

Dell™ PowerConnect™ M6220 사용 설명서

[소개](#)

[하드웨어 설명](#)

[Dell™ OpenManage™ 스위치 관리자 사용](#)

[케이블 및 포트 정보](#)

[Dell™ PowerConnect™ 구성](#)

[시스템 정보 구성](#)

[스위치 정보 구성](#)

[연결 종속성 만들기](#)

[통계/RMON 보기](#)

[관우팀 구성](#)

[IPv6 구성](#)

[서비스 품질 \(QoS\) 구성](#)

[IP 멀티캐스트 구성](#)

[도움말 열기](#)

주, 주의사항 및 주의



주: "주"는 컴퓨터를 보다 효율적으로 사용하는데 도움이 되는 중요 정보를 제공합니다.



주의사항: "주의사항"은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.



주의: "주의"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 나타냅니다.

본 설명서에 수록된 정보는 사전 통보 없이 변경될 수 있습니다.
© 2007 Dell Inc. 저작권 본사 소유.

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

본 설명서에 사용된 상표인 Dell, Dell OpenManage, DELL 로고, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet 및 Latitude는 Dell Inc.의 상표이며, Microsoft, Windows 및 Windows Vista는 미국 및 기타 국가에서 Microsoft Corporation의 상표 또는 등록 상표입니다. Procomm Plus는 미국 및 기타 국가에서 Symantec Corporation 또는 계열 회사의 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 상호 이름에 대한 어떠한 소유권도 보유하지 않습니다.

모델 M6220

2007년 9월 Rev. A00

[목차 페이지로 돌아가기](#)

케이블 및 포트 정보

Dell™ PowerConnect™ M6220 사용 설명서

- [10/100/1000 Ethernet 인터페이스](#)
- [듀얼 10G-슬롯 인터페이스](#)
- [직렬 케이블 연결](#)
- [전원 연결](#)

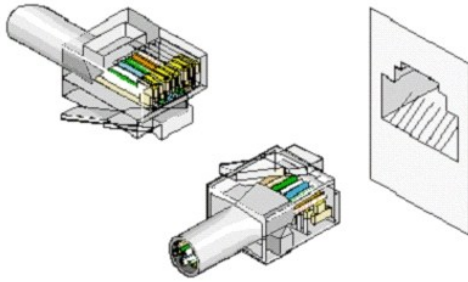
이 절에서는 스위치의 물리적 인터페이스에 대해 설명하고 케이블 연결에 대한 정보를 제공합니다.

스테이션은 전면 패널의 물리적 인터페이스 포트를 통해 스위치 포트에 연결됩니다. 각 스테이션의 경우 적절한 모드(반/전이중, 자동)로 설정됩니다.

10/100/1000 Ethernet 인터페이스

스위칭 포트는 똑바른 케이블을 사용하여 표준 RJ-45 Ethernet 스테이션에 연결된 스테이션에 연결할 수 있습니다. 서로 간에 연결된 전송 장치는 크로스 케이블을 사용합니다. [그림 4-1](#)은 RJ-45 커넥터를 보여줍니다.

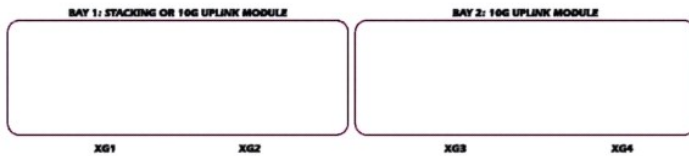
그림 4-1. RJ-45 Connector(RJ-45 커넥터)



듀얼 10G-슬롯 인터페이스

M6220은 듀얼 XAUI 인터페이스를 지원합니다. 이러한 인터페이스는 XFP 모듈을 지원하는 경우 10Gbps에서 작동하고 SFP 모듈을 지원하는 경우 12Gbps(위쪽에서 볼 때 왼쪽 슬롯만 해당)에서 작동합니다. [그림 4-2](#)은 XAUI 슬롯을 보여줍니다.

그림 4-2. XAUI slots(XAUI 슬롯)



직렬 케이블 연결

초기 설치 및 구성 시 USB 유형의 A-DB9 직렬 케이블을 사용하여 스위치를 터미널에 연결할 수 있습니다. 또한 터미널 에뮬레이션 소프트웨어를 실행하는 컴퓨터를 사용할 수 있습니다. 스위치의 직렬 케이블은 양 DB-9 크로스오버 케이블에 대해 USB 유형의 A입니다([그림 4-3](#) 참조).

그림 4-3. Serial Connectors(직렬 커넥터)



스위치를 터미널에 연결

1. 직렬 케이블을 터미널(콘솔) ASCII DTE RS-232에 연결하십시오.
2. 인터페이스 케이블을 스위치의 직렬 포트에 연결합니다.
3. 스택을 구성하는 경우 인터페이스 케이블을 마스터 스위치의 직렬 포트에 연결합니다.

Dell™ PowerConnect™ M6220 직렬 포트 연결에 대한 자세한 내용은 *M6220 시리즈 스택형 스위치 시작 안내서*를 참조하십시오.

전원 연결

PowerConnect M6220은 Dell Blade Server 새시에서 전원을 수신합니다. PowerConnect M6220 전원 공급 장치에 대한 자세한 내용은 *Dell Blade Server 새시 하드웨어 소유자 설명서*를 참조하십시오.

[목차 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

시스템 정보 구성

Dell™ PowerConnect™ M6220 사용 설명서

- [System\(시스템\) 페이지 열기](#)
- [일반 장치 정보 정의](#)
- [SNTP 설정 구성](#)
- [로그 관리](#)
- [IP 주소 지정 정의](#)
- [케이블 진단 프로그램 실행](#)
- [장치 보안 관리](#)
- [SNMP 매개변수 정의](#)
- [파일 관리](#)
- [고급 설정 정의](#)
- [스택형 배치 정의](#)

System(시스템) 페이지 열기

System(시스템) 페이지에 나열된 메뉴를 사용하여 스위치와 해당 환경의 관계를 정의할 수 있습니다. System(시스템) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)을 클릭합니다. System(시스템) 메뉴 페이지에는 다음 기능에 대한 링크가 있습니다.

- 1 [일반 장치 정보 정의](#)
- 1 [SNTP 설정 구성](#)
- 1 [로그 관리](#)
- 1 [IP 주소 지정 정의](#)
- 1 [케이블 진단 프로그램 실행](#)
- 1 [장치 보안 관리](#)
- 1 [SNMP 매개변수 정의](#)
- 1 [파일 관리](#)
- 1 [고급 설정 정의](#)
- 1 [스택형 배치 정의](#)

일반 장치 정보 정의

General(일반) 메뉴 페이지에는 장치 매개변수를 구성할 수 있는 페이지에 대한 링크가 있습니다. 이 페이지를 사용하여 다음 기능에 액세스할 수 있습니다.

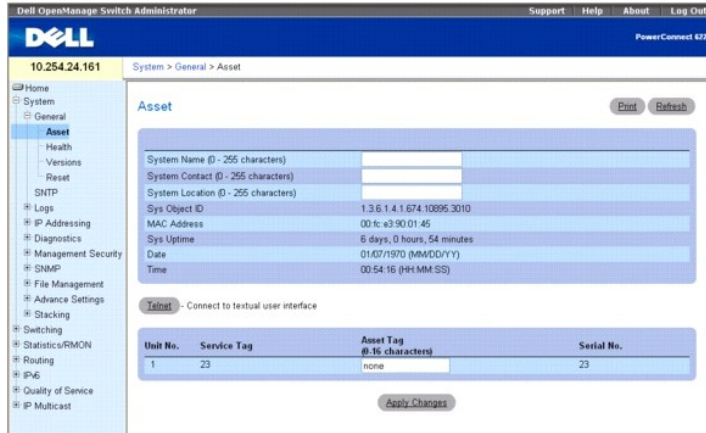
- 1 [자산](#)
- 1 [시스템 상태](#)
- 1 [버전](#)
- 1 [System\(시스템\) 리소스](#)
- 1 [표준 시간대 구성](#)
- 1 [서버 타임 구성](#)
- 1 [클럭 세부 사항](#)
- 1 [재설정](#)

자산

Asset(자산) 페이지 필드를 사용하여 일반 장치 정보를 구성하고 볼 수 있습니다.

Asset(자산) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → General(일반) → Asset(자산)을 클릭합니다.

그림 6-1. Asset(자산)



Asset(자산) 페이지에는 다음 필드가 있습니다.

System Name (0 -255 characters)(시스템 이름(0 - 255자)) — 장치 시스템 이름을 지정하는 데 사용합니다.

System Contact (0 -255 characters)(시스템 연락처(0 - 255자)) — 담당자 이름을 지정하는 데 사용합니다.

System Location (0 - 255 characters)(시스템 위치(0 - 255자)) — 시스템 위치를 지정하는 데 사용합니다.

Sys Object ID(시스템 개체 ID) — 지정된 시스템 개체 ID입니다.

MAC Address(MAC 주소) — 스위치의 MAC 주소를 표시합니다.

Sys Uptime(시스템 작동 시간) — 마지막 재시작 이후의 시간(일, 시간 및 분)을 표시합니다.

Date(날짜) — 현재 시스템 날짜를 표시합니다. 형식은 월, 일, 연도입니다(MM/DD/YY). 예를 들어 11/01/05는 2005년 11월 1일입니다.

Time(시간) — 현재 시스템 시간을 표시합니다. 형식은 시, 분, 초입니다(HH:MM:SS). 예를 들어 20:12:03은 오후 8:12:03입니다.

Unit No.(장치 번호) — 스택 내의 스위치 위치를 표시합니다.

Service Tag(서비스 태그) — 장치를 수리할 때 사용되는 서비스 참조 번호를 표시합니다.

Asset Tag (0 - 16 characters)(자산 태그(0 - 16자)) — 사용자 정의 장치 참조를 표시합니다.

Serial No.(일련 번호) — 장치 일련 번호를 표시합니다.


시스템 정보 정의

1. **Asset(자산)** 페이지를 엽니다.
2. 다음 필드를 정의합니다. **System Name(시스템 이름)**, **System Contact(시스템 연락처)**, **System Location(시스템 위치)** 및 **Asset Tag(자산 태그)**.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

시스템 매개변수가 적용되고 장치가 업데이트됩니다.

텔넷 세션 시작

1. **Asset(자산)** 페이지를 엽니다.

 **주:** 텔넷 세션을 시작하기 전에 해당 텔넷 매개변수가 설정됩니다. 자세한 내용은 "[초기 텔넷 암호 구성](#)"을 참조하십시오. 클라이언트에 Microsoft® Windows® 환경이 있는 경우 텔넷에 대해 프로그램을 구성해야 합니다. 클라이언트에 Unix 환경이 있는 경우에는 텔넷 프로그램이 경로에 있어야 합니다.

2. **Telnet(텔넷)**을 클릭합니다.

시스템이 임력을 받을 준비가 되었음을 나타내는 메시지가 표시됩니다.

CLI 명령을 사용하여 장치 정보 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

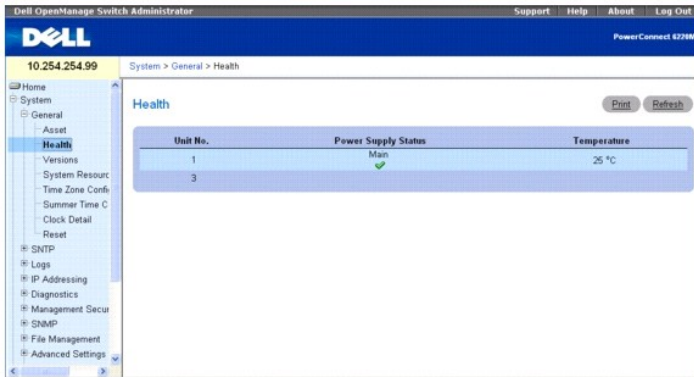
- 1 시스템 관리 명령
- 1 SNMP 명령
- 1 클럭 명령

시스템 상태

Health(상태) 페이지를 사용하여 스위치의 전원 및 통풍 공급 장치에 대한 정보를 비롯한 물리적 장치 정보를 볼 수 있습니다.

Health(상태) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **Health(상태)**를 클릭합니다.


그림 6-2. Health(상태)




Health(상태) 페이지에는 다음 필드가 있습니다.

Unit No.(장치 번호) — 스택 내의 장치 위치를 표시합니다.

Power Supply Status(전원 공급 장치 상태) — 전원 공급 장치 상태를 표시합니다.

 — 전원 공급 장치가 정상적으로 작동합니다.

 — 전원 공급 장치가 정상적으로 작동하지 않습니다.

Not Present(존재하지 않음) — 전원 공급 장치가 현재 없습니다.

Temperature(온도) — 장치가 현재 실행되고 있는 온도를 표시합니다.

CLI 명령을 사용하여 시스템 상태 정보 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

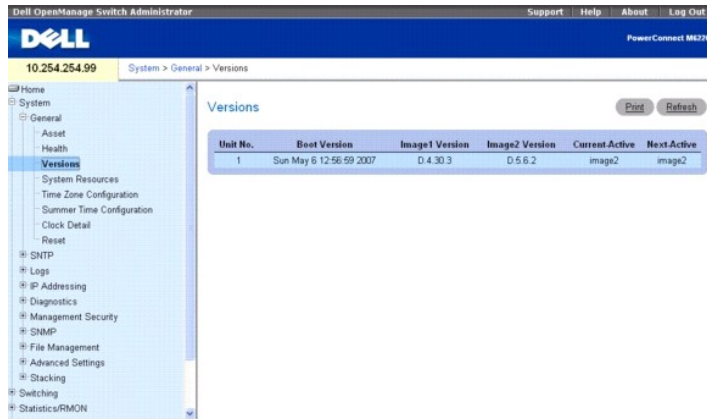
- 1 시스템 관리 명령

버전

Versions(버전) 페이지를 사용하여 현재 실행 중인 소프트웨어 버전에 대한 정보를 볼 수 있습니다.

Versions(버전) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **Versions(버전)**를 클릭합니다.

그림 6-3. Versions(버전)



Versions(버전) 페이지에는 다음 필드가 있습니다.

Unit No.(장치 번호) — 스택 내의 장치 위치를 표시합니다.

Boot Version(부팅 버전) — 활성 이미지의 부팅 이미지 버전을 표시합니다.

Image1 Version(이미지 1 버전) — 사용 가능한 두 개의 소프트웨어 이미지 중 하나의 버전 번호를 표시합니다.

Image2 Version(이미지 2 버전) — 사용 가능한 두 개의 소프트웨어 이미지 중 다른 하나의 버전 번호를 표시합니다.

Current-Active(현재 활성) — 장치에서 실행 중인 현재 소프트웨어 버전을 표시합니다.

Next-Active(다음 활성) — 현재 버전에 장애 발생 시 로드할 소프트웨어 버전을 표시합니다.

CLI를 사용하여 장치 버전 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

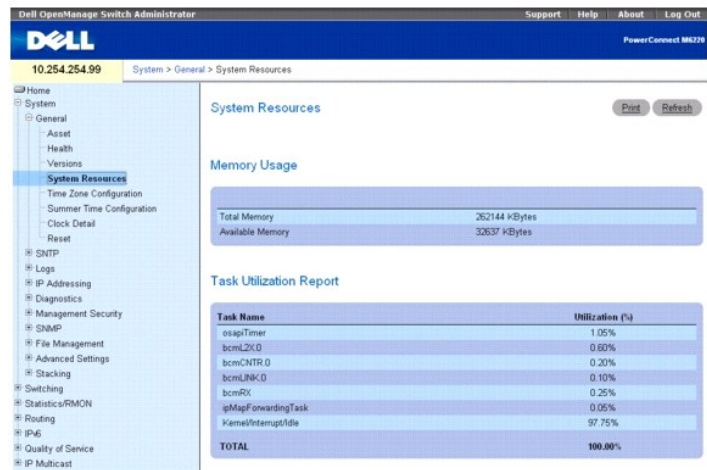
- 1 시스템 관리 명령

System(시스템) 리소스

System(시스템) 리소스 페이지를 통해 메모리 사용 및 작업 효율을 확인할 수 있습니다.

System(시스템) 리소스 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **System(시스템) 리소스**를 클릭합니다.

그림 6-4. System(시스템) 리소스



System(시스템) 리소스 페이지에는 다음 필드가 있습니다.

Total Memory(총 메모리) — 스위치의 현재 총 메모리를 표시합니다.

Available Memory(사용 가능한 메모리) — 스위치의 현재 사용 가능한(할당할 수 있는) 메모리를 표시합니다.

Task Name(작업 이름) — 스위치에서 실행 중인 활성 작업의 이름입니다.

Utilization(사용)(%) — 해당 작업에 사용되는 CPU 시간의 백분율로 2초의 시간에 대해 계산됩니다.

CLI를 사용하여 System(시스템) 리소스 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

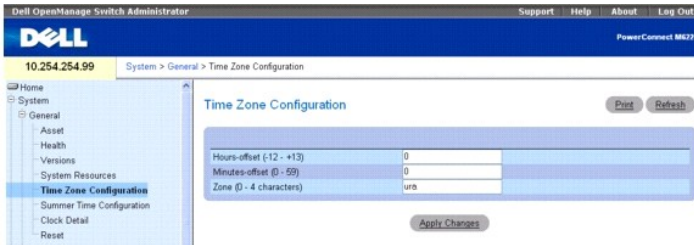
- 1 시스템 관리 명령

표준 시간대 구성

Time Zone Configuration(표준 시간대 구성)을 사용하여 UTC(Coordinated Universal Time)와의 표준 시간대 차이를 구성할 수 있습니다.

Time Zone Configuration(표준 시간대 구성) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **표준 시간대 구성**을 클릭합니다.

그림 6-5. Time Zone Configuration(표준 시간대 구성)



Time Zone Configuration(표준 시간대 구성) 페이지에는 다음 필드가 있습니다.

Hours-offset(시간 오프셋) — UTC와의 시간 차이를 설정합니다. (범위: -12 ~ +13)

Minutes-offset(분간 오프셋) — UTC와의 분간 차이를 설정합니다. (범위: 0-59)

Zone(구역) — 표준 시간대의 약어를 설정합니다. (범위: 0-4자)

표준 시간대 매개변수 정의

1. **Time Zone Configuration(표준 시간대 구성)** 페이지를 엽니다.
2. 필요에 따라 필드를 정의합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

표준 시간대 설정이 수정되고 장치가 업데이트됩니다.

CLI를 사용하여 표준 시간대 설정 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

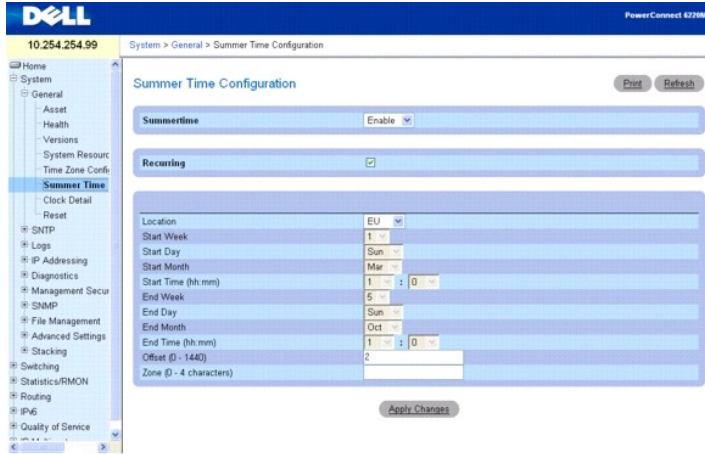
- 1 클럭 명령

서머 타임 구성

Summer Time Configuration(서머 타임 구성) 페이지를 사용하여 정의된 서머 타임 기간 및 오프셋을 지정할 수 있습니다.

Summer Time Configuration(서머 타임 구성) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **Summer Time Configuration(서머 타임 구성)**을 클릭합니다.

그림 6-6. Summer Time Configuration(서머 타임 구성)



Summer Time Configuration(서머 타임 구성) 페이지의 필드는 Recurring(반복) 확인란을 선택하거나 선택 해제하면 변경됩니다. Summer Time Configuration(서머 타임 구성) 페이지에는 다음 필드가 있습니다.

Recurring(반복) — 해당 구성이 매년 반복되도록 하려면 확인란을 선택합니다.

Location(위치) — 이 필드는 Recurring(반복) 확인란을 선택한 경우에만 표시됩니다. US(United States) 및 EU(European Union)에 대한 서머 타임 구성은 미리 정의됩니다. USA 또는 EU 이외의 위치에 대해 서머 타임을 설정하려면 None(없음)을 선택하십시오.

Start Week(시작 주) — 시작하는 주의 번호를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택한 경우에만 표시됩니다.

Start Day(시작 요일) — 시작하는 요일의 번호를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택한 경우에만 표시됩니다.

Start Month(시작 달) — 시작하는 달의 번호를 선택합니다.

Start Time(시작 시간) — hh:mm 형식의 시작하는 시간을 선택합니다.

Start Date(시작 날짜) — 시작하는 날짜를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택 해제한 경우에만 표시됩니다.

Start Year(시작 연도) — 시작하는 연도를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택 해제한 경우에만 표시됩니다.

End Week(끝 주) — 끝나는 주의 번호를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택한 경우에만 표시됩니다.

End Day(끝 요일) — 끝나는 요일의 번호를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택한 경우에만 표시됩니다.

End Month(끝 달) — 끝나는 달을 선택합니다.

End Time(끝 시간) — hh:mm 형식의 끝나는 시간을 선택합니다.

End Date(끝 날짜) — 끝나는 날짜를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택 해제한 경우에만 표시됩니다.

End Year(끝 연도) — 끝나는 연도를 선택합니다. 이 필드는 Recurring(반복) 확인란을 선택 해제한 경우에만 표시됩니다.

Offset(오프셋) — 서머 타임 기간 동안 추가할 분 수를 0 ~ 1440 범위에서 설정합니다.

Zone(구역) — 서머 타임이 시작할 때 표시될 표준 시간대의 약어를 설정합니다.

서머 타임 매개변수 정의

1. Summer Time Configuration(서머 타임 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 정의합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

서머 타임 설정이 수정되고 장치가 업데이트됩니다.

CLI를 사용하여 서머 타임 매개변수 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

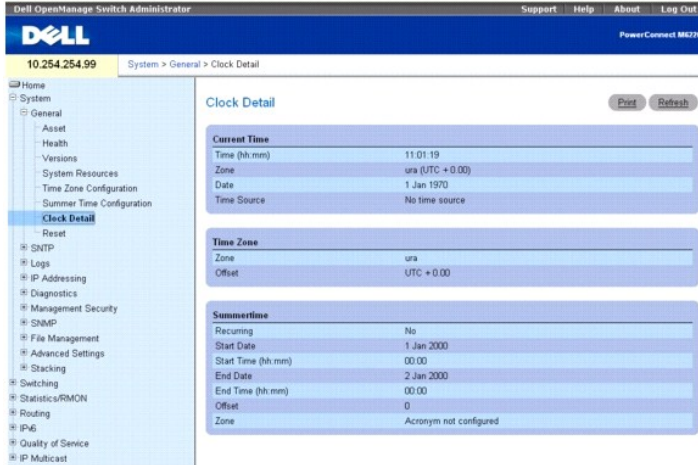
1. 클럭 명령

클럭 세부 사항

Clock Detail(클럭 세부 사항) 페이지를 사용하여 현재 시간, 표준 시간대 및 서머 타임 설정을 확인할 수 있습니다.

Clock Detail(클럭 세부 사항) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **Clock Detail(클럭 세부 사항)**을 클릭합니다.

그림 6-7. Clock Detail(클럭 세부 사항)



Clock Detail(클럭 세부 사항) 페이지에는 다음과 같은 클럭 기능에 대한 정보가 제공됩니다.

Current Time(현재 시간) — 여기에는 현재 시간이 표시됩니다.

Time Zone(표준 시간대) — 여기에는 표준 시간대 설정이 표시됩니다.

Summertime(서머 타임) — 여기에는 서머 타임 설정이 표시됩니다.

CLI를 사용하여 클럭 세부 사항 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

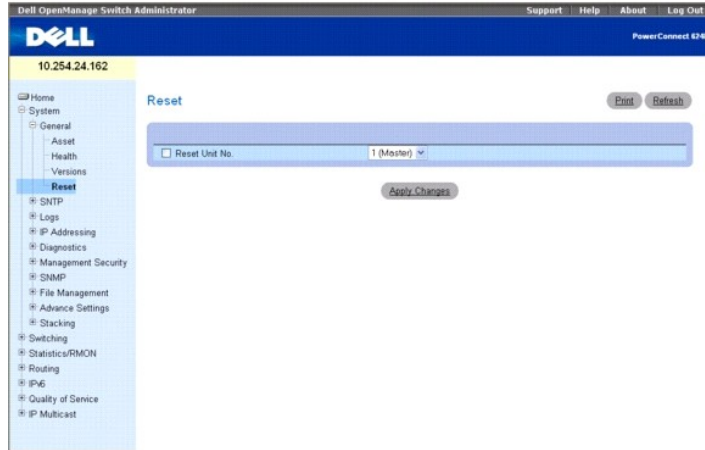
- 1 클럭 명령

재설정

Reset(재설정) 페이지를 사용하여 장치를 재설정할 수 있습니다.

Reset(재설정) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **General(일반)** → **Reset(재설정)**을 클릭합니다.

그림 6-8. Reset(재설정)



Reset(재설정) 페이지에는 다음 필드가 있습니다.

Reset Unit No.(장치 번호 재설정) — 스크린 내에서 재설정해야 하는 장치를 선택하는 데 사용됩니다.

장치 재설정

1. **Reset(재설정)** 페이지를 엽니다.
2. **Reset Unit No.(장치 번호 재설정)**를 클릭합니다.
3. **Individual Unit(개별 단위)** 또는 **All(전체)**를 선택합니다.
4. **Apply Changes(변경사항 적용)** 단추를 클릭합니다.
5. 확인 메시지가 표시되면 **확인**을 클릭합니다.
선택한 장치가 재설정됩니다. 장치가 재설정된 후 사용자 이름과 암호를 입력합니다.

SNTP 설정 구성

장치는 SNTP(Simple Network Time Protocol)를 지원합니다. SNTP는 밀리초 단위까지 정확한 네트워크 장치 클럭 시간 동기화를 보장합니다. 시간 동기화는 네트워크 SNTP 서버에서 수행됩니다. 장치는 SNTP 클라이언트로서만 작동하며 다른 시스템에 시간 서비스를 제공할 수 없습니다.

시간 소스는 계층에 의해 설정됩니다. 계층은 참조 클럭의 정확도를 정의합니다. 계층이 높을수록(0이 가장 높음) 클럭이 더 정확합니다. 장치는 계층 2 장치이므로 계층 1 이상에서 시간을 받습니다.

다음은 계층의 예입니다.

- 1 **Stratum 0(계층 0)** — 실제 시간 클럭이 시간 소스로 사용됩니다(예: GPS 시스템).
- 1 **Stratum 1(계층 1)** — Stratum 0(계층 0) 시간 소스에 직접 연결된 서버가 사용됩니다. Stratum 1(계층 1) 시간 서버는 기본 네트워크 시간 표준을 제공합니다.
- 1 **Stratum 2(계층 2)** — 시간 소스가 네트워크 경로에서 Stratum 1(계층 1) 서버로부터 떨어져 있습니다. 예를 들어 Stratum 2(계층 2) 서버는 네트워크 연결에서 NTP를 통해 Stratum 1(계층 1) 서버로부터 시간을 받습니다.

SNTP 서버로부터 받은 정보는 시간 레벨 및 서버 유형을 기준으로 평가됩니다.

SNTP 시간 정의는 다음 시간 레벨에 의해 평가 및 결정됩니다.

- 1 **T1** — 클라이언트가 원래 요청을 보낸 시간입니다.
- 1 **T2** — 서버가 원래 요청을 받은 시간입니다.
- 1 **T3** — 서버가 응답을 보낸 시간입니다.
- 1 **T4** — 클라이언트가 서버의 응답을 받은 시간입니다.

장치는 유니캐스트 및 브로드캐스트 서버 유형에서 서버 시간을 풀링할 수 있습니다.

유니캐스트 정보 풀링은 IP 주소가 알려진 서버를 풀링하는 데 사용됩니다. 장치에 구성된 SNTP 서버에서만 동기화 정보가 풀링됩니다. T1 - T4를 사용하여 서버 시간을 결정합니다. 가장 안전한 방법입니다. 이 방법으로 장치 시간을 동기화하는 것이 좋습니다. 이 방법을 선택하면 **SNTP Servers(SNTP 서버)** 페이지를 사용하여 장치에 정의된 SNTP 서버에서만 SNTP 정보를 받아들입니다.

브로드캐스트 정보는 서버 IP 주소를 알 수 없을 때 사용됩니다. SNMP 서버에서 브로드캐스트 메시지를 보내면 SNMP 클라이언트가 이 메시지를 수신합니다. 브로드캐스트 폴링을 활성화하면 장치에서 요청하지 않은 경우에도 모든 동기화 정보를 받아들입니다. 이는 가장 안전하지 않은 방법입니다.

장치는 능동적으로 정보를 요청하거나 각 폴링 간격마다 동기화 정보를 검색합니다. 유니캐스트 및 브로드캐스트 폴링을 활성화하면 다음 순서에 따라 정보가 검색됩니다.

- 1 장치에 정의된 서버의 정보가 우선합니다. 유니캐스트 폴링을 활성화하거나 장치에 정의된 서버가 없으면 장치는 응답하는 모든 SNMP 서버의 시간 정보를 받아들입니다.
- 1 여러 유니캐스트 장치가 응답할 경우 가장 계층이 낮은 장치의 동기화 정보가 우선합니다.
- 1 서버의 계층이 같으면 먼저 응답한 SNMP 서버의 동기화 정보를 받아들입니다.

MD5(Message Digest 5) 인 증은 SNMP 서버에 대한 장치 동기화 경로를 보호합니다. MD5는 128비트 해시를 생성하는 알고리즘입니다. MD5는 MD4의 변형으로, MD4 보안을 향상시킵니다. MD5는 통신의 무결성을 확인하고 통신의 출처를 인증합니다.

SNMP 메뉴 페이지에는 SNMP 매개변수를 구성할 수 있는 페이지에 대한 링크가 있습니다.

SNMP 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→SNMP**를 클릭합니다.

이 페이지를 사용하여 다음 기능으로 이동합니다.

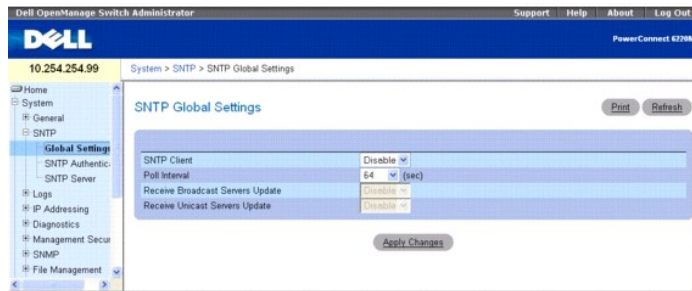
- 1 [SNMP 전역 설정](#)
- 1 [SNMP 인증](#)
- 1 [SNMP 서버](#)

SNMP 전역 설정

SNMP Global Settings(SNMP 전역 설정) 페이지를 사용하여 SNMP 매개변수를 보고 조정할 수 있습니다.

SNMP Global Settings(SNMP 전역 설정) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→SNMP→Global Settings(전역 설정)**를 클릭합니다.

그림 6-9. SNMP Global Settings(SNMP 전역 설정)



SNMP Global Settings(SNMP 전역 설정) 페이지에는 다음 필드가 있습니다.

SNMP Client(SNMP 클라이언트) — 드롭다운 목록을 사용하여 클라이언트를 활성화하거나 비활성화합니다. 클라이언트가 비활성화되면 아래의 일부 필드 역시 비활성화됩니다.

Poll Interval(폴링 간격) — SNMP 서버에서 유니캐스트 정보를 폴링하는 간격(초)을 정의합니다. 범위는 60~1024초입니다.

Receive Broadcast Servers Update(브로드캐스트 서버 업데이트 수신) — 활성화하면 선택한 인터페이스에서 SNMP 서버의 브로드캐스트 서버 시간 정보를 수신합니다. 동기화를 요청하지 않은 경우에도 SNMP 패킷을 받을 때마다 장치가 동기화됩니다.

Receive Unicast Servers Update(유니캐스트 서버 업데이트 수신) — 활성화하면 장치에 정의된 SNMP 서버에서 유니캐스트 서버 시간 정보를 폴링합니다.

SNMP 전역 매개변수 정의

1. SNMP Global Settings(SNMP 전역 설정) 페이지를 엽니다.
2. 필요에 따라 필드를 정의합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

SNMP 전역 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 전역 매개변수 정의

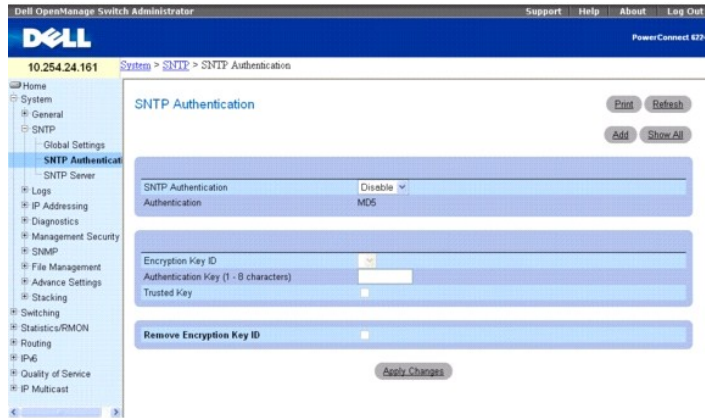
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

SNTP 인증

SNTP Authentication(SNTP 인증) 페이지를 사용하여 장치와 SNTP 서버 간의 SNTP 인증을 활성화하고 원하는 SNTP 서버를 선택할 수 있습니다. SNTP Authentication(SNTP 인증) 페이지에서 SNTP 인증을 활성화하거나 비활성화하고, 선택한 암호화 키 ID에 대한 인증 키를 수정하며, 선택한 인증 키를 신뢰할 수 있는 키로 지정하고, 선택한 암호화 키 ID를 제거할 수 있습니다.

SNTP Authentication(SNTP 인증) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→SNTP→Authentication(인증)을 클릭합니다.

그림 6-10. SNTP Authentication(SNTP 인증)



SNTP Authentication(SNTP 인증) 페이지에는 다음 필드가 있습니다.

SNTP Authentication(SNTP 인증) — 활성화하면 장치와 SNTP 서버 간의 SNTP 세션을 인증해야 합니다.

Authentication(인증) — 인증 유형입니다. 시스템은 MD5만 지원합니다.

Encryption Key ID(암호화 키 ID) — SNTP 서버 및 장치 인증에 사용되는 사용자 정의 키 ID 목록을 포함합니다. 가능한 필드 값은 다음과 같습니다. 1-4294767295

Authentication Key (1-8Characters)(인증 키(1-8자)) — 인증에 사용되는 키를 표시합니다.

Trusted Key(신뢰할 수 있는 키) — 사용할 암호화 키를 지정하려면 선택하고(유니캐스트) SNTP 서버를 인증하려면 선택 표시를 지웁니다(브로드캐스트).

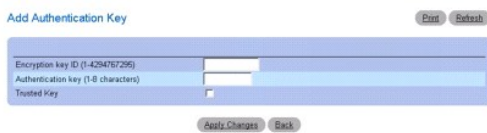
Remove Encryption Key ID(암호화 키 ID 제거) — 선택한 암호화 키를 제거하려면 선택합니다.

SNTP 인증 키 추가

1. SNTP Authentication(SNTP 인증) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add Authentication Key(인증 키 추가) 페이지가 표시됩니다.

그림 6-11. Add Authentication Key(인증 키 추가)



3. 필요에 따라 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

SNTP 인증 키가 추가되고 장치가 업데이트됩니다.

인증 키 표 표시

1. SNMP Authentication(SNTP 인증) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Authentication Key Table(인증 키 표) 페이지가 표시됩니다.

