.

표 7-90. IGMP 포트/LAG 구성원 포트 제어 설정

포트 제어	정의
D	포트/LAG가 <b>현재</b> 행에 동적으로 있는 멀티캐스트 그룹에 참여했습니다.
S	포트를 <b>정적</b> 행의 정적 구성원으로서 멀티캐스트 그룹에 첨부합니다. 포트/LAG가 <b>현재</b> 행에 정적으로 있는 멀티캐스트 그룹에 참여했습니다.
F	사용이 금지되어 있습니다.
비어 있음	포트가 멀티캐스트 그룹에 연결되어 있지 않습니다.

### 브리지 멀티캐스트 주소 추가

1. [Bridge Multicast Group](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

[Add Bridge Multicast Group](#) 페이지가 열립니다.

그림 7-42. 브리지 멀티캐스트 그룹 추가

### Add Bridge Multicast Group

Refresh

VLAN ID	<input type="text"/>	
New Bridge IP Multicast	<input type="text"/>	(X.X.X.X)
New Bridge MAC Multicast	<input type="text"/>	(XX:XX:XX:XX:XX:XX)

Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static	S																									
Current	S	D	D	D																						

3. **VLAN ID** 및 **New Bridge Multicast Address** 필드를 정의합니다.
4. 포트를 선택한 멀티캐스트 그룹에 참여시키려면 포트를 **S**로 토글합니다.
5. 특정 멀티캐스트 주소를 특정 포트에 추가하는 것을 금지하려면 포트를 **F**로 토글합니다.
6. **Apply Changes**를 클릭하십시오.

브리지 멀티캐스트 주소가 멀티캐스트 그룹에 지정되고 장치가 업데이트됩니다.

### 멀티캐스트 서비스 수신 포트 정의

1. [Bridge Multicast Group](#) 페이지를 여십시오.
2. **VLAN ID** 및 **Bridge Multicast Address** 필드를 정의합니다.
3. 포트를 선택한 멀티캐스트 그룹에 참여시키려면 포트를 **S**로 토글합니다.
4. 특정 멀티캐스트 주소를 특정 포트에 추가하는 것을 금지하려면 포트를 **F**로 토글합니다.
5. **Apply Changes**를 클릭하십시오.

포트가 멀티캐스트 그룹에 지정되고 장치가 업데이트됩니다.

### 멀티캐스트 서비스 수신 LAG 지정

1. [Bridge Multicast Group](#) 페이지를 여십시오.
2. **VLAN ID** 및 **Bridge Multicast Address** 필드를 정의합니다.
3. LAG를 선택한 멀티캐스트 그룹에 참여시키려면 LAG를 **S**로 토글합니다.
4. 특정 멀티캐스트 주소를 특정 LAG에 추가하는 것을 금지하려면 LAG를 **F**로 토글합니다.
5. **Apply Changes**를 클릭하십시오.

LAG가 멀티캐스트 그룹에 지정되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 멀티캐스트 서비스 구성원 관리

다음 표는 [Bridge Multicast Group](#) 페이지에 표시된 것과 같이 멀티캐스트 서비스 구성원을 관리할 수 있는 해당 CLI 명령을 요약합니다.

표 7-91. 멀티캐스트 서비스 구성원 CLI 명령

CLI 명령	설명
bridge multicast address {mac-멀티캐스트-주소   ip-멀티캐스트-주소}	MAC 층 멀티캐스트 주소를 브리지 표에 등록하고 정적 포트를 그룹에 추가합니다.
bridge multicast forbidden address {mac-멀티캐스트-주소   ip-멀티캐스트-주소}{add   remove} {ethernet 인터페이스-목록   port-channel 포트-채널-번호-목록}	특정 멀티캐스트 주소를 특정 포트에 추가하는 것을 금지합니다. 기본적으로 돌아가려면 이 명령의 no 형식을 사용합니다.
show bridge multicast address-table [vlan vlan-id] [address {mac-멀티캐스트-주소   ip-멀티캐스트-주소}] [format ip   mac]	멀티캐스트 MAC 주소 표 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table

```

Vlan	MAC Address	Type	Ports
----	-----	----	-----
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12

```

Forbidden ports for multicast addresses:

```

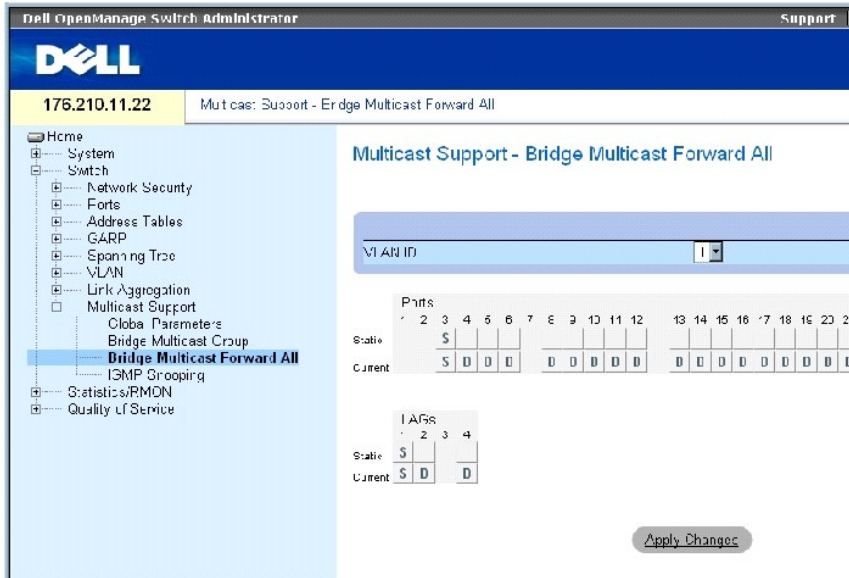
Vlan	MAC Address	Ports	
----	-----	-----	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	
console # show bridge multicast address-table format ip			
Vlan	IP Address	Type	Ports
----	-----	-----	-----
1	224-239.130 2.2.3	static	1/e11, 1/e12
19	224-239.130 2.2.8	static	1/e11-16
19	224-239.130 2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	-----	-----	
1	224-239.130 2.2.3	1/e8	
19	224-239.130 2.2.8	1/e8	

## 멀티캐스트 전체 전달 매개변수 지정

[Bridge Multicast Forward All](#) 페이지는 주변 멀티캐스트 라우터/스위치에 연결된 장치에 포트 또는 LAG를 연결할 수 있는 필드를 포함합니다. 일단 IGMP 스누핑이 활성화되면 멀티캐스트 패킷이 적절한 포트 또는 VLAN에 전달됩니다.

[Bridge Multicast Forward All](#) 페이지를 열려면, 트리 뷰에서 **Switch** → **Multicast Support** → [Bridge Multicast Forward All](#) 페이지를 클릭하십시오.

그림 7-43. 브리지 멀티캐스트 전체 전달



[브리지 멀티캐스트 전체 전달](#) 페이지에는 다음과 같은 필드가 포함되어 있습니다.

**VLAN ID** — VLAN을 식별합니다.

**Ports** — 멀티캐스트 서비스에 추가될 수 있는 포트입니다.

**LAGs** — 멀티캐스트 서비스에 추가될 수 있는 LAG입니다.

[브리지 멀티캐스트 전체 전달 스위치/포트 제어 설정 표](#)는 라우터 및 포트 설정을 관리할 수 있는 설정을 포함합니다.

### 브리지 멀티캐스트 전체 전달 스위치/포트 제어 설정 표 관리

다음 표는 포트 제어를 설정하는 데 사용되는 컨트롤을 설명합니다.

표 7-92. 브리지 멀티캐스트 전체 전달 스위치/포트 제어 설정 표

포트 제어	정의
D	포트를 멀티캐스트 라우터 또는 스위치에 동적 포트로 연결합니다.
S	포트를 멀티캐스트 라우터 또는 스위치에 정적 포트로 연결합니다.
F	사용이 금지되어 있습니다.
비어 있음	포트가 멀티캐스트 라우터 또는 스위치에 연결되어 있지 않습니다.

### 멀티캐스트 라우터 또는 스위치에 포트 연결

1. [Bridge Multicast Forward All](#) 페이지를 여십시오.
2. **VLAN ID** 필드를 정의합니다.

3. **포트** 표에서 포트를 선택하고 포트에 값을 지정합니다.
4. **Apply Changes**를 클릭하십시오.

포트가 멀티캐스트 라우터 또는 스위치에 연결됩니다.

### 멀티캐스트 라우터 또는 스위치에 LAG 연결

1. [Bridge Multicast Forward All](#) 페이지를 여십시오.
2. **VLANID** 필드를 정의합니다.
3. **LAG** 표에서 포트를 선택하고 LAG에 값을 지정합니다.
4. **Apply Changes**를 클릭하십시오.

LAG가 멀티캐스트 라우터 또는 스위치에 연결됩니다.

### CLI 명령을 사용하여 멀티캐스트 라우터에 연결된 LAG 및 포트 관리

다음 표는 [Bridge Multicast Forward All](#) 페이지에 표시된 것과 같이 멀티캐스트 라우터에 연결된 LAG 및 포트를 관리할 수 있는 해당 CLI 명령을 요약합니다.

표 7-93. 멀티캐스트 라우터에 연결된 LAG 및 포트를 관리하기 위한 CLI 명령

CLI 명령	설명
<code>show bridge multicast filtering vlan-id</code>	멀티캐스트 필터링 구성을 표시합니다.
<code>bridge multicast forward-all {add   remove} {ethernet 인터페이스-목록   port-channel 포트-채널-번호-목록}</code>	포트에서 모든 멀티캐스트 패킷의 전달을 활성화합니다. 기본값으로 돌아가려면 이 명령의 no 형식을 사용합니다.

다음은 CLI 명령의 예입니다.

```

Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1
  
```

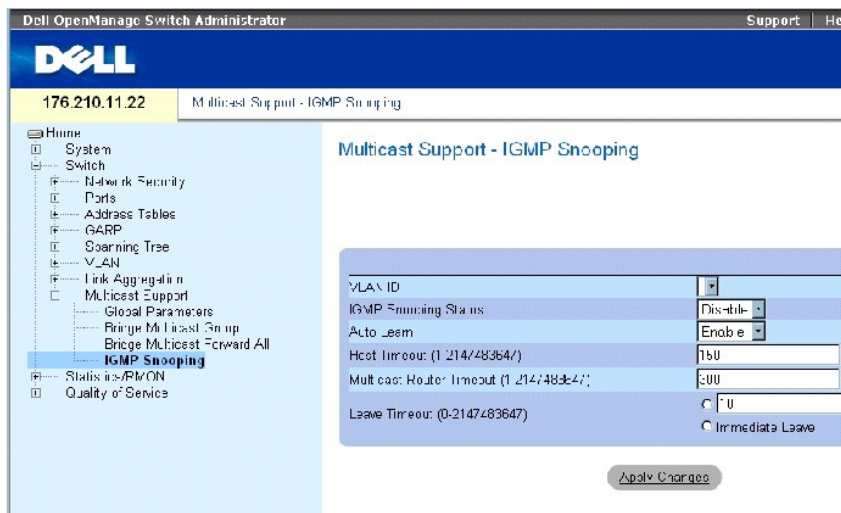
Filtering: Enabled		
VLAN:	Forward-All	
Port	Static	Status
-----	-----	-----
1/e11	Forbidden	Filter

1/e12	Forward	Forward(s)
1/e13	-	Forward(d)

## IGMP 스누핑

IGMP 스누핑 페이지는 VLAN 별로 IGMP 스누핑을 활성화하고 패킷의 수명 시간을 정의할 수 있는 필드를 포함합니다. [IGMP Snooping](#) 페이지를 열려면, 트리 뷰에서 **Switch→ Multicast Support→ IGMP Snooping**을 클릭하십시오.

그림 7-44. IGMP 스누핑



**VLAN ID** — VLAN ID를 지정합니다.

**IGMP Snooping Status** — VLAN에 IGMP 스누핑을 활성화 또는 비활성화합니다.

**Auto Learn** — 이더넷 장치에 자동 습득을 활성화 또는 비활성화합니다.

**Host Timeout (1-2147483647)** — IGMP 스누핑 항목의 수명이 만료될 때까지의 시간입니다. 기본값은 260초입니다.

**Multicast Router Timeout (1-2147483647)** — 멀티캐스트 라우터 항목의 수명이 만료될 때까지의 시간입니다. 기본값은 300초입니다.

**Leave Timeout (0-2147483647)** — 포트 나가기 메시지가 수신된 후 항목의 수명이 만료될 때까지의 시간(초)입니다. 기본값은 10초입니다.

### 장치에 IGMP 스누핑 활성화

1. [IGMP Snooping](#) 페이지를 여십시오.
2. IGMP 스누핑이 활성화되어야 할 장치에 대한 VLAN ID를 선택합니다.
3. **IGMP Snooping Status** 필드에서 **Enable**를 선택합니다.
4. 페이지의 필드를 작성합니다.
5. **Apply Changes**를 클릭하십시오.

장치에 IGMP 스누핑이 활성화됩니다.

## IGMP 스누핑 표 표시

1. [IGMP Snooping](#)을 여십시오.
2. **Show All**을 클릭하십시오.

IGMP 스누핑 표가 열립니다.

## CLI 명령을 사용한 IGMP 스누핑 구성

다음 표는 장치의 [IGMP 스누핑](#)을 구성할 수 있는 해당 CLI 명령을 요약합니다.

표 7-94. IGMP 스누핑 CLI 명령

CLI 명령	설명
<code>ip igmp snooping</code>	IGMP(인터넷 그룹 구성원 프로토콜) 스누핑을 활성화합니다.
<code>ip igmp snooping mrouter learn-pim-dvmrp</code>	특정 VLAN의 문맥에 있는 멀티캐스트 라우터 포트의 자동 습득을 활성화합니다.
<code>ip igmp snooping host-time-out time-out</code>	host-time-out을 구성합니다.
<code>ip igmp snooping mrouter-time-out 시간-초과</code>	mrouter-time-out을 구성합니다.
<code>ip igmp snooping leave-time-out { 시간-초과   immediate-leave }</code>	leave-time-out을 구성합니다.
<code>show ip igmp snooping groups [vlan vlan ID] [address ip-멀티캐스트-주소]</code>	IGMP 스누핑으로 습득한 멀티캐스트 그룹을 표시합니다.
<code>show ip igmp snooping interface vlan ID</code>	IGMP 스누핑 구성을 표시합니다.
<code>show ip igmp snooping mrouter [interface vlan-id]</code>	동적으로 습득한 멀티캐스트 라우터 인터페이스에 대한 정보를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console> enable

console# config

console(config)# ip igmp snooping

console(config)# interface vlan 1

console(config-if)# ip igmp
snooping mrouter learn-pim-dvmrp

console(config-if)# ip igmp
snooping host-time-out 300

Console(config-if)# ip igmp
snooping mrouter-time-out 200

console(config-if)# ip igmp
snooping leave-time-out 60
```

```
console(config-if)# end
```

```
console# show ip igmp snooping  
groups
```

Vlan	IP Address	Querier	Ports
-----	-----	-----	-----
-	-----	---	-----
---	---	---	---
1	224- 239.130 2.2.3	Yes	1/e11, 1/e12
19	224- 239.130 2.2.8	Yes	1/e11- 13

```
console# show ip igmp snooping  
interface 1/e1
```

```
IGMP Snooping is globally enabled
```

```
IGMP Snooping is enabled on VLAN 1
```

```
IGMP host timeout is 300 sec
```

```
IGMP Immediate leave is disabled.  
IGMP leave timeout is 60 sec
```

```
IGMP mrouter timeout is 200 sec
```

```
Automatic learning of multicast  
router ports is enabled
```

```
console# show ip igmp snooping  
mrouter
```

VLAN	Ports		
-----	-----		
1	1/e11		



[목차 페이지로 돌아가기](#)

## 통계 보기

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [표 보기](#)
- [ROMN 통계 보기](#)
- [차트 보기](#)

Statistic 페이지는 인터페이스, GVRP, Etherlike, RMON 및 장치 사용에 관한 장치 정보를 포함합니다. **Statistics** 페이지를 열려면 트리 뷰에서 **Statistics**를 클릭하십시오.

 **주:** CLI 명령은 통계 페이지에서 사용할 수 없습니다.

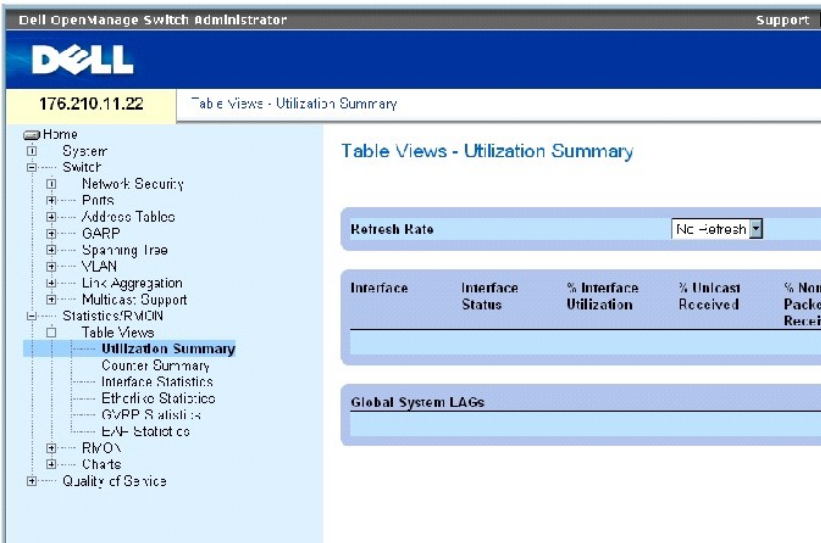
## 표 보기

Table Views 페이지는 표 형식으로 통계를 표시하는 데 관한 연결을 포함합니다. 페이지를 열려면 트리 뷰에서 **Statistics**→**Table**을 클릭하십시오.

## 사용 요약 내용 보기

[Utilization Summary](#) 페이지는 인터페이스 사용에 관한 통계를 포함합니다. 페이지를 열려면 트리 뷰에서 **Statistics**→**Table Views**→**Utilization Summary**를 차례로 클릭하십시오.

그림 8-1. 사용 요약 내용



 **주:** 이 화면은 주기적으로 재생되어 적은 메모리를 가진 컴퓨터에 대한 영향을 최소화합니다. 디스플레이는 이 기간에 중단될 수 있습니다.

[Utilization Summary](#) 페이지는 다음 필드를 포함합니다.

**Refresh Rate**—인터페이스 통계가 재생되기 전까지 경과한 총 시간을 표시합니다.

**Interface** — 인터페이스 번호입니다.

**Interface Status** — 인터페이스 상태입니다.

**% Interface Utilization** — 인터페이스의 이중 모드에 기반한 네트워크 인터페이스 사용 백분율을 표시합니다. 이 수치의 범위는 0~200%입니다. 전이중 연결의 최고 수치 200%는 인터페이스를 통과하는 처리량이 입력 및 출력 연결의 대역폭을 100% 사용하고 있음을 표시합니다. 반이중 연결의 최고 수치는 100%입니다.

**% Unicast Received** — 인터페이스에서 수신한 유니캐스트 패킷의 백분율입니다.

**% Non Unicast Packets Received** — 인터페이스에서 수신한 비 유니캐스트 패킷의 백분율입니다.

**% Error Packets Received** — 인터페이스에서 수신한 오류가 있는 패킷의 백분율입니다.

**Global System LAGs** — 현재 전역 LAG 사용 상황을 표시합니다.

## 카운터 요약 내용 보기

[Counter Summary](#) 페이지는 백분율에 대비한 포트 사용의 숫자 램 통계를 포함합니다. [Counter Summary](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Table Views** → **Counter Summary**를 차례로 클릭하십시오.

그림 8-2. 카운터 요약 내용

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Table Views - Counter Summary". It features a "Refresh Rate" dropdown menu currently set to "No Refresh". Below this is a table with the following columns: "Interface", "Interface Status", "Received Unicast Packets", "Transmit Unicast Packets", and "Received Non Unicast Packets". The table contains one row with the value "1" in the "Interface" column. Below the table is a section titled "Global System LAGs" which also displays the value "1". At the bottom of the page, there is a button labeled "Reset All Counters".

[Counter Summary](#) 페이지는 다음 필드를 포함합니다.

**Refresh Rate** — 인터페이스 통계가 재생되기 전에 경과한 총 시간을 표시합니다.

**Interface** — 인터페이스 번호입니다.

**Interface Status** — 인터페이스 상태입니다.

**Received Unicast Packets** — 인터페이스에서 수신한 유니캐스트 패킷의 수입니다.

**Transmit Unicast Packets** — 인터페이스에서 전송한 유니캐스트 패킷의 수입니다.

**Received Non Unicast Packets** — 인터페이스에서 수신한 비 유니캐스트 패킷의 수입니다.

**Transmit Non Unicast Packets** — 인터페이스에서 전송한 비 유니캐스트 패킷의 수입니다.

**Received Errors** — 인터페이스에서 수신한 오류가 있는 패킷 수입니다.

**Global System LAGs** — 전역 시스템 LAG의 카운터 요약 내용을 제공합니다.

## 인터페이스 통계 보기

[Interface Statistics](#) 페이지는 수신 및 전송한 패킷의 통계를 포함합니다. 수신 및 전송한 패킷에 대한 필드는 같습니다. [Interface Statistics](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Table Views** → **Interface Statistics**를 차례로 클릭하십시오.

표 8-3. 인터페이스 통계

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes the Dell logo and the text "Dell OpenManage Switch Administrator" and "Support". Below the navigation bar, the IP address "176.210.11.22" and the page title "Table Views - Interface Statistics" are visible. The left sidebar contains a tree view with the following items: Home, System, Switch, Network Security, Ports, Address Tables, GARP, Spanning Tree, VLAN, Link Aggregation, Multicast Support, Statistics/RMON, Table Views (highlighted), Utilization Summary, Counter Summary, Interface Statistics (highlighted), Etherlike Statistics, OVRP Statistics, EAP Statistics, RMON, Chassis, and Quality of Service. The main content area is titled "Table Views - Interface Statistics" and contains a filter section with "Interface" (set to "Port"), "LAGs", and "Refresh Rate" (set to "1s Refresh"). Below the filter section are two sections: "Receive Statistics" and "Transmit Statistics". Each section lists "Total Bytes (Octets)", "Unicast Packets", "Multicast Packets", and "Broadcast Packets". A "Reset All Counts" button is located at the bottom right of the main content area.

[Interface Statistics](#) 페이지는 다음 필드를 포함합니다.

**Interface** — 포트 또는 LAG의 통계를 표시하는지 여부를 지정합니다.

**Refresh Rate** — 인터페이스 통계가 재생되기 전에 경과한 총 시간입니다.

## 수신 통계

**Total Bytes (Octets)** — 선택된 인터페이스에서 수신한 옥텟의 총 수입니다.

**Unicast Packets** — 선택된 인터페이스에서 수신한 유니캐스트 패킷의 총 수입니다.

**Multicast Packets** — 선택된 인터페이스에서 수신한 멀티캐스트 패킷의 총 수입니다.

**Unicast Packets** — 선택된 인터페이스에서 수신한 브로드캐스트 패킷의 총 수입니다.

## 전송 통계

**Total Bytes (Octets)** — 선택된 인터페이스에서 전송한 옥텟의 총 수입니다.

**Unicast Packets** — 선택된 인터페이스에서 전송한 유니캐스트 패킷의 총 수입니다.

**Multicast Packets** — 선택된 인터페이스에서 전송한 멀티캐스트 패킷의 총 수입니다.

**Broadcast Packets** — 선택된 인터페이스에서 전송한 브로드캐스트 패킷의 총 수입니다.

## 인터페이스 통계 표시

1. [Interface Statistics](#) 페이지를 여십시오.
2. **Interface** 필드에서 인터페이스를 선택하십시오.

선택된 인터페이스의 통계가 표시됩니다.

## 인터페이스 통계 카운터 재설정

1. [Interface Statistics](#) 페이지를 여십시오.
2. **Reset All Counters**를 클릭하십시오.

인터페이스 통계 카운터가 재설정됩니다.

## CLI 명령을 사용하여 인터페이스 통계 보기

다음 표는 인터페이스 통계를 보는 CLI 명령을 포함합니다.

표 8-95. 인터페이스 통계 CLI 명령

CLI 명령	설명
--------	----

물리적 인터페이스에서 인식한 처리량을 표시합니다.

```
show interfaces counters[ethernet 인터페이스 | port-channel 포트-채널-번호]
```

다음은 CLI 명령의 예입니다.

```
console> enable

console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts
-----
1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

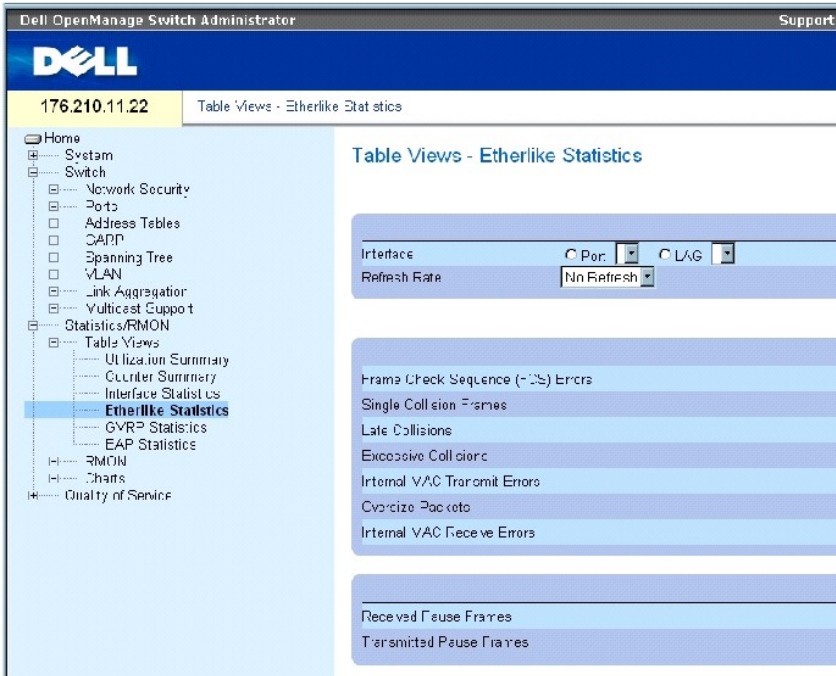
1/e9 0 0 0 0

1/e10 0 0 0 0
```

## Etherlike 통계 보기

[Etherlike Statistics](#) 페이지는 인터페이스 오류 통계를 포함합니다. [Etherlike Statistics](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Table Views** → **Etherlike Statistics**를 차례로 클릭하십시오.

그림 8-4. Etherlike 통계



[Etherlike Statistics](#) 페이지는 다음 필드를 포함합니다.

**Interface** — 포트 또는 LAG의 통계를 표시하는지 여부를 지정합니다.

**Refresh Rate** — 인터페이스 통계가 재생되기 전에 경과한 총 시간입니다.

**Frame Check Sequence (FCS) Errors** — 선택된 인터페이스에서 수신한 FCS 오류 수입니다.

**Single Collision Frames** — 선택된 인터페이스에서 수신한 단일 충돌 프레임 오류 수입니다.

**Late Collisions** — 선택된 인터페이스에서 수신한 지연 충돌 수입니다.

**Oversize Packets** — 선택된 인터페이스의 특대형 패킷 수입니다.

**Internal MAC Transmit Errors** — 선택된 인터페이스의 내부 MAC 전송 오류 수입니다.

**Received Pause Frames** — 선택된 인터페이스의 수신한 일시 중지 오류 수입니다.

**전송된 일시 중지 프레임** — 선택된 인터페이스의 전송 일시 중지 오류 수입니다.

### 인터페이스의 Etherlike 통계 표시

1. [Etherlike Statistics](#) 페이지를 여십시오.
2. **Interface** 필드에서 인터페이스를 선택하십시오.

## Etherlike 통계 재설정

1. [Etherlike Statistics](#) 페이지를 여십시오.
2. **Reset All Counters**를 클릭하십시오.

[Etherlike Statistics](#) 카운터가 재설정됩니다.

## CLI 명령을 사용하여 Etherlike 통계 보기

다음 표는 Etherlike 통계를 보는 CLI 명령을 포함합니다.

표 8-96. Etherlike 통계 CLI 명령

CLI 명령	설명
<code>show interfaces counters[ethernet 인터페이스   port-channel 포트-채널-번호]</code>	물리적 인터페이스에서 인식한 처리량을 표시합니다.

다음은 CLI 명령의 예입니다.

Console# <code>show interfaces counters ethernet 1/1</code>				
Port	IN Octets	InUcastPkts	InMcastPkts	InBcastPkts
----	-----	-----	-----	-----
1/e1	183892	1289	987	8
Port	OUT Octets	OutUcastPkts	OutMcastPkts	OutBcastPkts
----	-----	-----	-----	-----
1/e1	9188	9	8	0
FCS Errors: 8				
Single Collision Frames: 0				
Multiple Collision Frames: 0				

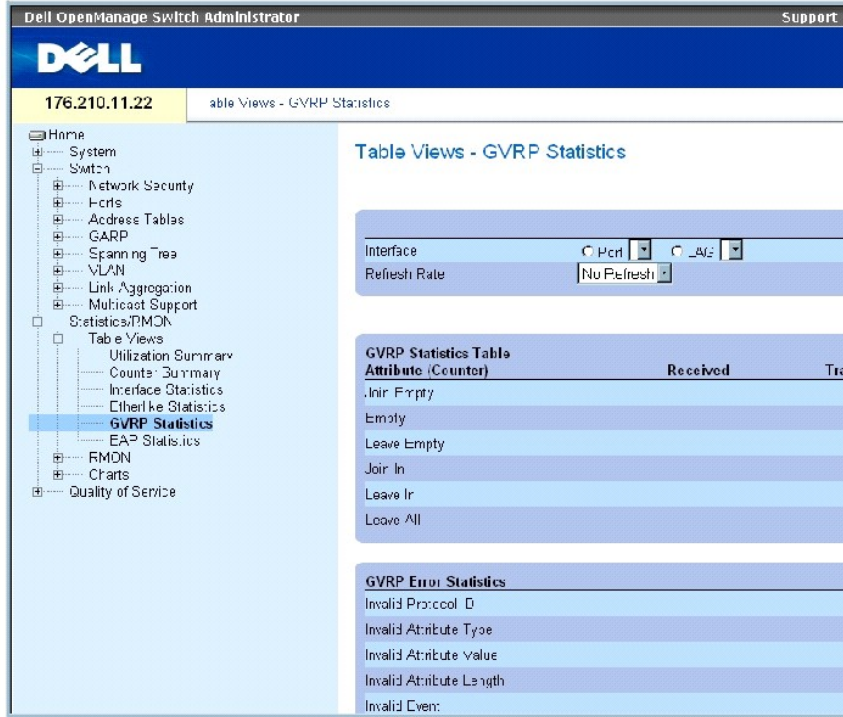
SQE Test Errors: 0	
Deferred Transmissions: 0	
Late Collisions: 0	
Excessive Collisions: 0	
Internal MAC Tx Errors: 0	
Carrier Sense Errors: 0	
Oversize Packets: 0	
Internal MAC Rx Errors: 0	
Received Pause Frames: 0	
Transmitted Pause Frames: 0	

## GVRP 통계 보기

[GVRP Statistics](#) 페이지는 GVRP에 대한 장치 통계를 포함합니다. 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Table Views** → **GVRP Statistics**를 차례로 클릭하십시오.