그림 6-12. Authentication Key Table(인증 키 표)

Encryption Key ID	Authentication Key	Trusted Key	Remove
4545	vsgjw	Yes	<input type="checkbox"/>

인증 키 제거

1. SNMP Authentication(SNTP 인증) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
3. Remove(제거) 확인란을 선택하여 Authentication Key Table(인증 키 표) 항목을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNTP 인증 설정 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

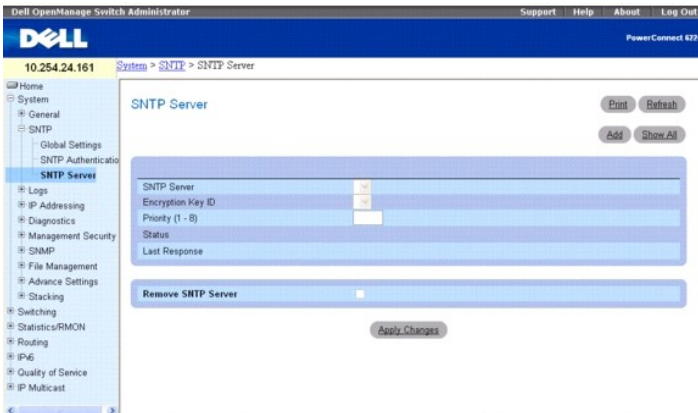
1. 클릭 명령

SNTP 서버

SNTP Server(SNTP 서버) 페이지를 사용하여 SNTP 서버 활성화에 대한 정보를 보고 수정하거나 새 SNTP 서버를 추가할 수 있습니다.

SNTP Server(SNTP 서버) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → SNTP → SNTP Server(SNTP 서버)를 클릭합니다.

그림 6-13. SNTP Servers(SNTP 서버)



SNTP Servers(SNTP 서버) 페이지에는 다음 필드가 있습니다.

SNTP Server(SNTP 서버) — 드롭다운 메뉴에서 사용자 정의 SNTP 서버 IP 주소를 선택합니다. Add(추가) 단추를 사용하여 최대 8개의 SNTP 서버를 정의할 수 있습니다.

Encryption Key ID(암호화 키 ID) — SNMP 서버와 장치 간의 통신에 사용되는 사용자 정의 키 ID를 지정합니다. Encryption Key ID(암호화 키 ID)는 **SNTP Authentication (SNTP 인증)** 페이지에서 정의됩니다.

Priority (1-8)(우선 순위(1-8)) — SNMP 요청이 전송되는 서버의 시퀀스를 결정할 때 사용되는 이 서버 항목의 우선 순위를 지정합니다. 값은 1 ~ 8이고, 기본값은 1입니다. 가장 숫자가 낮은 서버가 우선합니다.

Status(상태) — 작동하는 SNMP 서버 상태를 표시합니다. 가능한 필드 값은 다음과 같습니다.

Up(작동) — SNMP 서버가 현재 정상적으로 작동합니다.

Down(다운) — 현재 SNMP 서버를 사용할 수 없음을 나타냅니다. 예를 들어 SNMP 서버가 현재 연결되어 있지 않거나 현재 다운되었습니다.

In progress(진행 중) — SNMP 서버가 현재 SNMP 정보를 보내거나 받고 있습니다.

Unknown(알 수 없음) — 현재 전송 중인 SNMP 정보의 진행 상황을 알 수 없습니다. 예를 들어 장치가 현재 인터페이스를 찾고 있습니다.

Last Response(마지막 응답) — 마지막으로 SNMP 서버로부터 응답을 받은 시간을 표시합니다.

Remove SNMP Server(SNTP 서버 제거) — 선택하면 지정한 SNMP 서버를 **SNTP Servers(SNTP 서버)** 목록에서 제거합니다.

SNTP 서버 추가

1. **SNTP Servers(SNTP 서버)** 페이지를 엽니다.

2. **Add(추가)**를 클릭합니다.

Add SNMP Server(SNTP 서버 추가) 페이지가 표시됩니다.

그림 6-14. Add SNMP Server(SNTP 서버 추가)



3. 필요에 따라 필드를 정의합니다.

4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

SNTP 서버가 추가되고 장치가 업데이트됩니다.

SNTP 서버 표 표시

1. **SNTP Servers(SNTP 서버)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

SNTP Servers Table(SNTP 서버 표) 페이지가 표시됩니다.

그림 6-15. SNMP Servers Table(SNTP 서버 표)



SNTP Server	Encryption Key ID	Priority	Status	Last Response	Remove
1 10.240.1.10	None	1	Up	Thu 1 Jan 1970 00:00:00	<input type="checkbox"/> Edit

SNTP 서버 수정

1. **SNTP Servers(SNTP 서버)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

SNTP Servers Table(SNTP 서버 표)이 열립니다.

3. 수정할 **SNTP Server(SNTP 서버)** 항목 옆에 있는 **Edit(편집)**를 클릭합니다.

4. 관련 필드를 수정합니다.

5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

SNTP 서버 정보가 업데이트됩니다.

SNTP 서버 제거

1. **SNTP Servers(SNTP 서버)** 페이지를 엽니다.

2. **Show All(모두 표시)**을 클릭합니다.

SNTP Servers Table(SNTP 서버 표)이 열립니다.

3. **SNTP Server(SNTP 서버)** 항목을 선택합니다.

4. **Remove(제거)** 확인란을 선택합니다.

5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNTP 서버 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. 클릭 명령

로그 관리

스위치는 구성 또는 다른 발생의 변경사항은 물론 플랫폼에서 발생하는 이벤트, 장애 또는 오류에 응답하여 메시지를 생성할 수 있습니다. 이러한 메시지는 플랫폼에 로컬로 저장되고 모니터링 및 장기 보관 목적으로 하나 이상의 중앙 수집 지점으로 전달됩니다. 로깅 기능의 로컬 및 원격 구성에는 심각도에 따라 기록 또는 전달되는 메시지 필터링과 구성 요소 생성이 포함됩니다.

메모리 내 로그는 메시지 구성 요소 및 심각도에 대한 설정을 기준으로 메모리에 메시지를 저장합니다. 스택형 시스템에서 이 로그는 스택 플랫폼의 최상위에만 존재합니다. 스택 내의 다른 플랫폼은 해당 메시지를 스택 로그의 최상위로 전달합니다. 스택 플랫폼의 최상위에 없는 메모리 내 로그에는 액세스할 수 없습니다.

영구 로그는 영구 저장소에 저장됩니다. 두 가지 유형의 영구 로그를 구성할 수 있습니다.

1. 첫 번째 로그 유형은 **시스템 시작 로그**입니다. 시스템 시작 로그는 시스템 재부팅 이후에 받은 처음 N개 메시지를 저장합니다. 이 로그는 항상 로그 캡처 작업 속성이 켜져 있을 때 중지하도록 설정되어 있으며 최대 32개의 메시지를 저장할 수 있습니다.
1. 두 번째 로그 유형은 **시스템 작동 로그**입니다. 시스템 작동 로그는 시스템 작동 중에 받은 마지막 N개 메시지를 저장합니다. 이 로그는 항상 로그 캡처 속성이 덮어쓰도록 설정되어 있으며 최대 1000개의 메시지를 저장할 수 있습니다.

로그 서브시스템에서 받은, 저장 기준에 맞는 메시지가 시스템 시작 로그 또는 시스템 작동 로그 중 하나에 저장되며 둘 다에 저장되지는 않습니다. 즉, 시스템을 시작할 때 시작 로그가 구성되어 있으면 한도까지 시작 로그에 메시지가 저장됩니다. 그런 다음 작동 로그가 구성되어 있으면 작동 로그에 메시지가 저장되기 시작합니다.

시스템은 최대 세 가지 버전의 영구 로그, 즉 <FILE>0.txt, <FILE>1.txt 및 <FILE>2.txt를 유지합니다. 시스템을 시작할 때 <FILE>2.txt는 제거되고 <FILE>1.txt는 <FILE>2.txt로, <FILE>0.txt는 <FILE>1.txt로 이름이 변경되며 <FILE>0.txt가 생성되어 <FILE>0.txt에 로깅이 시작됩니다. 작동 로그의 경우 위의 예에서 <FILE>을 olog로 바꾸고 시작 로그의 경우 slog로 바꿉니다.

로컬 영구 로그는 CLI, 로컬 직렬 케이블의 xmodem 및 TFTP를 통해 검색할 수 있습니다.

Logs(로그) 메뉴 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→Logs(로그)**를 클릭합니다. 이 페이지를 사용하여 다음 기능으로 이동합니다.

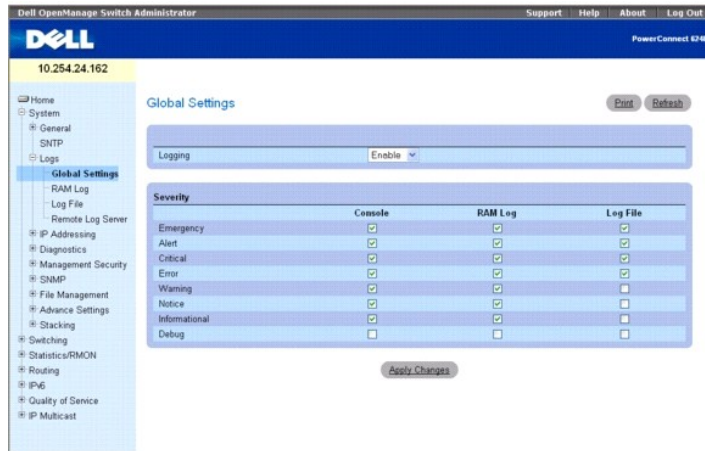
1. [전역 설정](#)
1. [RAM 로그 표](#)
1. [로그 파일](#)
1. [원격 로그 서버 설정](#)

전역 설정

Global Setting(전역 설정) 페이지를 사용하여 로그를 전체적으로 활성화하고 로그 매개변수를 정의할 수 있습니다. Severity(심각도) 로그 메시지는 가장 심각도가 높은 항목에서 낮은 항목순으로 나열됩니다.

Global Settings(전역 설정) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Logs(로그)→ Global Settings(전역 설정)를 클릭합니다.

그림 6-16. Global Settings(전역 설정)



Global Settings(전역 설정) 페이지에는 다음 필드가 있습니다.

Logging(로깅) — 캐시, 파일 및 서버 로그에 대한 장치 전역 로그를 활성화합니다. 콘솔에 인쇄된 모든 로그가 로그 파일에 저장됩니다. 가능한 필드 값은 다음과 같습니다.

Enable(활성) — 캐시(RAM), 파일(FLASH) 및 외부 서버에 로그를 저장합니다.

Disable(비활성) — 로그를 저장하지 않습니다. 콘솔에 인쇄된 로그의 로깅은 비활성화할 수 없습니다.

심각도

이 항목의 확인란을 사용하여 콘솔, 영구 메모리 및 로그 파일의 중요도를 조정할 수 있습니다.

특정 레벨을 선택하면 해당 레벨보다 높은 모든 레벨이 자동으로 선택됩니다. 예를 들어 Error(오류)를 선택하면 Error(오류), Critical(치명적), Alert(경보) 및 Emergency(긴급)가 자동으로 선택됩니다. Error(오류) 선택을 해제하면 모든 하위 레벨(예: Error(오류), Warning(경고), Notice(알림), Informational(정보), Debug(디버그))이 선택 해제됩니다.

Emergency(긴급) — 가장 높은 경고 레벨입니다. 장치가 다운되었거나 제대로 작동하지 않으면 긴급 로그가 장치에 저장됩니다.

Alert(경보) — 두 번째로 가장 높은 경고 레벨입니다. 모든 장치 기능이 다운된 경우 등 심각한 장치 오작동이 발생하면 경보 로그가 저장됩니다.

Critical(치명적) — 세 번째로 가장 높은 경고 레벨입니다. 두 개의 장치 포트가 작동하지 않고 나머지 장치 포트는 작동하는 경우 등 치명적인 장치 오동작이 발생하면 치명적 로그가 저장됩니다.

Error(오류) — 포트가 오프라인 상태인 경우 등 장치 오류가 발생했습니다.

Warning(경고) — 가장 낮은 장치 경고 레벨입니다.

Notice(알림) — 네트워크 관리자에게 장치 정보를 제공합니다.

Informational(정보) — 장치 정보를 제공합니다.

Debug(디버그) — 로그에 대한 자세한 정보를 제공합니다. 디버깅은 공인된 서비스 직원만 입력해야 합니다.

확인란은 다음 세 개의 열에 표시됩니다.

Console(콘솔) — 로그가 콘솔로 전송됩니다.

RAM Logs(RAM 로그) — 로그가 (캐시) RAM으로 전송됩니다.

Log File(로그 파일) — 로그가 파일(FLASH)로 전송됩니다.

로그 활성화

1. Global Settings(전역 설정) 페이지를 엽니다.
2. Logging(로깅) 드롭다운 메뉴에서 Enable(활성)을 선택합니다.

3. 확인란을 사용하여 로그 유형과 심각도를 선택합니다.

주: 심각도 레벨을 선택하면 해당 레벨보다 높은 모든 심각도 레벨이 자동으로 선택됩니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

로그 설정이 저장되고 장치가 업데이트됩니다.

CLI를 사용하여 전역 로그 활성화

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

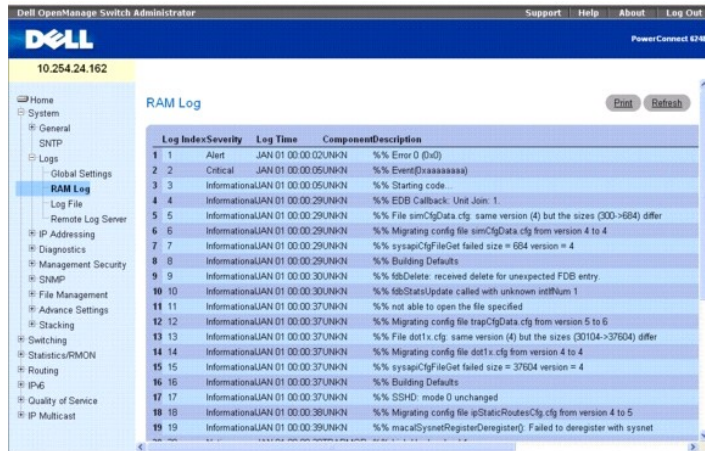
- 1 Syslog 명령

RAM 로그 표

RAM Log Table(RAM 로그 표) 페이지를 사용하여 로그가 입력된 시간, 로그 심각도, 로그 설명 등 특정 RAM(캐시) 로그 항목에 대한 정보를 볼 수 있습니다.

RAM Log Table(RAM 로그 표)을 표시하려면 디렉터리 화면에서 **System(시스템)**→ **Logs(로그)**→ **RAM Log(RAM 로그)**를 클릭합니다.

그림 6-17. RAM Log Table(RAM 로그 표)



RAM Log Table(RAM 로그 표) 페이지에는 다음 필드가 있습니다.

Log Index(로그 색인) — RAM Log Table(RAM 로그 표) 내의 로그 번호를 나타냅니다.

Severity(심각도) — 로그 심각도입니다.

Log Time(로그 시간) — 로그가 RAM Log Table(RAM 로그 표)에 입력된 시간입니다.

Component(구성 요소) — 기록되는 구성 요소입니다.

Description(설명) — 로그 설명입니다.

로그 정보 제거

1. **RAM Log Table(RAM 로그 표)** 페이지를 엽니다.

2. **Clear Log(로그 지우기)**를 클릭합니다.

로그 정보가 로그 파일 표에서 제거되고 장치가 업데이트됩니다.

CLI를 사용하여 로그 정보 제거

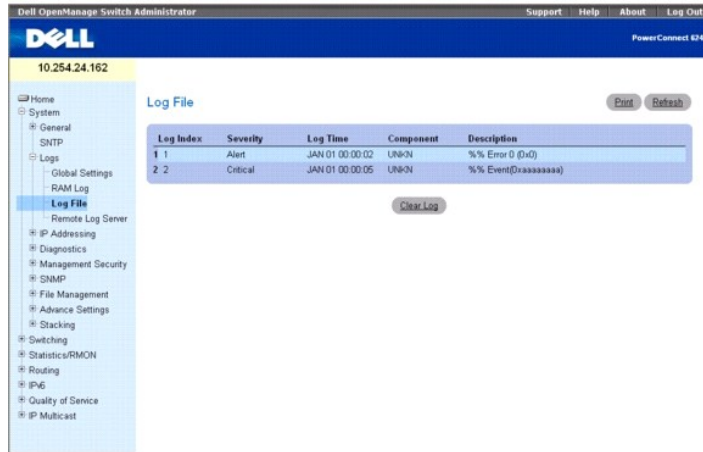
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

로그 파일

Log File(로그 파일)에는 로그가 입력된 시간, 로그 심각도, 로그 설명 등 특정 로그 항목에 대한 정보가 있습니다.

Log File(로그 파일)을 표시하려면 디렉터리 화면에서 System(시스템)→ Logs(로그)→ Log File(로그 파일)을 클릭합니다.

그림 6-18. Log File(로그 파일)



Log File Table(로그 파일 표) 페이지에는 다음 필드가 있습니다.

- 1 Log Index(로그 색인) — Log File Table(로그 파일 표) 내의 로그 번호입니다.
- 1 Severity(심각도) — 로그 심각도입니다.
- 1 Log Time(로그 시간) — 로그가 Log File Table(로그 파일 표)에 입력된 시간입니다.
- 1 Component(구성 요소) — 기록되는 구성 요소입니다.
- 1 Description(설명) — 로그 설명입니다.

로그 정보 제거

1. Log File Table(로그 파일 표) 페이지를 엽니다.
2. Clear Log(로그 지우기)를 클릭합니다.

로그 정보가 로그 파일 표에서 제거되고 장치가 업데이트됩니다.

CLI를 사용하여 로그 정보 제거

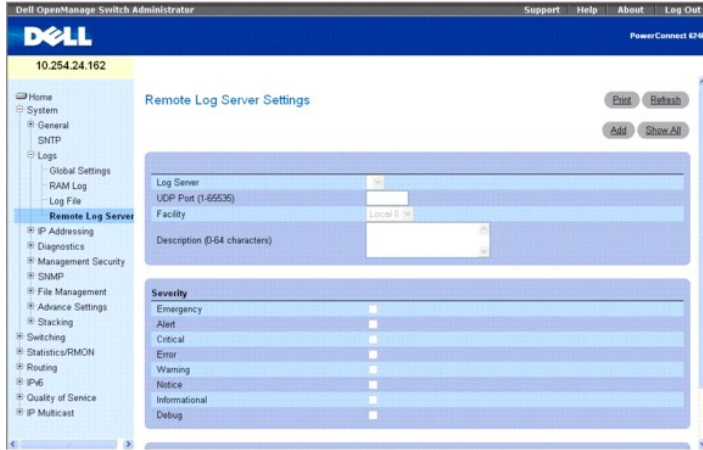
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

원격 로그 서버 설정

Remote Log Server Settings(원격 로그 서버 설정) 페이지를 사용하여 사용 가능한 로그 서버를 보고 새 로그 서버를 정의하며 서버로 전송되는 로그 이벤트의 심각도를 설정할 수 있습니다.

Remote Log Server Settings(원격 로그 서버 설정) 페이지를 표시하려면 System(시스템)→ Logs(로그)→ Remote Log Server(원격 로그 서버)를 클릭합니다.

그림 6-19. Remote Log Server Settings(원격 로그 서버 설정)



Remote Log Server Settings(원격 로그 서버 설정) 페이지에는 다음 필드가 있습니다.

Log Server(로그 서버) — 로그가 전송될 수 있는 서버입니다.

UDP Port (1-65535)(UDP 포트(1-65535)) — 로그가 전송되는 소스 UDP 포트를 설정합니다. 기본값은 514입니다.

Facility(설비) — 시스템 로그가 원격 서버로 전송되는 사용자 정의 소스 응용프로그램입니다. 단일 서버에 하나의 설비만 지정할 수 있습니다. 두 번째 설비 레벨을 지정하면 첫 번째 설비 레벨을 덮어씁니다. 장치에 대해 정의된 모든 응용프로그램은 서버의 같은 설비를 사용합니다. 가능한 필드 값은 **Local 0(로컬 0)** ~ **Local 7(로컬 7)**입니다.

Description(설명) — 서버 설명을 설정합니다. 최대 길이는 64자입니다.


Severity(심각도) — 로그 심각도를 선택합니다. 심각도 레벨을 선택하면 해당 레벨보다 높은 모든 심각도 레벨이 자동으로 선택됩니다.

Remove Log Server(로그 서버 제거) — Log Server(로그 서버) 목록에서 서버를 제거합니다. 확인란을 선택하면 서버가 목록에서 제거됩니다. 확인란 선택 표시를 지우면 서버가 목록에 그대로 있습니다.

또한 Remote Log Server Settings(원격 로그 서버 설정) 페이지에는 심각도 목록이 있습니다. 심각도 정의는 RAM Log Table(RAM 로그 표) 페이지의 심각도 정의와 같습니다.

로그를 서버로 보내기

1. Remote Log Server Settings(원격 로그 서버 설정) 페이지를 엽니다.
2. UDP Port(UDP 포트), Facility(설비) 및 Description(설명) 필드를 정의합니다.
3. Log Parameters(로그 매개변수) 확인란을 사용하여 로그 유형과 로그 심각도를 선택합니다.

 **주:** 심각도 레벨을 선택하면 해당 레벨보다 높은 모든 심각도 레벨이 자동으로 선택됩니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

로그 설정이 저장되고 장치가 업데이트됩니다.

새 서버 추가

1. Remote Log Server Settings(원격 로그 서버 설정) 페이지를 엽니다.
2. Add(추가)를 클릭하여 Add Remote Log Server(원격 로그 서버 추가) 페이지를 표시합니다.


 **주:** 새 서버를 추가하기 전에 원격 로그 서버의 IP 주소를 확인하십시오.

그림 6-20. Add Remote Log Server Settings(원격 로그 서버 설정 추가)

Add Remote Log Server Print Refresh

Log Server	<input type="text"/>
UDP Port (1-65535)	514
Facility	Local 7
Description (64 characters)	<input type="text"/>

Severity	
Emergency	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>
Notice	<input checked="" type="checkbox"/>
Informational	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>

Apply Changes Back

3. 대화상자의 필드를 입력하고 **Apply Changes(변경사항 적용)**를 클릭합니다.

Remote Log Server Settings(원격 로그 서버 설정) 페이지로 돌아가야만 Remote Log Server Settings(원격 로그 서버 설정) 페이지의 Available Server(사용 가능한 서버) 목록에 서버가 표시됩니다.

로그 서버 보기/제거

1. Remote Log Server Settings(원격 로그 서버 설정) 페이지를 엽니다.
2. Show All(모두 표시)를 클릭하여 Remote Log Servers Table(원격 로그 서버 표) 페이지를 표시합니다.

그림 6-21. Show All Log Servers(로그 서버 모두 표시)

Remote Log Servers Table Print Refresh

Log Server	UDP Port	Facility	Description	Minimum Severity	Remove
1 10.240.10.1	23	Local 7		Informational	<input type="checkbox"/> Edit

Apply Changes Back

3. 서버를 제거하려면 해당 **Remove(제거)** 확인란을 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

서버가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 원격 서버 로그 작업

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 Syslog 명령

IP 주소 지정 정의

IP Addressing(IP 주소 지정) 페이지를 사용하여 관리 인터페이스와 기본 게이트웨이 IP 주소를 지정하고, 도메인 이름 시스템과 교섭하며, 기본 도메인 이름을 설정하고, 호스트 이름 할당을 수행하며, 인터페이스에 대한 ARP 및 DHCP 매개변수를 정의할 수 있습니다.

IP Addressing(IP 주소 지정) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **IP Addressing(IP 주소 지정)**을 클릭합니다. 이 페이지를 사용하여 다음 기능으로 이동합니다.

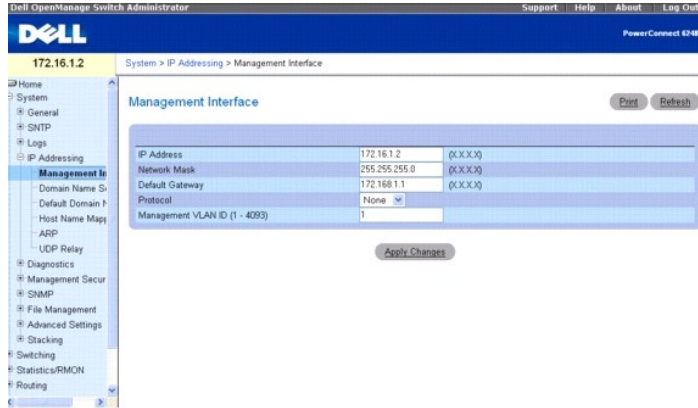
- 1 [관리 인터페이스](#)
- 1 [도메인 이름 서버\(DNS\)](#)
- 1 [기본 도메인 이름](#)
- 1 [호스트 이름 할당](#)
- 1 [ARP 표](#)
- 1 UDP 릴레이

관리 인터페이스

Management Interface(관리 인터페이스) 메뉴 페이지를 사용하여 관리 인터페이스 IP 주소, 서브넷 마스크, 기본 게이트웨이 IP 주소를 지정하고 부팅 프로토콜을 활성화하거나 비활성화할 수 있습니다.

Management Interface(관리 인터페이스) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → IP Addressing(IP 주소 지정) → Management Interface(관리 인터페이스)를 클릭합니다.

그림 6-22. Management Interface(관리 인터페이스)



Management Interface(관리 인터페이스) 페이지에는 다음 필드가 있습니다.

IP Address(IP 주소) — 관리 인터페이스 IP 주소를 표시합니다.

Network Mask(네트워크 마스크) — 소스 IP 주소의 서브넷 마스크입니다.

주: IP 주소의 각 부분은 0이 아닌 숫자로 시작해야 합니다. 예를 들어 IP 주소 001.100.192.6과 192.001.10.3은 유효하지 않습니다.

Default Gateway(기본 게이트웨이) — 기본 게이트웨이 IP 주소를 설정합니다.

Protocol — 드롭다운 메뉴를 사용하여 Bootp, DHCP 또는 None(없음)을 선택합니다.

Management VLAN ID (1-4093)(관리 VLAN ID(1-4093)) — 1-4093 범위에서 Management VLAN ID(관리 VLAN ID)를 설정합니다.

주의사항: Management VLAN(관리 VLAN ID)을 변경하면 웹 세션 연결이 끊어집니다.

관리 인터페이스 IP 주소 매개변수 수정

1. Management Interface(관리 인터페이스) 페이지를 엽니다.
2. IP Address(IP 주소) 필드의 IP 주소를 수정합니다.
3. 필요에 따라 다른 필드를 수정합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

매개변수가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IP 인터페이스 매개변수 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. IP 라우팅 명령

도메인 이름 서버(DNS)

도메인 이름 시스템은 사용자 정의 도메인 이름을 IP 주소로 변환합니다. 도메인 이름을 지정할 때마다 이 서비스는 해당 이름을 숫자 IP 주소로 변환합니다. 예를 들어 **www.ipexample.com**은 192.87.56.2로 변환됩니다. 도메인 이름 시스템 서버는 도메인 이름 데이터베이스와 해당 IP 주소를 유지 관리합니다.

Domain Name Server (DNS)(도메인 이름 서버(DNS)) 페이지를 사용하여 특정 DNS 서버를 활성화할 수 있습니다.

Domain Name Server(도메인 이름 서버) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ IP Addressing(IP 주소 지정)→ Domain Name Server(도메인 이름 서버)를 클릭합니다.

그림 6-23. Domain Name Server(도메인 이름 서버)



Domain Name Server (DNS)(도메인 이름 서버(DNS)) 페이지에는 다음 필드가 있습니다.

DNS Status(DNS 상태) — DNS 이름을 IP 주소로 변환하거나 변환하지 않습니다.

DNS Server(DNS 서버) — DNS 서버 목록을 포함합니다. DNS 서버는 Add DNS Server(DNS 서버 추가) 페이지에서 추가됩니다.

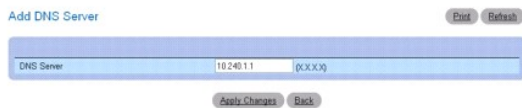
Remove(제거) — 선택하면 선택한 DNS 서버를 제거합니다.

DNS 서버 추가

1. Domain Name Server (DNS)(도메인 이름 서버(DNS)) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add DNS Server(DNS 서버 추가) 페이지가 표시됩니다.

그림 6-24. Add DNS Server(DNS 서버 추가)



3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

새 DNS 서버가 정의되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DNS 서버 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

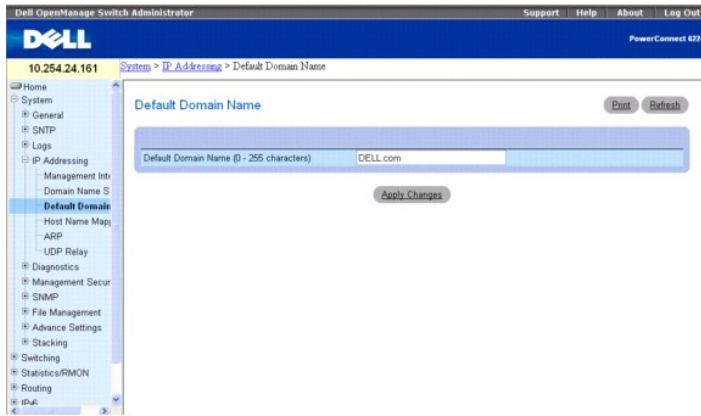
- 1 IP 주소 지정 명령

기본 도메인 이름

Default Domain Name(기본 도메인 이름) 페이지를 사용하여 기본 DNS 도메인 이름을 보고 정의할 수 있습니다.

Default Domain Name(기본 도메인 이름) 페이지를 표시하려면 System(시스템) → IP Addressing(IP 주소 지정) → Default Domain Name(기본 도메인 이름)을 클릭합니다.

그림 6-25. Default Domain Name(기본 도메인 이름)



Default Domain Name(기본 도메인 이름) 페이지에는 다음 필드가 있습니다.

Default Domain Name (0-255 characters) (기본 도메인 이름(0-255자)) — 사용자 정의 기본 도메인 이름을 포함합니다. 구성하면 정규화되지 않은 모든 호스트 이름에 기본 도메인 이름이 적용됩니다.

CLI 명령을 사용하여 DNS 도메인 이름 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

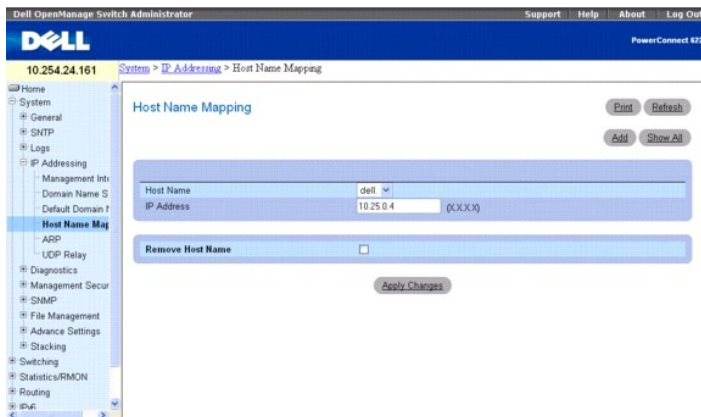
- 1 IP 주소 지정 명령

호스트 이름 할당

Host Name Mapping(호스트 이름 할당) 페이지를 사용하여 특정 호스트 이름에 IP 주소를 지정할 수 있습니다. **Host Name Mapping(호스트 이름 할당)** 페이지는 호스트당 하나의 IP 주소를 제공합니다.

Host Name Mapping(호스트 이름 할당) 페이지를 표시하려면 System(시스템) → IP Addressing(IP 주소 지정) → Host Name Mapping(호스트 이름 할당)을 클릭합니다.

그림 6-26. Host Name Mapping(호스트 이름 할당)



Host Name Mapping(호스트 이름 할당) 페이지에는 다음 필드가 있습니다.

Host Name(호스트 이름) — 호스트 이름 목록을 포함합니다. 호스트 이름은 Add Static Host Name Mapping(정적 호스트 이름 할당 추가) 페이지에서 정의됩니다. 각 호스트가 IP 주소 하나를 제공합니다.

IP Address(IP 주소) — 지정한 호스트 이름에 지정된 IP 주소를 제공합니다.

Remove Host Name(호스트 이름 제거) — 선택하면 호스트 이름 IP 할당을 제거합니다.

호스트 도메인 이름 추가

1. Host Name Mapping(호스트 이름 할당) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.
Add Static Host Name Mapping(정적 호스트 이름 할당 추가) 페이지가 표시됩니다.

그림 6-27. Add Static Host Name Mapping(정적 호스트 이름 할당 추가)

Host Name (0 - 255 characters)	DELL
IP Address	10.25.0.4 (X.X.X)

3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
IP 주소가 호스트 이름에 할당되고 장치가 업데이트됩니다.

정적 호스트 이름 할당표 표시

1. Host Name Mapping(호스트 이름 할당) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Static Host Name Mapping Table(정적 호스트 이름 할당표)가 표시됩니다.

그림 6-28. Static Host Name Mapping Table(정적 호스트 이름 할당표)

Host Name	IP Address	Remove
dell	10.25.0.4	<input type="checkbox"/>

IP 주소 할당에서 호스트 이름 제거

1. Host Name Mapping(호스트 이름 할당) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Host Name Mapping Table(호스트 이름 할당표)가 열립니다.
3. Host Name Mapping Table(호스트 이름 할당표) 항목을 선택합니다.
4. Remove(제거) 확인란을 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

Host Name Mapping Table(호스트 이름 할당표) 항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 도메인 호스트 이름에 IP 주소 할당

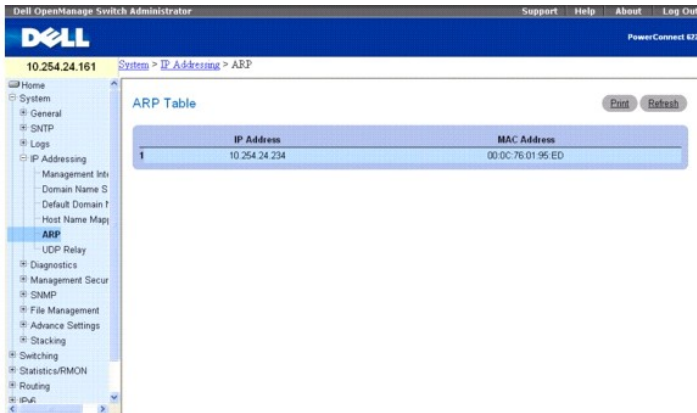
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

ARP 표

ARP Table(ARP 표) 페이지를 사용하여 IP 인터페이스에 대한 ARP 매개변수를 볼 수 있습니다. ARP 표에는 각 MAC 주소와 해당 IP 주소 간의 상관 관계가 표시됩니다.

ARP Table(ARP 표) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **IP Addressing(IP 주소 지정)** → **ARP**를 클릭합니다.

그림 6-29. ARP Table(ARP 표)



ARP Table(ARP 표) 페이지에는 다음 필드가 있습니다.

IP Address(IP 주소) — 아래에 입력한 MAC 주소와 연관된 스테이션 IP 주소입니다.

MAC Address(MAC 주소) — ARP 표에서 IP 주소와 연관된 스테이션 MAC 주소입니다.

CLI 명령을 사용하여 ARP 표 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

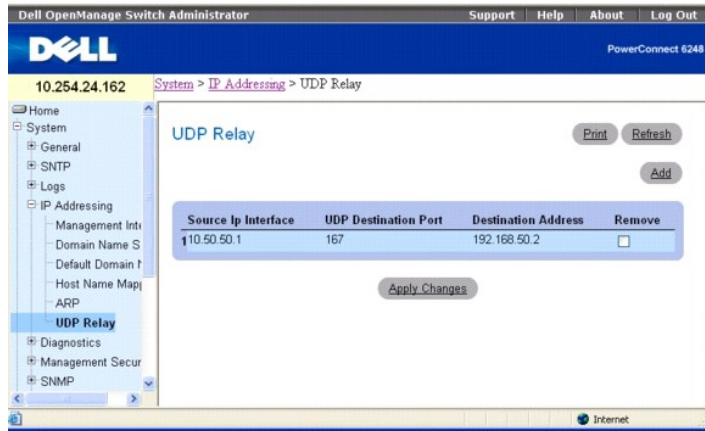
UDP 릴레이

UDP 릴레이는 장치가 한 인터페이스에서 다른 인터페이스로 특정 UDP 브로드캐스트를 전달할 수 있도록 합니다. 일반적으로 IP 브로드캐스트 패킷은 한 인터페이스에서 다른 인터페이스로 전달되지 않지만 일부 응용프로그램은 UDP 브로드캐스트를 사용하여 서비스의 가용성을 감지합니다. 다른 서비스는 다른 서브넷의 클라이언트에 서비스를 제공하기 위해 UDP 브로드캐스트 패킷을 라우팅해야 합니다. UDP 릴레이를 사용하면 워크스테이션에서 다른 네트워크의 서버를 찾아볼 수도 있습니다.