그림 8-5. GVRP 통계





[GVRP Statistics](#) 페이지는 다음 필드를 포함합니다.

**Interface** — 포트 또는 LAG의 통계를 표시하는지 여부를 지정합니다.

**Refresh Rate** — 인터페이스 통계가 재생되기 전에 경과한 총 시간입니다.

**Join Empty** — 장치 GVRP Join Empty 통계입니다.

**Leave Empty** — 장치 GVRP Leave Empty 통계입니다.

**Empty** — 공백 GVRP 개수 통계를 표시합니다.

**Join In** — 장치 GVRP Join In 통계입니다.

**Leave Empty** — 장치 GVRP Leave in 통계입니다.

**Leave All** — 장치 GVRP Leave all 통계입니다.

**Invalid Protocol ID** — 장치 GVRP 유효하지 않은 프로토콜 ID 통계입니다.

**Invalid Attribute Type** — 장치 GVRP 유효하지 않은 속성 ID 통계입니다.

**Invalid Attribute Value** — 장치 GVRP 유효하지 않은 속성 값 통계입니다.

**Invalid Attribute Length** — 장치 GVRP 유효하지 않은 속성 길이 통계입니다.

**Invalid Event** — 장치 GVRP 유효하지 않은 이벤트 통계입니다.

## 포트에 대한 GVRP 통계 표시

1. [GVRP Statistics](#) 페이지를 여십시오.
2. **Interface** 필드에서 인터페이스를 선택하십시오.

선택된 인터페이스에 대한 GVRP 통계가 표시됩니다.

## GVRP 통계 재설정

1. [GVRP Statistics](#) 페이지를 여십시오.
2. **Reset All Counters**를 클릭하십시오.

GVRP 통계 카운터가 재설정됩니다.

## CLI 명령을 사용하여 GVRP 통계 보기

다음 표는 GVRP 통계를 보는 CLI 명령을 포함합니다.

표 8-97. GVRP 통계 CLI 명령

CLI 명령	설명
<code>show gvrp statistics [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	GVRP 통계를 표시합니다.
<code>show gvrp error- statistics [ethernet 인터페이스   port-channel 포트-채널-번호]</code>	GVRP 오류 통계를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console# show ip interface

GVRP statistics:

-----

Legend:

rJE : Join Empty Received
```

rJIn : Join In Received

rEmp : Empty Received

rLIn : Leave In Received

rLE : Leave Empty Received

rLA : Leave All Received

sJE : Join Empty Sent

sJIn : Join In Sent

sEmp : Empty Sent

sLIn : Leave In Sent

sLE : Leave Empty Sent

sLA : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp : sLIn  
sLE sLA

-----

1/e1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Console# **show gvrp error-statistics**

GVRP error statistics:

-----

Legend:

INVPROT : Invalid Protocol Id

INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type

INVALEN : Invalid Attribute Type

INVAVAL : Invalid Attribute Type

INVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

-----

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0

sLE : Leave Empty Sent

sLA : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE  
sLA

-----

1/e1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

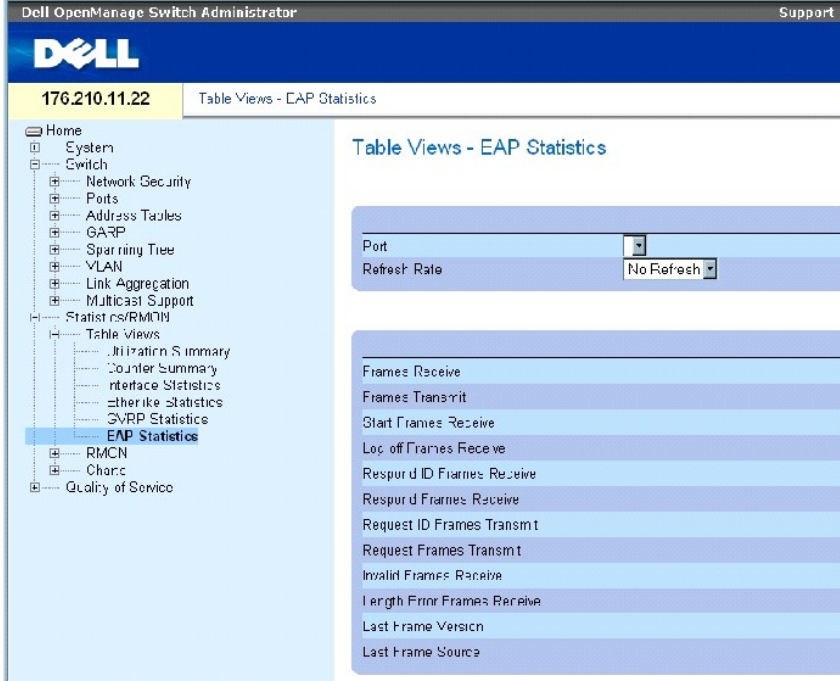
1/e5 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1/e6 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1/e7 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1/e8 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

### EAP 통계 보기

[EAP Statistics](#) 페이지는 특정 포트에서 수신한 EAP 패킷에 대한 정보를 포함합니다. EAP에 대한 자세한 내용은 "[포트 기반 인증 구성](#)"을 참조하십시오. [EAP Statistics](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Table Views** → **EAP Statistics**를 차례로 클릭하십시오.

그림 8-6. EAP 통계



[EAP Statistics](#) 페이지는 다음 필드를 포함합니다.

**Port** — 통계에 폴링한 포트를 표시합니다.

**Refresh Rate** — 인터페이스 통계가 재생되기 전에 경과한 총 시간입니다.

**Frames Receive** — 포트에서 수신한 유효한 EAPOL 프레임 수를 표시합니다.

**Frames Transmit** — 포트를 통해 전송한 EAPOL 프레임 수를 표시합니다.

**Start Frames Receive** — 포트에서 수신한 EAPOL 시작 프레임 수를 표시합니다.

**Log off Frames Receive** — 포트에서 수신한 EAPOL 로그오프 프레임 수를 표시합니다.

**Respond ID Frames Receive** — 포트에서 수신한 EAPOL Resp/Id 프레임 수를 표시합니다.

**Respond Frames Receive** — 포트에서 수신한 유효한 EAPOL 응답 프레임 수를 표시합니다.

**Request ID Frames Transmit** — 포트를 통해 전송한 EAP Req/IdL 프레임 수를 표시합니다.

**Request Frames Transmit** — 포트를 통해 전송한 EAP 요청 프레임 수를 표시합니다.

**Invalid Frames Receive** — 이 포트에서 수신한 인식되지 않은 EAPOL 프레임 수를 표시합니다.

**Length Error Frames Receive** — 이 포트에서 수신한 유효하지 않은 패킷 본체 길이를 가진 EAPOL 프레임 수를 표시합니다.

**Last Frame Version** — 가장 최근에 수신한 EAPOL 프레임에 장착된 프로토콜 버전 번호를 표시합니다.

**Last Frame Source** — 가장 최근에 수신한 EAPOL 프레임에 장착된 원본 MAC 주소를 표시합니다.

## 포트에 대한 EAP 통계 표시

1. [EAP Statistics](#) 페이지를 여십시오.
2. **Interface** 필드에서 인터페이스를 선택하십시오.

인터페이스 EAP 통계가 표시됩니다.

## EAP 통계를 재설정하려면

1. [EAP Statistics](#) 페이지를 여십시오.
2. **Reset All Counters**를 클릭하십시오.

EAP 통계 카운터가 재설정됩니다.

## CLI 명령을 사용하여 EAP 통계 보기

다음 표는 EAP 통계를 보는 CLI 명령을 요약합니다.

표 8-98. EAP 통계 CLI 명령

CLI 명령	설명
	지정된 인터페이스에 대한 802.1X 통계를 표시합니다.

```
show dot1x statistics
```

다음은 CLI 명령의 예입니다.

```
console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

---

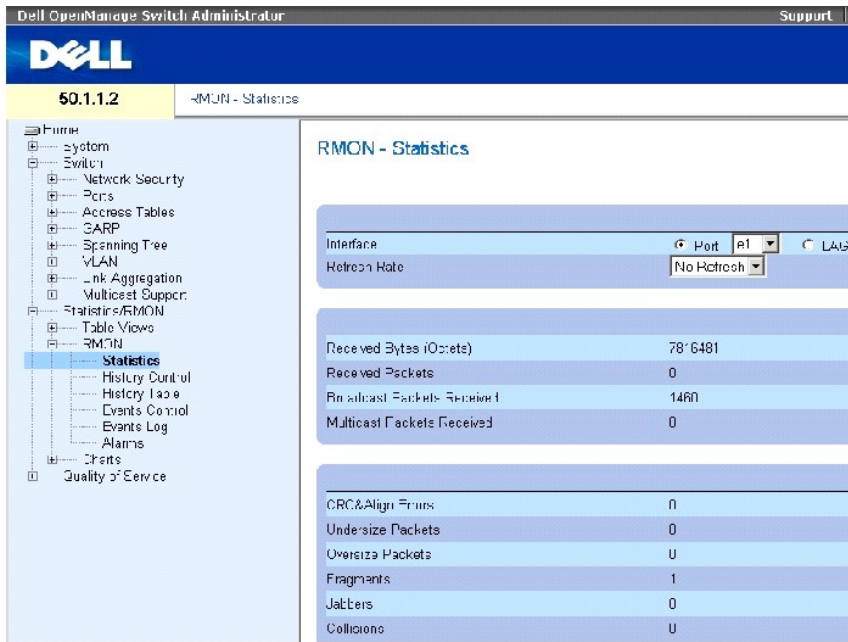
## RMON 통계 보기

ROMN(원격 모니터링)을 사용하면 네트워크 관리자가 원격 위치에서 네트워크 정보를 볼 수 있습니다. **RMON** 페이지를 열려면 트리 뷰에서 **Statistics/RMON→RMON**을 클릭하십시오.

## RMON 통계 그룹 보기

[RMON Statistics](#) 페이지를 사용하여 장치 사용 및 장치에 발생한 오류에 관한 정보를 보십시오. [RMON Statistics](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON→RMON→Statistics**를 차례로 클릭하십시오.

그림 8-7. RMON 통계



[RMON Statistics](#) 페이지는 다음 필드를 포함합니다.

**Interface** — 통계가 표시되는 포트 또는 LAG를 지정합니다.

**Refresh Rate** — 통계가 재생되기 전에 경과한 총 시간입니다.

**Received Bytes (Octets)** — 선택된 인터페이스에서 수신한 바이트 수입니다.

**Received Bytes (Octets)** — 선택된 인터페이스에서 수신한 패킷 수입니다.

**Broadcast Packets Received** — 장치가 최근 재생된 후 인터페이스에서 수신한 유효 브로드캐스트 패킷 수입니다. 이 수에는 멀티캐스트 패킷을 포함하지 않습니다.

**Multicast Packets Received** — 장치가 최근 재생된 후 인터페이스에서 수신한 유효 멀티캐스트 패킷 수입니다.

**CRC & Align Errors** — 장치가 최근 재생된 후 인터페이스에서 발생한 CRC 및 Align 오류 수입니다.

**Undersize Packets** — 장치가 최근 재생된 후 인터페이스에서 수신한 소형 패킷(64옥텟보다 적음) 수입니다.

**Oversize Packets** — 장치가 최근 재생된 후 인터페이스에서 수신한 특대형 패킷(1518옥텟보다 많음) 수입니다.

**Fragments** — 장치가 최근 재생된 후 인터페이스에서 수신한 조각(프레임 비트를 제외하고 FCS 옥텟을 포함한 64옥텟보다 적은 패킷) 수입니다.

**Jabbers** — 장치가 최근 재생된 후 인터페이스에서 수신한 재버(1518옥텟보다 긴 패킷) 수입니다.



**Collisions** — 장치가 최근 재생된 후 인터페이스에서 수신한 충돌 수입니다.

**Frames of xx Bytes** — 장치가 최근 재생된 후 인터페이스에서 수신한 xx바이트 프레임 수입니다.

## 인터페이스 통계 보기

1. [RMON Statistics](#) 페이지를 여십시오.
2. **Interface** 필드에서 인터페이스 종류 및 번호를 선택하십시오.

인터페이스 통계가 표시됩니다.

## CLI 명령을 사용하여 RMON 통계 보기

다음 표는 RMON 통계를 보는 CLI 명령을 포함합니다.

표 8-99. RMON 통계 CLI 명령

CLI 명령	설명
<code>show gvrp statistics[ethernet 인터페이스  port-channel 포트- 채널-번호]</code>	RMON 이더넷 통계를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0
```

```

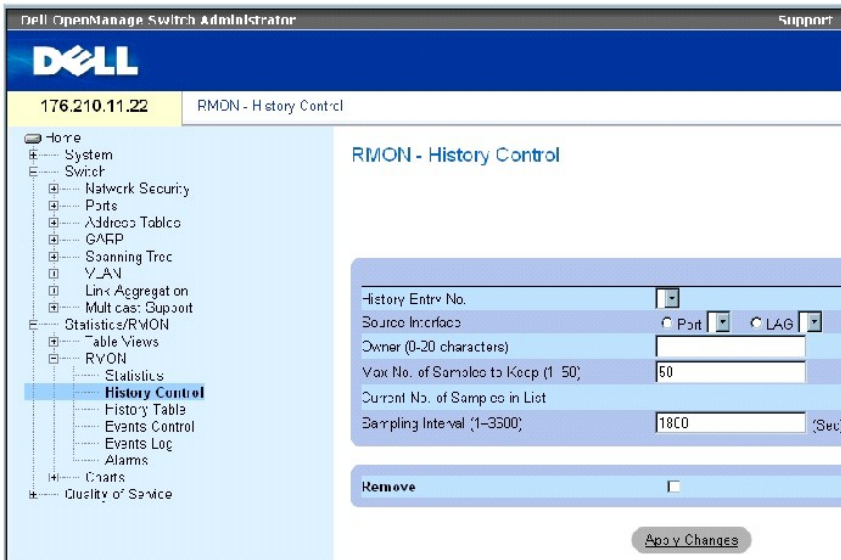
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389

```

## RMON 기록 제어 통계 보기

[RMON History Control](#)은 포트에서 가져온 데이터 견본에 대한 정보를 포함합니다. 예를 들어, 견본은 인터페이스 정의 또는 폴링 기간을 포함할 수 있습니다. [RMON History Control](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON→RMON→History Control**을 차례로 클릭하십시오.

그림 8-8. RMON 기록 제어



[RMON History Control](#) 페이지는 다음 필드를 포함합니다.

**History Entry No.** — History Control 페이지의 항목 번호입니다.

**Source Interface** — 기록 견본을 가져온 포트 또는 LAG입니다.

**Owner (0-20 characters)** — RMON 정보를 요청한 RMON 스테이션 또는 사용자입니다.

**Max No. of Samples to Keep (1-50)** — 저장되는 견본 수입니다. 기본값은 50입니다.

**Current No. of Samples in List** — 가져온 견본의 현재 수를 표시합니다.

**Sampling Interval (1-3600)** — 포트에서 견본을 가져오는 사이의 시간 간격을 초 단위로 표시합니다. 가능한 값은 1~3600초입니다. 기본값은 1800초(30분)입니다.

**Remove** — 선택한 경우 **History Control Table** 항목을 제거합니다.

## 기록 제어 항목 추가

1. [RMON History Control](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add History Entry** 페이지가 열립니다.

3. 대화상자의 필드를 완성하십시오.
4. **Apply Changes**를 클릭하십시오.

항목이 **History Control Table**에 추가됩니다.

## 기록 제어 표 항목 수정

1. [RMON History Control](#) 페이지를 여십시오.
2. **History Entry No.** 필드에서 한 항목을 선택하십시오.
3. 필요에 따라 필드를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

표 항목이 수정되고 장치가 업데이트됩니다.

## 기록 제어 표 항목 삭제

1. [RMON History Control](#) 페이지를 여십시오.
2. **History Entry No.** 필드에서 항목을 선택하십시오.
3. **Apply Changes**를 클릭하십시오.

표 항목이 삭제되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 RMON 기록 제어 보기

다음 표는 RMON 기록 제어를 보는 CLI 명령을 포함합니다.

표 8-100. RMON 기록 CLI 명령

CLI 명령	설명
<code>rmon collection history index [owner 소유자이름] [buckets 버킷-번호] [interval 초]</code>	인터페이스에서 RMON을 활성화하고 구성합니다.
<code>show rmon collection history [ethernet인터페이스   port-channel포트-채널-번호]</code>	RMON 수집 기록 통계를 표시합니다.

다음은 CLI 명령의 예입니다.

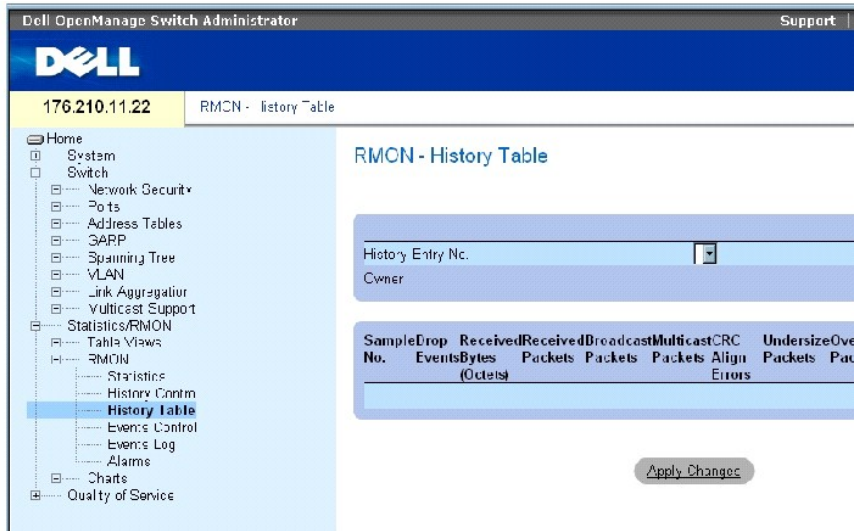
```
console(config)# interface ethernet 1/e8
```

```
console(config-if)# rmon collection history 1 interval 2400
```

## RMON 기록 표 보기

[RMON History Table](#)은 인터페이스 특정 통계 통계 네트워크 샘플링을 포함합니다. 각 표 항목은 단일 견본 중에 경과된 모든 카운터 값을 표시합니다. [RMON History Table](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON→RMON→History Table**을 차례로 클릭하십시오.

그림 8-9. RMON 기록 표



[RMON History Table](#) 페이지는 다음 필드를 포함합니다.

 **주:** 일부 필드는 RMON 기록 표에 표시되지 않습니다.

**History Entry No.** — **History Control** 페이지의 항목 번호를 지정합니다.

**Owner** — RMON 정보를 요청한 RMON 스테이션 또는 사용자를 표시합니다.

**Sample No.** — 표에서 정보가 반영하는 특정 견본 수를 표시합니다.

**Drop Events** — 샘플링 간격 동안 네트워크 자원의 부족으로 빠진 패킷 수입니다. 이 항목은 빠진 패킷의 정확한 수를 표시하지 못할 수 있지만 빠진 패킷이 감지된 횟수는 표시합니다.

**Received Bytes (Octets)** — 무효한 패킷을 포함한 네트워크에서 수신한 데이터 옥텟 수입니다.

**Received Packets** — 샘플링 간격 동안 수신한 패킷 수입니다.

**Broadcast Packets** — 샘플링 간격 동안 수신한 유효한 브로드캐스트 패킷 수입니다.

**Multicast Packets** — 샘플링 간격 동안 수신한 유효한 멀티캐스트 패킷 수입니다.

**CRC Align Errors** — 샘플링 세션 동안 수신한 64~1,518옥텟의 길이를 가진 패킷 수입니다. 그러나 패킷은 하나의 정수 옥텟을 가진 FCS(우호 패킷 검사 순서) 또는 하나의 비 정수 옥텟을 가진 FCS를 포함합니다.

**Undersize Packets** — 샘플링 세션 동안 수신한 64옥텟보다 적은 패킷 수입니다.

**Oversize Packets** — 샘플링 세션 동안 수신한 1,518옥텟보다 많은 패킷 수입니다.

**Fragments** — 샘플링 세션 동안 수신한 64옥텟보다 적고 FCS를 가진 패킷 수입니다.

**Jabbers** — 샘플링 세션 동안 수신한 1,518옥텟보다 많고 FCS를 가진 패킷 수입니다.

**Collisions** — 샘플링 세션 동안 발생한 패킷 충돌의 총 수를 추정합니다. 중복자 포트가 두 개 이상의 스테이션 동시 전송을 감지한 경우에 충돌이 감지됩니다.

**Utilization** — 세션 샘플링 동안 인터페이스의 주요 물리층 네트워크 사용을 추정합니다. 값은 백분율의 소수점 이하 두 자리까지 반영됩니다.

## 특정 기록 항목에 대한 통계 보기

1. [RMON History Table](#)를 여십시오.
2. **History Entry No.** 필드에서 항목을 선택하십시오.

항목 통계는 RMON 기록 표에서 표시됩니다.

## CLI 명령을 사용하여 RMON 기록 제어 보기

다음 표는 RMON 기록을 보는 CLI 명령을 포함합니다.

표 8-101. RMON 기록 제어 CLI 명령

CLI 명령	설명
show rmon history index {throughput   errors   other} [period seconds]	RMON 이더넷 통계 기록을 표시합니다.

다음은 색인 1에서의 작업량에 대한 RMON 이더넷 통계를 표시한 CLI 명령의 예입니다.

```
console> enable

console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50
```

Maximum table size: 270

Time Octets Packets Broadcast Multicast %

09-Mar-2003 18:29:32 0 0 0 0 0

09-Mar-2003 18:29:42 0 0 0 0 0

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0

## 장치 RMON 이벤트 정의

[RMON Events Control](#) 페이지를 사용하여 RMON 이벤트를 정의하십시오. [RMON Events Control](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON→ RMON→ Events Control**을 차례로 클릭하십시오.

그림 8-10. RMON 이벤트 제어

The screenshot shows the Dell OpenManage Switch Administrator interface. The top bar includes the Dell logo, the IP address 176.210.11.22, and the page title 'RMON - Events Control'. A navigation tree on the left shows the path: Home > System > Switch > Statistics/RMON > Events Control. The main content area is titled 'RMON - Events Control' and contains a form with the following fields:

- Event Entry: A dropdown menu.
- Community: A text input field.
- Description: A text input field.
- Type: A dropdown menu with 'None' selected.
- Time: A text input field.
- Owner: A text input field.

Below the form is a 'Remove' button with a checkbox and an 'Apply Changes' button.

[RMON Events Control](#) 페이지는 다음 필드를 포함합니다.

**Event Entry** — 이벤트를 표시합니다.

**Community** — 이벤트가 속하는 커뮤니티입니다.

**Description** — 사용자 정의 이벤트 설명입니다.

**Type** — 이벤트 종류를 설명합니다. 가능한 값:

**Log** — 이벤트 종류가 로그 항목입니다.

**Log** — 이벤트 종류가 트랩입니다.

**Log and Trap** — 이벤트 종류가 로그 항목 및 트랩입니다.

**None** — 이벤트가 없습니다.

**Time** — 이벤트가 발생한 시간입니다.

**Owner** — 이벤트를 정의한 장치 또는 사용자입니다.

**Remove** — 선택한 경우, RMON 이벤트 표에서 이벤트를 제거합니다.

## RMON 이벤트 추가

1. [RMON Events Control](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add an Event Entry** 페이지가 열립니다.

3. 대화상자에서 정보 입력을 완성하고 **Apply Changes**를 클릭하십시오.

**Event Table** 항목이 추가되고 장치가 업데이트됩니다.

## RMON 이벤트 수정

1. [RMON Events Control](#) 페이지를 여십시오.
2. **Event Table**에서 한 항목을 선택하십시오.
3. 대화상자에서 필드를 수정하고 **Apply Changes**를 클릭하십시오.

**Event Table** 항목이 수정되고 장치가 업데이트됩니다.


## RMON 이벤트 항목 삭제

1. [RMON Events Control](#) 페이지를 여십시오.
2. **Show All**을 클릭하십시오.

RMON Events Table 페이지가 열립니다.

3. 삭제하려는 이벤트의 **Remove** 확인란을 선택하고 **Apply Changes**를 클릭하십시오.

표 항목이 삭제되고 장치가 업데이트됩니다.

 **주:** RMON Events Control 페이지에서 **Remove** 확인란을 선택하여 단일 이벤트 항목을 제거할 수 있습니다.

## CLI 명령을 사용하여 장치 이벤트 정의

다음 표는 장치 이벤트를 정의하는 CLI 명령을 포함합니다.

표 8-102. 장치 이벤트 정의 CLI 명령

CLI 명령	설명
<code>rmon event 색인 종류 [community 텍스트] [description 텍스트] [ownername]</code>	RMON 이벤트를 구성합니다.
<code>show rmon events</code>	RMON 이벤트 표를 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# rmon event 1 log
console(config)# exit
console# show rmon events

```

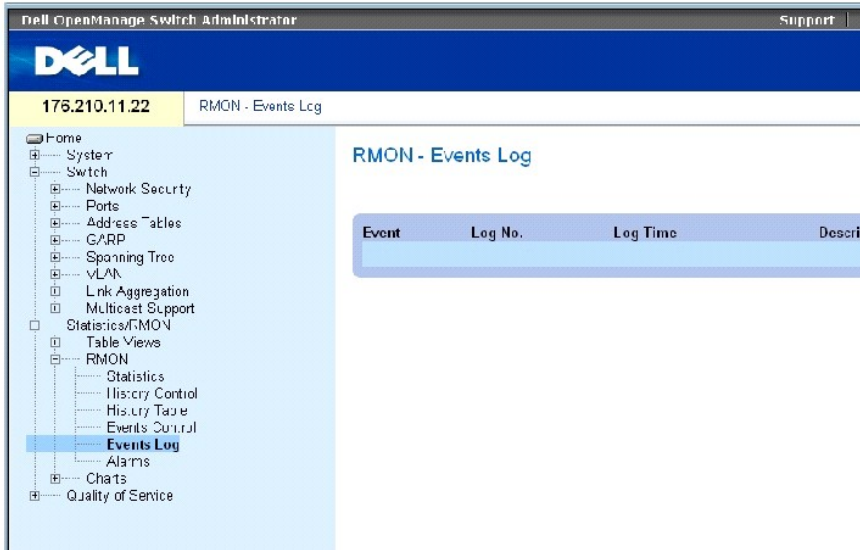
Index	Description	Type	Community	Owner	Last Time Sent
-----	-----	----	-----	-----	-----
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

## RMON 이벤트 로그 보기



[RMON Events Log](#) 페이지는 RMON 이벤트의 목록을 포함합니다. [RMON Events Log](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON→RMON→Events Log**를 차례로 클릭하십시오.

그림 8-11. RMON 이벤트 로그



[RMON Events Log](#) 페이지는 다음 필드를 포함합니다.

**Event** — RMON 이벤트 로그 번호입니다.

**Log No.** — 로그 번호입니다.

**Log Time** — 로그 항목이 입력된 시간입니다.

**Description** — 로그 항목을 설명합니다.

### CLI 명령을 사용하여 장치 이벤트 정의

다음 표는 장치 이벤트를 정의하는 CLI 명령을 포함합니다.

표 8-103. 장치 이벤트 정의 CLI 명령

CLI 명령	설명
<code>show rmon log [event]</code>	RMON 로깅 표를 표시합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# rmon event 1 log
```