UDP Relay(UDP 릴레이) 페이지를 사용하여 UDP 릴레이 구성을 추가, 표시 또는 삭제할 수 있습니다.

UDP Relay(UDP 릴레이) 페이지를 표시하려면 **System(시스템)** → **IP Addressing(IP 주소 지정)** → **UDP Relay(UDP 릴레이)**를 클릭합니다.

그림 6-30. UDP Relay(UDP 릴레이)



UDP Relay(UDP 릴레이) 페이지에는 다음 필드가 있습니다.

Source IP Interface(소스 IP 인터페이스) — UDP 패킷을 릴레이하는 임력 IP 인터페이스입니다. 이 필드가 255.255.255.255이면 모든 인터페이스의 UDP 패킷이 표시됩니다. 다음 주소 범위는 유효하지 않습니다.

- 0.0.0.0 ~ 0.255.255.255
- 127.0.0.0 ~ 127.255.255.255

UDP Destination Port (1-65535)(UDP 대상 포트(1-65535)) — 릴레이할 UDP 패킷의 대상 UDP 포트 ID 번호입니다. 다음 표에는 UDP 포트 할당이 나열되어 있습니다.

UDP 포트 번호	약어	응용프로그램
7	Echo	Echo
11	SysStat	활성 사용자
15	NetStat	NetStat
17	Quote	Quote of the Day
19	CHARGEN	Character Generator
20	FTP-data	FTP 데이터
21	FTP	FTP
37	시간	시간
42	NAMESERVER	호스트 이름 서버
43	NICNAME	Who is
53	DOMAIN	도메인 이름 서버
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	NT 서버-스테이션 연결
138	NetBiosDatagramService	NT 서버-스테이션 연결
139	NetBios	SessionServiceNT 서버-스테이션 연결
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management 트랩
513	who	Unix Rwho 데몬
514	syslog	시스템 로그
525	timed	시간 데몬

Destination Address(대상 주소) — UDP 패킷 릴레이를 받는 IP 인터페이스입니다. 이 필드가 0.0.0.0이면 UDP 패킷이 삭제됩니다. 이 필드가 255.255.255.255이면 UDP 패킷이 모든 IP 인터페이스로 플러딩됩니다.

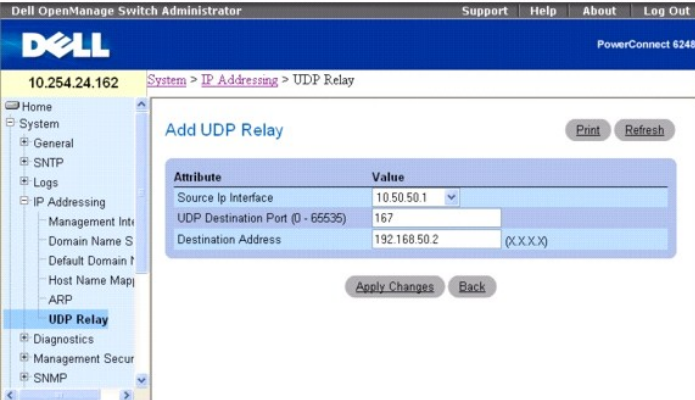
Remove(제거) — 지정한 UDP 릴레이를 제거하려면 확인란을 선택합니다.

UDP 릴레이 항목 추가

1. UDP Relay(UDP 릴레이) 페이지를 엽니다.

2. Add(추가)를 클릭하여 Add UDP Relay(UDP 릴레이 추가) 페이지를 표시합니다.

그림 6-31. Add UDP Relay(UDP 릴레이 추가)



3. Source IP Interface(소스 IP 인터페이스), UDP Destination Port(UDP 대상 포트) 및 Destination Address(대상 주소) 필드를 입력합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
UDP 릴레이가 추가되고 장치가 업데이트됩니다.
5. UDP Relay(UDP 릴레이) 페이지로 돌아가려면 Back(뒤로)을 클릭합니다.

주: UDP Relay(UDP 릴레이)를 활성화했지만 UDP 포트 번호를 지정하지 않은 경우 기본적으로 장치는 다음 서비스에 대해 UDP 브로드캐스트 패킷을 전달합니다: IEN-116 이름 서비스(포트 42), DNS(포트 53), NetBIOS 이름 서버(포트 137), NetBIOS 데이터그램 서버(포트 138), TACACS 서버(포트 49) 및 시간 서비스(포트 37).

UDP 릴레이 항목 제거

1. UDP Relay(UDP 릴레이) 페이지를 엽니다.
2. 삭제할 항목 옆에 있는 Remove(제거) 확인란을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.
UDP Relay(UDP 릴레이) 항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 UDP 릴레이 정보 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 IP 주소 지정 명령

케이블 진단 프로그램 실행

Diagnostics(진단) 메뉴 페이지를 사용하여 동케이블 및 광섬유 케이블에 대해 가상 케이블 검사를 수행할 수 있습니다.

Diagnostics(진단) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→Diagnostics(진단)**를 클릭합니다.

이 페이지를 사용하여 다음 기능으로 이동합니다.

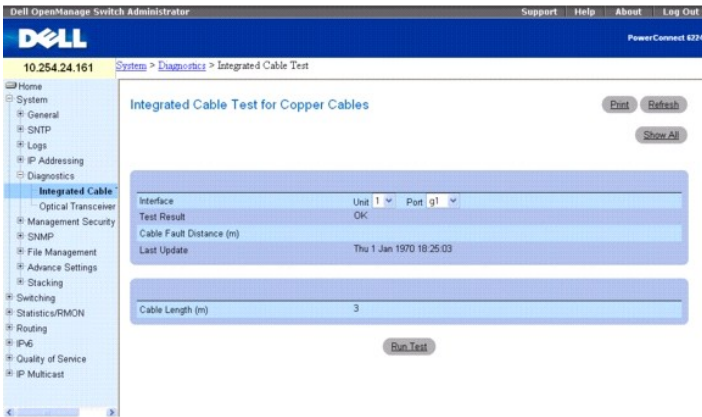
- 1 [동케이블에 대한 통합 케이블 검사](#)

동케이블에 대한 통합 케이블 검사

Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지를 사용하여 동케이블을 검사할 수 있습니다. 케이블 검사는 케이블에서 오류가 발생한 위치, 마지막으로 케이블을 검사한 시간 및 발생한 케이블 오류 유형에 대한 정보를 제공합니다. 이 검사는 TDR(Time Domain Reflectometry) 기술을 사용하여 포트에 연결된 동케이블의 품질과 특성을 검사합니다. 최대 120미터의 케이블을 검사할 수 있습니다. Approximated Cable Length(평균 케이블 길이) 검사를 제외하고 케이블은 포트가 다운 상태에 있을 때 검사됩니다.

Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Diagnostics(진단)→Integrated Cable Test(통합 케이블 검사)를 클릭합니다.

그림 6-32. 동케이블에 대한 통합 케이블 검사



Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지에는 다음 필드가 있습니다.

Interface(인터페이스) — 케이블이 연결된 인터페이스입니다.

Test Result(검사 결과) — 케이블 검사 결과입니다. 가능한 값은 다음과 같습니다.

No Cable(케이블 없음) — 포트에 케이블이 연결되어 있지 않습니다.

Open Cable(열린 케이블) — 케이블이 열려 있습니다.

Short Cable(단락 케이블) — 케이블에서 단락이 발생했습니다.

OK(양호) — 케이블이 검사에 합격했습니다.

Fiber Cable(광케이블) — 광케이블이 포트에 연결되어 있습니다.

Cable Fault Distance(케이블 장애 거리) — 케이블 오류가 발생한 포트에서의 거리입니다.

Last Update(마지막 업데이트) — 마지막으로 포트가 검사된 시간입니다.

Cable Length(케이블 길이) — 평균 케이블 길이입니다. 포트가 1Gbps로 작동 중인 경우에만 이 검사를 수행할 수 있습니다.

케이블 검사

1. 동케이블의 양 끝이 장치에 연결되어 있는지 확인합니다.
2. Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지를 엽니다.
3. Run Test(검사 실행)를 클릭합니다.

동케이블 검사가 수행되고 Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지에 결과가 표시됩니다.

통합 케이블 검사 결과 표 표시

1. Integrated Cable Test for Copper Cables(동케이블에 대한 통합 케이블 검사) 페이지를 엽니다.
2. Show All(모두 표시)를 클릭합니다.
3. 드롭다운 메뉴에서 원하는 장치를 선택합니다.

웹 페이지에 모든 포트에 대한 이전 검사 결과를 보여주는 Integrated Cable Test Results Table(통합 케이블 검사 결과 표) 페이지가 표시됩니다.

그림 6-33. Integrated Cable Test Results Table(통합 케이블 검사 결과 표)

Integrated Cable Test Results Table Print Refresh

Unit: 1 Net

Interface	Test Result	Cable Fault Distance (m)	Last Update	Cable Length (m)
1/g1	Test has not been performed			
1/g2	Test has not been performed			
1/g3	Test has not been performed			
1/g4	Test has not been performed			
1/g5	Test has not been performed			
1/g6	Test has not been performed			
1/g7	Test has not been performed			
1/g8	Test has not been performed			
1/g9	Test has not been performed			
1/g10	Test has not been performed			
1/g11	Test has not been performed			

CLI 명령을 사용하여 동케이블 검사

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 PHY 진단 명령

장치 보안 관리

Management Security(관리 보안) 메뉴 페이지를 사용하여 포트, 사용자 및 서버 보안에 대한 관리 보안 매개변수를 설정할 수 있습니다.

Management Security(관리 보안) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→Management Security(관리 보안)**를 클릭합니다. 이 페이지를 사용하여 다음 기능으로 이동합니다.

- 1 [액세스 프로파일](#)
- 1 [인증 프로파일](#)
- 1 [인증 선택](#)
- 1 [암호 관리](#)
- 1 [로컬 사용자 데이터베이스](#)
- 1 [라인 암호](#)
- 1 [암호 활성화](#)
- 1 [TACACS+ 설정](#)
- 1 [RADIUS 설정](#)
- 1 [텔넷 서버](#)
- 1 [서비스 거부](#)

액세스 프로파일

Access Profile(액세스 프로파일) 페이지를 사용하여 프로파일 및 장치 액세스 규칙을 정의할 수 있습니다. 특정 관리 기능, 특정 수신 인터페이스, 소스 IP 주소 및/또는 소스 IP 서버 네트워크에 대한 액세스를 제한할 수 있습니다.

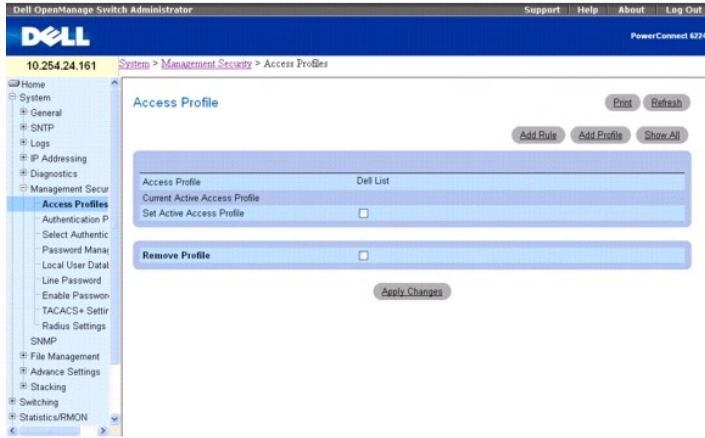
웹(HTTP), 보안 웹(HTTPS), 텔넷, SSH, SNMP 등 각 유형의 관리 액세스 방법에 대해 개별적으로 관리 액세스를 정의할 수 있습니다.

관리 액세스 목록에는 장치를 관리할 수 있는 사용자 및 방법을 결정하는 규칙이 있습니다. 사용자가 장치를 액세스하지 못하도록 차단할 수도 있습니다.

Access Profile(액세스 프로파일) 페이지를 사용하여 관리 목록을 구성하고 특정 인터페이스에 적용할 수 있습니다.

Access Profile(액세스 프로파일) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)→Management Security(관리 보안)→Access Profiles(액세스 프로파일)**를 클릭합니다.

그림 6-34. Access Profile(액세스 프로파일)



Access Profile(액세스 프로파일) — 액세스 프로파일을 표시합니다.

Current Active Access Profile(현재 활성 액세스 프로파일) — 활성화된 프로파일을 표시합니다.

Set Active Access Profile(활성 액세스 프로파일 설정) — 액세스 프로파일을 활성화합니다.

Remove Profile(프로파일 제거) — 선택하면 액세스 프로파일이 Access Profile(액세스 프로파일) 목록에서 제거됩니다.

주: 인터페이스에 액세스 프로파일을 지정하면 다른 인터페이스를 통한 액세스가 거부됩니다. 액세스 프로파일을 활성화하지 않으면 모두 장치에 액세스할 수 있습니다.

액세스 프로파일 표시

1. Access Profile(액세스 프로파일) 페이지를 엽니다.
2. Show All(모두 표시)를 클릭하여 Profile Rules Table(프로파일 규칙 표) 페이지를 표시합니다.

그림 6-35. Profile Rules Table(프로파일 규칙 표)

Interface	Management Method	Source IP Address	Subnet Mask	Action	Priority	Remove
1/1	SNMP	132.26.39.115	255.255.255.255	PERMIT	1	<input type="checkbox"/> Edit
2/1	SSH	192.168.22.15	255.255.255.255	PERMIT	3	<input type="checkbox"/> Edit

액세스 프로파일 추가

1. Access Profile(액세스 프로파일) 페이지를 엽니다.
 2. Add Profile(프로파일 추가)를 클릭합니다.
- Add an Access Profile(액세스 프로파일 추가) 페이지가 표시됩니다.

그림 6-36. Add an Access Profile(액세스 프로파일 추가)

3. **Access Profile Name(액세스 프로파일 이름)** 텍스트 상자에 프로파일 이름을 입력합니다.

4. 다음 필드를 입력합니다.

Management Method(관리 방법) — 드롭다운 상자에서 선택합니다. 선택한 관리에 따라 정책이 제한됩니다.

Interface(인터페이스) — 인터페이스를 기반으로 규칙을 정책에 적용해야 하는 경우 해당 인터페이스의 확인란을 선택합니다. 인터페이스는 물리적 인터페이스, LAG 또는 VLAN입니다.

Source IP Address(소스 IP 주소) — 정책의 규칙이 관리 트래픽을 보내는 클라이언트의 IP 주소를 기준으로 해야 하는 경우 **Source IP Address(소스 IP 주소)** 확인란을 선택합니다. 제공된 필드에 소스 IP 주소 및 마스크 정보를 입력합니다. 다음의 두 가지 형식으로 마스크 정보를 지정할 수 있습니다. 점으로 표시된 IP 형식(예: 255.255.255.0) 또는 점두어 길이(예: 32)

Action(동작) — 위에서 선택한 규칙과 일치하는 경우 수행할 동작을 선택합니다. 드롭다운 상자에서 Permit(허용) 또는 Deny(거부)를 선택하여 액세스를 허용하거나 거부합니다.

Rule Priority(규칙 우선 순위) — 규칙에 대한 우선 순위를 구성합니다. 수신되는 관리 요청에 대해 우선 순위(오름차순)별로 규칙을 검증합니다. 규칙이 일치하면 동작이 수행되고 이하의 규칙은 무시됩니다. 예를 들어 우선 순위가 1인 소스 IP 10.10.10.10을 Permit(허용)으로 구성하고, 우선 순위가 2인 소스 IP 10.10.10.10을 Deny(거부)로 구성한 경우 프로파일이 활성화되면 액세스가 허용되고 두 번째 규칙은 무시됩니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

새 액세스 프로파일이 추가되고 장치가 업데이트됩니다.

액세스 프로파일 활성화

1. **Access Profile(액세스 프로파일)** 페이지를 엽니다.

2. **Set Access Profile Active(액세스 프로파일을 활성화로 설정)**를 선택합니다.

3. **Apply Changes(변경사항 적용)**를 클릭합니다.

장치에 대해 액세스 프로파일이 활성화됩니다.

액세스 프로파일에 규칙 추가

1. **Access Profile(액세스 프로파일)** 페이지를 엽니다.

Access Profile(액세스 프로파일) 필드에는 **Add An Access Profile Rule(액세스 프로파일 규칙 추가)** 페이지를 표시할 때 규칙이 추가되는 프로파일이 표시됩니다.

2. **Add Route(경로 추가)**를 클릭합니다.

Add An Access Profile Rule(액세스 프로파일 규칙 추가) 페이지가 표시됩니다.

그림 6-37. Add an Access Profile Rule(액세스 프로파일 규칙 추가)

3. 대화상자에서 다음 필드를 입력합니다.

Management Method(관리 방법) — 드롭다운 상자에서 선택합니다. 선택한 관리에 따라 정책이 제한됩니다.

Interface(인터페이스) — 인터페이스를 기반으로 규칙을 정책에 적용해야 하는 경우 해당 인터페이스의 확인란을 선택합니다. 인터페이스는 물리적 인터페이스, LAG 또는 VLAN입니다.

Source IP Address(소스 IP 주소) — 정책의 규칙이 관리 트래픽이 발생한 클라이언트의 IP 주소를 기준으로 해야 하는 경우 **Source IP Address(소스 IP 주소)** 확인란을 선택합니다. 제공된 텍스트 상자에 소스 IP 주소 및 마스크 정보를 입력합니다. 점으로 표시된 IP 형식(예: 255.255.255.0) 또는 점두어 길이(예: 32)의 두 가지 형식으로 마스크를 지정할 수 있습니다.

Action(동작) — 위에서 선택한 규칙과 일치하는 경우 수행할 동작을 선택합니다. 드롭다운 상자에서 Permit(허용) 또는 Deny(거부)를 선택하여 액세스를 허용하거나 거부합니다.

Rule Priority(규칙 우선 순위) — 규칙에 대한 우선 순위를 구성합니다. 수신되는 관리 요청에 대해 우선 순위(오름차순)별로 규칙을 검증합니다. 규칙이 일치하면 동작이 수행되고 이하의 규칙은 무시됩니다. 예를 들어 우선 순위가 1인 소스 IP 10.10.10.10을 Permit(허용)으로 구성하고, 우선 순위가 2인 소스 IP 10.10.10.10을 Deny(거부)로 구성한 경우 프로파일이 활성화되면 액세스가 허용되고 두 번째 규칙은 무시됩니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

규칙이 액세스 프로파일에 추가되고 장치가 업데이트됩니다.

규칙 제거

1. **Access Profile(액세스 프로파일)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭하여 **Profile Rules Table(프로파일 규칙 표)** 페이지를 표시합니다.
3. 규칙을 선택합니다.
4. **Remove(제거)** 확인란을 선택합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

규칙이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 액세스 프로파일 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

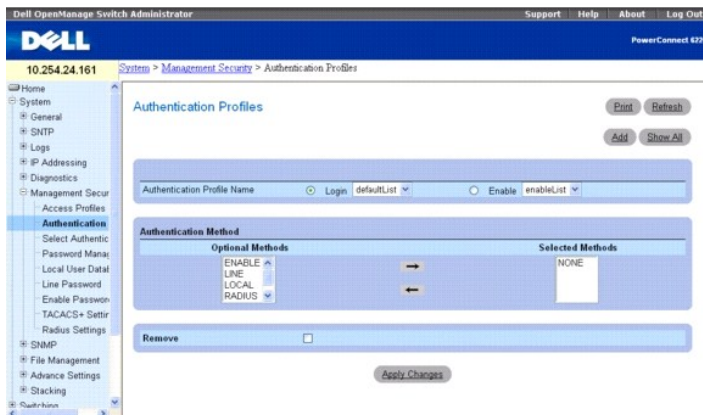
1. ACL 명령 관리

인증 프로파일

사용자 인증은 외부 서버에서 로컬로 수행됩니다. **Authentication Profiles(인증 프로파일)** 페이지를 사용하여 장치의 사용자 인증 방법을 선택할 수 있습니다.

Authentication Profiles(인증 프로파일) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)** → **Management Security(관리 보안)** → **Authentication Profiles(인증 프로파일)**를 클릭합니다.

그림 6-38. Authentication Profiles(인증 프로파일)



Authentication Profiles(인증 프로파일) 페이지에는 다음 필드가 있습니다.

Authentication Profile Name(인증 프로파일 이름)

사용자 정의 인증 프로파일이 추가되는 목록을 표시합니다. 라디오 단추를 사용하여 스위치 작동의 Login(로그인) 또는 Enable(활성) 부분을 제어하는 인증 프로파일을 적용하고 사용할 수 있는 다음 두 목록 중 하나를 선택합니다.

Login(로그인) — 스위치에 로그인할 수 있도록 합니다. 옵션은 **defaultList**, **networkList** 및 모든 사용자 정의 로그인 인증 프로파일입니다.

Enable(활성) — 권한 모드를 활성화합니다.

Authentication Method(인증 방법)

Optional Methods(선택적 방법) — 사용자 인증 방법입니다. 가능한 옵션은 다음과 같습니다.

None(없음) — 사용자 인증이 수행되지 않습니다.

Local(로컬) — 장치 레벨에서 사용자 인증이 수행됩니다. 장치가 인증을 위해 사용자 이름과 암호를 확인합니다.

RADIUS — RADIUS 서버에서 사용자 인증이 수행됩니다. RADIUS 서버에 대한 자세한 내용은 "[RADIUS 설정](#)"을 참조하십시오.

TACACS+ — TACACS+ 서버에서 사용자 인증이 수행됩니다. TACACS+ 서버에 대한 자세한 내용은 "[TACACS+ 설정](#)"을 참조하십시오.

Line(라인) — 라인 암호가 사용자 인증에 사용됩니다.

Enable(활성) — 활성화 암호가 인증에 사용됩니다.

주: 사용자 인증은 방법을 선택한 순서대로 수행됩니다. 인증 중에 오류가 발생하면 다음에 선택한 방법이 사용됩니다. 예를 들어 Local(로컬) 옵션을 선택한 다음 RADIUS 옵션을 선택하면 사용자가 먼저 로컬에서 인증된 다음 외부 RADIUS 서버를 통해 인증됩니다.

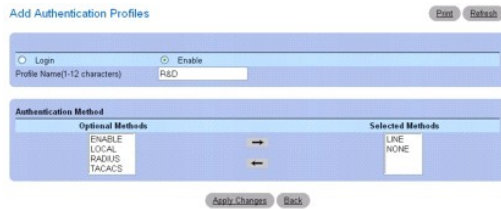
Selected Methods(선택한 방법) — 선택한 인증 방법입니다.

Remove(제거) — 선택한 프로파일을 제거합니다.

인증 프로파일 추가

1. Authentication Profiles(인증 프로파일) 페이지를 엽니다.
2. Add(추가)를 클릭하여 Add Authentication Profile(인증 프로파일 추가) 페이지를 표시합니다.

그림 6-39. Add Authentication Profile(인증 프로파일 추가)



3. Profile Name(프로파일 이름) 필드에 1 ~ 12자의 프로파일 이름을 입력합니다.

주: 프로파일 이름에 공백이 포함되면 안 됩니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

프로파일이 생성됩니다. System(시스템) → Management Security(관리 보안) → Select Authentication(인증 선택) 웹 페이지를 사용하여 인증 프로파일을 활성화할 수 있습니다.

인증 프로파일 수정

1. Authentication Profiles(인증 프로파일) 페이지를 엽니다.
2. Authentication Profile Name(인증 프로파일 이름) 필드의 목록에서 요소를 선택합니다.
3. 화살표를 사용하여 Optional Methods(선택적 방법)를 하나 이상 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

사용자 인증 프로파일이 장치에 업데이트됩니다.

인증 프로파일 항목 제거

1. Authentication Profiles(인증 프로파일) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Authentication Profiles Table(인증 프로파일 표)가 열립니다.

그림 6-40. Authentication Profiles Table(인증 프로파일 표)

Login Authentication Profiles			
ID	Name	Methods	Remove
1	defaultList	NONE,LINE	<input type="checkbox"/> Edit

Enable Authentication Profiles			
ID	Name	Methods	Remove
1	enableList	NONE	<input type="checkbox"/> Edit
2	RFD	LINE,NONE	<input type="checkbox"/> Edit

3. 제거할 프로파일 옆에 있는 Remove(제거) 확인란을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

항목이 제거됩니다.

CLI 명령을 사용하여 인증 프로파일 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

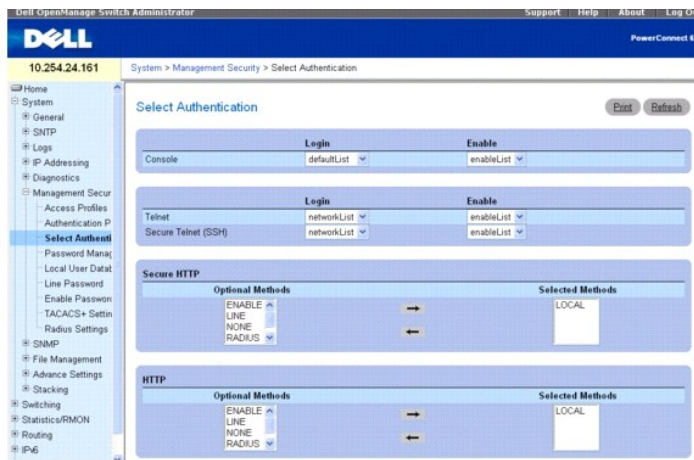
- 1 AAA 명령

인증 선택

인증 프로파일을 정의한 후 관리 액세스 방법에 적용할 수 있습니다. 예를 들어 콘솔 사용자는 Authentication Profile List 1(인증 프로파일 목록 1)로 인증하고 텔넷 사용자는 Authentication Profile List 2(인증 프로파일 목록 2)로 인증할 수 있습니다.

Select Authentication(인증 선택) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Management Security(관리 보안)→ Select Authentication(인증 선택)을 클릭합니다.

그림 6-41. Select Authentication(인증 선택)



Select Authentication(인증 선택) 페이지에는 다음 필드가 있습니다.

Console(콘솔) — 콘솔 사용자 인증에 사용되는 인증 프로파일입니다.

Telnet(텔넷) — 텔넷 사용자 인증에 사용되는 인증 프로파일입니다.

Secure Telnet (SSH)(보안 텔넷(SSH)) — 보안 셸(SSH) 사용자 인증에 사용되는 인증 프로파일입니다. SSH는 장치에 대한 암호화된 보안 원격 연결을 클라이언트에 제공합니다.

Secure HTTP and HTTP(보안 HTTP 및 HTTP) — 각각 보안 HTTP 액세스 및 HTTP 액세스에 사용되는 인증 방법입니다. 가능한 필드 값은 다음과 같습니다.

None(없음) — 액세스에 대해 인증 방법이 사용되지 않습니다.

Local(로컬) — 로컬에서 인증이 수행됩니다.

RADIUS — RADIUS 서버에서 인증이 수행됩니다.

TACACS+ — TACACS+ 서버에서 인증이 수행됩니다.

Local, None(로컬, 없음) — 먼저 로컬에서 인증이 수행됩니다.

RADIUS, None(RADIUS, 없음) — 먼저 RADIUS 서버에서 인증이 수행됩니다. 인증을 확인할 수 없는 경우 인증 방법이 사용되지 않습니다. 사용자 확인을 위해 원격 서버에 연결할 수 없는 경우 인증을 확인할 수 없습니다. 원격 서버에 연결할 수 있는 경우 원격 서버의 응답이 항상 신뢰됩니다.

TACACS+, None(TACACS+, 없음) — 먼저 TACACS+ 서버에서 인증이 수행됩니다. 인증을 확인할 수 없는 경우 인증 방법이 사용되지 않습니다. 사용자 확인을 위해 원격 서버에 연결할 수 없는 경우 인증을 확인할 수 없습니다. 원격 서버에 연결할 수 있는 경우 원격 서버의 응답이 항상 신뢰됩니다.

Local, RADIUS(로컬, RADIUS) — 먼저 로컬에서 인증이 수행됩니다. 로컬에서 인증을 확인할 수 없는 경우 RADIUS 서버에서 관리 방법을 인증합니다. RADIUS 서버에서 관리 방법을 인증할 수 없는 경우 세션이 차단됩니다.

Local, TACACS+(로컬, TACACS+) — 먼저 로컬에서 인증이 수행됩니다. 로컬에서 인증을 확인할 수 없는 경우 TACACS+ 서버에서 관리 방법을 인증합니다. TACACS+ 서버에서 관리 방법을 인증할 수 없는 경우 세션이 차단됩니다.

RADIUS, Local(RADIUS, 로컬) — 먼저 RADIUS 서버에서 인증이 수행됩니다. RADIUS 서버에서 인증을 확인할 수 없는 경우 로컬에서 세션이 인증됩니다. 로컬에서 세션을 인증할 수 없는 경우 세션이 차단됩니다.

TACACS+, Local(TACACS+, 로컬) — 먼저 TACACS+ 서버에서 인증이 수행됩니다. TACACS+ 서버에서 인증을 확인할 수 없는 경우 로컬에서 세션이 인증됩니다. 로컬에서 세션을 인증할 수 없는 경우 세션이 차단됩니다.

Local, RADIUS, None(로컬, RADIUS, 없음) — 먼저 로컬에서 인증이 수행됩니다. 로컬에서 인증을 확인할 수 없는 경우 RADIUS 서버에서 관리 방법을 인증합니다. RADIUS 서버에서 관리 방법을 인증할 수 없는 경우 세션이 허용됩니다.

RADIUS, Local, None(RADIUS, 로컬, 없음) — 먼저 RADIUS 서버에서 인증이 수행됩니다. RADIUS 서버에서 인증을 확인할 수 없는 경우 로컬에서 세션이 인증됩니다. 로컬에서 세션을 인증할 수 없는 경우 세션이 허용됩니다.

Local, TACACS+, None(로컬, TACACS+, 없음) — 먼저 로컬에서 인증이 수행됩니다. 로컬에서 인증을 확인할 수 없는 경우 TACACS+ 서버에서 관리 방법을 인증합니다. TACACS+ 서버에서 관리 방법을 인증할 수 없는 경우 세션이 허용됩니다.

TACACS+, Local, None(TACACS+, 로컬, 없음) — 먼저 TACACS+ 서버에서 인증이 수행됩니다. TACACS+ 서버에서 인증을 확인할 수 없는 경우 로컬에서 세션이 인증됩니다. 로컬에서 세션을 인증할 수 없는 경우 세션이 허용됩니다.

콘솔 세션에 인증 방법 목록 적용

1. **Select Authentication(인증 선택)** 페이지를 엽니다.
2. **Console(콘솔)** 필드에서 인증 프로파일을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

콘솔 세션에 인증 방법 목록이 지정됩니다.

텔넷 세션에 인증 프로파일 적용

1. **Select Authentication(인증 선택)** 페이지를 엽니다.
2. **Telnet(텔넷)** 필드에서 인증 프로파일을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

콘솔 세션에 인증 프로파일이 지정됩니다.

보안 텔넷(SSH) 세션에 인증 프로파일 적용

1. **Select Authentication(인증 선택)** 페이지를 엽니다.
2. **Secure Telnet (SSH)(보안 텔넷(SSH))** 필드에서 인증 프로파일을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

보안 텔넷(SSH) 세션에 인증 프로파일이 지정됩니다.

HTTP 세션에 인증 시퀀스 지정

1. **Select Authentication(인증 선택)** 페이지를 엽니다.
2. HTTP의 **Optional Methods(선택적 방법)** 필드에서 인증 방법을 선택하고 오른쪽 화살표 단추를 클릭합니다.
선택된 인증 방법이 **Selected Methods(선택된 방법)** 필드로 이동합니다.
3. 원하는 인증 순서가 **Selected Methods(선택된 방법)** 필드에 표시될 때까지 반복합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
HTTP 세션에 인증 시퀀스가 지정됩니다.

CLI 명령을 사용하여 액세스 방법, 인증 프로파일 또는 시퀀스 지정

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 AAA 명령

보안 HTTP 세션에 인증 시퀀스 지정

1. **Select Authentication(인증 선택)** 페이지를 엽니다.
2. **Secure HTTP(보안 HTTP)**의 **Optional Methods(선택적 방법)** 필드에서 인증 방법을 선택하고 오른쪽 화살표 단추를 클릭합니다.
선택된 인증 방법이 **Selected Methods(선택된 방법)** 필드로 이동합니다.
3. 원하는 인증 순서가 **Selected Methods(선택된 방법)** 필드에 표시될 때까지 반복합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
보안 HTTP 세션에 인증 시퀀스가 지정됩니다.

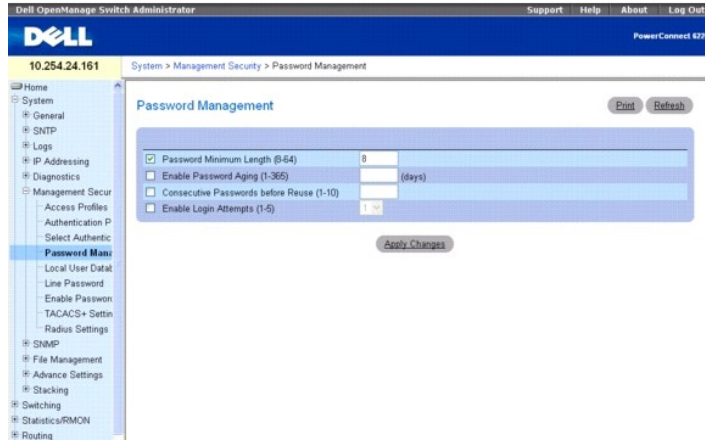
암호 관리

암호 관리를 사용하면 네트워크 보안이 향상되고 암호 제어 기능이 강화됩니다. SSH, 텔넷, HTTP, HTTPS 및 SNMP 액세스를 위한 암호에는 다음을 비롯한 보안 기능이 지정됩니다.

- 1 최소 암호 길이 정의
- 1 암호 만료
- 1 잘못된 암호 재사용 방지
- 1 로그인 시도 실패 후 사용자 잠금

Password Management(암호 관리) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)**→**Management Security(관리 보안)**→**Password Management(암호 관리)**를 클릭합니다.

그림 6-42. Password Management(암호 관리)



Password Management(암호 관리) 페이지에는 다음 필드가 있습니다.

Password Minimum Length (8-64)(암호 최소 길이(8-64)) — 선택하면 최소 암호 길이를 나타냅니다. 예를 들어 관리자는 모든 라인 암호가 최소 10자 이상이 되어야 하도록 정의할 수 있습니다.

Enable Password Aging (1-365)(암호 수명 활성화(1-365)) — 선택하면 암호 수명이 만료되기까지의 시간을 나타냅니다. 필드 값은 1 ~ 365일입니다. 암호 수명 기능은 스위치 클럭이 SNMP 서버와 동기화된 경우에만 작동합니다. 자세한 내용은 CLI 참조 안내서의 "클럭 명령" 절을 참조하십시오.

Consecutive Passwords Before Reuse (1-10)(재사용 전의 연속 암호(1-10)) — 암호를 재사용할 수 있기까지 암호가 변경되는 횟수를 나타냅니다. 가능한 필드 값은 1 ~ 10입니다.

주: 암호가 만료되기 전에 사용자에게 암호를 변경하라고 알려 줍니다. 웹 사용자에게는 이 알림이 표시되지 않습니다.

Enable Login Attempts (1-5)(로그인 시도 활성화(1-5)) — 선택하면 잘못된 암호가 정의된 횟수만큼 사용될 경우 사용자가 장치를 사용할 수 없도록 잠깁니다. 예를 들어 로그인 시도 횟수가 5로 정의된 경우 사용자가 잘못된 암호로 5번 로그인을 시도하면 6번째 시도에서 장치를 사용할 수 없도록 사용자가 잠깁니다. 이 경우 수퍼 사용자가 사용자 계정을 다시 활성화해야 합니다. 필드 범위는 1 ~ 5회 시도입니다.