```

Console> show rmon log

Maximum table size: 500

Event Description Time
-----
1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48

```

## RMON 장치 경보 정의

[RMON Alarms](#) 페이지를 사용하여 네트워크 경보를 설정하십시오. 네트워크 경보는 네트워크 고장이나 이벤트가 감지된 경우에 발생합니다. 상승 및 하강 임계값이 이벤트가 생성됩니다. 이벤트에 대한 자세한 내용은 "[RMON 이벤트 로그 보기](#)"를 참조하십시오.

[RMON Alarms](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **RMON** → **Alarms**를 차례로 클릭하십시오.

그림 8-12. RMON 경보

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes the Dell logo and the text 'Dell OpenManage Switch Administrator' and 'Support'. Below this, the IP address '176.210.11.22' and the page title 'RMON - Alarms' are displayed. The left sidebar contains a tree view with the following structure:

- Hcme
  - System
  - Switch
    - Network Security
    - Ports
    - Address Tables
    - GARP
    - Spanning Tree
    - VLAN
    - Link Aggregation
    - Multicast Support
    - Statistics/RMON
      - Table Views
      - RMON
        - Statistics
        - History Control
        - History Table
        - Events Control
        - Events Log
        - Alarms**
        - Charts
        - Quality of Service

The main content area is titled 'RMON - Alarms' and contains the following configuration fields:

- Alarm Entry: [Dropdown]
- Interface: [Port] [LAG] [Dropdown]
- Counter Name: [Dropdown]
- Counter Value: [Text]
- Sample Type: [Absolute] [Dropdown]
- Rising Threshold (0-4234967295): [100] [Text]
- Rising Event: [Dropdown]
- Falling Threshold (0-4234967295): [20] [Text]
- Falling Event: [Dropdown]
- Startup Alarm: [Rising Alarm] [Dropdown]
- Interval (1-4234967295): [100] (Sec) [Text]
- Owner: [Text]

At the bottom of the configuration area, there is a 'Remove' checkbox and an 'Apply Changes' button.

[RMON Alarms](#) 페이지는 다음 필드를 포함합니다.

**Alarm Entry** — 특정 경보를 표시합니다.

**Interface** — RMON 통계가 표시된 인터페이스를 표시합니다.

**Counter Name** — 선택된 MIB 변수를 표시합니다.

**Counter Value** — 선택된 MIB 변수 값입니다.

**Sample Type** — 선택된 변수에 대한 샘플링 및 임계값과 해당 값을 비교하는 방식을 지정합니다. 가능한 필드 값:

**Delta** — 현재 값에서 마지막에 추출된 값을 뺍니다. 값의 차를 임계값과 비교합니다.

**Absolute** — 샘플링 간격의 끝에서 해당 값을 임계값과 직접 비교합니다.

**Rising Threshold (0-4294967295)** — 상승 임계값 경보를 트리거하는 상승 카운터 값입니다. 상승 임계값은 그래프 막대의 상단에 표시됩니다. 각 모니터된 변수는 부동한 색상으로 지정됩니다. 필드 기본값은 100초입니다.

**Rising Event** — 로그, 트랩 또는 둘 다를 포함하여 경보를 보고하는 메커니즘입니다. 로그가 선택된 경우, 장치 또는 관리 시스템에는 저장 메커니즘이 없습니다. 그러나 장치가 재설정되지 않은 경우, 장치 로그 표에 유지됩니다. 트랩이 선택된 경우, 트랩 메커니즘을 통해 SNMP 트랩이 생성되며 보고됩니다. 트랩은 동일한 메커니즘을 사용하여 저장할 수 있습니다.

**Falling Threshold (0-4294967295)** — 하강 임계값 경보를 트리거하는 하강 카운터 값입니다. 하강 임계값은 그래프 막대의 상단에 도식적으로 표시됩니다. 각 모니터된 변수는 부동한 색상으로 지정됩니다. 필드 기본값은 20초입니다.

**Startup Alarm** — 경보 생성을 활성화하는 트리거입니다. 낮은 임계값으로부터 높은 임계값까지의 임계값을 연결하여 상승을 정의합니다.

**Interval (1-4294967295) (sec)** — 경보 간격 시간입니다. 필드 기본값은 100초입니다.

**Owner** — 경보를 정의한 장치 또는 사용자입니다.

**Remove** — 선택한 경우, RMON 경보를 제거합니다.

## 경보 표 항목 추가

1. [RMON Alarms](#) 페이지를 여십시오.
2. **Add**를 클릭하십시오.

**Add an Alarm Entry** 페이지가 열립니다.

그림 8-13. 경보 항목 페이지 추가

Refresh

### Add an Alarm Entry

Alarm Entry	
Interface	<input type="radio"/> Pct   <input type="radio"/> LAC
Counter Name	<input type="text"/>
Sample Type	Absolute
Rising Threshold (U=234067295)	<input type="text"/>
Rising Event	<input type="text"/>
Falling Threshold (F=429497297)	<input type="text"/>
Falling Event	<input type="text"/>
Send Alarm	Silent Alarm
Interval	<input type="text"/> (sec)
Owner	<input type="text"/>

Apply Changes

3. 인터페이스를 선택하십시오.
4. 필드를 작성하십시오.
5. **Apply Changes**를 클릭하십시오.

RMON 경보가 추가되고 장치가 업데이트됩니다.

### 경보 표 항목 수정

1. [RMON Alarms](#) 페이지를 여십시오.
2. **Alarm Entry** 드롭다운 메뉴에서 한 항목을 선택하십시오.
3. 필드를 수정하십시오.
4. **Apply Changes**를 클릭하십시오.

항목이 수정되고 장치가 업데이트됩니다.

### 경보 표 표시

1. [RMON Alarms](#) 페이지를 여십시오.
2. **Show All**를 클릭하십시오.

**Alarms Table**이 열립니다.

### 경보 표 항목 삭제

1. [RMON Alarms](#) 페이지를 여십시오.
2. **Alarm Entry** 드롭다운 메뉴에서 한 항목을 선택하십시오.
3. **Remove** 확인란을 선택하십시오.
4. **Apply Changes**를 클릭하십시오.

항목이 삭제되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 장치 경보 정의

다음 표는 장치 경보를 정의하는 CLI 명령을 포함합니다.

표 8-104. 장치 경고 CLI 명령

CLI 명령	설명
<code>rmon alarm index MIB_Object_ID interval rthreshold fthreshold revent fevent [type 종류] [startup 방향] [owner이름]</code>	RMON 경고 조건을 구성합니다.
<code>show rmon alarm-table</code>	경보 표의 요약 내용을 표시합니다.
<code>show rmon alarm</code>	RMON 경고 구성을 표시합니다.

다음은 CLI 명령의 예입니다.

```

console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1
360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index OID Owner
-----
1 1.3.6.1.2.1.2.2.1.10.1 CLI
2 1.3.6.1.2.1.2.2.1.10.1 Manager
3 1.3.6.1.2.1.2.2.1.10.9 CLI
    
```

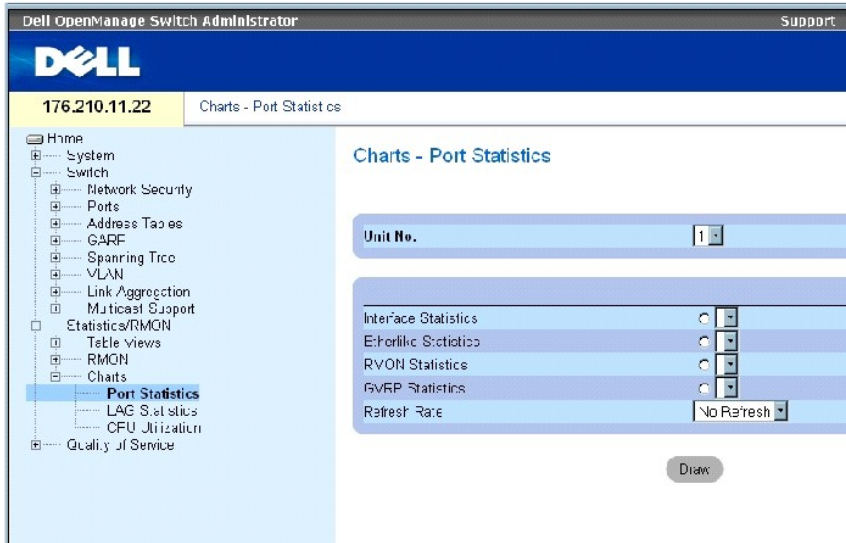
## 차트 보기

Chart 페이지는 차트 형식으로 통계를 표시하는 데 관한 연결을 포함합니다. 페이지를 열려면 트리 뷰에서 통계→차트를 클릭하십시오.

## 포트 통계 보기

Port Statistics 페이지를 사용하여 포트 요소에 대한 차트 형식으로 된 통계를 여십시오. Port Statistics 페이지를 열려면 트리 뷰에서 Statistics/RMON→Charts→Port Statistics를 차례로 클릭하십시오.

그림 8-14. 포트 통계



[Port Statistics](#) 페이지는 다음 필드를 포함합니다.

**Unit No.** — 통계가 표시되는 스테킹 단위를 표시합니다.

**Interface Statistics** — 표시할 인터페이스 통계를 선택합니다.

**Etherlike Statistics** — 표시할 Etherlike 통계를 선택합니다.

**RVON Statistics** — 표시할 RVON 통계를 선택합니다.

**GVRP Statistics** — 표시할 GVRP 통계를 선택합니다.

**Refresh Rate** — 통계가 재생되기 전에 경과한 총 시간입니다.

## 포트 통계 표시

1. [Port Statistics](#) 페이지를 여십시오.
2. 열려는 통계 종류를 선택하십시오.
3. **Refresh Rate** 드롭다운 메뉴에서 원하는 재생율을 선택하십시오.
4. **Draw**를 클릭하십시오.

선택된 통계에 대한 그래프가 표시됩니다.

## CLI 명령을 사용하여 포트 통계 보기

다음 표는 포트 통계를 보는 CLI 명령을 포함합니다.

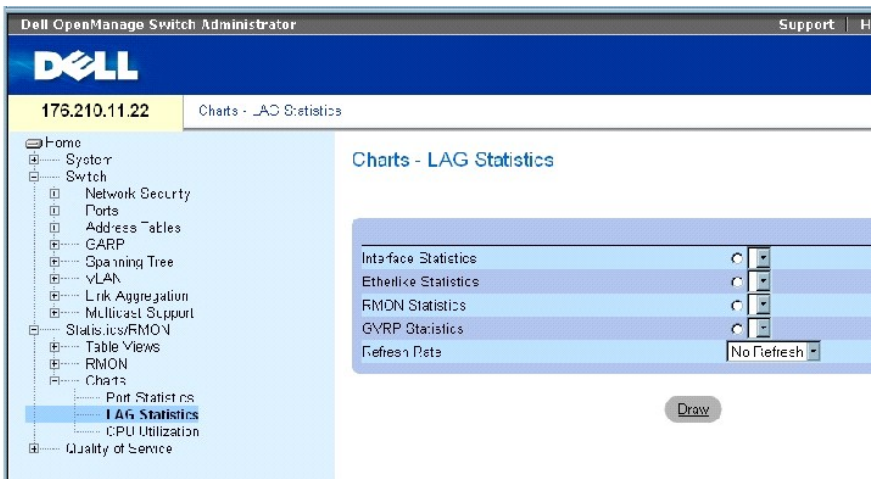
표 8-105. 포트 통계 CLI 명령

CLI 명령	설명
<code>show interfaces counters {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	물리적 인터페이스에서 인식한 처리량을 표시합니다.
<code>show rmon statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	RMON 이더넷 통계를 표시합니다.
<code>show gvrp statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	GVRP 통계를 표시합니다.
<code>show gvrp-error statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	GVRP 오류 통계를 표시합니다.

## LAG 통계 보기

[LAG Statistics](#) 페이지를 사용하여 LAG에 대한 차트 형식으로 된 통계를 여십시오. [LAG Statistics](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Charts** → **LAG Statistics**를 차례로 클릭하십시오.

그림 8-15. LAG 통계



[LAG Statistics](#) 페이지는 다음 필드를 포함합니다.

**Interface Statistics** — 표시할 인터페이스 통계를 선택합니다.

**Etherlike Statistics** — 표시할 Etherlike 통계를 선택합니다.

**RMON Statistics** — 표시할 RMON 통계를 선택합니다.

**GVRP Statistics** — 표시할 GVRP 통계를 선택합니다.

**Refresh Rate** — 통계가 재생되기 전에 경과한 총 시간입니다.

## LAG 통계 표시

1. [LAG Statistics](#) 페이지를 여십시오.
2. 열려는 통계 종류를 선택하십시오.
3. **Refresh Rate** 드롭다운 메뉴에서 원하는 재생율을 선택하십시오.
4. **Draw**를 클릭하십시오.

선택된 통계에 대한 그래프가 표시됩니다.

## CLI 명령을 사용하여 LAG 통계 보기

다음 표는 LAG 통계를 보는 CLI 명령을 포함합니다.

표 8-106. LAG 통계 CLI 명령

CLI 명령	설명
<code>show interfaces counters {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	물리적 인터페이스에서 인식한 처리량을 표시합니다.
<code>show rmon statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	RMON 이더넷 통계를 표시합니다.
<code>show gvrp statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	GVRP 통계를 표시합니다.
<code>show gvrp-error statistics {ethernet 인터페이스   port-channel 포트-채널-번호}</code>	GVRP 오류 통계를 표시합니다.

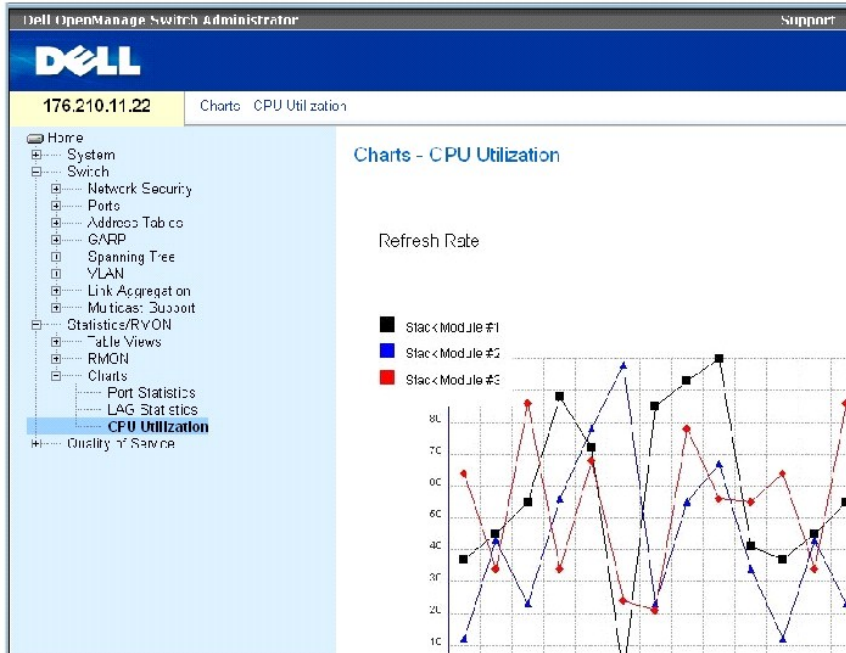
## CPU 사용 보기

[CPU Utilization](#) 페이지는 시스템 CPU 사용 및 각 스테킹 구성원이 소비한 CPU 자원의 백분율에 대한 정보를 포함합니다. 각 스테킹 구성원은 그래프에서 부동한 색상이 지정됩니다.

[CPU Utilization](#) 페이지를 열려면 트리 뷰에서 **Statistics/RMON** → **Charts** → **CPU Utilization** 를 차례로 클릭하십시오.

그림 8-16. CPU 통계





[CPU Utilization](#) 페이지는 다음 정보를 포함합니다.

**Refresh Rate** — 통계가 재생되기 전에 경과한 총 시간입니다.

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

## 서비스 품질 구성

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

- [QoS\(서비스 품질\) 개요](#)
- [QoS 전역 매개변수 정의](#)

이 항목에서는 QoS(서비스 품질) 매개변수를 정의하고 구성하는 데 대한 정보를 제공합니다. QoS 페이지를 열려면 트리 뷰에서 서비스 품질을 클릭하십시오.

### QoS(서비스 품질) 개요

QoS는 네트워크 내에서 QoS 및 우선순위 대기열을 구현하는 기능을 제공합니다.

QoS를 필요하는 구현 예에는 다른 처리량이 낮은 우선순위 대기열에 할당될 수 있을 때 높은 우선순위에 지정될 수 있는 음성, 비디오 및 실시간 처리량과 같은 특정 유형의 처리량을 포함합니다. 결과는 높은 수요가 있는 처리량의 향상된 처리량 흐름입니다.

QoS는 다음에 의해 정의됩니다.


1. 분류 — 지정된 값과 일치한 패킷 필드를 지정합니다. 사용자 정의된 사양과 일치한 모든 패킷은 함께 분류됩니다.
1. 기능 — 전달되는 패킷이 패킷 정보, VPT(VLAN 우선순위 태그) 및 DSCP(DiffServ 코드 점)과 같은 패킷 필드 값을 기반으로 하는 처리량 관리를 정의합니다.

### VPT 분류 정보

VLAN 우선순위 태그는 패킷을 송신 대기열 중 하나에 매핑하여 패킷을 분류하는 데 사용됩니다. 대기열 할당의 VLAN 우선순위 태그는 사용자가 정의할 수 있습니다. 아래의 표는 대기열 기본 설정값의 VPT를 상세하게 설명합니다.

표 9-107. 표 기본값을 매핑하는 대기열의 CoS

CoS 값	대기열 전달 값
0	q1(최저 우선순위)
1	q1(최저 우선순위)
2	q1(최저 우선순위)
3	q1(최저 우선순위)
4	q2
5	q2
6	q3
7	q3

 **주:** 스택 구성에서 대기열 4는 스택 처리량 전달에 사용됩니다. 그러므로 대기열 4에 추가 처리량을 할당하면 처리량 전달을 방해할 수 있습니다.

대그없이 착신된 패킷에 퍼 포트에 설정된 기본 VPT 값이 할당됩니다. 할당된 VPT는 패킷을 송신 대기열에 매핑하는 데 사용됩니다.

DSCP 값은 우선순위 대기열에 매핑될 수 있습니다. 다음 표에는 송신 대기열 값에 매핑되는 기본 DSCP가 포함됩니다.

표 9-108. 표 기본값을 매핑하는 대기열의 DSCP

DSCP 값	대기열 전달 값
0-15	q1(최저 우선순위)
16-39	q2

DSCP 매핑은 퍼 시스템으로 활성화됩니다.

### CoS 서비스

패킷이 특정 송신 대기열에 할당된 후, CoS 서비스는 해당 대기열에 지정될 수 있습니다. 다음 중 한 가지 방법에 의해 송신 대기열은 예약 구성표로 구성됩니다.

- 1. 엄격한 우선순위 — 시간에 민감한 응용프로그램이 항상 전달되는지 확인하십시오. SP(엄격한 우선순위)는 미션 크리티컬, 시간에 민감한 처리량을 시간에 민감한 정도로 약한 응용프로그램 위로 우선순위에 줍니다. 예를 들어, 엄격한 우선순위에서 IP 처리량을 통한 음성용 우선순위에 높일 수 있기에 FTP 또는 전자 우편(SMTP) 처리량 전에 전달됩니다.
- 1. 가중치 적용 라운드 로빈 — 다일 응용프로그램이 장치 전달 용량을 차지하지 않는지 확인하십시오. WRR(가중치 적용 라운드 로빈)는 전체 대기열을 라운드 로빈 순서로 전달합니다. SP 대기열을 예정한 상태에서 모든 대기열은 WRR에 참여할 수 있습니다. SP 대기열은 WRR 대기열 전에 제공됩니다. 처리량 흐름이 미량이고 SP 대기열이 포트에 지정된 전체 대역폭을 차지하지 못한 경우, WRR 대기열은 SP 대기열과 대역폭을 공유할 수 있습니다. 나머지 대역폭이 중량비에 따라 배포되는지 확인하십시오. WRR이 선택된 경우 다음 가중치가 대기열에 할당됩니다. 1, 2, 4, 8.

### QoS 전역 매개변수 정의

QoS 매개변수 페이지에는 QoS 전역 매개변수 설정을 활성화하는 페이지 연결이 포함됩니다.

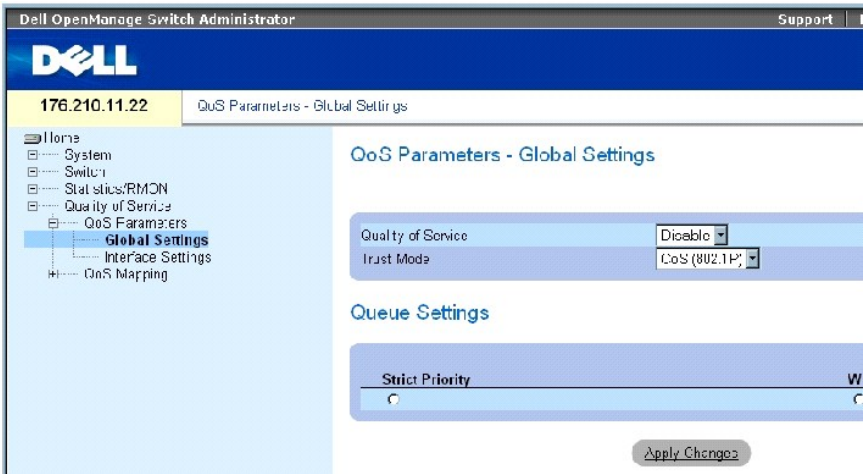
### QoS 전역 설정 구성

[전역 설정](#) 페이지에는 QoS 활성화 또는 비활성화 필드가 포함되어 신뢰 모드 선택 필드도 포함됩니다. 신뢰 모드는 패킷의 미리 정의된 필드에 의지하여 송신 대기열을 확인합니다.

또한, [전역 설정](#) 페이지는 SP(엄격한 우선순위) 또는 WRR(가중치 적용 라운드 로빈)로 대기열 정의를 활성화합니다.

[전역 설정](#) 페이지를 열려면 트리 뷰에서 **서비스 품질** → **QoS 매개변수** → **전역 설정**을 차례로 클릭하십시오.

그림 9-1. 전역 설정



[전역 설정](#) 페이지에는 다음 항목이 포함됩니다.

- 1. QoS 설정
- 1. 대기열 설정


### QoS 설정

**서비스 품질** — QoS를 사용하여 네트워크 처리량 관리를 활성화 또는 비활성화합니다.

**신뢰 모드** — 장치를 시작하는 패킷을 분류하는 데 사용하는 패킷 필드를 결정합니다. 규칙이 정의되지 않은 경우 미리 정의된 CoS 또는 DSCP 패킷 필드를 포함한 처리량은 선택한 신뢰 모드에 따라 매핑됩니다. 미리 정의된 패킷 필드를 포함하지 않은 처리량은 최선형 대기열(q2)에 매핑됩니다. 가능한 신뢰 모드 필드 값:

**CoS(802.1p)** — 송신 대기열 할당은 IEEE802.1p VPT(LAN 우선순위 태그) 또는 포트에 할당된 기본 VPT에 의해 결정됩니다. 장치 기본값은 IEEE802.1p입니다.

**DSCP** — 송신 대기열 할당은 DSCP 필드에 의해 결정됩니다.

 **주:** 인터페이스 신뢰 설정은 전역 신뢰 설정을 재지정합니다.

## 대기열 설정

**엄격한 우선순위** — 선택된 경우 시스템 대기열은 SP 대기열임을 표시합니다.

**WRR** — 선택된 경우 시스템 대기열은 WRR 대기열임을 표시합니다.

## 서비스 품질 활성화:

1. [전역 설정](#) 페이지를 엽니다.
2. **서비스 품질** 필드에서 **활성화**를 선택합니다.
3. **변경 사항 적용**을 클릭합니다.

장치에서 서비스 등급이 활성화됩니다.

## 신뢰 모드 활성화:

1. [전역 설정](#) 페이지를 엽니다.
2. **신뢰 모드** 필드를 정의합니다.
3. **변경 사항 적용**을 클릭합니다.

장치에서 신뢰 모드는 활성화됩니다.

## CLI 명령을 사용하여 신뢰를 활성화

다음 표에서는 [전역 설정](#) 페이지에 있는 구성 필드의 동등한 CLI 명령을 요약합니다.

표 9-109. QoS 설정 CLI 명령

CLI 명령	설명
<code>qos trust [cos   dscp]</code>	시스템을 신뢰 모드로 구성합니다.
<code>no qos trust</code>	비 신뢰 상태로 되돌립니다.

다음은 CLI 명령의 예입니다.

```
console(config)# qos trust dscp
```

## QoS 인터페이스 설정 정의

[인터페이스 설정](#) 페이지에는 신뢰 모드 비활성화 및 태그없는 수신된 패킷의 기본 CoS 값 설정에 대한 필드를 포함합니다. [인터페이스 설정](#) 페이지를 열려면 트리 뷰에서 **서비스 품질** → **QoS 매개변수** → **인터페이스 설정**을 차례로 클릭하십시오.

그림 9-2. 인터페이스 설정



[인터페이스 설정](#) 페이지에는 다음 필드가 포함됩니다.

**인터페이스** — 구성할 특정 포트 또는 LAG.

**인터페이스의 "신뢰" 모드 비활성화** — 특정 인터페이스의 신뢰 모드 비활성화합니다. 이 설정은 장치에 구성된 신뢰 모드를 전역적으로 재지정합니다.

**수신 처리량의 기본 CoS 설정** — 태그없는 패킷의 기본 CoS 태그 값을 설정합니다. CoS 태그 값은 0-7입니다. 기본값은 0입니다.

### 인터페이스의 QoS 설정 할당:

1. [인터페이스 설정](#) 페이지를 엽니다.
2. **인터페이스** 필드에서 인터페이스를 선택합니다.
3. 필드를 정의합니다.
4. **변경 사항 적용**을 클릭합니다.

CoS 설정이 인터페이스에 할당됩니다.

### QoS/CoS 설정 표시:

1. [인터페이스 설정](#) 페이지를 엽니다.
2. **모두 표시**를 클릭합니다.

인터페이스 표가 표시됩니다.

## CLI 명령을 사용하여 QoS 인터페이스 할당

다음 표에서는 [인터페이스 설정](#) 페이지에 있는 구성 필드의 동등한 CLI 명령을 요약합니다.

표 9-110. QoS 인터페이스 CLI 명령

CLI 명령	설명
qos trust	신뢰 모드를 활성화합니다.
no qos trust	각 포트의 신뢰 상태를 비활성화합니다.

다음은 CLI 명령의 예입니다.

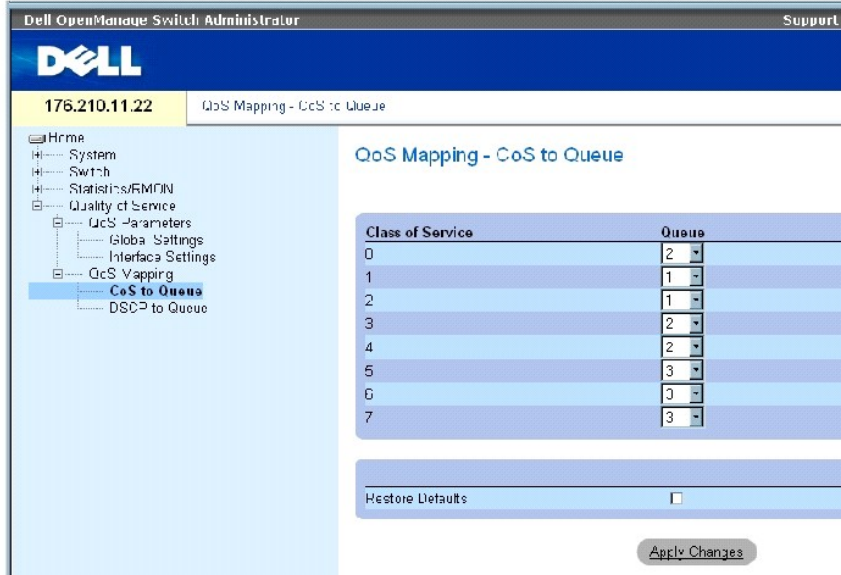
```
console(config)# interface
ethernet 1/e15

console(config-if)# qos
trust
```

## CoS 값을 대기열에 매핑

[대기열의 CoS](#) 페이지에는 CoS 설정을 처리량 대기열에 분류하는 필드가 포함됩니다. [대기열의 CoS](#) 페이지를 열려면 트리 뷰에서 **서비스 품질** → **QoS 매핑** → **대기열의 CoS**를 차례로 클릭하십시오.

그림 9-3. 대기열의 CoS



[대기열의 CoS](#) 페이지에는 다음 필드가 포함됩니다.

**서비스 등급** — CoS 우선순위 태그 값(최저값이 0이고 최고값이 7)을 지정합니다.

**대기열** — CoS 우선순위가 매핑되는 대기열입니다. 4개의 처리량 우선순위 대기열이 지원됩니다.

기본값 복원 — CoS 값을 송신 대기열에 매핑하는 장치 출하 시 기본값을 복원합니다.

### CoS 값을 대기열에 매핑

1. [대기열의 CoS](#) 페이지를 엽니다.
2. CoS 항목을 선택합니다.
3. 대기열 필드에서 대기열 번호를 정의합니다.
4. 변경 사항 적용을 클릭합니다.

CoS 값은 송신 대기열에 매핑되고 장치는 업데이트됩니다.

### CLI 명령을 사용하여 CoS 값을 대기열에 할당

다음 표에서는 [대기열의 CoS](#) 페이지에 있는 구성 필드의 동등한 CLI 명령을 요약합니다.

표 9-111. 대기열의 CoS 설정 CLI 명령

CLI 명령	설명
wrr-queue cos-map queue-id cos0.cos7	할당된 CoS 값을 송신 대기열에 매핑합니다.

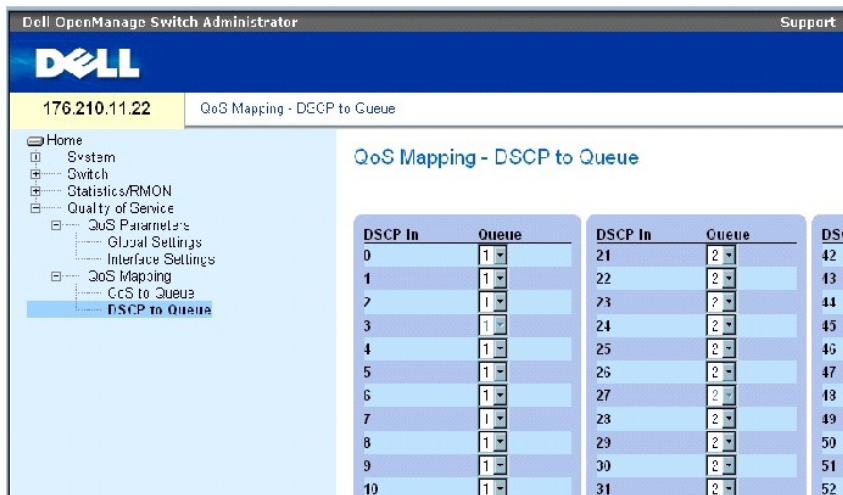
다음은 CLI 명령의 예입니다.

```
console(config)# wrr-queue
cos-map 4 7
```

### DSCP 값을 대기열에 매핑

[대기열의 DSCP](#) 페이지는 송신 대기열을 특정 DSCP 필드에 정의하는 필드를 제공합니다. [대기열의 DSCP](#) 페이지를 열려면 트리 뷰에서 서비스 품질 → CoS 매핑 → 대기열의 DSCP를 차례로 클릭하십시오.

그림 9-4. 대기열의 DSCP



[대기열의 DSCP](#) 페이지에는 다음 필드가 포함됩니다.

**DSCP In** — 수신 패킷 내의 DSCP 필드 값입니다.

**대기열** — 특정 DSCP 값을 가진 패킷이 할당된 대기열입니다. 값은 1~4로서 1은 최소 값이고 4는 최대 값입니다.

### DSCP 값 매핑 및 우선순위 대기열 할당

1. [대기열의 DSCP](#) 페이지를 엽니다.
2. **DSCP In** 열에서 값을 선택합니다.
3. **대기열** 필드를 정의합니다.
4. **변경 사항 적용**을 클릭합니다.

DSCP는 덮어쓰기되고 해당 값에 송신 대기열이 할당됩니다.

### CLI 명령을 사용하여 DSCP 값 할당

다음 표에서는 [대기열의 DSCP](#) 페이지에 있는 구성 필드의 동등한 CLI 명령을 요약합니다.

표 9-112. 대기열의 DSCP 값 CLI 명령

CLI 명령	설명
<code>qos map dscp-queue dscp-list to queue-id</code>	대기열의 DSCP 매핑을 수정합니다.

다음은 CLI 명령의 예입니다.