암호 제한 조건 정의

1. Password Management(암호 관리) 페이지를 엽니다.
2. 관련 필드를 정의합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

암호 제한 조건이 정의되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 암호 제한 조건 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

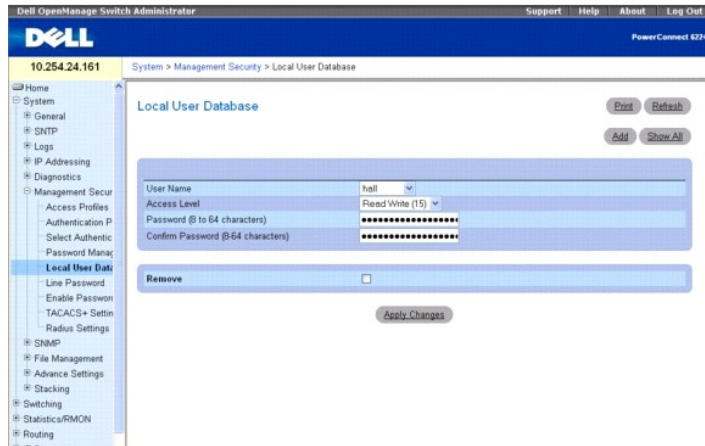
1. 암호 관리 명령

로컬 사용자 데이터베이스

Local User Database(로컬 사용자 데이터베이스) 페이지를 사용하여 사용자의 암호와 액세스 권한을 정의하고 계정이 일시 중단된 사용자를 다시 활성화할 수 있습니다.

Local User Database(로컬 사용자 데이터베이스) 페이지를 표시하려면 디렉터리 화면에서 **System(시스템)**→ **Management Security(관리 보안)**→ **Local User Database(로컬 사용자 데이터베이스)**를 클릭합니다.

그림 6-43. Local User Database(로컬 사용자 데이터베이스)



Local User Database(로컬 사용자 데이터베이스) 페이지에는 다음 필드가 있습니다.

User Name(사용자 이름) — 사용자 목록입니다.

Access Level(액세스 레벨) — 사용자 액세스 레벨입니다. 가장 낮은 사용자 액세스 레벨은 **1(읽기 전용)**이고 **15(읽기/쓰기)**가 가장 높습니다. 사용자 액세스를 일시 중단하려면 레벨 0으로 설정합니다(레벨 15 사용자만 이 작업을 수행할 수 있음).

Password (8- 64 characters)(암호(8- 64자)) — 사용자 정의 암호입니다.

Confirm Password(암호 확인) — 사용자 정의 암호를 확인합니다.

Remove(제거) — 선택하면 로컬 사용자 데이터베이스에서 사용자를 제거합니다.

사용자에게 액세스 권한 할당

1. Local User Database(로컬 사용자 데이터베이스) 페이지를 엽니다.
2. **User Name(사용자 이름)** 필드에서 사용자를 선택합니다.
3. 필요에 따라 필드를 정의합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

사용자의 액세스 권한과 암호가 정의되고 장치가 업데이트됩니다.


로컬 사용자 데이터베이스에 사용자 추가

1. Local User Database(로컬 사용자 데이터베이스) 페이지를 엽니다.
2. **Add(추가)**를 클릭하여 **Add User(사용자 추가)** 페이지를 표시합니다.
Add a New User(새 사용자 추가) 페이지가 표시됩니다.

그림 6-44. Add a New User(새 사용자 추가)



3. 필드를 입력합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
새 사용자가 정의되고 장치가 업데이트됩니다.

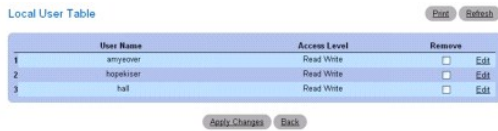
 주: 장치에서 최대 8명의 로컬 사용자를 정의할 수 있습니다.

로컬 사용자 데이터베이스의 사용자 표시

1. Local User Database(로컬 사용자 데이터베이스) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭하여 Local User Table(로컬 사용자 표) 페이지를 표시합니다.

로컬 사용자 데이터베이스의 모든 멤버가 표시됩니다.

그림 6-45. Local User Table(로컬 사용자 표)



	User Name	Access Level	Remove
1	amycover	Read Write	<input type="checkbox"/> Edit
2	hopeuser	Read Write	<input type="checkbox"/> Edit
3	hal	Read Write	<input type="checkbox"/> Edit

로컬 사용자 데이터베이스에서 사용자 제거

1. Local User Database(로컬 사용자 데이터베이스) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭하여 Local User Table(로컬 사용자 표) 페이지를 표시합니다.
3. User Name(사용자 이름)을 선택합니다.
4. Remove(제거)를 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

사용자가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 사용자 지정

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

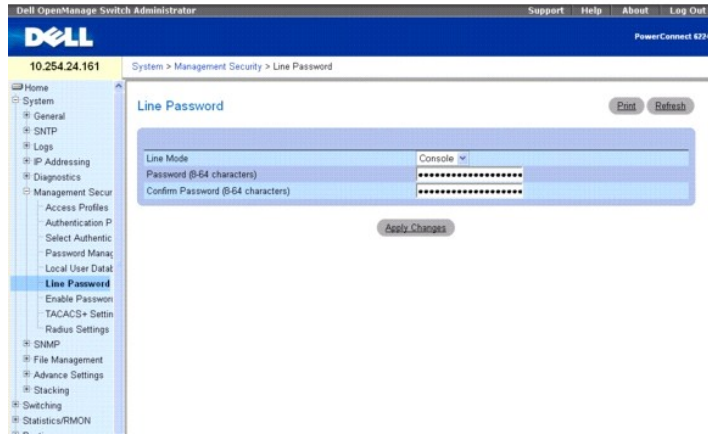
1 AAA 명령

라인 암호

Line Password(라인 암호) 페이지를 사용하여 관리 방법에 대한 라인 암호를 정의할 수 있습니다.

Line Password(라인 암호) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Management Security(관리 보안)→ Line Password(라인 암호)를 클릭합니다.

그림 6-46. Line Password(라인 암호)



Line Password(라인 암호) 페이지에는 다음 필드가 있습니다.

Line Mode(라인 모드) — 다른 다른 메뉴에서 콘솔, 텔넷 또는 보안 텔넷(SSH) 세션을 통해 액세스할 수 있는 장치를 지정합니다.

Line Password (8 - 64 characters)(라인 암호(8 - 64자)) — 콘솔, 텔넷 또는 보안 텔넷 세션을 통해 장치에 액세스하기 위한 라인 암호입니다. 암호는 ***** 형식으로 표시됩니다.

Confirm Password (8 - 64 characters)(암호 확인(8 - 64자)) — 새 라인 암호를 확인합니다. 암호는 ***** 형식으로 표시됩니다.

라인 암호 정의

1. Line Password(라인 암호) 페이지를 엽니다.
2. 콘솔, 텔넷 또는 보안 텔넷(SSH) 세션을 통해 액세스하려는 장치를 선택합니다.
3. 장치에 연결하는 데 사용할 세션 유형에 대한 Line Password(라인 암호) 필드를 정의합니다.
4. Line Password(라인 암호)를 확인합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

세션 유형에 대한 라인 암호가 정의되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 라인 암호 지정

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

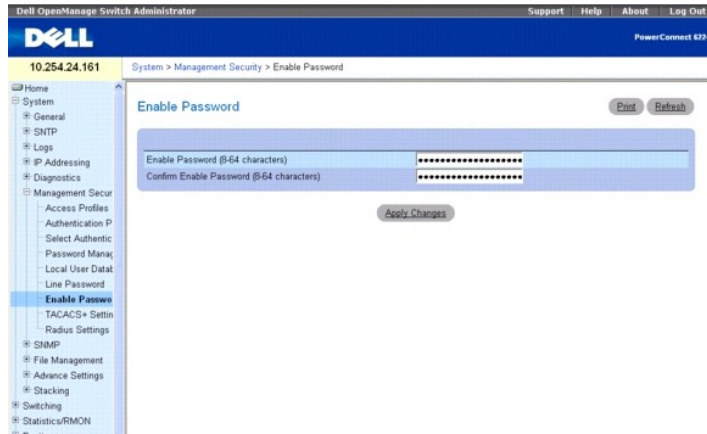
- 1 AAA 명령

암호 활성화

Enable Password(Enable 암호) 페이지를 사용하여 일반 레벨 및 권한 레벨에 대한 액세스를 제어하는 로컬 암호를 설정할 수 있습니다.

Enable Password(Enable 암호) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Management Security(관리 보안)→ Enable Password(Enable 암호)를 클릭합니다.

그림 6-47. Enable Password(Enable 암호)



Enable Password(Enable 암호) 페이지에는 다음 필드가 있습니다.

Enable Password (8-64 characters)(Enable 암호(8-64자)) — 일반 레벨 및 권한 레벨에 대한 액세스를 제어하는 Enable 암호입니다. 암호는 ***** 형식으로 표시됩니다.

Confirm Enable Password(Enable 암호 확인) — 새 Enable 암호를 확인합니다. 암호는 ***** 형식으로 표시됩니다.

Enable 암호 정의

1. Enable Password(Enable 암호) 페이지를 엽니다.
2. Enable 암호를 지정합니다.
3. Enable 암호를 확인합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

Enable 암호가 설정됩니다.

CLI 명령을 사용하여 Enable 암호 지정

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 AAA 명령

TACACS+ 설정

장치는 TACACS+(Terminal Access Controller Access Control System) 클라이언트를 지원합니다. TACACS+는 장치를 액세스하는 사용자 확인을 위해 중앙 집중식 보안을 제공합니다.

TACACS+는 RADIUS 및 기타 인증 프로세스와의 일관성을 유지하면서 중앙 집중식 사용자 관리 시스템을 제공합니다. TACACS+는 다음 서비스를 제공합니다.

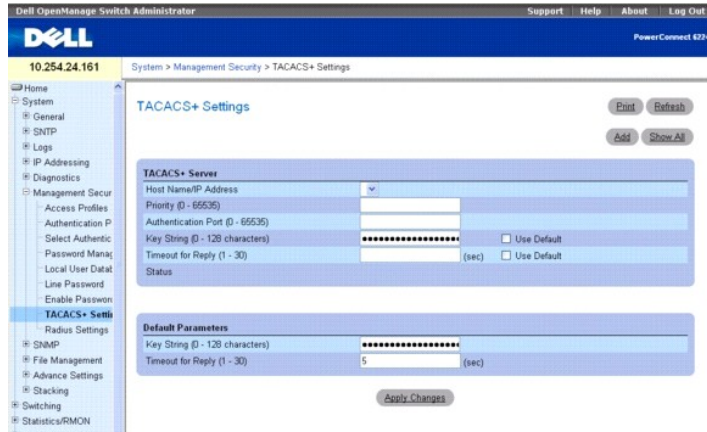
- 1 Authentication(인증) — 로그인 중에 사용자 이름 및 사용자 정의 암호를 통해 인증을 제공합니다.
- 1 Authorization(승인) — 로그인할 때 수행됩니다. 인증 세션이 완료되면 인증된 사용자 이름을 사용하여 승인 세션이 시작됩니다. TACACS+ 서버는 사용자 권한을 확인합니다.

TACACS+ 프로토콜은 장치와 TACACS+ 서버 간의 암호화된 프로토콜 교환을 통해 네트워크 보안을 보장합니다.

TACACS+ Settings(TACACS+ 설정) 페이지에는 대역내 관리 포트에 대한 사용자 정의 및 기본 TACACS+ 설정이 있습니다.

TACACS+ Settings(TACACS+ 설정) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Management Security(관리 보안)→ TACACS+ Settings(TACACS+ 설정)를 클릭합니다.

그림 6-48. TACACS+ Settings(TACACS+ 설정)



TACACS+ Settings(TACACS+ 설정) 페이지에는 다음 필드가 있습니다.

Host Name / IP Address(호스트 이름/IP 주소) – TACACS+ 서버를 지정합니다.

Priority (0-65535)(우선 순위(0-65636)) – TACACS+ 서버가 사용되는 순서를 지정합니다. 기본값은 0입니다.

Authentication Port (0-65535)(인증 포트(0-65535)) – TACACS+ 세션이 발생하는 포트 번호입니다. 기본값은 49입니다.

Key String (0-128 Characters)(키 문자열(0-128자)) – 장치와 TACACS+ 서버 간의 TACACS+ 통신을 위한 인증 및 암호화 키를 정의합니다. 이 키는 TACACS+ 서버에서 사용된 암호화와 일치해야 합니다. 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Timeout for Reply (1-30)(응답 타임아웃(1-30)) – 장치와 TACACS+ 서버 간의 연결이 타임아웃되기까지의 시간입니다. 필드 범위는 1 ~ 30초입니다. 출하시 기본값을 선택하려면 Use Default(기본값 사용)를 선택합니다.

Status(상태) – 장치와 TACACS+ 서버 간의 연결 상태입니다. 가능한 필드 값은 다음과 같습니다.

Connected(연결됨) – 장치와 TACACS+ 서버가 현재 연결되어 있습니다.

Not Connected(연결되어 있지 않음) – 장치와 TACACS+ 서버가 현재 연결되어 있지 않습니다.

이 페이지의 Default Parameters(기본 매개변수) 항목에 있는 필드 값은 새 TACACS+ 서버에 자동으로 적용됩니다.

Key String (0-128 Characters)(키 문자열(0-128자)) – 장치와 TACACS+ 서버 간의 TACACS+ 통신을 위한 기본 인증 및 암호화 키를 입력합니다.

Timeout for Reply (1-30)(응답 타임아웃(1-30)) – 장치와 TACACS+ 간의 연결이 타임아웃되기까지의 전역 사용자 구성 시간을 입력합니다.

TACACS+ 매개변수 정의

1. TACACS+ Settings(TACACS+ 설정) 페이지를 엽니다.
2. 필요에 따라 필드를 정의합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

TACACS+ 설정이 장치에 업데이트됩니다.

TACACS+ 서버 추가

1. TACACS+ Settings(TACACS+ 설정) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.
Add TACACS+ Host(TACACS+ 호스트 추가) 페이지가 표시됩니다.

그림 6-49. Add TACACS+ Host(TACACS+ 호스트 추가)

Add TACACS+ Host Print Refresh

Host Name/IP Address	10.240.13.45	(XXX.X)
Priority (0 - 65536)	258	
Authentication Port (0 - 65536)	43	
Key String (0 - 128 characters)	*****	<input type="checkbox"/> Use Default
Timeout for Reply (1 - 30)	5	<input type="checkbox"/> Use Default

Apply Changes Back

3. 필요에 따라 필드를 정의합니다.
 4. Apply Changes(변경사항 적용)를 클릭합니다.
- TACACS+ 서버가 추가되고 장치가 업데이트됩니다.

TACACS+ 서버 목록 표시

1. TACACS+ Settings(TACACS+ 설정) 페이지를 엽니다.
 2. Show All(모두 표시)을 클릭합니다.
- TACACS+ Servers Table(TACACS+ 서버 표)이 열립니다.

그림 6-50. TACACS+ Servers Table(TACACS+ 서버 표)

TACACS+ Servers Table Print Refresh

Host IP Address	Priority	Authentication Port	Timeout For Reply (sec)	Status	Remove
10.240.13.45	258	43	5	Not Connected	<input type="checkbox"/> Edit

Apply Changes Back

TACACS+ 서버 목록에서 TACACS+ 서버 제거

1. TACACS+ Settings(TACACS+ 설정) 페이지를 엽니다.
 2. Show All(모두 표시)을 클릭합니다.
- TACACS+ Servers Table(TACACS+ 서버 표)이 열립니다.
3. TACACS+ Servers Table(TACACS+ 서버 표) 항목을 선택합니다.
 4. Remove(제거) 확인란을 선택합니다.
 5. Apply Changes(변경사항 적용)를 클릭하십시오.
- TACACS+ 서버가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 TACACS+ 서버 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

```
1 TACACS+ 명령
```

RADIUS 설정

RADIUS(Remote Authorization Dial-In User Service) 서버는 네트워크에 추가 보안을 제공합니다. RADIUS 서버는 사용자별 인증 정보가 들어 있는 사용자 데이터 베이스를 유지 관리합니다. RADIUS 서버는 다음에 대한 중앙 집중식 인증 방법을 제공합니다.

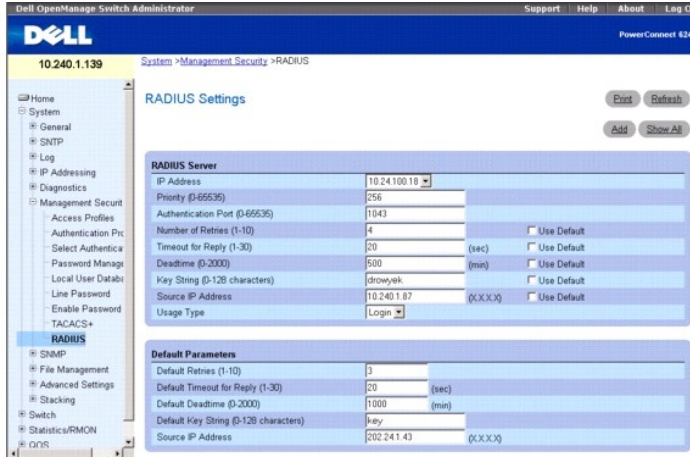
1. 텔넷 액세스
1. 웹 액세스

- 1 콘솔-스위치 액세스
- 1 액세스 제어 포트(802.1x)

RADIUS Settings(RADIUS 설정) 페이지에는 사용자 정의 및 기본 RADIUS 설정이 있습니다.

RADIUS Settings(RADIUS 설정) 페이지를 표시하려면 디렉터리 화면에서 System Management(시스템 관리)→ Security(보안)→ RADIUS Settings(RADIUS 설정)를 클릭합니다.

그림 6-51. RADIUS Settings(RADIUS 설정)



RADIUS Settings(RADIUS 설정) 페이지에는 다음 필드가 있습니다.

IP Address(IP 주소) — RADIUS 서버의 IP 주소입니다.

Priority (0-65535)(우선 순위(0-65535)) — 포트 우선 순위를 나타냅니다. 가능한 값은 0 ~ 65535입니다.

Authentication Port (0-65535)(인증 포트(0-65535)) — RADIUS 서버 인증 확인에 사용되는 인증 포트를 식별합니다.

Number of Retries (1-10)(재시도 횟수(1-10)) — 실패하기까지 RADIUS 서버로 전송되는 요청 횟수입니다. 가능한 필드 값은 1 ~ 10이고 기본값은 3입니다. 호스트별 값을 지정하지 않은 경우 전역 값이 각 호스트에 적용됩니다. 사용자 정의 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Timeout for Reply (1-30)(응답 타임아웃(1-30)) — 타임아웃되기까지 장치가 RADIUS 서버의 응답을 기다리는 시간(초)입니다. 가능한 필드 값은 1 ~ 30이고 기본값은 3입니다. 호스트별 값을 지정하지 않은 경우 전역 값이 각 호스트에 적용됩니다. 사용자 정의 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Deadtime (0-2000)(우회 시간(0-2000)) — 서비스 요청에 대해 RADIUS 서버가 우회되는 시간(분)입니다. 범위는 0 ~ 2000입니다. 호스트별 값을 지정하지 않은 경우 전역 값이 각 호스트에 적용됩니다. 사용자 정의 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Key String (0-128 Characters)(키 문자열(0-128자)) — 장치와 RADIUS 서버 간의 모든 RADIUS 통신을 인증 및 암호화하는 데 사용되는 키 문자열입니다. 이 키는 RADIUS 암호화와 일치해야 합니다. 호스트별 값을 지정하지 않은 경우 전역 값이 각 호스트에 적용됩니다. 사용자 정의 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Source IP Address(소스 IP 주소) — RADIUS 서버에 액세스하는 장치의 IP 주소입니다. 사용자 정의 기본값을 사용하려면 Use Default(기본값 사용)를 선택합니다.

Usage Type(사용 유형) — RADIUS 사용 유형을 선택하는 데 사용되는 드롭다운 상자입니다.

주: 이 페이지의 기본 매개변수는 사용자 정의됩니다.

Default Retries (1-10)(기본 재시도 횟수(1-10)) — 실패하기까지 RADIUS 서버로 전송되는 기본 요청 횟수입니다.

Default Timeout for Reply (1-30)(기본 응답 타임아웃(1-30)) — 타임아웃되기까지 장치가 RADIUS 서버의 응답을 기다리는 기본 시간(초)입니다. 가능한 필드 값은 1 ~ 30입니다.

Default Deadtime (0-2000)(기본 우회 시간(0-2000)) — 서비스 요청에 대해 RADIUS 서버가 우회되는 기본 시간(분)을 지정합니다. 범위는 0 ~ 2000입니다.

Default Key String (0-128 Characters)(기본 키 문자열(0-128자)) — 장치와 RADIUS 서버 간의 모든 RADIUS 통신을 인증 및 암호화하는 데 사용되는 기본 키 문자열입니다. 이 키는 RADIUS 암호화와 일치해야 합니다.

Source IP Address(소스 IP 주소) — RADIUS 서버에 액세스하는 장치의 기본 IP 주소입니다.

RADIUS 서버 추가

1. RADIUS Settings(RADIUS 설정) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add RADIUS Server(RADIUS 서버 추가) 페이지가 표시됩니다.

그림 6-52. Add RADIUS Server(RADIUS 서버 추가)

Apply Changes Back

3. 대화상자에서 필드를 정의합니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

새 RADIUS 서버가 추가되고 장치가 업데이트됩니다.

RADIUS 매개변수 정의

1. RADIUS Settings(RADIUS 설정) 페이지를 엽니다.

2. 대화상자에서 필드를 정의합니다.

3. Apply Changes(변경사항 적용)를 클릭합니다.

RADIUS 설정이 장치에 업데이트됩니다.

RADIUS 서버 설정 수정

1. RADIUS Settings(RADIUS 설정) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

RADIUS Servers Table(RADIUS 서버 표)이 표시됩니다.

그림 6-53. RADIUS Servers Table(RADIUS 서버 표)

IP Address	Priority	Authentication Port	Number of Retries	Timeout For Reply (sec)	Deadtime (min)	Source IP Address	Usage Type	Remove
1 10.240.10.13	2	23	45	56	3	10.240.13.45	Login	Edit
2 10.240.10.40	4	25	34	53	2	10.240.13.15	Login	Edit
3 10.240.10.14	2	23	43	57	1	10.240.13.45	Login	Edit

Apply Changes Back

3. 선택한 항목에 대해 Edit(편집)를 클릭합니다.

4. RADIUS Settings(RADIUS 설정) 페이지에서 RADIUS 서버의 설정을 변경합니다.

5. Apply Changes(변경사항 적용)를 클릭합니다.

RADIUS 서버 설정이 수정되고 장치가 업데이트됩니다.

RADIUS 서버 목록에서 RADIUS 서버 제거

1. RADIUS Settings(RADIUS 설정) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

RADIUS Servers Table(RADIUS 서버 표)이 표시됩니다.

3. RADIUS 서버를 선택하고 Remove(제거)를 선택합니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

RADIUS 서버가 목록에서 제거됩니다.

CLI 명령을 사용하여 RADIUS 서버 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

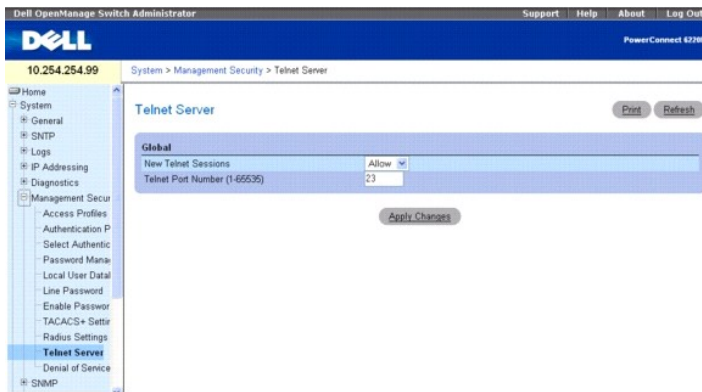
- 1 RADIUS 명령

텔넷 서버

Telnet Server(텔넷 서버) 페이지를 사용하여 스위치의 텔넷 서비스를 활성화 또는 비활성화하거나 텔넷 포트를 수정합니다.

Telnet Server(텔넷 서버) 페이지를 표시하려면 System(시스템)→ Management Security(관리 보안)→ Telnet Server(텔넷 서버)를 클릭합니다.

그림 6-54. Telnet Servers(텔넷 서버)



Telnet Server(텔넷 서버) 페이지에는 다음 필드가 있습니다.

New Telnet Sessions(새 텔넷 세션) — 인바운드 텔넷 세션의 관리 모드를 제어합니다. 모드를 Block(블록)으로 설정하면 새 텔넷 세션은 허용되지 않지만 기존 세션에는 아무런 문제가 없습니다. 기본값은 Allow(허용)입니다.

Telnet Port Number(텔넷 포트 번호) — 텔넷 세션이 시작되는 포트 번호입니다. 스위치의 새 인바운드 텔넷 세션에 대해 이 포트가 사용됩니다. 텔넷 서버 포트를 수정하면 새 인바운드 텔넷 세션은 새 포트를 사용하고 기존 텔넷 세션에는 아무런 영향이 없습니다.

텔넷 서버 설정 수정

1. Telnet Server Configuration(텔넷 서버 구성) 페이지를 엽니다.

2. 관련 필드를 구성합니다.

3. Apply Changes(변경사항 적용)를 클릭합니다.

설정이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 텔넷 서버 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 텔넷 서버 명령

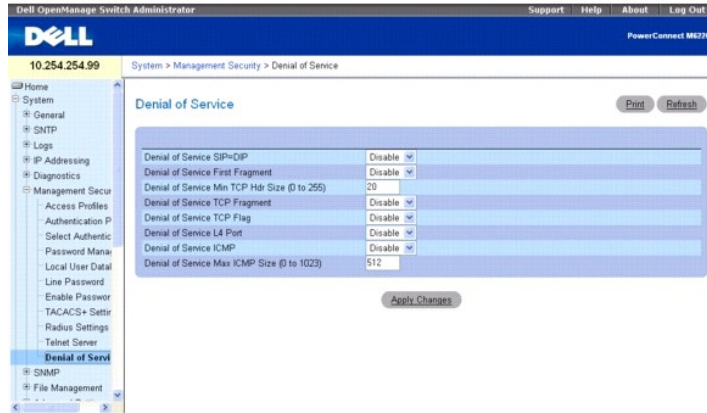
서비스 거부

Denial of Service(서비스 거부)는 호스트의 서비스를 방해하거나 네트워크를 불안정하게 만드는 여러 가지 취약성을 이용해 발생합니다. Denial of Service(서비스 거

부) 페이지를 사용하여 서비스 거부 공격을 방지하도록 설정을 구성합니다.

Denial of Service(서비스 거부) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → Management Security(관리 보안) → Denial of Service(서비스 거부)를 클릭합니다.

그림 6-55. Denial of Service(서비스 거부)



Denial of Service(서비스 거부) 페이지에는 다음과 같은 필드가 있습니다.

Denial of Service SIP=DIP(서비스 거부 SIP=DIP) — SIP=DIP DoS 방지를 활성화하면 대상 IP 주소와 동일한 소스 IP 주소를 가진 패킷이 스위치에서 삭제됩니다.

Denial of Service First Fragment(서비스 거부 처음 조각화) — 처음 조각화 DoS 방지를 활성화하면 구성된 최소 TCP 헤더 크기(Min TCP Hdr Size)보다 작은 TCP 헤더를 가진 패킷이 스위치에서 삭제됩니다.

Denial of Service Min TCP Hdr Size(서비스 거부 최소 TCP 헤더 크기) — 허용할 최소 TCP 헤더 크기를 지정합니다. 처음 조각화 DoS 방지를 활성화하면 이 구성된 값보다 작은 TCP 헤더 크기를 가진 패킷이 스위치에서 삭제됩니다.

Denial of Service TCP Fragment(서비스 거부 TCP 조각화) — TCP 조각화 DoS 방지를 활성화하면 1과 동일한 IP 조각 오프셋을 가진 패킷이 스위치에서 삭제됩니다.

Denial of Service TCP Flag(서비스 거부 TCP 플래그) — TCP 플래그 DoS 방지를 활성화하면 다음 조건 중 어느 하나에 만족하는 경우 패킷이 스위치에서 삭제됩니다.

- 1 TCP 플래그 SYN 설정 및 1024 미만의 TCP 소스 포트
- 1 0으로 설정된 TCP 제어 플래그 및 0으로 설정된 TCP 순서 번호
- 1 TCP 플래그 FIN, URG 및 PSH 설정 및 0으로 설정된 TCP 순서 번호
- 1 양 TCP 플래그 SYN 및 FIN 설정

Denial of Service L4 Port(서비스 거부 L4 포트) — L4 포트 DoS 방지를 활성화하면 TCP/UDP 대상 포트와 동일한 TCP/UDP 소스 포트를 가진 패킷이 스위치에서 삭제됩니다.

Denial of Service ICMP(서비스 거부 ICMP) — ICMP DoS 방지를 활성화하면 구성된 ICMP 패킷 크기(ICMP Pkt Size)보다 크고 ECHO_REQ(ping)로 설정된 유형을 가진 ICMP 패킷이 스위치에서 삭제됩니다.

Denial of Service Max ICMP Pkt Size(서비스 거부 최대 ICMP 패킷 크기) — 허용할 최대 ICMP 패킷 크기를 지정합니다. ICMP DoS 방지를 활성화하면 이 구성된 값보다 큰 크기의 ICMP ping 패킷이 스위치에서 삭제됩니다.

서비스 거부 설정 구성

1. Denial of Service(서비스 거부) 페이지를 엽니다.
2. 원하는 설정을 지정합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

장치가 새 설정으로 업데이트됩니다.

CLI 명령을 사용하여 서비스 거부 설정 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 서비스 거부 명령

SNMP 매개변수 정의

SNMP(Simple Network Management Protocol)는 네트워크 장치 관리 방법을 제공합니다. 장치는 SNMP 버전 1, SNMP 버전 2 및 SNMP 버전 3을 지원합니다.

주: 기본적으로 SNMPv2는 장치에서 자동으로 활성화됩니다. SNMPv3을 활성화하려면 장치에 대해 로컬 엔진 ID를 정의해야 합니다. 로컬 엔진 ID는 기본적으로 스위치 MAC 주소로 설정되지만, 스위치가 스택형 모드로 작동하는 경우 스택에 대한 로컬 엔진 ID를 수동으로 구성해야 합니다. 이 로컬 엔진 ID는 네트워크에서 고유하도록 정의해야 합니다. 스택 내의 기본 엔진 ID는 마스터 장치의 MAC 주소인데, 마스터 장치에서 오류가 발생하여 다른 장치가 스택을 처리할 경우 MAC 주소가 변경될 수 있으므로 이렇게 작업하는 것이 중요합니다. 로컬 엔진 ID 구성 방법에 대한 자세한 내용은 "[SNMP 전역 매개변수](#)"를 참조하십시오.

SNMP v1 및 v2

SNMP 에이전트는 장치 관리에 사용되는 변수 목록을 유지 관리합니다. 변수는 MIB(Management Information Base)에 정의되어 있습니다. MIB는 에이전트가 제어하는 변수를 표시합니다. SNMP 에이전트는 MIB 사양 형식과 네트워크 정보에 액세스할 때 사용되는 형식을 정의합니다. SNMP 에이전트에 대한 액세스 권한은 액세스 문자열에 의해 제어됩니다.

SNMP v3

SNMP v3에서도 SNMPv1 및 SNMPv2 PDU에 액세스 제어와 세 트랩 메커니즘을 적용합니다. 뿐만 아니라 SNMPv3에 대해 정의된 사용자 보안 모델(USM)에는 다음이 포함됩니다.

- 1 Authentication(인증) — 데이터 무결성과 데이터 출처 인증을 제공합니다.
- 1 Privacy(개인 정보 보호) — 메시지 내용의 공개를 방지합니다. 암호화를 위해 CBC(Cipher-Block-Chaining)가 사용됩니다. SNMP 메시지에 대해 인증이 활성화되거나, SNMP 메시지에 대해 인증과 개인 정보 보호가 모두 활성화됩니다. 그러나 인증을 활성화하지 않고 개인 정보 보호를 활성화할 수는 없습니다.
- 1 Timeliness(적시성) — 메시지 지연 또는 메시지 중복을 방지합니다. SNMP 에이전트는 수신되는 메시지를 메시지 시간 정보와 비교합니다.
- 1 Key Management(키 관리) — 키 생성, 키 업데이트 및 키 사용을 정의합니다.

장치는 개체 ID(OID)를 기준으로 하는 SNMP 알림 필터를 지원합니다. OID는 시스템에서 장치 기능을 관리하는 데 사용됩니다. SNMP v3은 다음 기능을 지원합니다.

- 1 보안
- 1 기능 액세스 제어
- 1 트랩

인증 또는 개인 정보 보호 키는 SNMPv3 사용자 보안 모델(USM)에서 수정됩니다.

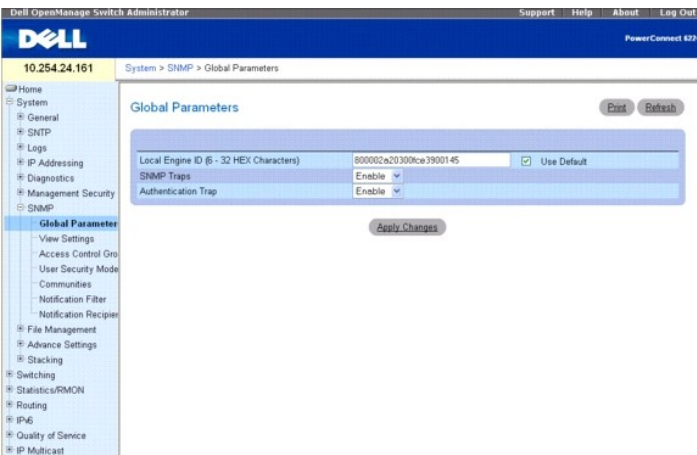
SNMP 페이지를 사용하여 SNMP 매개변수를 정의할 수 있습니다. SNMP 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → SNMP를 클릭합니다.

SNMP 전역 매개변수

Global Parameters(전역 매개변수) 페이지를 사용하여 SNMP 및 인증 알림을 활성화할 수 있습니다.

Global Parameters(전역 매개변수) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → SNMP → Global Parameters(전역 매개변수)를 클릭합니다.

그림 6-56. Global Parameters(전역 매개변수)



Global Parameters(전역 매개변수) 페이지에는 다음 매개변수가 있습니다.

Local Engine ID (6 - 32 hexadecimal characters)(로컬 엔진 ID(16진수 6 - 32자)) — 로컬 SNMP 엔진 ID를 설정합니다.

Use Default(기본값 사용) — 기본 SNMP 엔진 ID를 사용하도록 장치를 구성합니다.

SNMP Traps(SNMP 트랩) — 장치의 SNMP 알림 전송을 활성화하거나 비활성화합니다.

Authentication Trap(인증 트랩) — 인증이 실패한 경우 장치의 SNMP 트랩 전송을 활성화하거나 비활성화합니다.

로컬 SNMP 엔진 ID 설정

1. Global Parameters(전역 매개변수) 페이지를 엽니다.
2. Local Engine ID(로컬 엔진 ID) 필드에 원하는 16진수 ID를 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.
새 로컬 엔진 ID가 설정되고 장치가 업데이트됩니다.

기본 SNMP 엔진 ID 사용

1. Global Parameters(전역 매개변수) 페이지를 엽니다.
2. Use Default(기본값 사용) 확인란을 클릭합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.
MAC 주소를 기준으로 하는 기본 SNMP 엔진 ID가 생성되고 장치가 업데이트됩니다.

SNMP 트랩 활성화

1. Global Parameters(전역 매개변수) 페이지를 엽니다.
2. SNMP Traps(SNMP 트랩) 필드에서 Enable(활성)을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.
SNMP 알림이 활성화되고 장치가 업데이트됩니다.

인증 트랩 활성화

1. Global Parameters(전역 매개변수) 페이지를 엽니다.
2. Authentication trap(인증 트랩) 필드에서 Enable(활성)을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.
인증 알림이 활성화되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 알림 활성화

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. SNMP 명령

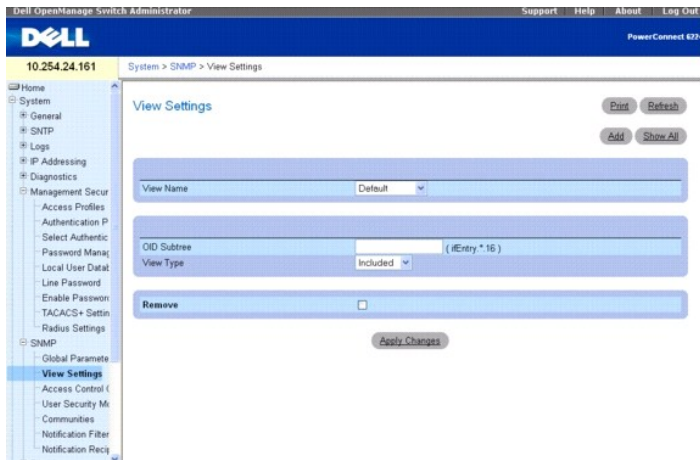
SNMP 보기 설정

이 페이지를 사용하여 액세스할 수 있는 장치 기능 및 차단되는 장치 기능을 정의하는 보기를 만들 수 있습니다. 인터페이스에 해당하는 OID가 포함되어 있거나 제외된 보기를 만들 수 있습니다.

SNMP View Settings(SNMP 보기 설정) 페이지를 사용하여 SNMP 보기를 정의할 수 있습니다.

SNMP View Settings(SNMP 보기 설정) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→SNMP→View Settings(보기 설정)를 클릭합니다.

그림 6-57. SNMP View Settings(SNMP 보기 설정)



SNMP View Settings(SNMP 보기 설정) 페이지에는 다음 필드가 있습니다.

View Name(보기 이름) — 사용자 정의 보기 목록을 포함합니다. 보기 이름은 최대 30자의 영숫자 문자를 포함할 수 있습니다.

OID Subtree(OID 하위 트리) — * 등의 메타 문자를 포함할 수 있는 유효한 SNMP OID 문자열을 지정합니다.

View Type(보기 유형) — 보기에 개체 ID를 포함할지 또는 제외할지 지정합니다.

Remove(제거) — 표시된 보기 유형을 제거하려면 선택합니다.

보기 추가

1. SNMP View Settings(SNMP 보기 설정) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add View(보기 추가) 페이지가 표시됩니다.

그림 6-58. Add View(보기 추가)



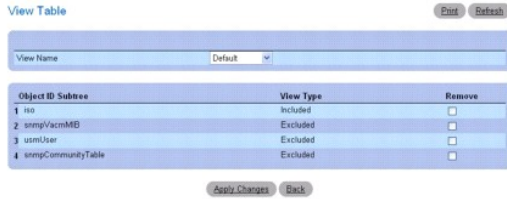
3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.
SNMP 보기가 추가되고 장치가 업데이트됩니다.

보기 표 표시

1. SNMP View Settings(SNMP 보기 설정) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

View Table(보기 표) 페이지가 표시됩니다.

그림 6-59. View Table(보기 표)



SNMP 보기 제거

1. SNMP View Settings(SNMP 보기 설정) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
View Table(보기 표) 페이지가 표시됩니다.
3. SNMP 보기를 선택합니다.
4. Remove(제거) 확인란을 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭하십시오.
SNMP 보기가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 보기 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

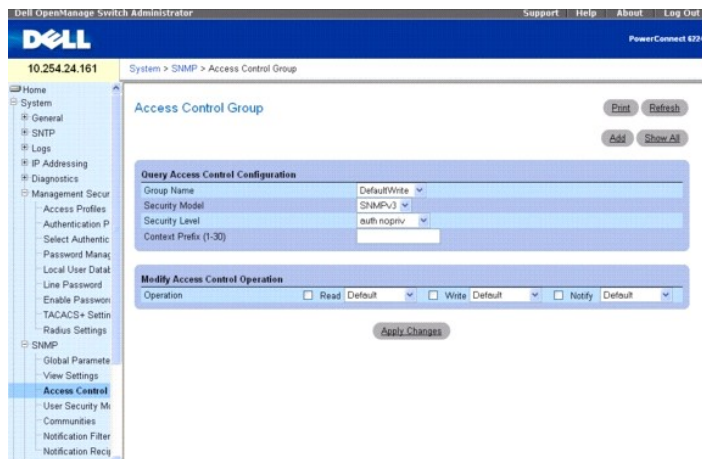
1. SNMP 명령

액세스 제어 그룹

Access Control Group(액세스 제어 그룹) 페이지를 사용하여 SNMP 그룹 만들기에 대한 정보를 보고 SNMP 액세스 권한을 할당할 수 있습니다. 그룹을 사용하면 네트워크 관리자가 특정 장치 기능이나 기능 부분에 액세스 권한을 할당할 수 있습니다.

Access Control Group(액세스 제어 그룹) 페이지를 표시하려면 *디렉터리 화면*에서 System(시스템)→SNMP→Access Control Group(액세스 제어 그룹)을 클릭합니다.

그림 6-60. Access Control Group(액세스 제어 그룹)



Access Control Group(액세스 제어 그룹) 페이지에는 다음 필드가 있습니다.

Group Name(그룹 이름) — 액세스 제어 규칙이 적용되는 사용자 정의 그룹 목록을 포함합니다. 그룹 이름은 최대 30자의 영숫자 문자를 포함할 수 있습니다.

Security Model(보안 모델) — 그룹에 연결된 SNMP 버전을 정의합니다. 가능한 필드 값은 다음과 같습니다.

SNMPv1 — 그룹에 대해 SNMPv1이 정의됩니다.

SNMPv2 — 그룹에 대해 SNMPv2가 정의됩니다.

SNMPv3 — 그룹에 대해 SNMPv3 사용자 보안 모델(USM)이 정의됩니다.

Security Level(보안 레벨) — 그룹에 연결된 보안 레벨입니다. 보안 레벨은 SNMPv3 그룹에만 적용됩니다. 가능한 필드 값은 다음과 같습니다.

noauth nopriv(인증 없음/개인 정보 보호 없음) — 그룹에 Authentication(인증) 및 Privacy(개인 정보 보호) 보안 레벨이 모두 지정되지 않습니다.

auth nopriv(인증/개인 정보 보호 없음) — SNMP 메시지를 암호화하지 않고 인증합니다.

auth priv(인증/개인 정보 보호) — SNMP 메시지를 암호화하고 인증합니다.

Context Prefix (1-30)(Context 접두어(1-30)) — 이 필드에 Context 이름의 처음 1 ~ 30자를 입력하여 Context 이름을 지정합니다.

Operation(작업) — 그룹 액세스 권한을 정의합니다. 가능한 필드 값은 다음과 같습니다.

Read(읽기) — 관리 액세스를 에이전트 내용 보기로 제한하는 보기를 선택합니다. 보기를 선택하지 않은 경우 community-table, SNMPv3 사용자 및 액세스 테이블을 제외한 모든 개체를 볼 수 있습니다.

Write(쓰기) — 에이전트 내용에 대한 관리 읽기-쓰기 권한을 허용하는 보기를 선택합니다.

Notify(알림) — SNMP 트랩 전송을 허용하거나 알리는 보기를 선택합니다.

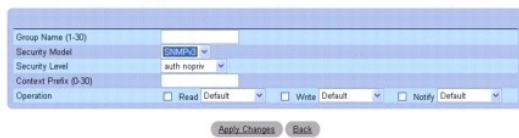
SNMP 그룹 추가

1. Access Control Configuration(액세스 제어 구성) 페이지를 엽니다.

2. Add(추가)를 클릭합니다.

Add an Access Control Configuration(액세스 제어 구성 추가) 페이지가 표시됩니다.

그림 6-61. Add an Access Control Configuration(액세스 제어 구성 추가)



3. 필요에 따라 필드를 정의합니다.

4. Apply Changes(변경사항 적용)를 클릭하십시오.

그룹이 추가되고 장치가 업데이트됩니다.

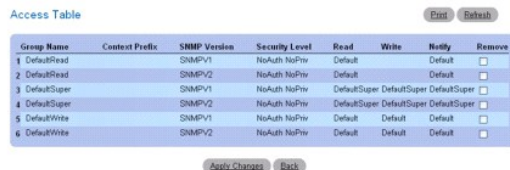
액세스 표 표시

1. Access Control Configuration(액세스 제어 구성) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

Access Table(액세스 표) 페이지가 표시됩니다.

그림 6-62. Access Table(액세스 표)



Group Name	Context Prefix	SNMP Version	Security Level	Read	Write	Notify	Remove
1 DefaultRead		SNMPv1	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
2 DefaultRead		SNMPv2	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
3 DefaultSuper		SNMPv1	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
4 DefaultSuper		SNMPv2	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
5 DefaultWrite		SNMPv1	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
6 DefaultWrite		SNMPv2	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>

그룹 제거

1. Access Control Configuration(액세스 제어 구성) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Access Table(액세스 표)이 열립니다.
3. 그룹을 선택합니다.
4. Remove(제거)를 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭하십시오.
그룹이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 액세스 제어 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

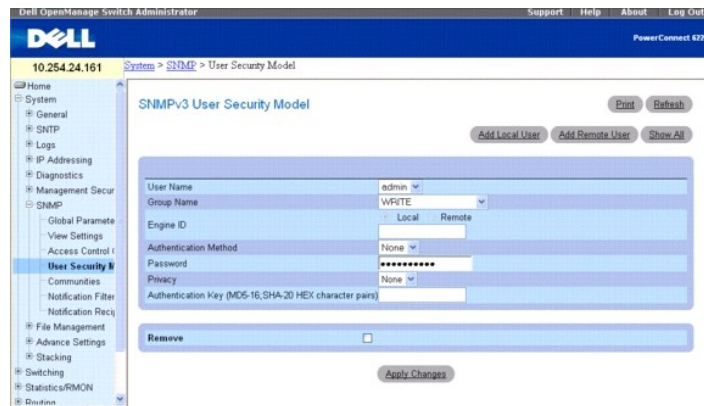
1. SNMP 명령

SNMPv3 사용자 보안 모델(USM)

SNMPv3 User Security Model (USM)(사용자 보안 모델(USM)) 페이지를 사용하여 SNMP 그룹에 시스템 사용자를 할당하고 사용자 인증 방법을 정의할 수 있습니다.

SNMPv3 User Security Model (USM)(사용자 보안 모델(USM)) 페이지를 표시하려면 *디렉터리 화면*에서 System(시스템)→SNMP→User Security Model(사용자 보안 모델)을 클릭합니다.

그림 6-63. SNMPv3 User Security Model (USM)(사용자 보안 모델(USM))



SNMPv3 User Security Model (USM)(사용자 보안 모델(USM)) 페이지에는 다음 필드가 있습니다.

User Name(사용자 이름) — 사용자 정의 사용자 이름 목록을 포함합니다.

Group Name(그룹 이름) — 사용자 정의 SNMP 그룹 목록을 포함합니다. SNMP 그룹은 Access Control Group(액세스 제어 그룹) 페이지에서 정의됩니다.

Engine ID(엔진 ID) — 선택한 사용자를 로컬 SNMPv3 사용 장치에 연결할지 또는 지정한 원격 SNMPv3 사용 장치에 연결할지 선택합니다.

Remote Engine ID(원격 엔진 ID) — 사용자가 원격 SNMPv3 사용 장치에서 구성되었음을 나타냅니다.

Authentication Method(인증 방법) — 사용자 인증에 사용되는 인증 방법을 지정합니다. 가능한 필드 값은 다음과 같습니다.

None(없음) — 사용자 인증이 사용되지 않습니다.

MD5 — HMAC-MD5-96 인증 레벨을 사용하여 사용자를 인증합니다. 사용자가 암호를 지정해야 합니다.

SHA — HMAC-SHA-96 인증 레벨을 사용하여 사용자를 인증합니다. 사용자가 암호를 입력해야 합니다.

Password(암호) — 그룹에 대해 사용자 정의된 암호를 수정합니다. 암호는 최대 32자를 포함할 수 있습니다. 암호는 인증 방법이 MD5 또는 SHA 암호인 경우에만 정의됩니다. Add Local User(로컬 사용자 추가) 페이지에서 암호를 정의합니다.

Privacy(개인 정보 보호) — 인증 키의 사용 여부를 지정합니다. 다음 값 중 하나를 선택하십시오.

None(없음) — 인증 키를 사용하지 않습니다.

des — 인증 키에 대해 CBS-DES Symantec 암호화 암호를 사용합니다.

des-key — 미리 생성된 HMAC-MD5-96 인증 키를 사용합니다.

Authentication Key(MD5-16; SHA-20 HEX character pairs)(인증 키(MD5-16; SHA-20 HEX 문자 쌍)) — 인증 키를 지정합니다. 인증 키는 인증 방법이 MD5 또는 SHA 인 경우에만 정의됩니다.

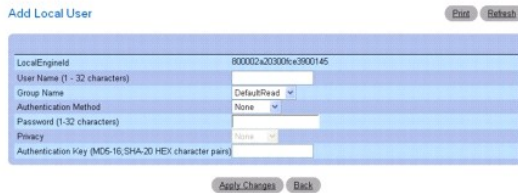
Remove(제거) — 선택하면 지정한 그룹에서 지정한 사용자를 제거합니다.

그룹에 SNMPv3 로컬 사용자 추가

1. SNMPv3 User Security Model(SNMPv3 사용자 보안 모델) 페이지를 엽니다.
2. Add Local User(로컬 사용자 추가)를 클릭합니다.

Add Local User(로컬 사용자 추가) 페이지가 표시됩니다.

그림 6-64. Add Local User(로컬 사용자 추가)



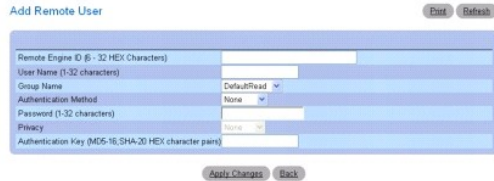
3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.
5. 사용자가 그룹에 추가되고 장치가 업데이트됩니다.

그룹에 SNMPv3 원격 사용자 추가

1. SNMPv3 User Security Model(SNMPv3 사용자 보안 모델) 페이지를 엽니다.
2. Add Remote User(원격 사용자 추가)를 클릭합니다.

Add Remote User(원격 사용자 추가) 페이지가 표시됩니다.

그림 6-65. Add Remote User(원격 사용자 추가)



3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.
5. 사용자가 그룹에 추가되고 장치가 업데이트됩니다.

사용자 보안 모델 표 보기

1. SNMPv3 User Security Model (USM)(SNMPv3 사용자 보안 모델(USM)) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

User Security Model Table(사용자 보안 모델 표)이 표시됩니다.

그림 6-66. User Security Model Table(사용자 보안 모델 표)

User Name	Group Name	Remote Engine ID	Authentication	Remove
1 Admin	DefaultRead	800002a203006e4900145	NONE	<input type="checkbox"/>
2 pippin	DefaultRead	800002a203006e4900145	NONE	<input type="checkbox"/>
3 gandalf	DefaultRead	800002a203006e4900145	NONE	<input type="checkbox"/>

User Security Model Table(사용자 보안 모델 표) 항목 제거

1. User Security Model(사용자 보안 모델) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
- User Security Model Table(사용자 보안 모델 표) 페이지가 표시됩니다.
3. 항목을 선택합니다.
4. Remove(제거) 확인란을 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭하십시오.

항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 사용자 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. SNMP 명령

커뮤니티

액세스 권한은 SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지에서 커뮤니티를 정의하여 관리합니다. 커뮤니티 이름을 변경하면 액세스 권한도 변경됩니다. SNMP 커뮤니티는 SNMP v1 및 SNMP v2에 대해서만 정의됩니다.

SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→SNMP→Communities(커뮤니티)를 클릭합니다.

그림 6-67. SNMPv1, 2 Community(SNMPv1, 2 커뮤니티)

SNMPv1, 2 Community 페이지에는 다음 필드가 있습니다.

Community String(커뮤니티 문자열) — 암호 역할을 하며 SNMP 관리 스테이션을 장치에 인증하는 데 사용되는 사용자 정의 커뮤니티 문자열 목록을 포함합니다. 커뮤니티 문자열은 최대 20자를 포함할 수 있습니다.

SNMP Management Station(SNMP 관리 스테이션) — 커뮤니티 문자열이 정의된 관리 스테이션 IP 주소 목록을 포함합니다.

Basic(기본) — 선택한 커뮤니티에 대해 SNMP 기본 모드를 활성화합니다. 가능한 필드 값은 다음과 같습니다.

Access Mode(엑세스 모드) — 커뮤니티의 액세스 권한을 정의합니다. 가능한 필드 값은 다음과 같습니다.

Read-Only(읽기 전용) — 보기에 구성된 MIB 개체에 대해 커뮤니티에 읽기 전용 권한이 있습니다.

Read-Write(읽기-쓰기) — 보기에 구성된 MIB 개체에 대해 커뮤니티에 읽기/수정 권한이 있습니다.

Super User(수퍼 사용자) — 모든 MIB 개체에 대해 커뮤니티에 읽기/수정 권한이 있습니다.

View Name(보기 이름) — 사용자 정의 SNMP 보기 목록을 포함합니다.

Advanced(고급) — 사용자 정의 그룹 목록을 포함합니다. SNMP 고급 모드를 선택하면 그룹을 구성하는 SNMP 액세스 제어 규칙이 선택한 커뮤니티에 대해 활성화됩니다. 또한 고급 모드는 특정 SNMP 커뮤니티에 대해 SNMP 그룹을 활성화합니다. SNMP 고급 모드는 SNMPv3에서만 정의됩니다.

Remove(제거) — 선택하면 커뮤니티를 제거합니다.

새 커뮤니티 추가

1. SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지를 엽니다.

2. Add(추가)를 클릭합니다.

Add SNMPv1,2 Community(SNMPv1, 2 커뮤니티 추가) 페이지가 표시됩니다.

그림 6-68. Add SNMPv1,2 Community(SNMPv1,2 커뮤니티 추가)

3. 관련 필드를 입력합니다.

SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지의 필드 외에도 Add SNMPv1,2 Community(SNMPv1,2 커뮤니티 추가) 페이지에는 모든 관리 스테이션에서 커뮤니티를 사용할 수 있음을 나타내는 All(0.0.0.0)(모두(0.0.0.0)) 필드가 있습니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

새 커뮤니티가 저장되고 장치가 업데이트됩니다.

커뮤니티 표시

1. SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

Basic Table(기본 표) 페이지가 표시됩니다.

그림 6-69. Basic Table(기본 표)

Basic Table [Print] [Refresh]

Management Station	Community String	Access Mode	View Mode	Remove
1 All	private	Read Only	Default	<input type="checkbox"/>
2 All	public	Read Write	Default	<input type="checkbox"/>

Advanced Table

Community String	Management Station	Group Name
1 private	All	DefaultRead
2 public	All	DefaultWrite

[Apply Changes] [Back]

커뮤니티 제거

1. SNMPv1, 2 Community(SNMPv1, 2 커뮤니티) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Basic Table(기본 표)페이지가 표시됩니다.
3. 커뮤니티를 선택하고 Remove(제거) 확인란을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
커뮤니티 항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 커뮤니티 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- n SNMP 명령

알림 필터

Notification Filter(알림 필터) 페이지를 사용하여 OID를 기준으로 필터링 트랩을 설정할 수 있습니다. 각 OID는 장치 기능이나 기능 부분에 연결되어 있습니다. Notification Filter(알림 필터) 페이지에서 알림을 필터링할 수도 있습니다.

Notification Filter(알림 필터) 페이지를 표시하려면 *다렉터리 화면*에서 System(시스템)→SNMP→Notification Filters(알림 필터)를 클릭합니다.

그림 6-70. Notification Filter(알림 필터)

Notification Filter(알림 필터) 페이지에는 다음 필드가 있습니다.

Notification Filter Name(알림 필터 이름) — 사용자 정의 알림 필터 목록을 포함합니다. 알림 필터 이름은 최대 30자를 포함할 수 있습니다.

New Object Identifier Tree(새 개체 식별자 트리) — 선택한 필터에 대해 구성된 OID를 표시합니다. 이 필드는 편집할 수 있습니다.

Filter Type(필터 유형) — OID와 관련해서 알림이나 트랩을 트랩 수신자에게 보낼지 여부를 나타냅니다.

Excluded(제외됨) — OID 트랩 또는 알림 전송을 제한합니다.

Included(포함됨) — OID 트랩 또는 알림을 보냅니다.

SNMP 필터 추가

1. Notification Filter(알림 필터) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.
Add Filter(필터 추가) 페이지가 표시됩니다.

그림 6-71. Add Filter(필터 추가)

Filter Name (1-30 characters)	Useofilter
New Object Identifier Tree	1.3.6.3.2.1.1.7
Filter Type	Included

3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.
새 필터가 추가되고 장치가 업데이트됩니다.

필터 표 표시

1. Notification Filter(알림 필터) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
선택한 필터 이름에 대해 구성된 모든 필터를 보여 주는 Filter Table(필터 표) 페이지가 표시됩니다.

그림 6-72. Show Notification(알림 표시)

Object ID Subtree	Filter Type	Remove
-------------------	-------------	--------

필터 제거

1. Notification Filter(알림 필터) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Show Notification(알림 표시) 페이지가 표시됩니다.
3. Filter Table(필터 표) 항목을 선택합니다.
4. Remove(제거)를 선택합니다.
필터 항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 알림 필터 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 SNMP 명령

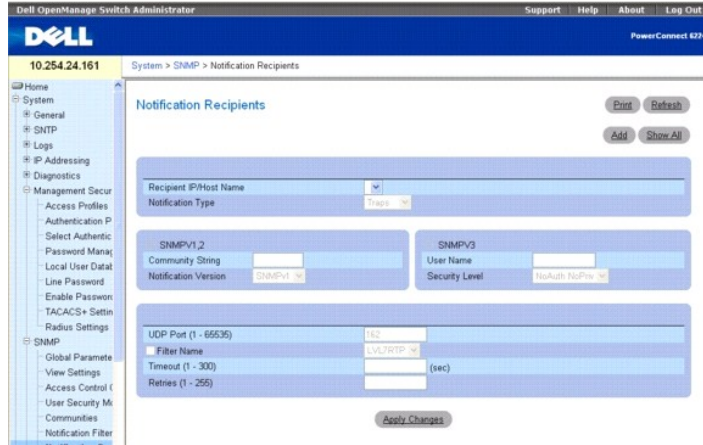
알림 수신자

Notification Recipients(알림 수신자) 페이지를 사용하여 특정 사용자에게 트랩을 보낼지 여부 및 전송되는 트랩 유형을 결정하는 필터 정의에 대한 정보를 볼 수 있습니다. SNMP 알림 필터는 다음 서비스를 제공합니다.

- 1 관리 트랩 대상 식별
- 1 트랩 필터링
- 1 트랩 생성 매개변수 선택
- 1 액세스 제어 확인

Notification Recipients(알림 수신자) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→SNMP→Notification Recipients(알림 수신자)를 클릭합니다.

그림 6-73. Notification Recipients(알림 수신자)



Notification Recipients(알림 수신자) 페이지에는 다음 필드가 있습니다.

Recipient IP(수신자 IP) — 알림 수신자 IP 주소의 사용자 정의 목록을 포함합니다.

Notification Type(알림 유형) — 전송되는 알림 유형입니다. 가능한 필드 값은 다음과 같습니다.

- Trap(트랩) — 트랩이 전송됩니다.
- Inform(알림) — 알림이 전송됩니다.

SNMPv1,2 — 선택한 수신자에 대해 SNMP 버전 1 또는 2가 활성화됩니다. 가능한 필드 값은 다음과 같습니다.

- Community String(커뮤니티 문자열) — 알림과 함께 전송될 커뮤니티 문자열을 표시합니다.
- Notification Version(알림 버전) — 알림 버전을 결정합니다. 가능한 필드 값은 다음과 같습니다.

- SNMP V1 — SNMP 버전 1 트랩이 전송됩니다. Notification Type(알림 유형)으로 Inform(알림)을 선택하면 SNMPv1을 선택할 수 없습니다.
- SNMP V2 — SNMP 버전 2 트랩 또는 알림이 전송됩니다.

SNMPv3 — 선택한 수신자에 대해 SNMP 버전 3이 활성화됩니다. 가능한 필드 값은 다음과 같습니다.

- User Name(사용자 이름) — 알림을 생성하려면 기존 사용자를 선택합니다.
 - Security Level(보안 레벨) — 알림에 연결된 보안 레벨입니다. 가능한 필드 값은 다음과 같습니다.
- NoAu NoPriv(인증 없음/개인 정보 보호 없음) — 패킷이 인증 및 암호화되지 않습니다.
 - Auth NoPriv(인증/개인 정보 보호 없음) — 패킷이 인증됩니다.
 - Auth Priv(인증/개인 정보 보호) — 패킷이 인증 및 암호화됩니다.

UDP Port (1-65535)(UDP 포트(1-65535)) — 알림 전송에 사용되는 UDP 포트입니다. 기본값은 162입니다.

Filter Name(필터 이름) — 드롭다운 메뉴에서 선택한 사용자 정의 SNMP 필터를 알림에 적용하려면 이 확인란을 선택합니다.

Timeout (1-300)(타임아웃(1-300)) — 장치에서 알림을 다시 보내기까지 기다리는 시간(초)입니다. 기본값은 15초입니다.

Retries (1-255)(재시도(1-255)) — 장치에서 알림 요청을 다시 보내는 최대 횟수입니다. 기본값은 3입니다.

새 알림 수신자 추가

1. Notification Recipients(알림 수신자) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Notification Recipients(알림 수신자) 페이지가 표시됩니다.

그림 6-74. Add Notification Recipients(알림 수신자 추가)

3. 관련 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

알림 수신자가 추가되고 장치가 업데이트됩니다.

알림 수신자 표 표시

1. Notification Recipients(알림 수신자) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Notification Recipient Tables(알림 수신자 표) 페이지가 열립니다.

그림 6-75. Notification Recipient Tables(알림 수신자 표)

알림 수신자 제거

1. Notification Recipients(알림 수신자) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Notification Recipient Tables(알림 수신자 표) 페이지가 열립니다.

3. SNMPV1,2 Notification Recipient(SNMPV1,2 알림 수신자) 및/또는 SNMPV3 Notification Recipient Tables(SNMPV3 알림 수신자 표)에서 알림 수신자가 한 명 이상인 경우 Remove(제거) 확인란을 선택하십시오.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

수신자가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 SNMP 알림 수신자 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 SNMP 명령

파일 관리

File Management(파일 관리) 메뉴 페이지를 사용하여 장치 소프트웨어, 이미지 파일 및 구성 파일을 관리할 수 있습니다. TFTP 서버를 통해 파일을 다운로드하거나 업로드할 수 있습니다. 시스템은 두 가지 버전의 소프트웨어를 처리합니다. 이전 소프트웨어 버전을 실행하는 시스템은 최신 소프트웨어 버전으로 만든 구성 파일을 무시(로드하지 않음)합니다. 이전 소프트웨어 버전을 실행하는 시스템이 최신 소프트웨어 버전으로 만든 구성 파일을 발견하면 사용자에게 해당 경고가 표시됩니다.

관리 파일 개요

관리 파일 구조는 다음 파일로 이루어져 있습니다.

- 1 Startup configuration file(시작 구성 파일) — 장치 전원을 끄거나 재부팅할 때 정확한 장치 구성을 유지합니다. 시작 파일은 구성 명령을 유지 관리하며, 실행 구성 파일의 구성 명령을 시작 파일에 저장할 수 있습니다.
- 1 Running configuration file(실행 구성 파일) — 모든 시작 파일 명령과 현재 세션 중에 입력된 모든 명령을 포함합니다. 장치 전원을 끄거나 재부팅하면 실행 구성 파일에 저장된 모든 명령이 손실됩니다. 시작 프로세스 중에 시작 파일에 있는 모든 명령이 실행 구성 파일에 복사되고 장치에 적용됩니다. 세션 중에 입력된 모든 새 명령은 실행 구성 파일에 있는 명령에 추가되며 명령을 덮어쓰지 않습니다. 시작 파일을 업데이트하려면 장치 전원을 끄기 전에 실행 구성 파일을 시작 구성 파일에 복사해야 합니다. 다음에 장치를 다시 시작하면 명령이 시작 구성 파일에서 실행 구성 파일로 다시 복사됩니다.
- 1 Backup Configuration File(백업 구성 파일) — 장치 구성의 백업 복사본을 포함합니다. 실행 구성 파일 또는 시작 파일을 백업 파일로 복사하면 백업 파일이 변경됩니다. 파일에 복사된 명령이 백업 파일에 저장된 기존 명령을 교체합니다. 백업 파일 내용을 실행 구성 파일 또는 시작 구성 파일로 복사할 수 있습니다. 원격 TFTP 서버에서 백업 파일 시작 파일로 복사하거나 백업 파일 및 시작 파일에서 원격 서버로 복사할 수도 있습니다.
- 1 Image Files(이미지 파일) — 시스템 이미지는 이미지(Image 1(이미지 1) 및 Image 2(이미지 2))라는 두 개의 플래시 섹터에 저장됩니다. 활성 이미지는 활성 복사본을 저장하고 다른 이미지는 보조 복사본을 저장합니다. 장치는 활성 이미지에서 부팅 및 실행됩니다. 활성 이미지가 손상되면 시스템이 자동으로 비활성 이미지에서 부팅됩니다. 이는 부팅 업그레이드 프로세스 중에 발생하는 장애에 대한 안전 기능입니다.

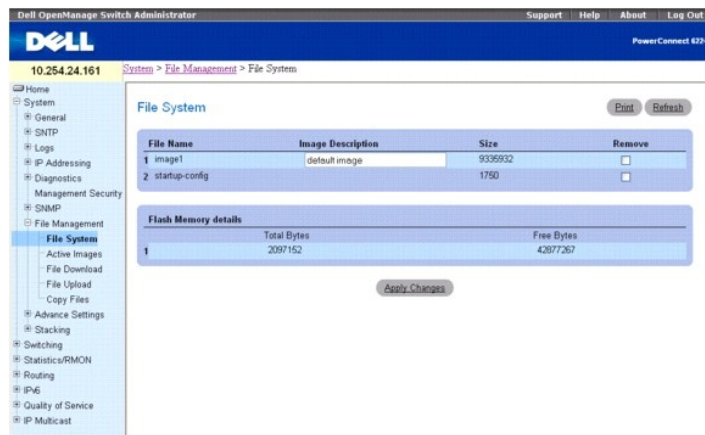
File Management(파일 관리) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → File Management(파일 관리)를 클릭합니다.

파일 시스템

File System(파일 시스템) 페이지를 사용하여 장치에 있는 파일 목록을 볼 수 있습니다.

File System(파일 시스템) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → File Management(파일 관리) → File System(파일 시스템)을 클릭합니다.

그림 6-76. File System(파일 시스템)



File System(파일 시스템) 페이지에는 다음 필드가 있습니다.

File Name(파일 이름) — 텍스트 필드에 파일 시스템에 있는 파일 이름이 나열됩니다.

Image Description (0-128)(이미지 설명(0-128)) — 이 필드를 사용하여 이미지의 설명을 구성하거나 표시할 수 있습니다. 설명은 128자 이내로 입력하십시오.

Size(크기) — 지정된 파일의 크기를 표시합니다.

Remove(제거) — 지정된 파일을 제거하려면 선택합니다.

Flash Memory Details(플래시 메모리 세부사항) — 플래시 메모리의 상태를 표시합니다.

Total Bytes(총 바이트) — 사용 중인 플래쉬 메모리 양을 표시합니다.

Free Bytes(사용 가능한 바이트) — 사용 가능한 플래쉬 메모리 양을 표시합니다.

파일 제거

1. File System(파일 시스템) 페이지를 엽니다.
2. File Name(파일 이름) 필드를 사용하여 제거할 파일을 선택합니다.
3. Remove(제거) 확인란을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

파일이 제거됩니다.

CLI 명령을 사용하여 파일 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

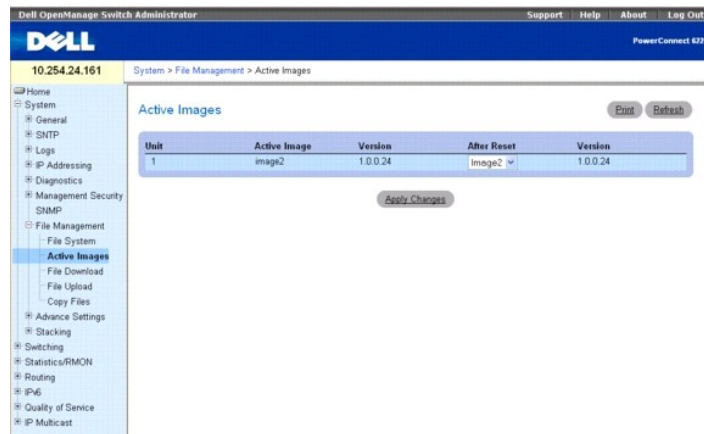
- 1 구성 및 이미지 파일 명령

활성 이미지

Active Images(활성 이미지) 페이지를 사용하여 부팅 이미지를 설정할 수 있습니다.

Active Images(활성 이미지) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→File Management(파일 관리)→Active Images(활성 이미지)를 클릭합니다.

그림 6-77. Active Images(활성 이미지)



Active Images(활성 이미지) 페이지에는 다음 필드가 있습니다.

Unit(장치) — 스택에 있는 시스템의 장치 수를 식별합니다.

Active Image(활성 이미지) — 현재 활성 이미지의 이름을 표시합니다.

Version(버전) — 현재 활성 이미지의 버전 번호를 표시합니다.

After Reset(재설정 후) — 드롭다운 메뉴에서 다음 재설정 후 활성화될 이미지를 선택합니다.

Version(버전) — 차후 재설정 이후에 활성화될 이미지의 버전 번호를 표시합니다.

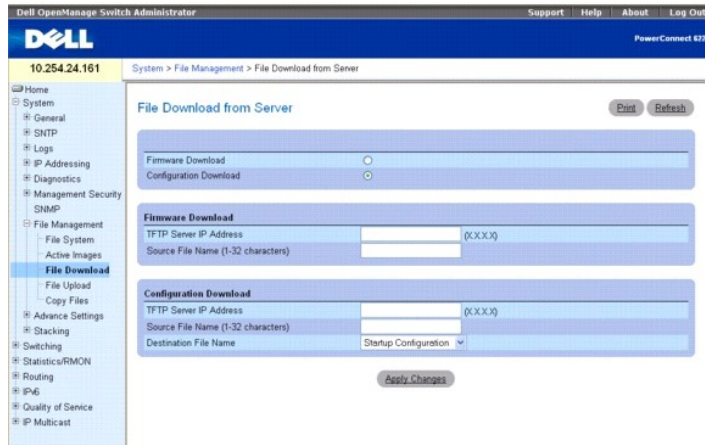
서버에서 파일 다운로드

File Download From Server(서버에서 파일 다운로드) 페이지를 사용하여 TFTP 서버의 구성(ASCII) 및 이미지(바이너리)를 장치로 다운로드할 수 있습니다.

File Download From Server(서버에서 파일 다운로드) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→File Management(파일 관리)→File Download

(파일 다운로드)를 클릭합니다.

그림 6-78. File Download From Server(서버에서 파일 다운로드)



File Download From Server(서버에서 파일 다운로드) 페이지에는 다음 필드가 있습니다.

Firmware Download(펌웨어 다운로드) — 선택하면 펌웨어 파일이 다운로드됨을 나타냅니다. 이 옵션을 선택하면 Configuration Download(구성 다운로드) 필드가 회색으로 표시됩니다.

Configuration Download(구성 다운로드) — 선택하면 구성 파일이 다운로드됨을 나타냅니다. Configuration Download(구성 다운로드)를 선택하면 Firmware Download(펌웨어 다운로드) 필드가 회색으로 표시됩니다.

펌웨어 다운로드

TFTP Server IP Address(TFTP 서버 IP 주소) — 다운로드할 펌웨어 파일이 있는 TFTP 서버 IP 주소입니다.