```
console(config)# qos map dscp-queue 33 40 41 to 1
```

---

[목차 페이지로 돌아가기](#)



[목차 페이지로 돌아가기](#)

## Dell™ PowerConnect™ 34XX 시스템 사용 설명서



**주:** 주는 컴퓨터를 보다 효율적으로 사용할 수 있도록 중요 정보를 제공합니다.



**주의사항:** 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.



**주의:** 주의는 위험한 상황, 심각한 부상 또는 사망할 우려가 있음을 알려줍니다.

본 설명서에 수록된 정보는 사전 통보 없이 변경될 수 있습니다.  
© 2005 Dell Inc. 저작권 본사 소유.

Dell Inc. 의 사전 승인 없이 어떠한 경우에도 무단 복제하는 것을 엄격히 금합니다.

본 설명서에 사용된 상표: Dell, Dell OpenManage, DELL 로고, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet 및 Latitude는 Dell Inc.의 상표이며 Microsoft 및 Windows는 Microsoft Corporation의 등록 상표입니다.

본 설명서에서 특정 회사의 표시나 제품 이름을 지칭하기 위해 기타 상표나 상호를 사용할 수도 있습니다. Dell Inc.는 자사가 소유하고 있는 것 이외에 기타 모든 등록 상표 및 상표명에 대한 어떠한 소유권도 없습니다.

2005년 3월

---

[목차 페이지로 돌아가기](#)

## 장치 기능 상호 작용 정보

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

다음 표에는 기능 상호 작용에 대한 정보가 들어있습니다.

기능	기능 정보
802.1x 인증되지 않은 VLAN	802.1x 인증되지 않은 VLAN는 다음으로 기능을 제한합니다. <ul style="list-style-type: none"> <li>1 802.1X 게스트 VLAN</li> <li>1 개인 VLAN</li> <li>1 고립형 VLAN</li> <li>1 커뮤니티 VLAN</li> <li>1 특수 VLAN</li> </ul>
802.1x 인증되지 않은 VLAN 포트	802.1x 인증되지 않은 VLAN 포트는 다음으로 기능을 제한합니다. <ul style="list-style-type: none"> <li>1 고립형 포트</li> <li>1 커뮤니티 포트</li> <li>1 무차별 포트</li> <li>1 MAC 기반 VLAN 포트</li> <li>1 수신 필터링</li> </ul>
ACL	ACL 기능은 다음에 의해 제한됩니다. <ul style="list-style-type: none"> <li>1 MAC 기반 ACL</li> <li>1 특수 VLAN</li> </ul>
자동 조정	기능 상호 작용 제한이나 한계가 없습니다.
배압 지원	
브리지 멀티캐스트 필터링	기능 상호 작용 제한이나 한계가 없습니다.
케이블 검사	기능 상호 작용 제한이나 한계가 없습니다.
커뮤니티 포트	커뮤니티 포트는 잠긴 포트 기능을 제한합니다.
커뮤니티 VLAN	커뮤니티 VLAN은 다음으로 기능을 제한합니다. <ul style="list-style-type: none"> <li>1 정적 MAC 주소</li> <li>1 ACL</li> <li>1 GVRP</li> <li>1 IGMP 스누핑</li> <li>1 특수 VLAN</li> </ul>
DNS	제한이나 한계가 없습니다.
이중 모드	
흐름 제어	기능 상호 작용 제한이나 한계가 없습니다.
GARP	기능 상호 작용 제한이나 한계가 없습니다.
게스트 VLAN	게스트 VLAN은 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 개인 VLAN</li> <li>1 고립형 VLAN</li> <li>1 커뮤니티 VLAN</li> <li>1 MAC 기반 VLAN</li> <li>1 특수 VLAN</li> </ul>
GVRP	기능 상호 작용 제한이나 한계가 없습니다.
IGMP 스누핑	기능 상호 작용 제한이나 한계가 없습니다.
수신 필터링	기능 상호 작용 제한이나 한계가 없습니다.
고립형 포트	고립형 포트는 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 커뮤니티 포트</li> <li>1 무차별 포트</li> <li>1 포트 잠금</li> <li>1 GVRP</li> <li>1 MAC 기반 ACL</li> <li>1 수신 필터링</li> </ul>
고립형 VLAN	고립형 VLAN은 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 커뮤니티 VLAN</li> <li>1 정적 MAC 주소</li> <li>1 ACL</li> </ul>

	<ul style="list-style-type: none"> <li>1 GVRP</li> <li>1 IGMP 스누핑</li> <li>1 특수 VLAN</li> </ul>
LAG 통계 자료	기능 상호 작용 제한이나 한계가 없습니다.
연결 집계	기능 상호 작용 제한이나 한계가 없습니다. 그러나 이 기능에는 연결 집계 구성에 대한 여러 가지 지침이 있습니다. 모든 기능 지침은 " <a href="#">LAG 매개변수 정의</a> "를 참조하십시오.
장간 포트	장간 포트 기능은 다음에 의해 제한됩니다. <ul style="list-style-type: none"> <li>1 MAC 기반 ACL</li> <li>1 수신 필터링</li> </ul>
로깅	기능 상호 작용 제한이나 한계가 없습니다.
MAC 주소 지원	기능 상호 작용 제한이나 한계가 없습니다.
MDI/MDIX 감지	기능 상호 작용 제한이나 한계가 없습니다.
멀티캐스트 필터링	기능 상호 작용 제한이나 한계가 없습니다.
멀티캐스트 호스트	802.1X 표준(다중 호스트)은 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 고립형 포트</li> <li>1 MAC 기반 VLAN 포트</li> </ul>
다중 스페닝 트리	다중 스페닝 트리는 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 고립형 포트</li> <li>1 수신 필터링</li> </ul>
포트 기반 인증	포트 기반 인증은 다음으로 기능을 제한합니다. <ul style="list-style-type: none"> <li>1 802.1 단일</li> <li>1 고립형 포트</li> <li>1 장간 포트</li> <li>1 MAC 기반 VLAN</li> <li>1 수신 포트</li> </ul>
포트 미러링	기능 상호 작용 제한이나 한계가 없습니다. 그러나 이 기능에는 스톱 제어 구성에 대한 몇 가지 지침이 있습니다. 모든 기능 지침은 " <a href="#">포트 미러링 세션 정의</a> "를 참조하십시오.
포트 통계 자료	기능 상호 작용 제한이나 한계가 없습니다.
개인 VLAN	개인 VLAN은 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 고립형 포트</li> <li>1 커뮤니티 포트</li> <li>1 GVRP</li> <li>1 IGMP 스누핑</li> <li>1 특수 VLAN</li> </ul>
개인 VLAN	개인 VLAN는 다음으로 기능을 제한합니다. <ul style="list-style-type: none"> <li>1 고립형 VLAN</li> <li>1 GVRP</li> <li>1 IGMP 스누핑</li> <li>1 특수 VLAN</li> </ul>
무차별 포트	무차별 포트는 다음과 함께 작동할 수 없습니다. <ul style="list-style-type: none"> <li>1 장간 포트</li> <li>1 GVRP</li> <li>1 MAC 기반 VLAN 포트</li> </ul>
서비스 품질	기능 상호 작용 제한이나 한계가 없습니다.
RMON 통계 자료	기능 상호 작용 제한이나 한계가 없습니다.
SNMP 인증 알림	기능 상호 작용 제한이나 한계가 없습니다.
SNMP 알림	기능 상호 작용 제한이나 한계가 없습니다.
SNTP 인증	기능 상호 작용 제한이나 한계가 없습니다.
스페인 트리	기능 상호 작용 제한이나 한계가 없습니다.
특수 VLAN	기능 상호 작용 제한이나 한계가 없습니다.
정적 MAC	기능 상호 작용 제한이나 한계가 없습니다.
스톱 제어	기능 상호 작용 제한이나 한계가 없습니다.
시스템 로그	기능 상호 작용 제한이나 한계가 없습니다.
시스템 시간 동기화	기능 상호 작용 제한이나 한계가 없습니다.

기화	
인증되지 않은 VLAN 포트	인증되지 않은 VLAN 포트는 다음으로 기능을 제한합니다. <ul style="list-style-type: none"><li>1 고립형 포트</li><li>1 커뮤니티 포트</li><li>1 무차별 포트</li><li>1 GVRP</li><li>1 MAC 기반 VLAN 포트</li><li>1 수신 필터링</li></ul>

---

[목록 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

## 용어집

Dell™ PowerConnect™ 34XX 시스템 사용 설명서

이 용어집에는 주요 기술 용어가 포함됩니다.

<a href="#">가</a>	<a href="#">나</a>	<a href="#">다</a>	<a href="#">라</a>	<a href="#">마</a>	<a href="#">바</a>	<a href="#">사</a>	<a href="#">아</a>	<a href="#">자</a>	<a href="#">차</a>	<a href="#">카</a>	<a href="#">타</a>	<a href="#">파</a>	<a href="#">한</a>	<a href="#">영어</a>
-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	--------------------

### 가

#### 기가비트 이더넷

기가비트 이더넷은 1000Mbps 속도로 전송하며, 기존 10/100Mbps 이더넷 표준과 호환됩니다.

### 나

#### 노드

네트워크 연결 끝점 또는 여러 네트워크 선의 공통 교차점입니다. 노드에는 다음이 포함됩니다.

- 1 프로세서
- 1 컨트롤러
- 1 워크스테이션

### 다

#### 대역폭

대역폭은 일정 시간 동안 전송할 수 있는 데이터 양을 지정합니다. 디지털 스위치 모듈의 경우 대역폭은 초당 비트 수(bps) 또는 초당 바이트 수로 정의됩니다.

#### 대역폭 할당

특정 응용프로그램, 사용자 또는 인터페이스에 할당된 대역폭의 양

#### 도메인

공통 규칙과 절차로 묶어진 네트워크상의 컴퓨터 및 장치 그룹입니다.

### 라

#### 라우터

분리된 두 네트워크를 연결하는 장치입니다. 라우터는 둘 이상의 네트워크 간에 패킷을 전달합니다. 라우터는 총 3 레벨에서 작동합니다.

## 마

### 마스크

특정 값, 예를 들어 IP 주소의 일부를 포함하거나 제외하는 필터입니다.

예를 들어, 장치 2가 10분 주기의 처음 1분에 삽입되고 장치 1이 같은 주기의 제5분에 삽입되면 해당 장치는 같은 시간을 가진 것으로 간주됩니다.

### 멀티캐스트

단일 패킷의 사본을 여러 포트에 전송합니다.

## 바

### 배업

포트가 메시지를 수신할 수 없도록 하는 반이중 모드에 사용되는 메커니즘입니다.

### 백업 구성 파일

스위치 모듈 구성의 백업 사본이 들어있습니다. 실행 구성 파일 또는 시작 구성 파일이 백업 파일에 복사되는 경우 백업 파일이 변경됩니다.

### 보드

매 초에 전송되는 신호 요소 수입니다.

### 부트 버전

부트 버전입니다.

### 부하 균형

데이터 우수 배포 또는 사용 가능한 네트워크 자원을 통한 패킷 처리를 활성화합니다. 예를 들어, 부하 균형은 수신 패킷을 균등하게 모든 서버에 배포하거나 패킷을 사용 가능한 다음 서버로 향하도록 합니다.

### 브로드캐스트 도메인

지정 세트의 장치에서 고안한 브로드캐스트 프레임 수신하는 장치 세트입니다. 라우터가 브로드캐스트 프레임을 전달하지 않으므로, 라우터는 브로드캐스트 도메인을 바인드합니다.

### 브로드캐스트 스톱

단일 포트에 의해 네트워크에서 동시에 전송된 브로드캐스트 메시지의 초과 양입니다. 전달된 메시지 응답이 네트워크에 쌓여서 네트워크 자원에 과부하를 주거나 네트워크의 제한 시간 초과를 유발합니다.

브로드캐스트 스템에 대한 자세한 내용은 ["LAG 매개변수 정의"](#)를 참조하십시오.

## 브로드캐스팅

네트워크상의 모든 포트에 패킷을 전송하는 방법입니다.

## 브리지

두 네트워크를 연결하는 장치. 브리지는 특정 하드웨어용이지만 프로토콜과 독립적으로 사용됩니다. 브리지는 총 1이나 총 2 레벨로 작동합니다.

## 사

## 서버

서비스를 네트워크상의 다른 컴퓨터에 제공하는 중앙 컴퓨터입니다. 서비스에는 파일 저장 공간 및 응용프로그램에 대한 액세스가 포함될 수 있습니다.

## 서브넷 마스크

서브넷 주소에 사용된 IP 주소의 전부 또는 일부를 숨기는 데 사용됩니다.

## 서브넷

서브 네트워크(Sub-network)의 약칭. 서브넷은 공통 주소 구성요소를 공유하는 네트워크의 일부입니다. TCP/IP 네트워크상에서 한 프리픽스를 공유하는 장치는 동일한 서브넷의 부분입니다. 예를 들어, 프리픽스 157.100.100.100이 있는 모든 장치는 동일 서브넷의 부분입니다.

## 서비스 등급

CoS(서비스 등급). 서비스 등급은 802.1p 우선순위 구성표입니다. CoS는 우선순위 정보로 패킷에 태그를 붙이는 방법을 제공합니다. 0~7 사이의 CoS 값이 패킷의 총 II 헤더에 추가됩니다. 여기서 0은 최저 우선순위이고 7은 최고 우선순위입니다.

둘 이상의 충돌되는 패킷의 겹치기 전달. 전송된 데이터는 사용할 수 없으며 세션은 재시작합니다.

## 송신 포트

네트워크 처리량을 전송하는 포트입니다.

## 수신 포트

네트워크 처리량이 수신되는 포트입니다.

## 스위치

LAN 세그먼트 간에 패킷을 필터하고 전달합니다. 스위치는 모든 패킷 프로토콜 종류를 지원합니다.

## 스패닝 트리 프로토콜

네트워크 처리량의 루프를 방지합니다. STP(스패닝 트리 프로토콜)는 모든 브리지 배열에 트리 위상을 제공합니다. STP는 루프를 무시하고 한 네트워크상의 최종 스테이션 사이에 경로를 제공합니다.

## 시작 구성

스위치 모듈 전원이 꺼지거나 재부팅된 경우 정확한 모듈 구성을 보유합니다.

## 실행 구성 파일

현재 세션 동안 입력한 명령뿐만 아니라 모든 시작 구성 파일 명령이 들어있습니다. 스위치 모듈 전원이 꺼지거나 재부팅된 후, 실행 구성 파일에 저장된 모든 명령은 유실됩니다.

## 아

## 액세스 모드

시스템으로의 사용자 액세스가 승인되는 방법을 지정합니다.

## 액세스 프로파일

네트워크 관리자가 스위치 모듈에 액세스하는 데 대한 프로파일 및 규칙을 정의하도록 허용합니다. 관리 기능 액세스는 다음 조건에 의해 정의된 사용자 그룹에 제한될 수 있습니다.

- 1 수신 인터페이스
- 1 원본 IP 주소 또는 원본 IP 서브넷

## 와일드카드 마스크

사용되는 IP 주소 비트와 무시되는 비트를 지정합니다. 와일드 스위치 모듈 마스크 255.255.255.255는 중요한 비트가 없음을 나타냅니다. 와일드카드 0.0.0.0은 비트가 모두 중요함을 나타냅니다.

예를 들어, 대상 IP 주소가 149.36.184.198이고 와일드카드 마스크가 255.36.184.00인 경우, IP 주소의 처음 두 비트는 사용되지만 뒤의 두 비트는 무시됩니다.