Source File Name (1 - 32 characters)(소스 파일 이름(1 - 32자)) — ftp 서버에 있는 파일 이름으로, tftpboot 디렉터리의 상대 경로로 표시됩니다. 예를 들어 원격 서버에서 TFTP가 구성되고 tftpboot 디렉터리가 e:\tftp이며 파일 test.scr 이 e:\tftp\latest\test.scr에 있는 경우 \latest\test.scr을 입력합니다.

구성 다운로드

TFTP Server IP Address(TFTP 서버 IP 주소) — 다운로드할 구성 파일이 있는 TFTP 서버 IP 주소입니다.

Source File Name (1 - 32 characters)(소스 파일 이름(1 - 32자)) — TFTP 서버에 있는 파일 이름입니다.


Destination File Name(대상 파일 이름) — 구성 파일로 다운로드되는 대상 파일입니다. 가능한 값은 다음과 같습니다.

Startup Configuration(시작 구성) — 시작 구성 파일을 다운로드합니다.

Backup Configuration(백업 구성) — 백업 구성 파일을 다운로드합니다.

파일 다운로드

1. File Download From Server(서버에서 파일 다운로드) 페이지를 엽니다.
2. TFTP 서버의 IP 주소를 확인하고 다운로드할 소프트웨어 이미지 또는 부팅 파일을 TFTP 서버에서 사용할 수 있는지 확인합니다.
3. TFTP Server IP Address(TFTP 서버 IP 주소) 및 Source File Name(소스 파일 이름)(TFTP 서버 IP 주소가 없는 전체 경로) 필드를 작성합니다.

 주: 활성 이미지를 덮어쓰지 않는 것이 좋습니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.


 주: 파일 다운로드를 시작하면 페이지가 새로 고쳐지고 전송 바이트 수를 표시하는 전송 상태 필드가 나타납니다. 파일 다운로드가 완료될 때까지 웹 인터페이스를 사용할 수 없습니다.

그림 6-79. File Download Progress(파일 다운로드 진행 상태)

0% — 50% — 100%	
Percent Complete	Upload Completed
TFTP Server IP Address	172.16.1.1
TFTP Path	/
TFTP Filename	07-06-04 dell_jos.stk
Data Type	Code
Local Filename	image

소프트웨어가 장치로 다운로드됩니다.

CLI 명령을 사용하여 파일 다운로드

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 구성 및 이미지 파일 명령

파일 업로드

File Upload to Server(서버로 파일 업로드) 페이지를 사용하여 장치의 구성(ASCII) 및 이미지(바이너리)를 TFTP 서버로 업로드할 수 있습니다.

File Upload to Server(서버로 파일 업로드) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → File Management(파일 관리) → File Upload(파일 업로드)를 클릭합니다.

그림 6-80. File Upload to Server(서버로 파일 업로드)

File Upload to Server(서버로 파일 업로드) 페이지에는 다음 필드가 있습니다.

Firmware Upload(펌웨어 업로드) — 펌웨어 파일이 업로드됨을 나타냅니다. Firmware Upload(펌웨어 업로드)를 선택하면 Configuration Upload(구성 업로드) 필드가 회색으로 표시됩니다.

Configuration Upload(구성 업로드) — 구성 파일이 업로드됨을 나타냅니다. Configuration Upload(구성 업로드)를 선택하면 Firmware Upload(펌웨어 업로드) 필드가 회색으로 표시됩니다.

소프트웨어 이미지 업로드

TFTP Server IP Address(TFTP 서버 IP 주소) — 소프트웨어 이미지가 업로드되는 TFTP 서버 IP 주소입니다.

Destination File Name (1 - 32 characters)(대상 파일 이름(1 - 32자)) — 파일이 업로드된 이후에 갖게 되는 이름입니다.

Transfer File Name(전송 파일 이름) — 업로드할 소스 파일을 선택합니다.

구성 업로드

TFTP Server IP Address(TFTP 서버 IP 주소) — 구성 파일이 업로드되는 TFTP 서버 IP 주소입니다.

Destination File Name (1 - 32 characters)(대상 파일 이름(1 - 32자)) — 파일이 업로드된 이후에 갖게 되는 이름입니다.

Transfer File Name(전송 파일 이름) — 업로드할 소스 파일을 선택합니다. 유효한 필드 값은 다음과 같습니다.

Running Configuration(실행 구성) — 실행 구성 파일을 업로드합니다.

Startup Configuration(시작 구성) — 시작 구성 파일을 업로드합니다.

Backup Configuration(백업 구성) — 백업 구성 파일을 업로드합니다.

파일 업로드

1. *File Upload to Server*(서버로 파일 업로드) 페이지를 엽니다.
2. 페이지에서 관련 필드를 정의합니다.
3. **Apply Changes**(변경사항 적용)를 클릭합니다.


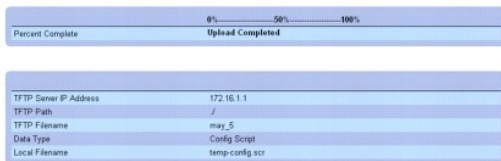
 **주:** 파일 업로드를 시작하면 페이지가 새로 고쳐지고 전송 바이트 수를 표시하는 전송 상태 필드가 나타납니다. 파일 업로드가 완료될 때까지 웹 인터페이스를 사용할 수 없습니다.

그림 6-81. File Upload Progress(파일 업로드 진행 상태)



소프트웨어가 서버로 업로드됩니다.

CLI 명령을 사용하여 파일 업로드

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 구성 및 이미지 파일 명령

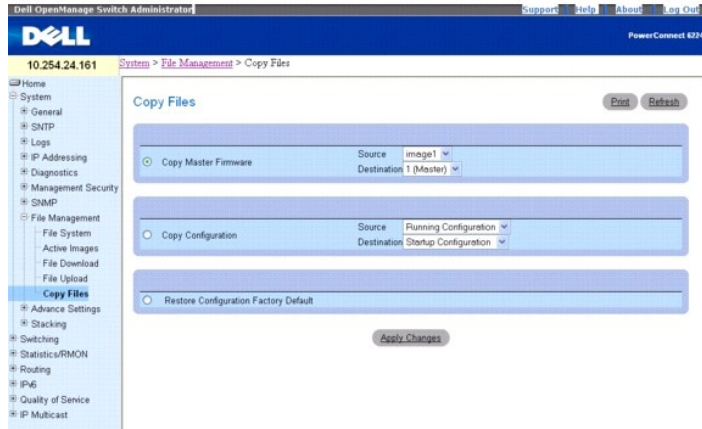
파일 복사

Copy Files(파일 복사) 웹 페이지를 사용하여 다음 작업을 수행할 수 있습니다.

- 1 파일 시스템 내의 이미지 복사
- 1 원격 서버로 이미지 복사 및 원격 서버에서 이미지 복사
- 1 로컬 또는 원격 시스템에 이미지 백업
- 1 로컬 또는 원격 시스템에서 이미지 복원
- 1 파일 시스템 내의 구성 파일 백업

Copy Files(파일 복사) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → File Management(파일 관리) → Copy(복사)를 클릭합니다.

그림 6-82. Copy Files(파일 복사)



Copy Files(파일 복사) 페이지에는 다음 필드가 있습니다.

Copy Master Firmware(마스터 펌웨어 복사) — 소프트웨어 이미지 파일이 복사되도록 지정합니다.

Source(소스) — 복사할 파일이 있는 소프트웨어 이미지 소스 파일입니다.

Destination(대상) — 파일이 복사되는 대상 장치입니다.

Copy Configuration(구성 복사) — 구성 파일이 복사되도록 지정합니다.

Source(소스) — 복사할 파일이 있는 구성 소스 파일(실행, 시작, 백업)입니다.

Destination(대상) — 파일이 복사되는 대상 구성 파일(실행, 시작, 백업)입니다.

Restore Configuration Factory Default(출하시 구성 기본값 복원) — 선택하면 출하시 구성 기본 파일이 재설정되도록 지정합니다. 선택 해제하면 현재 구성 설정이 유지됩니다.

파일 복사

1. Copy Files(파일 복사) 페이지를 엽니다.
2. Copy(복사) 또는 Restore(복원)를 선택하고 필드를 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

파일이 복사됩니다.

CLI 명령을 사용하여 파일 복사

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 구성 및 이미지 파일 명령

고급 설정 정의

Advanced Settings(고급 설정)를 사용하여 장치의 기타 전역 속성을 설정할 수 있습니다. 이러한 속성에 대한 변경사항은 장치를 재설정 한 이후에만 적용됩니다. Advanced Settings(고급 설정) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Advanced Settings(고급 설정)을 클릭합니다.

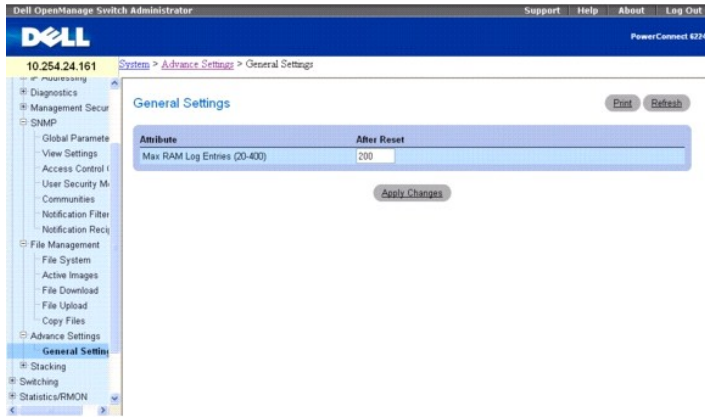
Advanced Settings(고급 설정) 페이지에는 일반 설정 구성을 위한 링크가 있습니다.

일반 설정

General Settings(일반 설정) 페이지를 사용하여 일반 장치 매개변수를 정의할 수 있습니다.

General Settings(일반 설정) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Advanced Settings(고급 설정)→General(일반)을 클릭합니다.

그림 6-83. General Settings(일반 설정)



General Settings(일반 설정) 페이지에는 다음 필드가 있습니다.

Attribute(속성) — RAM 로그 표의 최대 항목 수입니다. 기본값은 200개 항목입니다.

After Reset(재설정 후) — 값이 재설정된 후의 최대 항목 수입니다. 이 옆에 값을 입력하면 필드 표에 메모리가 할당됩니다.

RAM 로그 항목 할당 크기 조정

1. General Settings(일반 설정) 페이지를 엽니다.
2. After Reset(재설정 후) 필드에 원하는 새 값을 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

RAM 로그 항목에 할당된 공간은 다음에 장치를 재설정 한 이후에 적용됩니다.

CLI 명령을 사용하여 일반 설정 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 Syslog 명령

스택형 배치 정의

Stacking(스택형 배치) 메뉴를 사용하여 장치의 스택형 특성을 설정할 수 있습니다. 이러한 속성에 대한 변경사항은 장치를 재설정 한 이후에만 적용됩니다. Stacking(스택형 배치) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Stacking(스택형 배치)을 클릭합니다. 이 페이지를 사용하여 다음 기능으로 이동합니다.

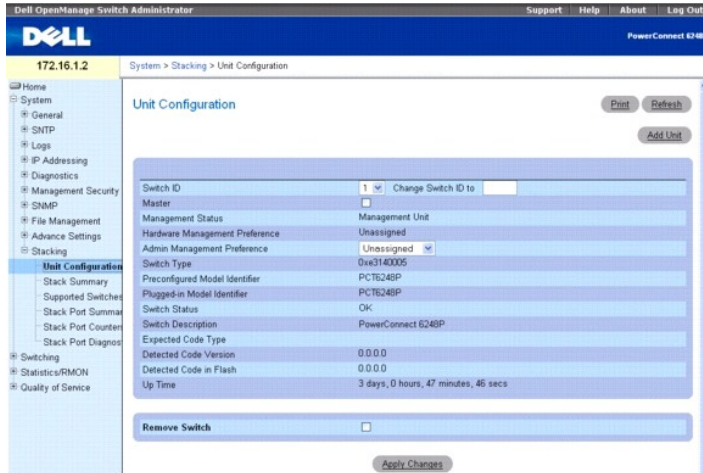
- 1 [장치 구성](#)
- 1 [스택 요약](#)
- 1 [지원되는 스위치](#)
- 1 [스택 포트 요약](#)
- 1 [스택 포트 카운터](#)
- 1 [스택 포트 진단](#)

장치 구성

Unit Configuration(장치 구성) 페이지를 사용하여 일반 장치 매개변수를 정의할 수 있습니다.

Unit Configuration(장치 구성) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Stacking(스택형 배치)→ Unit Configuration(장치 구성)을 클릭합니다.

그림 6-84. Unit Configuration(장치 구성)



Unit Configuration(장치 구성) 페이지에는 다음 필드가 있습니다.

Switch ID(스위치 ID) — 구성할 장치를 지정합니다.

Change Switch ID to(스위치 ID를 다음으로 변경) — 선택한 장치의 장치 번호를 변경합니다.

Master(마스터) — 이 장치를 다른 장치의 마스터(관리) 장치로 설정하려면 선택합니다. 이 설정의 기본값은 Unassigned(지정되지 않음)입니다.

Management Status(관리 상태) — 선택한 장치가 Management Unit(관리 장치)인지 또는 Stack Member(스택 멤버)인지 표시합니다.

Hardware Management Preference(하드웨어 관리 기본 설정) — 관리 장치로 선택할 때 고려할 하드웨어 구성별 관리 기본 설정입니다.

Admin Management Preference(관리자 관리 기본 설정) — 이 장치가 마스터 스위치가 될 수 있는지 여부를 결정합니다. 값은 Disable(비활성) (장치에서 마스터 스위치 기능을 지원할 수 없음)에서 Preference 15(기본 설정 15)까지 다양합니다. 값이 높은 장치는 값이 낮은 장치에 비해 관리 기능을 실행하기에 더 적합합니다. 기본 설정이 구성되어 있지 않으며 스택 장치에 의해 마스터가 선택됨을 나타내는 Unassigned(지정되지 않음) 값도 사용할 수 있습니다.

Switch Type(스위치 유형) — 스위치의 유형을 결정하는 시스템에 지정된 하드웨어 ID입니다.

Preconfigured Model Identifier(미리 구성된 모델 식별자) — 선택한 장치의 미리 구성된 모델을 식별하는 16바이트 문자열입니다.

Plugged-in Model Identifier(연결된 모델 식별자) — 선택한 장치의 연결된 모델을 식별하는 16바이트 문자열입니다.

Switch Status(스위치 상태) — 선택한 장치의 상태를 표시합니다. 가능한 값은 다음과 같습니다.

OK(양호) — 장치가 설치되어 작동하고 있습니다.

Unsupported(지원되지 않음) — 장치가 설치되었지만 스택 멤버로 작동할 수 없습니다.

Code Mismatch(코드 불일치) — 스위치의 소프트웨어가 마스터 장치 소프트웨어와 일치하지 않습니다.

Config Mismatch(구성 불일치) — 스위치의 구성이 마스터 장치 구성과 일치하지 않습니다.

Not Present(존재하지 않음) — 선택한 장치가 없습니다.

Switch Description(스위치 설명) — 장치를 식별하는 데 사용되는 80바이트 데이터 필드입니다.

Expected Code Type(예상 코드 유형) — 예상 코드 식별자를 표시합니다.

Detected Code Version(감지된 코드 버전) — 실행 코드 버전의 릴리즈 번호 및 버전 번호입니다.

Detected Code in Flash(플래시에서 감지된 코드) — 플래시에서 감지된 코드의 릴리즈 번호 및 버전 번호입니다.

Up Time(작동 시간) — 마지막 재설정 이후 장치가 실행된 시간을 표시합니다.

Remove Switch(스위치 제거) — 스택에서 스위치를 제거하려면 선택합니다.

장치 구성 정의

1. Unit Configuration(장치 구성) 페이지를 엽니다.
2. 필드에 원하는 새 값을 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

변경사항은 다음 장치가 재설정된 이후에 적용됩니다.

스위치 제거

1. Unit Configuration(장치 구성) 페이지를 엽니다.
2. Remove Switch(스위치 제거)를 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

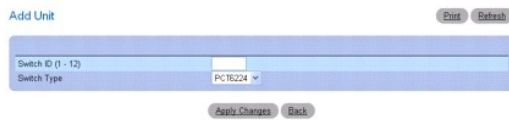
변경사항은 다음 장치가 재설정된 이후에 적용됩니다.

장치 추가

Add Unit(장치 추가) 페이지를 사용하여 일반 장치 매개변수를 정의할 수 있습니다.

Supported Switches(지원되는 스위치) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Stacking(스택형 배치)→Unit Configuration(장치 구성)을 클릭한 다음, Add Unit(장치 추가)을 클릭합니다.

그림 6-85. Add Unit(장치 추가)



Add Unit(장치 추가) 페이지에는 다음 필드가 있습니다.

Switch ID(스위치 ID) — 스택에서 선택한 스위치의 스위치 ID를 표시합니다. 관리자 사용자는 이 값을 수정하여 선택한 스위치의 스위치 ID를 다시 지정할 수 있습니다. 액세스 레벨 15의 사용자만이 웹 인터페이스를 사용하여 이 필드를 수정할 수 있습니다.

Switch Type(스위치 유형) — 스위치에 지정된 하드웨어 ID를 식별합니다.

장치 추가

1. Unit Configuration(장치 구성) 페이지를 엽니다.
2. Add Unit(장치 추가)을 클릭합니다.
Add Unit(장치 추가) 페이지가 표시됩니다.
3. Switch ID(스위치 ID) 필드에 원하는 새 값을 입력합니다.
4. Switch Type(스위치 유형) 드롭다운 목록에서 원하는 값을 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

변경사항은 다음 장치가 재설정된 이후에 적용됩니다.

CLI 명령을 사용하여 장치 구성 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

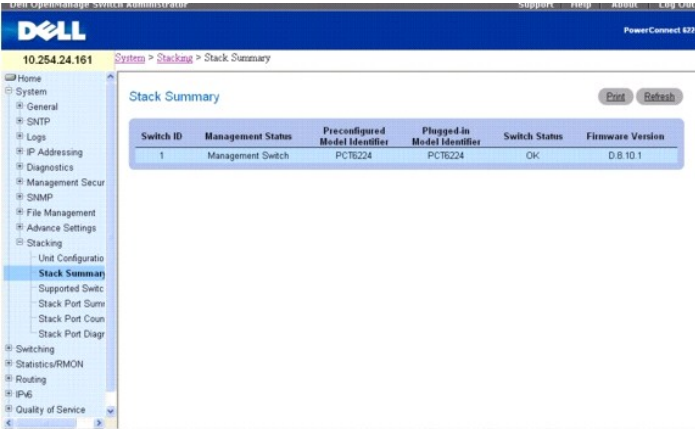
- 1 시스템 관리 명령

스택 요약

Stack Summary(스택 요약) 페이지를 사용하여 스택에 포함된 스위치 요약물을 볼 수 있습니다.

Stack Summary(스택 요약) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→Stacking(스택형 배치)→Stack Summary(스택 요약)를 클릭합니다.

그림 6-86. Stack Summary(스택 요약)



Stacking Summary(스택 요약) 페이지에는 다음 필드가 있습니다.

Switch ID(스위치 ID) — 장치의 ID입니다. 스택에 허용되는 최대 장치 수는 8개입니다.

Management Status(관리 상태) — 이 필드에는 스위치가 관리 스위치인지 스택 멤버인지, 상태가 지정되지 않은인지 표시됩니다.

Pre-configured Model Identifier(미리 구성된 모델 식별자) — 이 필드에는 미리 구성된 장치를 식별하기 위해 장치 제조업체에서 지정한 16자 필드가 표시됩니다.

Plugged-in Model Identifier(연결된 모델 식별자) — 이 필드에는 연결된 장치를 식별하기 위해 장치 제조업체에서 지정한 16자 필드가 표시됩니다.

Switch Status(스위치 상태) — 장치 상태를 나타냅니다. 가능한 5가지 상태 값은 다음과 같습니다.

OK(양호) — 장치가 설치되어 제대로 작동하고 있습니다.

Unsupported(지원되지 않음) — 장치의 스택형 배치가 허용되지 않습니다.

Code Mismatch(코드 불일치) — 이 장치의 소프트웨어 이미지가 스택의 마스터 스위치에서 사용되는 이미지와 일치하지 않습니다.

Config Mismatch(구성 불일치) — 이 장치의 구성 파일이 스택의 마스터 스위치에서 사용되는 파일과 일치하지 않습니다.

Not Present(존재하지 않음) — 장치가 없습니다.

Firmware Version(펌웨어 버전) — 이 장치에서 감지된 코드 버전을 나타냅니다.

CLI 명령을 사용하여 스택 요약 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 시스템 관리 명령

지원되는 스위치

Supported Switches(지원되는 스위치) 페이지를 사용하여 스택형 배치에 대해 지원되는 각 스위치 유형에 관한 정보 및 지원되는 스위치에 관한 정보를 볼 수 있습니다.

Supported Switches(지원되는 스위치) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → Stacking(스택형 배치) → Supported Switches(지원되는 스위치)를 클릭합니다.

그림 6-87. Supported Switches(지원되는 스위치)



Supported Switches(지원되는 스위치) 페이지에는 다음 필드가 있습니다.

Supported Switches(지원되는 스위치) — 드롭다운 목록에서 지원되는 스위치를 선택합니다.

Switch Index(스위치 색인) — 지원되는 스위치 유형의 데이터베이스에 색인을 지정합니다.

Switch Type(스위치 유형) — 스위치에 지정된 하드웨어 ID입니다.

Switch Model ID(스위치 모델 ID) — 지원되는 스위치 모델을 식별하는 16바이트 문자열을 표시합니다.

Description(설명) — 장치를 식별하는 데 사용되는 256바이트 데이터 필드를 표시합니다.

Management Preference(관리 기본 설정) — 이 장치가 마스터 스위치가 될 수 있는지 여부를 결정합니다. 값을 0으로 설정하면 장치에서 마스터 스위치 기능을 지원할 수 없습니다. 값이 높은 장치는 값이 낮은 장치에 비해 관리 기능을 실행하기에 더 적합합니다. 장치 제조업체에서 이 필드의 초기 값을 설정합니다.

Expected Code Type(예상 코드 유형) — 예상되는 코드의 릴리즈 번호 및 버전 번호를 표시합니다.

지원되는 스위치 특성 보기

1. Supported Switches(지원되는 스위치) 페이지를 엽니다.
2. Supported Switch(지원되는 스위치) 드롭다운 목록에서 원하는 스위치를 선택합니다.

CLI 명령을 사용하여 지원되는 스위치 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

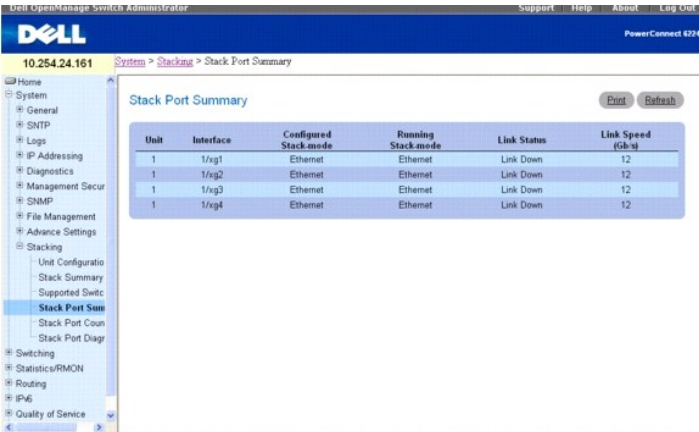
- 1 시스템 관리 명령

스택 포트 요약

Stack Port Summary(스택 포트 요약) 페이지를 사용하여 존재하는 스택형 포트를 볼 수 있습니다. 이 화면에는 장치, 스택형 인터페이스, 인터페이스의 구성된 모드, 실행 모드, 스택형 포트의 연결 상태 및 연결 속도가 표시됩니다.

Stack Port Summary(스택 포트 요약) 페이지를 표시하려면 디렉터리 화면에서 System(시스템) → Stacking(스택형 배치) → Stack Port Summary(스택 포트 요약)를 클릭합니다.

그림 6-88. Stack Port Summary(스택 포트 요약)



Stack Port Summary(스택 포트 요약) 페이지에는 다음 필드가 있습니다.

Unit(장치) — 장치의 ID 번호입니다.

Interface(인터페이스) — 장치에 지정된 스택 인터페이스를 식별합니다.

Configured Stack Mode(구성된 스택 모드) — 각 장치가 스택에 포함될 수 있는지 여부를 나타냅니다.

Running Stack Mode(실행 스택 모드) — 각 장치가 실제로 스택에 포함되어 있는지 여부를 나타냅니다.

Link Status(연결 상태) — 각 장치의 스택 인터페이스가 작동하고 있는지 여부를 나타냅니다.

Link Speed (Gb/s)(연결 속도(Gb/초)) — 각 장치 연결의 정격 속도를 나타냅니다.

CLI 명령을 사용하여 스택 포트 요약 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

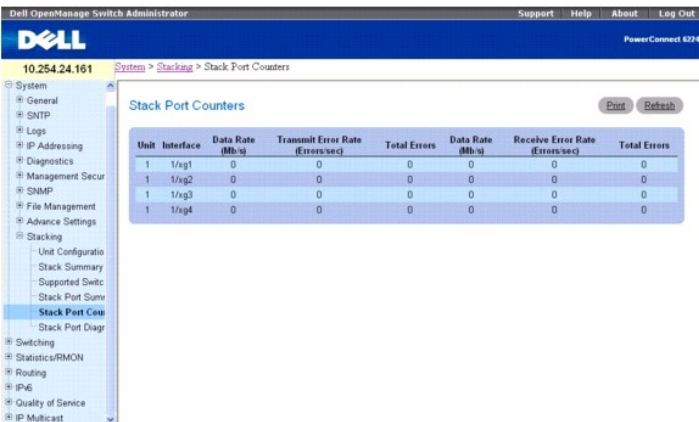
- 1 시스템 관리 명령

스택 포트 카운터

Stack Port Counters(스택 포트 카운터) 페이지를 사용하여 데이터 전송 속도 및 오류 비율을 비롯한 송수신 통계를 볼 수 있습니다.

Stack Port Counters(스택 포트 카운터) 페이지를 표시하려면 디렉터리 화면에서 System(시스템)→ Stacking(스택형 배치)→ Stack Port Counters(스택 포트 카운터)를 클릭합니다.

그림 6-89. Stack Port Counters(스택 포트 카운터)



Stack Port Counters(스택 포트 카운터) 페이지에는 다음 필드가 있습니다.

Unit(장치) — 표시되는 종속 스위치를 나타냅니다.

Interface(인터페이스) — 인터페이스 이름을 나타냅니다.

Data Rate (Mb/s)(데이터 전송 속도(Mb/초)) - 데이터가 전송되는 속도를 나타냅니다.

Transmit Error Rate (Errors/sec)(전송 오류 비율(오류/초)) - 초당 전송된 오류 수를 나타냅니다.

Total Errors(총 오류) - 전송된 총 오류 수입니다.

Data Rate (Mb/s)(데이터 전송 속도(Mb/초)) - 데이터가 수신되는 속도를 나타냅니다.

Receive Error Rate (Errors/sec)(수신 오류 비율(오류/초)) - 초당 수신된 오류 수를 나타냅니다.

Total Errors(총 오류) - 수신된 총 오류 수입니다.

스택 포트 카운터 보기

1. Stack Port Counters(스택 포트 카운터) 페이지를 엽니다.

CLI 명령을 사용하여 스택 포트 카운터 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 시스템 관리 명령

스택 포트 진단

Stack Port Diagnostics(스택 포트 진단) 페이지는 필드 응용프로그램 엔지니어(FAE) 및 개발자를 위한 기능입니다.

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

스위치 정보 구성

Dell™ PowerConnect™ M6220 사용 설명서

- [네트워크 보안 구성](#)
- [포트 구성](#)
- [트래픽 미러링 구성](#)
- [주소 표 구성](#)
- [GARP 구성](#)
- [스패닝 트리 프로토콜 구성](#)
- [VLAN 구성](#)
- [포트 결합](#)
- [멀티캐스트 지원 관리](#)
- [LLDP\(Link Layer Discovery Protocol\) 구성](#)

이 절에서는 네트워크 보안, 포트, 주소 표, GARP, VLAN, 스패닝 트리, 포트 결합 및 멀티캐스트 지원에 대한 일반 정보와 모든 시스템 작동에 대해 설명합니다.

Switching(스위치) 메뉴 페이지에는 다음 기능에 대한 링크가 있습니다.

- 1 [네트워크 보안 구성](#)
- 1 [포트 구성](#)
- 1 [트래픽 미러링 구성](#)
- 1 [주소 표 구성](#)
- 1 [GARP 구성](#)
- 1 [스패닝 트리 프로토콜 구성](#)
- 1 [VLAN 구성](#)
- 1 [포트 결합](#)
- 1 [멀티캐스트 지원 관리](#)
- 1 [LLDP\(Link Layer Discovery Protocol\) 구성](#)

네트워크 보안 구성

Network Security(네트워크 보안) 메뉴 페이지에서 포트 기반 인증, 잠긴 포트, DHCP 필터링 구성 및 액세스 제어 목록을 통해 네트워크 보안을 설정합니다.

Network Security(네트워크 보안) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치) → Network Security(네트워크 보안)를 클릭합니다.

Network Security(네트워크 보안) 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

- 1 [포트 기반 인증](#)
- 1 [다중 호스트](#)
- 1 [인증된 사용자](#)
- 1 [포트 보안](#)
- 1 [DHCP 필터링](#)
- 1 [액세스 제어 목록](#)
- 1 [ACL 바인드 구성](#)

포트 기반 인증

포트 기반 인증 모드에서는 802.1x가 포트에서 전역으로 활성화되어 있는 경우, 포트에 연결된 요청자가 한 명이라도 성공적으로 인증되면 모든 사용자가 제한 없이 포트를 사용할 수 있습니다. 이 모드에서는 특정 시간에 한 명의 요청자만 포트에 인증을 시도할 수 있습니다. 이 모드에서 포트는 양방향으로 제어됩니다. 이 모드는 기본 인증 모드입니다.

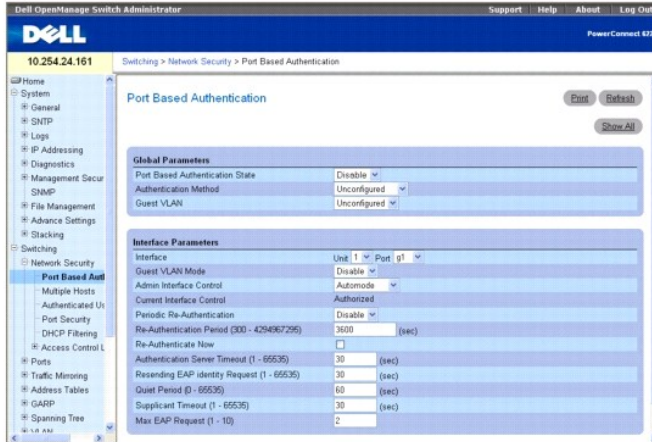
802.1x 네트워크에는 다음과 같은 세 가지 구성 요소가 있습니다.

- 1 **인증자** — 시스템으로의 액세스를 허용하기 전에 인증되는 포트를 지정합니다.
- 1 **Supplicants(요청자)** — 시스템 서비스로의 액세스를 요청하는 인증된 포트에 연결된 호스트를 지정합니다.
- 1 **Authentication Server(인증 서버)** — 인증자 대신 인증을 수행하는 RADIUS 서버와 같은 외부 서버를 지정하고, 사용자가 시스템 서비스에 액세스하도록 허가되었는지 여부를 나타냅니다.

Port Based Authentication(포트 기반 인증) 페이지에서 포트의 일반 802.1x 매개변수를 구성합니다.

Port Based Authentication(포트 기반 인증) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치) → Network Security(네트워크 보안) → Port Based Authentication(포트 기반 인증)을 클릭합니다.

그림 7-1. Port Based Authentication(포트 기반 인증)



Port Based Authentication(포트 기반 인증) 페이지에는 다음 필드가 포함되어 있습니다.

전역 매개변수

Port Based Authentication State(포트 기반 인증 상태) — 스위치에 포트 기반 인증을 허용합니다. 가능한 필드 값은 다음과 같습니다.

Enable(활성) — 스위치에 포트 기반 인증을 사용합니다.

Disable(비활성) — 스위치에 포트 기반 인증을 사용하지 않습니다.

Authentication Method(인증 방법) — 사용되는 인증 방법을 선택합니다. 가능한 필드 값은 다음과 같습니다.

Unconfigured(구성되지 않음) — 인증 방법을 선택하지 않았음을 나타냅니다.

None(없음) — 인증 방법이 사용되지 않음을 나타냅니다.

RADIUS — RADIUS 서버에서 인증이 수행됨을 나타냅니다.

RADIUS, None(RADIUS, 없음) — RADIUS 서버에서 인증이 수행됨을 나타냅니다. RADIUS 서버를 사용할 수 없는 경우 인증 방법이 사용되지 않습니다.

None, RADIUS(없음, RADIUS) — 인증 방법이 사용되지 않음을 나타냅니다. 인증이 필요한 경우 RADIUS 서버에서 수행됩니다.

Guest VLAN(게스트 VLAN) — 모든 포트에 대한 게스트 VLAN을 지정합니다. 가능한 필드 값은 다음과 같습니다.

Unconfigured(구성되지 않음) — 게스트 VLAN이 모든 포트에 구성되지 않았습니다.

VLAN ID — 시스템에 구성된 VLAN의 ID를 표시합니다. 모든 포트에 대해 게스트 VLAN으로 사용할 VLAN을 선택합니다.

인터페이스 매개변수

Interface(인터페이스) — 적용할 장치와 포트를 선택합니다.

Guest VLAN Mode(게스트 VLAN 모드) — 이 인터페이스에서 게스트 VLAN 모드를 활성화하거나 비활성화합니다.

Admin Interface Control(관리 인터페이스 제어) — 포트 인증 상태를 정의합니다. 가능한 필드 값은 다음과 같습니다.

Automode(자동 모드) — 인터페이스의 모드를 자동으로 감지합니다.

Authorized(허가됨) — 인터페이스를 인증되지 않은 채 허가된 상태로 지정합니다. 인터페이스는 클라이언트 포트 기반 인증 없이 일반 트래픽을 전송하고 수신합니다.

Unauthorized(허가되지 않음) — 인터페이스를 허가되지 않은 상태로 전환하여 선택된 인터페이스 시스템으로의 액세스를 거부합니다. 스위치는 인터페이스를 통해 클라이언트에 대한 인증 서비스를 제공할 수 없습니다.

Current Interface Control(현재 인터페이스 제어) — 현재 포트 인증 상태를 표시합니다.

Periodic Re-Authentication(주기적 재인증) — 이 기능이 활성화되면 선택된 포트를 주기적으로 재인증합니다.

Re-Authentication Period(재인증 기간)(300-4294967295) — 선택된 포트가 재인증되는 시간을 나타냅니다. 필드 값의 단위는 초입니다. 필드 기본값은 3600초입니다.

Re-Authenticate Now(지금 재인증) — 이 기능이 선택된 경우 즉시 포트 재인증을 강제로 수행합니다.

Authentication Server Timeout(인증 서버 타임아웃)(1-65535) — 스위치가 요청을 인증 서버로 재전송할 때까지 경과되는 시간을 정의합니다. 필드 값의 단위는 초입니다. 필드 기본값은 30초입니다.

Resending EAP Identity Request(EAP ID 요청 재전송) (1-65535) — EAP 요청을 재전송할 때까지 경과되는 시간을 정의합니다. 필드 값의 단위는 초입니다. 필드 기본값은 30초입니다.

Quiet Period(Quiet 기간) (0-65535) — 인증 교환 실패 후 스위치가 Quiet 상태를 유지하는 시간을 정의합니다. 가능한 필드 범위는 0-65535이고 필드 값의 단위는 초입니다. 필드 기본값은 60초입니다.

Supplicant Timeout(요청자 타임아웃) (1-65535) — EAP 요청을 사용자에게 재전송할 때까지 경과되는 시간을 정의합니다. 필드 값의 단위는 초입니다. 필드 기본값은 30초입니다.

Max EAP Requests(최대 EAP 요청) (1-10) — 응답이 수신되지 않는 경우 인증 프로세스를 다시 시작하기 전에 스위치가 EAP 요청을 전송할 수 있는 최대 횟수를 정의합니다. 가능한 필드 범위는 1-10이고 필드 기본값은 2회입니다.

포트 기반 인증 표 표시

1. **Port Based Authentication(포트 기반 인증)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.

Port Based Authentication Table(포트 기반 인증 표) 페이지가 열리고 표의 왼쪽이 표시됩니다.

그림 7-2. Port Based Authentication Table(포트 기반 인증 표)

Ports	Admin Port Control	Current Port Control	Periodic Re-Authentication	Re-Authentication Period	Re-Authenticate Now	On Port
1 1/ig1	Automatic	Authorized	Disable	3600		리
2 1/ig2	Automatic	Authorized	Disable	3600		리
3 1/ig3	Automatic	Authorized	Disable	3600		리
4 1/ig4	Automatic	Authorized	Disable	3600		리
5 1/ig5	Automatic	Authorized	Disable	3600		리
23 1/ig23	Automatic	Authorized	Disable	3600		리
24 1/ig24	Automatic	Authorized	Disable	3600		리
25 1/ig1	Automatic	Authorized	Disable	3600		리
26 1/ig2	Automatic	Authorized	Disable	3600		리
27 1/ig3	Automatic	Authorized	Disable	3600		리
28 1/ig4	Automatic	Authorized	Disable	3600		리

3. 표의 오른쪽을 보려면 화면의 아래쪽에 있는 가로 스크롤바를 사용하거나 오른쪽 화살표를 클릭합니다.
4. 스택의 다른 장치(존재하는 경우)에 대해 **Port Based Authentication Table(포트 기반 인증 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

한 개의 포트 재인증

1. **Port Based Authentication(포트 기반 인증)** 페이지를 엽니다.
2. 재인증할 장치/포트를 선택하려면 **Edit(편집)**를 선택합니다.
3. **Reauthenticate Now(지금 재인증)**를 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

지정된 포트가 재인증되고 장치가 업데이트됩니다.

포트 기반 인증 표에서 여러 포트 재인증

1. **Port Based Authentication(포트 기반 인증)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.
Port Based Authentication Table(포트 기반 인증 표)이 표시됩니다.
3. 재인증할 장치/포트를 선택하려면 **Edit(편집)**를 선택합니다.
4. 주기적으로 재인증하려면 **Periodic Re-Authentication(주기적 재인증)**을 Enable(활성)로 설정하고 원하는 모든 포트에 **Re-Authentication Period(재인증 기간)**를 지정합니다.

5. 즉시 재인증하려면 재인증할 모든 포트에 대해 **Reauthenticate Now(지금 재인증)**를 선택합니다.

6. **Apply Changes(변경사항 적용)**를 클릭하십시오.

지정된 포트가 즉시 또는 주기적으로 재인증되고 장치가 업데이트됩니다.

관리 포트 제어 변경

1. **Port Based Authentication(포트 기반 인증)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

Port Based Authentication Table(포트 기반 인증 표)이 표시됩니다.

3. 표의 오른쪽으로 스크롤하여 구성할 각 포트에 대해 **Edit(편집)** 확인란을 선택합니다. 선택한 포트에 대한 필요에 따라 **Admin Port Control(관리 포트 제어)**을 **Authorized(허가됨)**, **Unauthorized(허가되지 않음)** 또는 **Automode(자동 모드)**로 변경합니다. 실제로 **Automode(자동 모드)**만 dot1x를 사용하여 인증합니다. **Authorized(허가됨)** 및 **Unauthorized(허가되지 않음)**는 수동으로 무시됩니다.

4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

Admin Port Control(관리 포트 제어)이 지정된 포트에 대해 업데이트되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 포트 기반 인증 활성화

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 802.1X 명령

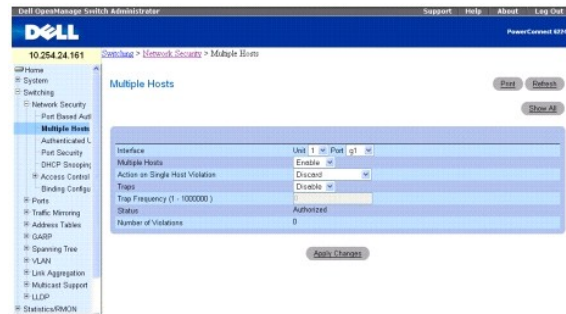
다중 호스트

포트가 다중 호스트 모드에 있을 경우 해당 포트에서 한 개의 스위치만 인증해야 합니다. 이렇게 하면 해당 포트에서 모든 스위치의 네트워크 액세스가 허용됩니다. 포트가 어떤 이유로든 허가되지 않은 상태가 되면, 모든 스위치는 네트워크 액세스 권한을 잃게 되고 인증 프로세스를 다시 시작해야 합니다.

Multiple Hosts(다중 호스트) 페이지에는 특정 포트에 대한 고급 포트 기반 인증 설정을 정의하는 위한 정보가 나와 있습니다.

Multiple Hosts(다중 호스트) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Network Security(네트워크 보안)**→**Multiple Host(다중 호스트)**를 클릭합니다.

그림 7-3. Multiple Host(다중 호스트)



Multiple Hosts(다중 호스트) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 고급 포트 기반 인증 설정을 구성할 장치와 포트 번호를 지정합니다.

Multiple Hosts(다중 호스트) — 단일 호스트에서 시스템 액세스에 대한 여러 호스트 허가를 활성화하거나 비활성화합니다. 수신 필터링을 비활성화하거나 선택된 포트에서 포트 잠금 보안을 사용하려면 이 설정을 활성화해야 합니다.

Action on Single Host Violation(단일 호스트 위반 시 동작) — 호스트의 MAC 주소가 클라이언트(요청자) MAC 주소가 아닌 단일 호스트 모드에서 수신되는 패킷에 적용할 동작을 정의합니다. 가능한 필드 값은 다음과 같습니다.

Forward(전달) — 알 수 없는 소스의 패킷을 전달합니다. 그러나 MAC 주소는 탐지되지 않습니다.

Discard(삭제) — 알 수 없는 소스의 패킷을 삭제합니다. 이 값은 기본값입니다.

Discard Shutdown(삭제 종료) — 알 수 없는 소스에서 패킷을 삭제하고 포트를 종료합니다. 포트는 활성화되거나 스위치가 재설정될 때까지 종료 상태로 남게 됩니다.

Traps(트랩) — 위반이 발생하면 호스트로의 트랩 전송을 활성화하거나 비활성화합니다.

Trap Frequency(트랩 빈도) (1-1000000) — 트랩이 호스트로 전송되는 기간을 정의합니다. 기본값은 10초입니다. 보안 트랩은 위반 수에 따라 10초에 한 번씩 전송됩니다.

Status(상태) — 호스트 상태를 표시합니다. 가능한 필드 값은 다음과 같습니다.

Authorized(허가됨) — 포트 제어가 현재 자동 모드로 되어 있고 클라이언트가 포트에 완전히 접근할 수 있음을 나타냅니다.

Unauthorized(허가되지 않음) — 포트 제어가 Force Unauthorized(강제 허가되지 않음)이고 포트 링크가 다운되었거나 포트 제어가 Auto(자동)이지만 클라이언트가 포트를 통해 인증되지 않았음을 나타냅니다.

Not in auto mode(자동 모드 아님) — 포트 제어가 Forced Authorized(강제 허가됨)이고 클라이언트가 포트에 완전히 접근할 수 있음을 나타냅니다.

Single-host Lock(단일 호스트 잠금) — 포트 제어가 Auto(자동)이고 단일 클라이언트가 포트를 통해 인증되었음을 나타냅니다.

No Single Host(단일 호스트 없음) — Multiple Host(다중 호스트)가 활성화되었음을 나타냅니다.

Number of Violations(위반 수) — 호스트의 MAC 주소가 클라이언트(요청자) MAC 주소가 아닌 단일 호스트 모드에서 인터페이스에 수신된 패킷의 수를 표시합니다.

다중 호스트 표 표시

1. Multiple Hosts(다중 호스트) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

Multiple Host Table(다중 호스트 표)이 표시됩니다.

그림 7-4. Multiple Host Table(다중 호스트 표)

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations	Edit
1 1/ig1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
2 1/ig2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
3 1/ig3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
4 1/ig4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
...
48 1/ig8	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
49 1/ig1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
50 1/ig2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
51 1/ig3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
52 1/ig4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>

3. 스택의 다른 장치(존재하는 경우)에 대해 Multiple Host Table(다중 호스트 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

한 포트에 여러 호스트 활성화/비활성화

1. Multiple Hosts(다중 호스트) 페이지를 엽니다.

2. 적용할 장치와 포트를 Interface(인터페이스)에서 선택합니다.

3. 원하는 대로 변수를 정의합니다.

4. Apply Changes(변경사항 적용)를 클릭하십시오.

지정된 포트에 대해 여러 호스트가 활성화되고 장치가 업데이트됩니다.

여러 포트에 여러 호스트 활성화/비활성화

1. Multiple Hosts(다중 호스트) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭하여 Multiple Host Table(다중 호스트 표)을 표시합니다.

- 구성할 포트와 연결된 Edit(편집) 확인란을 선택합니다.
- 원하는 포트의 변수를 변경합니다.
- Apply Changes(변경사항 적용)**를 클릭하십시오.
편집된 포트가 업데이트되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 고급 포트 인증 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

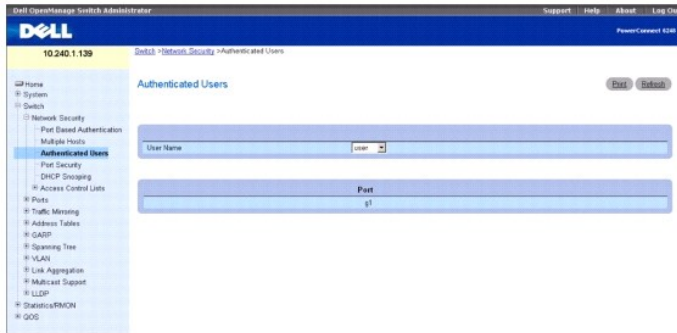
1 802.1X 명령

인증된 사용자

Authenticated Users(인증된 사용자) 페이지에는 사용자 포트 액세스 목록이 표시됩니다.

Authenticated Users(인증된 사용자) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Network Security(네트워크 보안)** → **Authenticated Users(인증된 사용자)**를 클릭합니다.

그림 7-5. Authenticated Users(인증된 사용자)



Authenticated Users(인증된 사용자) 페이지에는 다음 필드가 포함되어 있습니다.

User Name(사용자 이름) — RADIUS 서버를 통해 허가된 사용자 목록에서 한 명의 사용자를 지정합니다.

Port(포트) — 인증에 사용되는 포트를 나열합니다.

CLI 명령을 사용하여 인증된 사용자 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 802.1X 명령

포트 보안

포트 보안은 포트별로 활성화할 수 있습니다. 포트가 잠겨 있으면 허용 가능한 소스 MAC 주소를 가진 패킷만 전달할 수 있습니다. 다른 패킷은 모두 삭제됩니다. MAC 주소는 동적 또는 정적 방법 중 하나를 사용하여 허용되는 대로 정의할 수 있습니다. 포트가 잠겨 있으면 두 방법 모두 동시에 사용됩니다.

동적 잠금은 포트 보안에 대한 '최초 수신' 메커니즘을 구현합니다. 잠긴 포트에서 탐지할 수 있는 주소의 수를 지정합니다. 제한에 도달하지 않으면 알 수 없는 소스 MAC 주소를 가진 패킷이 탐지되어 정상적으로 전달됩니다. 제한에 도달하면 포트에서 더 이상의 주소가 탐지되지 않습니다. 아직 탐지되지 않은 소스 MAC 주소를 가진 패킷은 모두 삭제됩니다. 허용 가능한 동적 항목 수를 0으로 설정하면 동적 잠금을 효과적으로 비활성화할 수 있습니다.

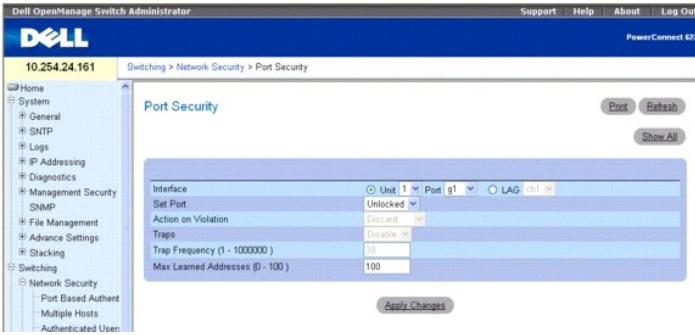
정적 잠금을 사용하면 포트에 허용되는 MAC 주소의 목록을 지정할 수 있습니다. 패킷 동작은 동적 잠금에 대한 동작과 동일합니다. 즉, 허용되는 소스 MAC 주소를 가진 패킷만 전달할 수 있습니다.

특정 포트에서 탐지된 MAC를 확인하거나 포트에 정적 MAC를 추가하거나, 정적 MAC 항목을 삭제하려면 [주소 표 구성](#)을 참조하십시오.

비활성화된 포트는 **Configuring Ports(포트 구성)** 페이지에서만 활성화할 수 있습니다.

Port Security(포트 보안) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Network Security(네트워크 보안)** → **Port Security(포트 보안)**를 클릭합니다.

그림 7-6. Port Security(포트 보안)



Interface(인터페이스) — 포트 보안 설정을 구성할 장치와 포트 또는 LAG를 선택합니다.

Set Port(포트 설정) — 포트/LAG 잠금을 활성화합니다. 포트가 잠겨 있으면 해당 포트의 스위치로 동적으로 탐지된 현재 주소가 모두 데이터베이스에서 제거됩니다.

Action on Violation(위반 시 동작) — 포트/LAG에 수신되는 패킷에 적용된 동작을 지정합니다. 포트/LAG의 잠금이 해제되어 있으면 필드가 회색으로 표시됩니다. 가능한 값은 다음과 같습니다.

Discard(삭제) — 알 수 없는 소스의 패킷을 삭제합니다. 이 값은 기본값입니다.

Forward(전달) — 알 수 없는 소스의 패킷을 전달합니다. MAC 주소는 탐지되지 않습니다.

Shutdown(종료) — 탐지되지 않은 소스에서 패킷을 삭제하고 트랩을 전송합니다. 또한 수신 포트가 비활성화됩니다.

Traps(트랩) — 잠긴 포트/LAG에서 패킷이 수신되면 트랩 전송을 활성화하거나 비활성화합니다.

Trap Frequency(트랩 빈도) (1-1000000) — 트랩 간의 시간(초)을 지정합니다.

Max Learned Addresses(최대 탐지 주소) (1-100) — 포트에서 탐지할 수 있는 최대 보안 MAC 주소 수를 지정합니다.

잠긴 포트 정의

1. **Port Security(포트 보안)** 페이지를 엽니다.
2. 인터페이스 유형 및 번호를 선택합니다.
3. **Set Port(포트 설정)** 드롭다운 메뉴에서 **Locked(잠김)**를 선택합니다.
4. 나머지 필드를 입력합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

잠긴 포트/LAG가 포트 보안 표에 추가되고 장치가 업데이트됩니다.

포트 보안 표 보기

1. **Port Security(포트 보안)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
Port Security Table(포트 보안 표)이 표시됩니다.

그림 7-7. Port Security Table(포트 보안 표)

Port Security Table Print Refresh

Ports	Current Port Control	Set Port	Set Port Action	Trap	Trap Frequency	Edit
1 1/g1	Link Up	Unlock	Discard	Disable	30	
2 1/g2	Link Down	Unlock	Discard	Disable	30	
3 1/g3	Link Up	Unlock	Discard	Disable	30	

26 1/g2	Link Down	Unlock	Discard	Disable	30	
27 1/g3	Link Down	Unlock	Discard	Disable	30	
28 1/g4	Link Down	Unlock	Discard	Disable	30	

Apply Changes Back

3. 스왕의 다른 장치(존재하는 경우)에 대해 **Port Security Table(포트 보안 표)**를 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

잠겨진 여러 포트 정의

1. **Port Security(포트 보안)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
Port Security Table(포트 보안 표)이 표시됩니다.
3. 매개변수를 변경할 각 포트에 대해 **Edit(편집)**를 클릭합니다.
4. 이제 이 포트에 대한 필드를 필요에 따라 편집할 수 있습니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 보안 표에 변경사항이 적용되고 장치가 업데이트됩니다.

CLI 명령으로 포트 보안 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 주소 표 명령

DHCP 필터링

DHCP 필터링은 허가되지 않은 DHCP 서버에 대한 보안 방법으로 사용할 수 있는 유용한 기능입니다. 알려진 공격은 허가되지 않은 DHCP 서버가 IP 주소를 요청하는 클라이언트에 응답하는 경우입니다. 서버는 클라이언트의 게이트웨이가 서버의 IP 주소와 같아지도록 구성합니다. 이 경우 클라이언트는 다른 네트워크를 대상으로 하는 모든 IP 트래픽을 허가되지 않은 시스템으로 전송합니다. 이렇게 하면 공격자는 트래픽을 스누핑하여 암호를 알아내거나 중간에서 가로채어 공격할 수 있게 됩니다. DHCP 필터링은 관리자가 각 포트를 신뢰할 수 있는 포트나 신뢰할 수 없는 포트 중 하나로 구성하도록 허용하는 과정에서 작동합니다. 허가된 DHCP 서버가 있는 포트는 신뢰할 수 있는 포트로 구성되어야 합니다. 신뢰할 수 있는 포트에 수신된 모든 DHCP 응답은 전달됩니다. 다른 모든 포트는 신뢰할 수 없는 포트로 구성해야 합니다. 수신되는 모든 DHCP(또는 BootP) 응답은 삭제됩니다.

DHCP Filtering(DHCP 필터링) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Network Security(네트워크 보안)** → **DHCP Filtering(DHCP 필터링)**을 클릭합니다.

그림 7-8. DHCP Filtering(DHCP 필터링)



DHCP Filtering(DHCP 필터링) 페이지에는 다음 필드가 포함되어 있습니다.

DHCP Filtering Global Mode(DHCP 필터링 전역 모드) — DHCP 필터링을 켜거나 끕니다. 기본값은 Disabled(비활성)입니다.

Interface(인터페이스) — 적용할 장치와 포트 또는 LAG를 지정합니다. 드롭다운 메뉴에서 LAG에 대해 원하는 장치와 포트를 선택합니다.

DHCP Trust Mode(DHCP 신뢰 모드) — 신뢰 모드를 활성화하거나 비활성화합니다. 기본값은 Disable(비활성)입니다.

DHCP Filtering(DHCP 필터링) 추가

1. DHCP Filtering(DHCP 필터링) 페이지를 엽니다.
2. 적용할 Interface(인터페이스) 또는 LAG를 지정합니다.
3. DHCP Filtering Global Mode(DHCP 필터링 전역 모드) 및 DHCP Filtering Trust Mode(DHCP 필터링 신뢰 모드)를 원하는 설정으로 설정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

장치가 업데이트됩니다.

DHCP 필터링 인터페이스 구성 표 표시

1. DHCP Filtering(DHCP 필터링) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
DHCP Filtering Table(DHCP 필터링 표) 페이지에는 모든 포트, 해당 장치 및 DHCP Trust Modes(DHCP 신뢰 모드)가 표시됩니다.

그림 7-9. DHCP Filtering Interface Configuration Table(DHCP 필터링 인터페이스 구성 표)

Port	DHCP Trust Mode	Edit
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>

26	<input type="checkbox"/>	<input type="checkbox"/>
27	<input type="checkbox"/>	<input type="checkbox"/>
28	<input type="checkbox"/>	<input type="checkbox"/>

3. 스택의 다른 장치(존재하는 경우)에 대해 DHCP Filtering Table(DHCP 필터링 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

여러 포트에 DHCP 필터링 구성

1. DHCP Filtering(DHCP 필터링) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
DHCP Filtering Interface Configuration Table(DHCP 필터링 인터페이스 구성 표)이 표시됩니다.
3. 구성할 각 포트에 대해 Edit(편집)를 클릭합니다.
4. 이 포트에 대한 DHCP Trust Mode(DHCP 신뢰 모드) 필드를 필요에 따라 활성화하거나 비활성화합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

DHCP 필터링 인터페이스 구성 표에 변경사항이 적용되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DHCP 필터링 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

IP ACL 구성

네트워크 관리자는 액세스 제어 목록(ACL)을 사용하여 분류 동작 및 특정 수신 포트에 대한 규칙을 정의합니다. 이 스위치는 최대 100개의 ACL을 지원합니다. 그러나 하드웨어 자원이 제한되어 있기 때문에 완전히 채워진 100개의 ACL이 모두 지원되지 않을 수 있습니다.

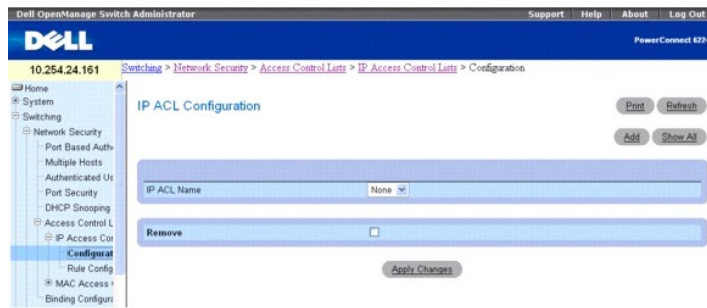
패킷은 수신 시 필터링될 수 있습니다. 필터 규칙이 일치하면 패킷 삭제 또는 포트 비활성화 등과 같은 일부 동작을 수행할 수 있습니다. 예를 들어 네트워크 관리자는 포트 번호 2001 TCP 패킷을 수신할 수 있다는 ACL 규칙을 정의합니다. 그러나, UDP 패킷이 수신되면 해당 패킷은 삭제됩니다.

ACL은 트래픽 분류를 결정하는 필터로 구성된 액세스 제어 항목(ACE) 또는 규칙으로 구성됩니다. 각 ACL에 대해 정의할 수 있는 총 규칙 수는 10개입니다.

IP ACL Configuration(IP ACL 구성) 페이지에서 IP 기반 ACL을 추가하거나 제거합니다.

IP ACL Configuration(IP ACL 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Network Security(네트워크 보안)** → **Access Control Lists(액세스 제어 목록)** → **IP Access Control Lists(IP 액세스 제어 목록)** → **Configuration(구성)**를 클릭합니다.

그림 7-10. IP ACL Configuration(IP ACL 구성)



IP ACL Configuration(IP ACL 구성) 페이지에는 다음 필드가 포함되어 있습니다.

IP ACL Name(IP ACL 이름) — ACL에 대한 사용자 정의 이름을 지정합니다.

Remove(제거) — IP ACL 필드에서 선택된 IP ACL을 제거합니다.

IP 기반 ACL 추가

1. **IP ACL Configuration(IP ACL 구성)** 페이지를 엽니다.

2. **Add(추가)**를 클릭합니다.

Add IP ACL(IP ACL 추가) 페이지가 표시됩니다.

그림 7-11. Add IP ACL(IP ACL 추가)



3. **관련 입력 필드**에 원하는 **ACL Name(ACL 이름)**을 입력합니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

MAC 기반 ACL이 추가되고 장치가 업데이트됩니다.

IP 기반 ACL 제거

1. **IP ACL Configuration(IP ACL 구성)** 페이지를 열고 **IP ACL** 드롭다운 목록에서 삭제할 ACL을 선택합니다.

2. **Remove ACL(ACL 제거)** 확인란을 선택합니다.

3. **Apply Changes(변경사항 적용)**를 클릭합니다.

IP 기반 ACL이 제거되고 장치가 업데이트됩니다.

IP ACL 표시

1. IP ACL Configuration(IP ACL 구성) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

모든 IP ACL과 관련 데이터가 IP ACL Table(IP ACL 표)에 표시됩니다.

그림 7-12. IP ACL Table(IP ACL 표)

IP ACL Name	Rules	Direction	Interface	VLAN
1	ACL1	1	NONE	NONE
2	ACL2	1	NONE	NONE

CLI 명령을 사용하여 IP 기반 ACL 추가

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. ACL 명령

IP ACL 규칙 구성

IP ACL Rule Configuration(IP ACL 규칙 구성) 페이지에서 IP 기반 ACL에 대한 규칙을 정의합니다. 액세스 목록 정의에는 기준과 일치하는 트래픽이 정상적으로 전달되는지 또는 삭제되는지 여부를 지정하는 규칙이 포함되어 있습니다. 또한 트래픽을 특정 대기열로 할당하고 일부 트래픽을 필터링하며, VLAN 태그를 변경하고 포트를 중요할 뿐만 아니라 트래픽을 특정 포트로 재지정하도록 지정할 수 있습니다.

주의사항: ACL 목록의 끝에는 암시적인 "모두 거부" 규칙이 있습니다. 이 규칙은 ACL이 패킷에 적용되었을 때 명시적인 규칙이 일치하지 않으면, 마지막 암시적인 "모두 거부" 규칙이 적용되어 패킷이 삭제됨을 의미합니다.

IP ACL Rule Configuration(IP ACL 규칙 구성) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭) → Network Security(네트워크 보안) → Access Control Lists(액세스 제어 목록) → IP Access Control Lists(IP 액세스 제어 목록) → Rule Configuration(규칙 구성)을 클릭합니다.

그림 7-13. IP ACL - Rule Configuration (Standard)(규칙 구성(표준))

The screenshot shows the configuration page for an IP ACL rule. The IP ACL Name is set to 'ACL1' and the Rule ID is '1'. The Action is set to 'Permit'. The Source IP Address is '0.0.0.0' with a Wild Card Mask of '255.255.255.255'. The Destination IP Address is '10.0.0.0' with a Wild Card Mask of '0.0.0.0'. The Service Type is 'IP DSCP' with a Match to Port of '0-63'. The IP TOS Bits are '0' and the IP TOS Mask is '00-FF'.

IP ACL Rule Configuration(IP ACL 규칙 구성) 페이지에는 다음 필드가 포함되어 있습니다.

IP ACL Name(IP ACL 이름) — 기존 IP ACL을 지정합니다. 새 IP ACL을 설정하려면 "IP ACL 구성" 페이지를 사용합니다.

Rule ID(규칙 ID) — 사용자 정의된 ACL을 선택하거나 만듭니다. 기존 규칙 ID를 입력하거나, 드롭다운 메뉴에서 Create(만들기)를 선택하고 옆에 있는 필드에 원하는 새 규칙 ID를 입력하여 새 규칙 ID를 만듭니다. Apply Changes(변경사항 적용)를 클릭하면 새 ID가 만들어집니다. 각 ACL에 대해 최대 10개의 규칙을 만들 수 있습니다.

Action(동작) — ACL 전달 동작을 선택합니다. 드롭다운 메뉴 옵션에서 적용할 전달 동작을 선택합니다. 가능한 값은 다음과 같습니다.

Permit(허용) — ACL 기준과 일치하는 패킷을 전달합니다.

Deny(거부) — ACL 기준과 일치하는 패킷을 삭제합니다.

Assign Queue ID(대기열 ID 할당) — 확인란을 클릭하여 이 기준을 적용한 후 0 ~ 6의 식별 번호를 입력합니다.

Redirect Interface(인터페이스 재지정) — 인터페이스의 드롭다운 목록에서 이 규칙에 적용되는 패킷을 재지정할 인터페이스를 선택합니다.

Mirror Interface(미러 인터페이스) — 인터페이스의 드롭다운 목록에서 이 규칙에 적용되는 패킷을 미러링할 인터페이스를 선택합니다.

Logging(로깅) — 확인란을 선택하면 특정 ACL에 대한 로깅을 활성화합니다. Logging(로깅)은 Deny(거부) 작업에 대해서만 지원됩니다.

Match Every(모두 일치) — 패킷이 해당 ACL의 기준과 일치해야 합니다. 확인란을 클릭하여 이 기준을 적용합니다. Match Every(모두 일치)는 다른 필터링 규칙에 배타적이므로 이 항목을 선택하면 화면의 다른 규칙에 액세스할 수 없습니다.

Protocol(프로토콜) — 패킷의 프로토콜이 여기에 나열된 프로토콜과 일치해야 합니다. 확인란을 클릭하여 이 기준을 적용한 후 다음 중 하나를 선택합니다.

Select from List(목록에서 선택) — 규칙의 기반이 될 수 있는 프로토콜 드롭다운 목록에서 선택합니다.

Match to Value(값 일치) — 패킷을 규칙과 일치시킬 사용자 정의 프로토콜 ID를 추가하려면 클릭합니다.

Source IP Address(소스 IP 주소) — 패킷의 소스 포트 IP 주소가 여기에 나열된 주소와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 주소를 입력합니다.

Wild Card Mask(와일드카드 마스크) — 소스 IP 주소 와일드카드 마스크를 지정합니다. 와일드카드 마스크에 따라 사용되는 비트와 무시되는 비트가 결정됩니다. 와일드카드 마스크가 255.255.255.255이면 중요한 비트가 없는 것입니다. 와일드 카드가 0.0.0.0이면 모든 비트가 중요한 것입니다. **Source IP Address(소스 IP 주소)**를 선택한 경우 이 필드는 필수 항목입니다.

Source L4 Port(소스 L4 포트) — 패킷의 TCP/UDP 소스 포트가 여기에 나열된 포트와 일치해야 합니다. 확인란을 클릭하여 이 기준을 적용한 후 드롭다운 메뉴에서 다음 중 하나를 선택합니다.

Select From List(목록에서 선택) — 규칙의 기반이 될 수 있는 소스 포트 목록에서 선택합니다.

Match to Port(포트 일치) — 패킷을 규칙과 일치시킬 사용자 정의 포트 ID를 추가하려면 클릭합니다.

Destination IP Address(대상 IP 주소) — 패킷의 대상 포트 IP 주소가 여기에 나열된 주소와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 주소를 입력합니다.

Wild Card Mask(와일드카드 마스크) — 대상 IP 주소 와일드카드 마스크를 지정합니다. **Source IP Address(소스 IP 주소)**를 선택한 경우 이 필드는 필수 항목입니다.

Destination L4 Port(대상 L4 포트) — 패킷의 TCP/UDP 대상 포트가 여기에 나열된 포트와 일치해야 합니다. 확인란을 클릭하여 이 기준을 적용한 후 다음 중 하나를 선택합니다.

Select From List(목록에서 선택) — 규칙의 기반이 될 수 있는 대상 포트 목록에서 선택합니다.

Match to Port(포트 일치) — 패킷을 규칙과 일치시킬 사용자 정의 포트 ID를 추가하려면 클릭합니다.

Service Type(서비스 유형) 필드

패킷을 ACL과 일치시킬 때 사용할 다음 세 가지 Match(일치) 필드 중에서 하나를 선택합니다.

IP DSCP — 패킷 DSCP 값을 규칙과 일치시킵니다. DSCP 값 또는 IP 우선 순위 값을 사용하여 패킷을 ACL과 일치시킵니다.

Select From List(목록에서 선택) — DSCP 키워드 값 목록에서 선택합니다.

Match to Port(포트 일치) — 사용자 정의 포트 ID를 추가합니다.

IP Precedence(IP 우선 순위) — 패킷 IP 우선 순위 값을 규칙과 일치시킵니다. 일치시킬 IP 우선 순위 값을 입력합니다. DSCP 값 또는 IP 우선 순위 값을 사용하여 패킷을 ACL과 일치시킵니다.


IP TOS Bits(IP TOS 비트) — IP 헤더의 Type of Service(서비스 유형) 비트와 일치시킵니다.

TOS Bits(TOS 비트) — 패킷의 TOS 필드에 있는 비트가 여기에 입력된 2자리 16진수 숫자와 일치해야 합니다.

TOS Mask(TOS 마스크) — 패킷의 IP TOS 필드에 대한 비교에 사용할 비트 위치를 지정합니다.

Remove(제거) — Remove(제거)가 선택되었을 때 **Apply Changes(변경사항 적용)**를 클릭하면 규칙 ID를 제거합니다.

IP 기반 규칙 수정

 **주:** 규칙이 속하는 ACL이 인터페이스에 연결되지 않는 경우에만 규칙을 수정할 수 있습니다.

1. **IP ACL Rule Configuration(IP ACL 규칙 구성)** 페이지를 엽니다.
2. **IP ACL 드롭다운 메뉴에서 원하는 ACL**을 선택합니다.
3. **Rule ID(규칙 ID)** 드롭다운 메뉴에서 원하는 규칙을 선택합니다.

- 필요에 따라 나머지 필드를 수정합니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.
IP 기반 규칙이 수정되고 장치가 업데이트됩니다.

IP 기반 ACL에 새 규칙 추가

- IP ACL Rule Configuration(IP ACL 규칙 구성) 페이지를 엽니다.
- IP ACL 드롭다운 메뉴에서 원하는 ACL을 선택합니다.
- Rule ID(규칙 ID) 드롭다운 메뉴에서 Create Rule(규칙 만들기)를 선택하고 새 ID 번호를 입력합니다.
- 필요에 따라 나머지 필드를 정의합니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.
새 규칙이 지정된 IP 기반 ACL에 할당됩니다.

CLI 명령을 사용하여 IP 기반 ACL 규칙 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

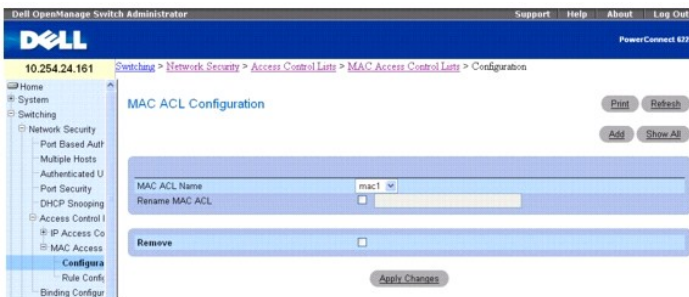
- ACL 명령

MAC ACL 구성

MAC ACL Configuration(MAC ACL 구성) 페이지에서는 네트워크 관리자가 MAC 기반 ACL을 정의할 수 있습니다. ACL의 설명에 대해서는 "[IP ACL 구성](#)"을 참조하십시오.

MAC ACL Configuration(MAC ACL 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Network Security(네트워크 보안)** → **Access Control Lists(액세스 제어 목록)** → **MAC Access Control Lists(MAC 액세스 제어 목록)** → **Configuration(구성)**를 클릭합니다.

그림 7-14. MAC ACL Configuration(MAC ACL 구성)



MAC ACL Configuration(MAC ACL 구성) 페이지에는 다음 필드가 포함되어 있습니다.

MAC ACL Name(MAC ACL 이름) — 사용자 정의된 ACL 이름입니다.

Rename MAC ACL(MAC ACL 이름 변경) — MAC ACL 이름을 변경하려면 확인란을 선택하고 필드에 새 MAC ACL 이름을 입력합니다.

Remove(제거) — 이 필드를 클릭한 다음 Apply Changes(변경사항 적용) 단추를 클릭하여 MAC ACL 필드에 나열된 MAC ACL을 삭제합니다.

MAC 기반 ACL 추가

- MAC ACL Configuration(MAC ACL 구성) 페이지를 엽니다.
- Add(추가)**를 클릭하여 **Add MAC ACL(MAC ACL 추가)** 페이지를 표시합니다.

그림 7-15. Add MAC ACL(MAC ACL 추가)



3. **입력 필드에** 원하는 MAC ACL Name(ACL 이름)을 입력합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
MAC 기반 ACL이 추가되고 장치가 업데이트됩니다.

MAC 기반 ACL 제거

1. **MAC ACL Configuration(MAC ACL 구성)** 페이지를 열고 **MAC ACL** 드롭다운 목록에서 삭제할 ACL을 선택합니다.
2. **Remove(제거)** 확인란을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.
MAC 기반 ACL이 제거되고 장치가 업데이트됩니다.

MAC ACL 표시

1. **MAC ACL Configuration(MAC ACL 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
모든 MAC ACL과 관련 데이터가 화면에 표시됩니다.