## 유니캐스트

한 패킷을 한 사용자에게 전송하는 라우팅 형식입니다.

## 이더넷

이더넷은 IEEE 802.3을 기준으로 표준화됩니다. 이더넷은 가장 일반적으로 구현되는 LAN 표준입니다. Mbps 수준의 데이터 전송 속도를 지원합니다. 여기서 10, 100 또는 1000Mbps가 지원됩니다.

## 이미지 파일



시스템 이미지는 이미지(이미지 1 및 이미지 2)라 불리는 2개의 플래시 섹터에 저장됩니다. 활성 이미지는 활성 사본을 저장하고 다른 한 이미지는 두 번째 사본을 저장합니다.

## 이중 모드

데이터의 동시 송수신을 허용합니다. 이중 모드에는 다음과 같은 2가지 종류가 있습니다.

- 1 **전이중 방식 모드**— 2중 동기식 통신(예: 전화)을 허용합니다. 양 쪽에서 정보를 동시에 전송할 수 있습니다.
- 1 **반이중 방식 모드**— 비동기식 통신(예: 워키 토키)을 허용합니다. 매 번 한 쪽에서만 정보를 전송할 수 있습니다.

## 인증 프로파일

로그인을 활성화하는 규칙 및 사용자와 응용프로그램의 인증입니다.

## 자

### 자동 조정

다음 기능을 위해 10/100Mbps 또는 10/100/1000Mbps 이더넷 포트 설정을 허용합니다.

- 1 이중/반이중 방식 모드
- 1 흐름 제어
- 1 속도

### 자산 태그

사용자 정의된 스위치 모듈 참조를 지정합니다.

### 정보 프레임

동일한 데이터를 더 적은 프레임으로 전송할 수 있도록 합니다. 정보 프레임은 오버헤드, 처리 시간, 중단 횟수를 줄입니다.

### 조각

576비트 미만의 이더넷 패킷

### 조각내기

브리지하기 위해 LAN을 분리된 LAN 세그먼트로 분할합니다. 조각내기는 LAN 대역폭 제한을 무시합니다.

### 집계된 VLAN

여러 VLAN을 단일 집계된 VLAN으로 묶습니다. 집계 VLAN은 라우터를 활성화하여 동일한 슈퍼 VLAN에 종속되는 다른 서브 VLAN에 있는 노드에 대한 ARP 요청에 응답하도록 합니다. 라우터는 해당 MAC 주소와 함께 응답합니다.

## 차

## 최선형(Best Effort)

처리량이 최저 우선순위 대기열에 할당되고 패킷 전달이 보장되지 않습니다.

## 최종 시스템

네트워크상의 최종 사용자 장치입니다.

## 층 2

데이터 연결 층 또는 MAC 층, 클라이언트 또는 서버 스테이션의 실제 주소가 들어있습니다. 층 2 처리는 처리할 정보가 적기 때문에 층 3 처리보다 빠릅니다.

## 층 4

연결을 설정하고 모든 데이터가 해당 대상 위치에 전송되도록 합니다. 층 4 레벨에서 검색된 패킷은 해당 응용프로그램을 기반으로 분석되어 결정을 전달합니다.

## 카

### 커뮤니티

동일한 시스템 액세스 권한을 보유한 사용자 그룹을 지정합니다.

### 캐리

정보를 데이터베이스로부터 추출하여 사용하도록 표시합니다.

## 타

### 텔넷

단말기 에뮬레이션 프로토콜. 시스템 사용자가 로그인하고 원격 네트워크상의 자원을 사용하도록 합니다.

### 트랩

SNMP에세 보낸, 시스템 이벤트가 발생함을 나타내는 메시지입니다.

### 트렁킹

연결 징계. 포트 그룹을 함께 연결하여 단일 트렁크(징계된 그룹)를 형성함으로써 포트 사용을 최적화합니다.

## 파

## 패킷

패킷 스위치 시스템에서의 전송에 대한 정보 블록

## 포트 미러링

한 포트에서 모니터링 포트로 수신 및 발신 패킷의 사본을 전달하여 네트워크 처리량을 모니터링하고 미러합니다.

포트 미러링에 대한 자세한 내용은 **포트 미어링 세션 정의**를 참조하십시오.

## 포트 속도

포트의 포트 속도를 나타냅니다. 포트 속도는 다음을 포함합니다.

- 1 이더넷 10Mbps
- 1 고속 이더넷 100Mbps
- 1 기가비트 이더넷 1000Mbps

## 포트

실제 포트는 마이크로프로세서가 주변 장치와 통신할 수 있도록 하는 연결 구성요소를 제공합니다.

## 프레임

실제 매체에서 요구하는 헤더 및 트레일러 정보가 들어 있는 패킷입니다.

## 프로토콜

장치가 네트워크를 통해 정보를 교환하는 방식을 관리하는 한 조의 규칙입니다..

## 플래핑

인터페이스 상태가 빈번하게 변경될 경우 플래핑이 발생합니다. 예를 들어, STP 포트는 듣기-기억-전달로 지속적으로 변경됩니다. 이는 처리량 유실을 초래할 수 있습니다.

## 하

## 호스트

정보의 공급자 역할을 하거나 다른 컴퓨터에 서비스를 제공하는 컴퓨터입니다.

## 후연관

스위치 모듈에서 정보를 나르는 주 버스입니다.

## 흐름 제어

지속 장치가 고속 장치와 통신할 수 있게 합니다. 즉, 고속 장치가 패킷을 전송하는 것을 억제합니다.

## 영어

### ARP

주소 확인 프로토콜(Address Resolution Protocol)의 약칭. IP 주소를 실제 주소로 전환하는 프로토콜입니다.

### ASIC

응용 주문형 직접 회로(Application Specific Integrated Circuit)의 약칭. 특정 응용프로그램을 위해 설계된 사용자 칩입니다.

### BootP

부트스트랩 프로토콜(Bootstrap Protocol)의 약칭. 워크스테이션이 IP 주소, 네트워크에 있는 BootP 서버의 IP 주소 또는 스위치 모듈의 부트에 로드된 구성 파일을 검색할 수 있도록 합니다.

### BPDU

브리지 프로토콜 데이터 장치(Bridge Protocol Data Unit)의 약칭. 메시지 형식으로 브리지 정보를 제공합니다. BPDU는 스페닝 트리 구성과 함께 스위치 모듈 정보를 통해 전송됩니다. BPDU 패킷에는 포트, 주소, 우선순위 및 전달 비용에 대한 정보가 들어있습니다.

### CDB

구성 데이터 베이스(Configuration Data Base)의 약칭. 장치의 구성 정보가 들어있는 파일.

### CLI

명령줄 인터페이스(Command Line Interface)의 약칭. 시스템을 구성하는 데 사용되는 한 조의 명령줄입니다. CLI 사용에 대한 자세한 내용은 CLI 사용을 참조하십시오.

### CPU

중앙 처리 장치(Central Processing Unit)의 약어. 컴퓨터에서 정보를 처리하는 부분입니다. CPU는 제어 장치 및 ALU로 구성되었습니다.

### DHCP 클라이언트

DHCP를 사용하여 네트워크 주소와 같은 구성 매개변수를 얻는 장치입니다.

### DRAC/MC

DRAC/MC. Dell 모듈러 서버 시스템 구성요소에 대한 단일 점 제어를 제공합니다.

## DSCP

DiffServe 코드 점(DiffServe Code Point)의 약어. DSCP는 QoS 우선순위 정보로 IP 패킷에 태그를 붙이는 방법을 제공합니다.

## EWS

내포된 웹 서버(Embedded Web Server)의 약칭. 표준 웹 브라우저를 통해 장치 관리를 제공합니다. 내포된 웹 서버는 CLI 또는 NMS에 추가로(또는 대신) 사용됩니다.

## FFT

고속 전달 표(Fast Forward Table)의 약칭. 전달 루트의 정보를 제공합니다. 패킷이 알려진 루트를 통해 장치에 전송된 경우 해당 패킷은 FFT에 나열된 루트를 통해 전송됩니다. 알려진 루트가 없는 경우 CPU가 패킷을 전달하고 FFT를 업데이트합니다.

## FIFO

선입 선출(First In First Out)의 약칭. 대기열의 맨 앞의 패킷이 맨 먼저 패킷에서 전송되는 패킷인 대기열 프로세서입니다.

## GARP

일반 특성 등록 프로토콜(General Attributes Registration Protocol)의 약칭. 사용자 국가를 멀티캐스트 도메인으로 등록합니다.

## GVRP

GARP VLAN 등록 프로토콜(GARP VLAN Registration Protocol)의 약칭. 사용자 국가를 VLAN으로 등록합니다.

## HOL

헤드 라인(Head of Line)의 약칭. 패킷이 대기열에 놓입니다. 대기열의 처음에 있는 패킷이 행의 끝에 있는 패킷보다 먼저 전달됩니다.

## HTTP

하이퍼텍스트 전송 프로토콜(HyperText Transport Protocol)의 약칭. 인터넷상에서 서버와 클라이언트 간에 HTML 문서를 전송합니다.

## IC

직접 회로(Integrated Circuit)의 약칭. 직접 회로는 반도체 금속으로 구성된 소형 전자 장치입니다.

## ICMP

인터넷 제어 메시지 프로토콜(Internet Control Message Protocol)의 약칭. 게이트웨이 또는 대상 호스트가 원본 호스트와 통신할 수 있도록 합니다(예: 처리 오류 보고).

## IEEE 802.1d

스패닝 트리 프로토콜에 사용되는 IEEE 802.1d는 MAC 브리지를 지원하여 네트워크 루프를 방지합니다.

## IEEE 802.1p

데이터 연결/MAC 하위 층에서 네트워크 처리량에 우선순위를 정합니다.

## IEEE 802.1Q

브리지된 LAN 인프라 내 VLAN의 정의, 작업 및 관리를 허용하는 VLAN 브리지의 작업을 정의합니다.

## IEEE

전기전자학회(Institute of Electrical and Electronics Engineers)의 약칭. 통신 및 네트워킹 표준을 개발하는 엔지니어링 기관입니다.

## IP

인터넷 프로토콜(Internet Protocol)의 약칭. 패킷의 형식 및 주소 지정 방식을 지정합니다. IP가 패킷에 주소를 지정하여 해당 패킷을 올바른 포트에 전달합니다.

## IP 주소

인터넷 프로토콜 주소(Internet Protocol Address)의 약칭. 둘 이상의 상호 연결된 LAN 또는 WAN이 있는 네트워크 장치에 할당된 고유 주소입니다.

## LAG

연결 집계된 그룹(Link Aggregated Group)의 약칭. 포트 또는 VLAN을 단일 가상 포트 또는 VLAN에 집계시킵니다.

LAG에 대한 자세한 내용은 **LAG 멤버십 정의**를 참조하십시오.

## LAN

근거리 통신망(Local Area Network)의 약칭. 한 방, 빌딩, 캠퍼스 또는 기타 제한된 지리적 범위 내의 네트워크입니다.

## MAC 주소 학습

MAC 주소 학습은 패킷의 원본 MAC 주소가 기록되는 학습 브리지의 특징을 가집니다. 특정 주소에 지정된 패킷은 이 주소가 있는 브리지 인터페이스로만 전달됩니다. 알 수 없는 주소로 지정된 패킷은 모든 브리지 인터페이스로 전달됩니다. MAC 주소 학습은 연결된 LAN의 처리량을 최소화합니다.

## MAC 층

DTL(데이터 연결 제어) 층의 하위 층입니다.

## MAC Address

매체 액세스 제어 주소(Media Access Control Address)의 약칭. MAC 주소는 각 네트워크 노드를 식별하는 하드웨어별 주소입니다.

## **MD5**

메시지 다이제스트 5(Message Digest 5)의 약칭. 128비트 해시를 생성하는 알고리즘입니다. MD5는 MD4의 변형이며 MD4의 보안을 향상시킵니다. MD5는 통신의 무결성을 확인하고 통신의 원본을 인증합니다.

## **MDI**

매체 의존 인터페이스(Media Dependent Interface)의 약칭. 최종 스테이션에 사용되는 케이블입니다.

## **MDIX**

크로스오버가 있는 매체 의존 인터페이스(Media Dependent Interface with Crossover)의 약칭. 허브 및 스위치에 사용되는 케이블입니다.

## **MIB**

관리 정보 베이스(Management Information Base)의 약칭. MIB에는 네트워크 구성요소의 특정 측면을 설명하는 정보가 들어있습니다.

## **NMS**

네트워크 관리 시스템(Network Management System)의 약칭. 시스템 관리 방식을 제공하는 인터페이스입니다.

## **OID**

객체 식별자(Object Identifier)의 약칭. SNMP에 사용되어 관리 객체를 식별합니다. SNMP 관리자/에이전트 네트워크 관리 패러다임에서 각 관리 객체는 해당 객체를 식별하는 OID가 있어야 합니다.

## **PDU**

프로토콜 데이터 장치(Protocol Data Unit)의 약칭. 프로토콜 제어 정보 및 총 사용자 데이터로 구성된 총 프로토콜에 지정된 데이터 장치입니다.

## **PING**

패킷 인터넷 그로퍼(Packet Internet Groper)의 약칭. 특정 IP 주소가 사용 가능한지를 확인합니다. 패킷을 다른 IP 주소로 전송하고 응답을 기다립니다.

## **QoS**

서비스 품질(Quality of Service)의 약칭. QoS는 네트워크 관리자가 우선순위, 응용프로그램 종류, 및 원본과 대상 주소에 따라 네트워크 처리량 전달 방법과 종류를 결정하도록 합니다.

## **RADIUS**

원격 인증 다이얼 인 사용자 서비스(Remote Authentication Dial-In User Service)의 약칭. 시스템 사용자 인증 및 연결 시간 추적 방식입니다.

## **RMON**

원격 모니터링(Remote Monitoring)의 약칭. 단일 워크스테이션에서 수집할 네트워크 정보를 제공합니다.

## **RSTP**

고속 스페닝 트리 프로토콜(Rapid Spanning Tree Protocol)의 약칭. 전달 루프를 작성하지 않고 스페닝 트리의 빠른 수렴을 허용하는 네트워크 위상을 감지하고 사용합니다.

## **SNMP**

단순 네트워크 관리 프로토콜(Simple Network Management Protocol)의 약칭. LAN을 관리합니다. SNMP 기반 소프트웨어는 내포된 SNMP 에이전트가 있는 네트워크 장치와 통신합니다. SNMP 에이전트는 네트워크 활성화 및 장치 상태 정보를 수집하여 워크스테이션에 돌려 보냅니다.

## **SNTP**

단순 네트워크 시간 프로토콜(Simple Network Time Protocol)의 약칭. SNTP는 정확한 네트워크 스위치 클럭 시간을 밀리초 단위까지 확실하게 합니다.

## **SoC**

시스템 온 칩(System on a Chip)의 약칭. 전체 시스템을 포함한 ASIC입니다. 예를 들어, 텔레콤 SoC 응용프로그램에는 마이크로프로세서, 디지털 신호 프로세서, RAM 및 ROM을 포함할 수 있습니다.

## **SSH**

**보안 셸(Secure Shell)**의 약칭. 네트워크를 통해 다른 컴퓨터로의 로그인을 허용하고 원격 컴퓨터에서 명령을 실행하며 한 컴퓨터에서 다른 컴퓨터로 파일을 이동합니다. 보안 셸은 불안정한 채널에 강력한 인증 및 보안 통신 방법을 제공합니다.

## **TCP/IP**

전송 제어 프로토콜(Transmission Control Protocol)의 약칭. 두 호스트가 서로 통신하고 데이터 스트림을 교환할 수 있도록 합니다. TCP는 패킷 전송을 보장하며 패킷이 전송된 순서대로 송수신됨을 보장합니다.

## **TFTP**

소형 파일 전송 프로토콜(Trivial File Transfer Protocol)의 약칭. 보안 기능 없이 UDP(사용자 데이터 프로토콜)를 사용하여 파일을 전송합니다.

## **UDP**

사용자 데이터 프로토콜(User Data Protocol)의 약칭. 패킷을 전송하나 전송 성공을 보장하지 않습니다.

## **VLAN**

가상 근거리 통신망(Virtual Local Area Network)의 약칭. 하드웨어 솔루션을 정의하는 것이 아니라 소프트웨어를 통해 작성된 LAN(근거리 통신망)의 논리 서브 그룹입니다.

## **WAN**

광역 통신망(Wide Area Networks)의 약칭. 광범위한 지리적 범위를 포괄하는 네트워크입니다.



---

[목록 페이지로 돌아가기](#)