그림 7-16. MAC ACL Table(MAC ACL 표)

MAC ACL Name	Rules	Direction	Interface	VLAN
big_mac	1	NONE	NONE	

CLI 명령을 사용하여 MAC 기반 ACL 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

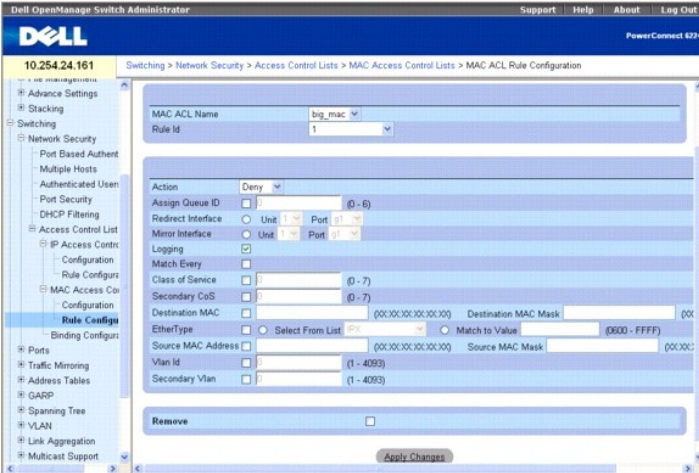
1. ACL 명령

MAC ACL 규칙 구성

MAC ACL Rule Configuration(MAC ACL 규칙 구성) 페이지에서 MAC 기반 ACL에 대한 규칙을 정의합니다. 액세스 목록 정의에는 기준과 일치하는 트래픽이 정상적으로 전달되는지 또는 삭제되는지 여부를 지정하는 규칙이 포함되어 있습니다. 기본 '모두 거부' 규칙은 모든 목록의 마지막 규칙입니다.

MAC ACL Rule Configuration(MAC ACL 규칙 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Network Security(네트워크 보안)** → **Access Control Lists(액세스 제어 목록)** → **MAC Access Control Lists(MAC 액세스 제어 목록)** → **Rule Configuration(규칙 구성)**를 클릭합니다.

그림 7-17. MAC ACL - Rule Configuration(규칙 구성)



MAC ACL Rule Configuration(MAC ACL 규칙 구성) 페이지에는 다음 필드가 포함되어 있습니다.

MAC ACL Name(MAC ACL 이름) — 기존 MAC ACL을 지정합니다. 새 MAC ACL을 설정하려면 [MAC ACL 구성](#) 페이지를 사용합니다.

Rule ID(규칙 ID) — 사용자 정의된 ACL을 선택하거나 만듭니다. 기존 규칙 ID를 입력하거나, 드롭다운 메뉴에서 Create(만들기)를 선택하고 옆에 있는 필드에 원하는 새 규칙 ID를 입력하여 새 규칙 ID를 만듭니다. Apply Changes(변경사항 적용)를 클릭하면 새 ID가 만들어집니다.

Action(동작) — 다음 ACL 전달 동작 중 하나를 선택합니다.

Permit(허용) — ACL 기준과 일치하는 패킷을 전달합니다.

Deny(거부) — ACL 기준과 일치하는 패킷을 삭제합니다.

Assign Queue ID(대기열 ID 할당) — 확인란을 클릭하여 이 기준을 적용한 후 0 ~ 6의 식별 번호를 입력합니다.

Redirect Interface(인터페이스 재지정) — 인터페이스의 드롭다운 목록에서 이 규칙에 적용되는 패킷을 재지정할 인터페이스를 선택합니다.

Mirror Interface(미러 인터페이스) — 인터페이스의 드롭다운 목록에서 이 규칙에 적용되는 패킷을 미러링할 인터페이스를 선택합니다.

Logging(로깅) — 이 ACL에 대한 로깅을 활성화하려면 확인란을 선택합니다. 이 기능은 Deny(거부) 작업에 대해서만 지원됩니다.

Match Every(모두 일치) — 패킷이 해당 ACL의 기준과 일치해야 합니다. 확인란을 클릭하여 이 기준을 적용합니다.

Class of Service(서비스 클래스) — 패킷의 CoS가 여기에 나열된 CoS 값과 일치해야 합니다. 확인란을 클릭하고 0과 7 사이의 CoS 값을 입력하여 이 기준을 적용합니다.

Secondary CoS(보조 CoS) — 패킷의 보조 CoS가 여기에 나열된 CoS 값과 일치해야 합니다. 확인란을 클릭하고 0과 7 사이의 CoS 값을 입력하여 이 기준을 적용합니다.

Destination MAC Address(대상 MAC 주소) — 패킷의 대상 포트 MAC 주소가 여기에 나열된 주소와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 주소를 입력합니다.

Destination MAC Mask(대상 MAC 마스크) — 원하는 경우 일치시킬 대상 MAC 마스크와 연결된 MAC 마스크를 입력합니다.

EtherType — 패킷의 EtherType이 여기에 나열된 EtherType과 일치해야 합니다. 확인란을 클릭하고 목록에서 선택하거나 EtherType ID를 입력합니다.

Select from List(목록에서 선택) — 드롭다운 메뉴에서 원하는 EtherType을 선택합니다.

Match to Value(값 일치) — 일치시킬 원하는 포트 번호를 입력합니다.

Source MAC Address(소스 MAC 주소) — 패킷의 소스 포트 MAC 주소가 여기에 나열된 주소와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 주소를 입력합니다.

Source MAC Mask(소스 MAC 마스크) — 원하는 경우 일치시킬 소스 MAC 주소의 MAC 마스크를 입력합니다.

VLAN ID — 패킷의 VLAN ID가 여기에 나열된 ID와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 VLAN ID를 입력합니다. 가능한 필드 값은 다음과 같습니다. 1-4093

Secondary VLAN(보조 VLAN) — 패킷의 보조 VLAN ID가 여기에 나열된 ID와 일치해야 합니다. 확인란을 클릭하고 이 기준을 적용할 보조 VLAN ID를 입력합니다. 가능한 필드 값은 다음과 같습니다. 1-4093

Remove(제거) — Remove(제거)가 선택되었을 때 Apply Changes(변경사항 적용)를 클릭하면 MAC ACL 규칙을 제거합니다.

MAC 기반 규칙 수정

주: 규칙이 속하는 ACL이 인터페이스에 연결되지 않는 경우에만 규칙을 수정할 수 있습니다.

1. MAC ACL Rule Configuration(MAC ACL 규칙 구성) 페이지를 엽니다.

2. **MAC ACL 드롭다운 메뉴**에서 **원하는 ACL**을 선택합니다.
3. **Rule ID(규칙 ID)** 드롭다운 메뉴에서 원하는 규칙을 선택합니다.
4. 필요에 따라 나머지 필드를 수정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
IP 기반 ACL이 수정되고 장치가 업데이트됩니다.

MAC 기반 ACL에 새 규칙 추가

1. **MAC ACL Rule Configuration(MAC ACL 규칙 구성)** 페이지를 엽니다.
2. **MAC ACL 드롭다운 메뉴**에서 **원하는 ACL**을 선택합니다.
3. **Rule ID(규칙 ID)**에 대해 **Create New Rule(새 규칙 만들기)**를 지정합니다.
4. 새 ID 번호를 입력합니다.
5. 필요에 따라 나머지 필드를 정의합니다.
6. **Apply Changes(변경사항 적용)**를 클릭합니다.
새 규칙이 지정된 MAC 기반 ACL에 할당됩니다.

MAC 기반 ACL에서 규칙 제거

1. ACL을 선택합니다.
2. **Rule ID(규칙 ID)** 드롭다운 메뉴에서 규칙을 선택합니다.
3. **Remove(제거)** 확인란을 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
MAC 기반 ACL이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 MAC 기반 ACL 규칙 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. ACL 명령

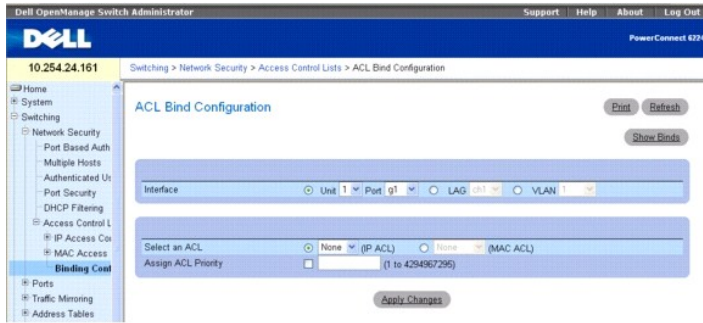
ACL 바인드 구성

ACL이 인터페이스에 연결되면 정의된 모든 규칙이 선택된 인터페이스에 적용됩니다. **ACL Bind Configuration(ACL 바인드 구성)** 페이지에서 ACL 목록을 ACL 우선 순위 및 인터페이스에 할당합니다.

해당 포트에 들어오는 패킷에 규칙이 적용되도록 웹 인터페이스에서 수신 방향의 ACL 규칙을 구성할 수 있습니다. CLI에서 수신 또는 발신 방향의 ACL 규칙을 구성할 수 있습니다. 발신 ACL은 포트에서 전송되는 트래픽의 보안 규칙을 구현합니다. ACL은 10G를 포함한 모든 물리적 인터페이스, LAG 또는 라우팅 포트에 적용될 수 있습니다.

ACL Bind Configuration(ACL 바인드 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Network Security(네트워크 보안)** → **Access Control Lists(액세스 제어 목록)** → **Binding Configuration(바인딩 구성)**을 클릭합니다.

그림 7-18. ACL Bind Configuration(ACL 바인드 구성)



ACL Bind Configuration(ACL 바인드 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 라디오 단추를 사용해 장치/포트, LAG 또는 VLAN을 선택합니다.

Select an ACL(ACL 선택) — 수신 패킷을 일치시킬 ACL 유형을 선택합니다. 패킷은 IP 기반 또는 MAC 기반 ACL과 일치시킬 수 있습니다.

Assign ACL Priority(ACL 우선 순위 할당) — 이 ACL의 우선 순위를 할당합니다. 인터페이스에 둘 이상의 ACL이 적용된 경우 가장 높은 우선 순위를 가진 ACL의 일치 조건이 제일 먼저 검사됩니다.

ACL을 인터페이스에 할당

1. **ACL Bind Configuration(ACL 바인드 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에 구성할 장치 및 포트, LAG 또는 VLAN을 지정합니다.
3. **Select an ACL(ACL 선택)** 필드에 IP 또는 MAC ACL을 선택합니다.

주: 포트, LAG 또는 VLAN에서 ACL이 할당될 때마다 ACL과 일치하지 않는 해당 수신 인터페이스의 흐름은 일치하지 않는 패킷을 삭제하는 기본 규칙과 일치합니다.

4. **Assign ACL Priority(ACL 우선 순위 할당)**에 우선 순위를 지정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

ACL이 지정된 인터페이스에 연결됩니다.

ACL에서 인터페이스 제거

1. **ACL Bind Configuration(ACL 바인드 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
3. 해당 인터페이스에 대한 ACL 바인딩을 확인하려면 **Interface(인터페이스)** 필드에 장치 및 포트, LAG 또는 VLAN을 지정합니다.
4. 제거할 하나 이상의 ACL에 대해 **Remove(제거)** 확인란을 선택합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

지정된 ACL이 인터페이스에서 제거됩니다.

CLI 명령을 사용하여 ACL 멤버십 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. ACL 명령

포트 구성

Ports(포트) 메뉴 페이지에는 뇌우 제어 및 포트 미러링과 같은 고급 기능을 비롯하여, 포트 기능을 구성하고 가상 포트 테스트를 수행하기 위한 링크가 제공됩니다.

페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→ **Ports(포트)**를 클릭합니다. **Ports(포트)** 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

- 1 [전역 매개변수](#)
- 1 [포트 구성](#)
- 1 [보호된 포트 구성](#)
- 1 [LAG 구성](#)
- 1 [뇌우 제어](#)

전역 매개변수

전역 매개변수를 사용하여 흐름 제어를 구성합니다. 흐름 제어를 사용하면 한 스위치의 트래픽을 지정된 시간 동안 스로울링할 수 있으며, 흐름 제어는 직접 연결된 스위치에 대해 정의됩니다. 흐름 제어는 전이중 작동 모드로 구성된 포트에 대해서만 설정할 수 있습니다. 자동 교성으로 설정된 포트는 LAG 구성원으로 추가되지 않을 수 있기 때문에 LAG 구성원 포트는 흐름 제어를 자동으로 구성할 수 없습니다.

주: 흐름 제어는 헤드 라인 블로킹 방지 모드와 호환되지 않습니다. 스위치는 어떤 모드에서도 작동할 수 있지만 동시에 작동하지는 않습니다.

Global Parameters(전역 매개변수) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→ **Ports(포트)**→ **Global Parameters(전역 매개변수)**를 클릭합니다.

그림 7-19. Global Port Parameters(전역 포트 매개변수)



Global Parameters(전역 매개변수) 페이지에는 다음 필드가 포함되어 있습니다.

Flow Control(흐름 제어) — 드롭다운 메뉴에서 활성화 또는 비활성화를 선택합니다. 이 명령은 스택의 모든 포트에 적용됩니다. 기본값은 Enable(활성)입니다.

Enabled(활성) — 스위치의 수신 백 프레서 메커니즘을 켭니다.

Disabled(비활성) — 스위치 작동을 헤드 라인 블로킹 방지로 복원합니다.

수신 백 프레서 활성화

1. **Ports Global Parameters(포트 전역 매개변수)** 페이지를 엽니다.
2. **Flow Control(흐름 제어)** 필드의 드롭다운 메뉴에서 Enable(활성)을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.
4. 이제 수신 백 프레서가 활성화되었습니다.

CLI 명령을 사용하여 흐름 제어 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

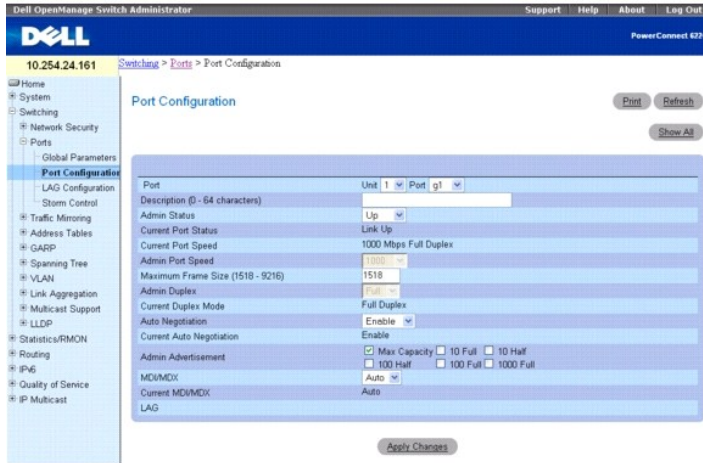
- 1 이더넷 구성 명령

포트 구성

Port Configuration(포트 구성) 페이지에서 포트 매개변수를 정의합니다.

Port Configuration(포트 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→ **Ports(포트)**→ **Port Configuration(포트 구성)**을 클릭합니다.

그림 7-20. Port Configuration(포트 구성)



Port Configuration(포트 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Port(포트) — 포트 매개변수가 정의된 장치와 포트를 지정합니다.

Description(설명) (0-64자) — 이더넷 등과 같은 간단한 인터페이스를 설명합니다.

Admin Status(관리 상태) — 포트를 통한 트래픽 전달을 활성화(Up)하거나 비활성화(Down)합니다.

Current Port Status(현재 포트 상태) — 포트의 현재 작동 가능 여부를 지정합니다.

Current Port Speed(현재 포트 속도) — 실제 동기화된 포트 속도(bps)를 표시합니다.

Admin Port Speed(관리 포트 속도) — 포트 속도를 선택한 값(10M, 100M, 1000M 또는 10000M)으로 강제 지정합니다.

Maximum Frame Size(최대 프레임 크기) (1518-9216) — 이 크기를 초과하는 패킷이 삭제되는 임계값을 지정합니다. 기본값은 1518입니다.

Admin Duplex(관리 이중) — 포트 이중 모드를 지정합니다. 옵션에는 전이중 또는 반이중이 있습니다.

Full(전이중) — 인터페이스가 스위치와 클라이언트 사이의 전송을 동시에 양방향으로 지원함을 나타냅니다.

Half(반이중) — 인터페이스가 스위치와 클라이언트 사이의 전송을 한 번에 한 방향으로만 지원함을 나타냅니다.

Current Duplex Mode(현재 이중 모드) — 동기화된 포트 이중 모드를 표시합니다.

Auto Negotiation(자동 교섭) — 포트에서 자동 교섭을 활성화합니다.

Auto Negotiation(자동 교섭)은 포트가 전송 속도, 이중 모드 및 흐름 제어 기능을 파트너에게 알릴 수 있도록 하는 두 링크 파트너 간의 프로토콜입니다.

Current Auto Negotiation(현재 자동 교섭) — 현재 자동 교섭 설정을 표시합니다.

Admin Advertisement(관리 알림) — 포트에서 알릴 수 있는 기능을 지정합니다. 가능한 필드 값은 다음과 같습니다.

Max Capability(최대 기능) — 허용 가능한 모든 포트 속도와 이중 모드 설정을 나타냅니다.

10 Half(10 반이중) — 포트가 100Mbps 속도와 반이중 모드 설정임을 알립니다.

10 Full(10 전이중) — 포트가 1000Mbps 속도와 전이중 모드 설정임을 알립니다.

100 Half(100 반이중) — 포트가 100Mbps 속도와 반이중 모드 설정임을 알립니다.

100 Full(100 전이중) — 포트가 1000Mbps 속도와 전이중 모드 설정임을 알립니다.

1000 Full(1000 전이중) — 포트가 1000Mbps 속도와 전이중 모드 설정임을 알립니다.

MDI/MDX — 스위치가 교차 및 비교차 케이블 간의 암호를 해독할 수 있습니다.

허브와 스위치는 종단국이 배선된 것과 반대로 배선되어 있어 허브나 스위치가 종단국에 연결되었을 때 스트레이트 스루 이더넷 케이블을 사용할 수 있으며, 쌍이 올바르게 일치합니다. 두 허브/스위치가 서로 연결되어 있거나, 두 개의 종단국이 서로 연결되어 있는 경우 교차 케이블을 사용하여 올바른 쌍이 연결되도록 합니다.

가능한 값은 다음과 같습니다.

On(켜기) — 스위치가 연결 유형을 감지할 수 있습니다.

Off(끄기) — 스위치에 연결하려면 올바른 케이블 유형이 필요합니다.

Auto(자동) — 값이 자동으로 설정됩니다.

Current MDI/MDX(현재 MDI/MDX) — 현재 스위치 MDX 설정을 나타냅니다. 가능한 필드 값은 다음과 같습니다.

MDI — 현재 MDI 설정이 MDI입니다.

MDX — 현재 MDI 설정이 MDX입니다.

Auto(자동) — 값이 자동으로 설정됩니다.

LAG — 이 포트가 LAG의 구성원인 경우 LAG 번호를 표시합니다.

포트 매개변수 정의

1. **Port Configuration(포트 구성)** 페이지를 엽니다.
2. **Unit(장치)** 및 **Port(포트)** 필드에서 장치와 포트를 선택합니다.
3. 화면에서 사용 가능한 필드를 정의합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 매개변수가 스위치에 저장됩니다.

포트 표 표시

1. **Port Configuration(포트 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.

Port Configuration Table(포트 구성 표)이 표시됩니다.

그림 7-21. Port Configuration Table(포트 구성 표)

Port	Port Status	Port Speed	Max Frame Size	Duplex Mode	Auto Negotiation	Flow Control	MDI/MDX	Copy To	Edit
1 1/1g1	Up	1000	1518	Full	Disable	Disable	Auto		
2 1/1g2	Up	10	1518	Full	Disable	Disable	Auto		
3 1/1g3	Up	100	1518	Full	Disable	Disable	Auto		

26 1/1ag2	Up	10	1518	Full	Disable	Disable	Auto		
27 1/1ag3	Up	10	1518	Full	Disable	Disable	Auto		
28 1/1ag4	Up	10	1518	Full	Disable	Disable	Auto		

3. 스택의 다른 장치(존재하는 경우)에 대해 **Port Configuration Table(포트 구성 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

포트 구성 설정 복사

1. **Port Configuration(포트 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
Port Configuration Table(포트 구성 표)이 표시됩니다.
3. **Copy Parameters From(매개변수 복사 위치)**에서 복사할 장치와 포트를 지정합니다.
4. 이 매개변수를 수신할 각 포트에 대해 **Copy To(복사 위치)**를 클릭합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 구성 설정이 복사되고 장치가 업데이트됩니다.

여러 포트에 대해 포트 구성 설정 수정

1. **Port Configuration(포트 구성)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

Port Configuration Table(포트 구성 표)이 표시됩니다.

3. 수정할 각 포트에 대해 **Edit(편집)**를 클릭합니다.

4. 필요에 따라 포트 구성 필드를 편집합니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 구성 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령으로 포트 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

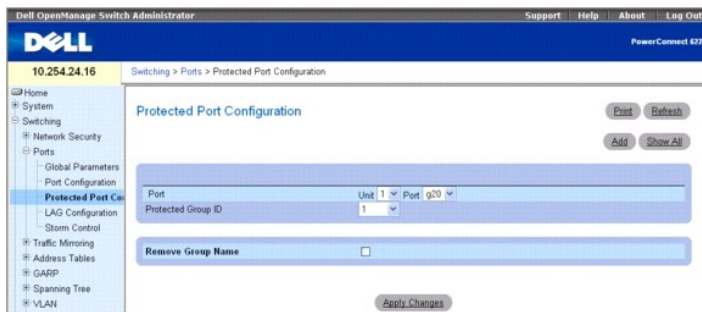
- 1 이더넷 구성 명령

보호된 포트 구성

PVE(사설 VLAN 예치) 포트는 동일한 VLAN의 구성원인 포트 간에 포트 기반 보안을 제공하는 계층 2 보안 기능으로, 이 기능을 지정하려면 **Protected Port Configuration(보호된 포트 구성)**을 사용합니다. 보호된 포트에서 들어오는 트래픽은 업링크 포트로만 전송되며 VLAN 내의 다른 포트로는 전송될 수 없습니다.

Port Configuration(포트 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Ports(포트)** → **Protected Port Configuration(보호된 포트 구성)**을 클릭합니다.

그림 7-22. Protected Port Configuration(보호된 포트 구성)



Protected Port Configuration(보호된 포트 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Port(포트) — 포트 매개변수가 정의된 장치와 포트를 지정합니다.

Protected Group ID(보호된 그룹 ID) — 포트를 그룹 0, 1 또는 2에 할당하는 드롭다운 메뉴입니다.

Remove Group Name(그룹 이름 제거) — 보호된 그룹에서 선택한 포트 연결을 끊으려면 이 확인란을 선택합니다.

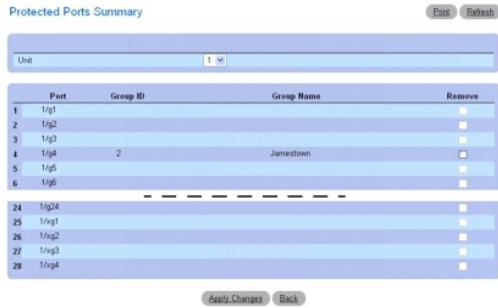
보호된 포트 표 표시

1. **Protected Port Configuration(보호된 포트 구성)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

Protected Ports Summary Table(보호된 포트 요약 표)이 표시됩니다.

그림 7-23. Protected Port Summary Table(보호된 포트 요약 표)



3. 보호된 그룹에서 포트 연결을 끊으려면 **Remove(제거)** 확인란을 선택하고 **Apply Changes(변경사항 적용)**를 클릭합니다.
4. 스크의 다른 장치(존재하는 경우)에 대해 **Protected Port Summary Table(보호된 포트 요약 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

보호된 포트 그룹 추가

1. **Protected Port Configuration(보호된 포트 구성)** 페이지를 엽니다.
2. **Add(추가)**를 클릭합니다.

Add Protected Group(보호된 그룹 추가) 페이지가 표시됩니다.

그림 7-24. Add Protected Port(보호된 포트 추가)



3. **Protected Group ID(보호된 그룹 ID)**에 번호(0, 1 또는 2)를 할당하려면 드롭다운 메뉴를 사용합니다.
4. **Protected Group Name(보호된 그룹 이름)(1-32 characters)**을 입력합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

Protected Group(보호된 그룹) 설정이 복사되고 장치가 업데이트됩니다.

CLI 명령으로 보호된 포트 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

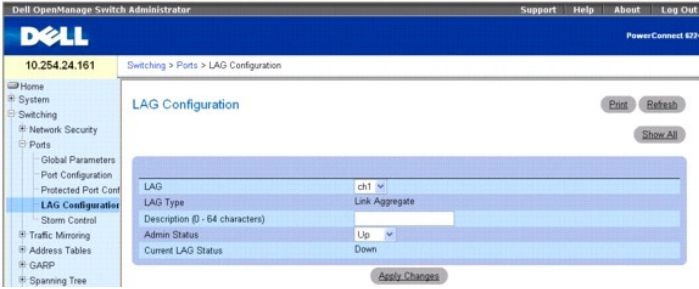
- 1 스위치 포트 보호 명령

LAG 구성

링크 결함을 사용하면 하나 이상의 전이중 이더넷 링크를 함께 결합하여 LAG(Link Aggregation Group)를 만들 수 있습니다. 스위치는 LAG를 단일 링크로 취급할 수 있습니다.

LAG Configuration(LAG 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Ports(포트)** → **LAG Configuration(LAG 구성)**을 클릭합니다.

그림 7-25. LAG Configuration(LAG 구성)



LAG Configuration(LAG 구성) 페이지에는 다음 필드가 포함되어 있습니다.

LAG — LAG 구성원의 목록이 포함되어 있습니다.

LAG Type(LAG 유형) — LAG를 구성하는 포트 유형입니다.

Description(설명) (0-64자) — 포트의 설명입니다.

Admin Status(관리 상태) — 선택한 LAG를 통해 전달되는 트래픽을 활성화하거나 비활성화합니다.

Current LAG Status(현재 LAG 상태) — 선택한 LAG가 작동하는지 또는 다운되었는지 표시합니다.

LAG 매개변수 정의

1. LAG Configuration(LAG 구성) 페이지를 엽니다.
2. LAG 필드에서 LAG를 선택합니다.
3. 화면에서 사용 가능한 필드를 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

LAG 매개변수가 스위치에 저장됩니다.

LAG 구성 표 표시

1. LAG Configuration(LAG 구성) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
3. LAG Configuration Table(LAG 구성 표)이 표시됩니다.

그림 7-26. LAG Configuration Table(LAG 구성 표)

LAG Configuration Table Print Refresh

LAG	Description	LAG Type	Admin Status	Current Flow Control	Edit
1 lag1		Link Aggregation	Up	Disable	<input type="checkbox"/>
2 lag2		Link Aggregation	Up	Disable	<input type="checkbox"/>
3 lag3		Link Aggregation	Up	Disable	<input type="checkbox"/>
4 lag4		Link Aggregation	Up	Disable	<input type="checkbox"/>
5 lag5		Link Aggregation	Up	Disable	<input type="checkbox"/>
6 lag6		Link Aggregation	Up	Disable	<input type="checkbox"/>
7 lag7		Link Aggregation	Up	Disable	<input type="checkbox"/>
8 lag8		Link Aggregation	Up	Disable	<input type="checkbox"/>

Apply Changes Back

LAG 매개변수 편집

1. LAG Configuration(LAG 구성) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
3. LAG Configuration Table(LAG 구성 표)이 표시됩니다.

- 수정할 모든 LAG에 대해 **Edit(편집)**를 클릭합니다.
- 이제 **Admin Status(관리 상태)** 및 **Description(설명)**을 필요에 따라 편집할 수 있습니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.

LAG 매개변수가 스위치에 저장됩니다.

CLI 명령으로 LAG 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 포트 채널 명령

뇌우 제어

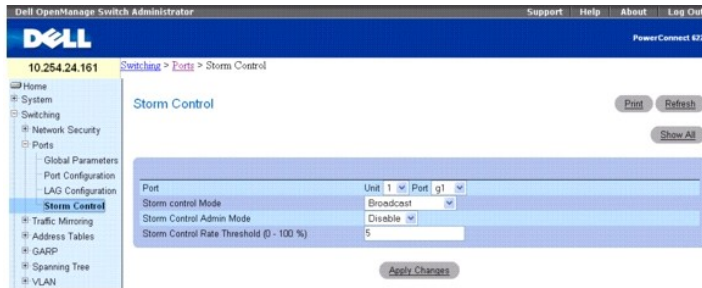
브로드캐스트 뇌우는 단일 포트에서 네트워크로 과도한 브로드캐스트 메시지 수가 동시에 전송된 결과입니다. 전달된 메시지 응답은 네트워크 자원의 용량을 초과하거나 네트워크 타임아웃을 유발할 수 있습니다.

스위치는 포트당 수신 브로드캐스트/멀티캐스트/알 수 없는 유니캐스트 패킷 속도를 측정하고 이 속도가 정의된 값을 초과하면 패킷을 삭제합니다. 뇌우 제어는 패킷이 전송되는 속도와 패킷 유형을 정의함으로써 인터페이스별로 활성화됩니다.

뇌우 제어를 활성화하고 구성하려면 **Storm Control(뇌우 제어)** 페이지를 사용합니다.

Storm Control(뇌우 제어) 인터페이스를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Ports(포트)** → **Storm Control(뇌우 제어)**를 클릭합니다.

그림 7-27. Storm Control(뇌우 제어)



Storm Control(뇌우 제어) 페이지에는 다음 필드가 포함되어 있습니다.

Port(포트) — 뇌우 제어가 활성화된 **Unit(장치)** 및 **Port(포트)**를 지정합니다.

Storm Control Mode(뇌우 제어 모드) — 뇌우 제어의 영향을 받는 브로드캐스트 모드를 지정합니다.

Broadcast(브로드캐스트) — 인터페이스에 수신되는 L2 브로드캐스트 트래픽의 속도가 구성된 임계값을 초과하여 증가하면 트래픽이 삭제됩니다.

Multicast(멀티캐스트) — 인터페이스에 수신되는 L2 멀티캐스트 트래픽의 속도가 구성된 임계값을 초과하여 증가하면 트래픽이 삭제됩니다.

Unknown Unicast(알 수 없는 유니캐스트) — 인터페이스에 수신되는 알 수 없는 L2 유니캐스트(대상 조회 실패)의 속도가 구성된 임계값을 초과하여 증가하면 트래픽이 삭제됩니다.

Storm Control Admin Mode(뇌우 제어 관리 모드) — 뇌우 제어를 활성화하거나 비활성화합니다.

Storm Control Rate Threshold(뇌우 제어율 임계값) (0-100%) — 알 수 없는 패킷이 전달되는 최대 비율을 지정합니다. 범위는 총 임계값의 1%입니다.

뇌우 제어 포트 매개변수 정의

- Storm Control(뇌우 제어)** 인터페이스를 엽니다.
- 화면의 필드를 편집합니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.

뇌우 제어 포트 매개변수가 스위치에 저장됩니다.

뇌우 제어 설정 표 표시

1. Storm Control(뇌우 제어) 인터페이스를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Storm Control Settings Table(뇌우 제어 설정 표)이 표시됩니다.

그림 7-28. Storm Control Settings Table(뇌우 제어 설정 표)

Unit	Broadcast Control Mode	Broadcast Rate Threshold	Multicast Control Mode	Multicast Rate Threshold	Unicast Control Mode	Unicast Rate Threshold	Edit
1 1/g1	Disable	5	Disable	5	Disable	5	<input checked="" type="checkbox"/>
2 1/g2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
3 1/g3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>

26 1/g2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
27 1/g3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
28 1/g4	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>

3. 스택의 다른 장치(존재하는 경우)에 대해 Storm Control Settings Table(뇌우 제어 설정 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

브로드캐스트 제어 수정

1. Storm Control(뇌우 제어) 인터페이스를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
Storm Control Settings Table(뇌우 제어 설정 표)이 표시됩니다.
3. Broadcast Control(브로드캐스트 제어)을 수정할 각 포트에 대해 Edit(편집)를 선택합니다.
4. 필요에 따라 Broadcast Control(브로드캐스트 제어)을 편집합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

뇌우 제어 포트 매개변수가 스위치에 저장됩니다.

CLI 명령으로 뇌우 제어 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. 이더넷 구성 명령

트래픽 미러링 구성

트래픽 미러링을 통해 사용자는 미러링 포트에 미러링되는 포트에서 패킷의 사본을 전송하도록 스위치를 구성할 수 있습니다. 미러링은 포트 기반이거나 흐름 기반일 수 있습니다.

Traffic Mirroring(트래픽 미러링) 메뉴 페이지에서 포트 미러링 세션을 정의하고 흐름 기반 미러링을 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치)→ Traffic Mirroring(트래픽 미러링)을 클릭합니다. Traffic Mirroring(트래픽 미러링) 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

1. [포트 미러링](#)
1. [흐름 기반 미러링](#)

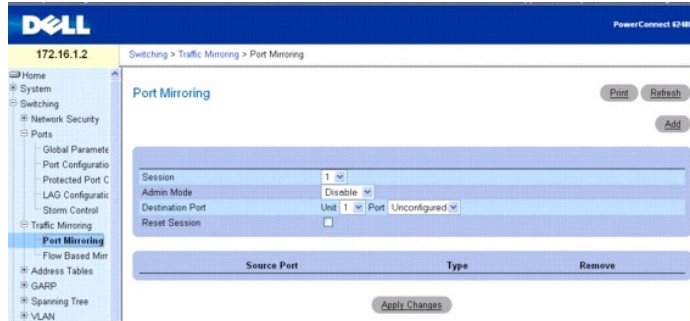
포트 미러링

포트 미러링은 네트워크 분석기에 의한 분석을 위해 네트워크 트래픽을 선택합니다. 이 작업은 스위치의 특정 포트에 대해 수행됩니다. 따라서 많은 스위치 포트가 소스 포트에 구성되고 하나의 스위치 포트가 대상 포트에 구성됩니다. 사용자는 소스 포트에서 미러링되는 트래픽의 양을 구성할 수 있습니다. 소스 포트에 수신되고 포트에서 전송되거나 수신 및 전송되는 패킷은 대상 포트에서 미러링할 수 있습니다.

대상 포트에 복사되는 패킷은 배선의 원래 패킷과 형식이 같습니다. 따라서 미러에서 수신된 패킷을 복사하는 경우, 복사된 패킷은 소스 포트에서 수신될 때 VLAN 태그가 지정되거나 해제됩니다. 미러에서 전송되는 패킷을 복사하는 경우, 복사된 패킷은 소스 포트에서 전송될 때 VLAN 태그가 지정되거나 해제됩니다.

Port Mirroring(포트 미러링) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **Traffic Mirroring(트래픽 미러링)** → **Port Mirroring(포트 미러링)**을 클릭합니다.

그림 7-29. Port Mirroring(포트 미러링)



Port Mirroring(포트 미러링) 페이지에는 다음 필드가 포함되어 있습니다.

Session(세션) — 모니터링 세션을 지정합니다.

Admin Mode(관리 모드) — 포트 미러링을 활성화하거나 비활성화합니다.

Destination Port(대상 포트) — 포트 트래픽을 복사할 수 있는 대상 포트를 선택합니다.

Reset Session(세션 재설정) — 포트 미러링 세션을 재설정할 수 있습니다.

Source Port(소스 포트) — Add Source Port(소스 포트 추가) 페이지에서 추가된 소스 포트를 나열합니다.

Type(유형) — 소스 포트에서 모니터링 유형 트래픽을 표시합니다.

포트 미러링 세션 추가

주: 포트는 대상 미러가 될 경우 VLAN 또는 LAG에서 제거됩니다.

1. **Port Mirroring(포트 미러링)** 페이지를 엽니다.
2. **Add(추가)**를 클릭하여 **Add Source Port(소스 포트 추가)** 페이지를 표시합니다.

그림 7-30. Add Source Port(소스 포트 추가)



3. 다음 필드를 구성합니다.

Session(세션) — 모니터링 세션을 선택합니다.

Source Port(소스 포트) — 트래픽을 미러링 장치와 포트를 선택합니다. 최대 4개의 소스 포트를 대상 포트에 미러링할 수 있습니다.

Type(유형) — 모니터링되는 트래픽의 유형을 지정합니다. 가능한 필드 값은 다음과 같습니다.

- TX** — 전송된 패킷만 모니터링합니다.
- RX** — 수신된 패킷만 모니터링합니다.
- TX and RX(TX 및 RX)** — 전송 및 수신된 패킷을 모니터링합니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

장치와 포트에 대해 새 포트 미러링 세션이 활성화되고 장치가 업데이트됩니다. 소스 포트가 Port Mirroring(포트 미러링) 페이지의 Source Port(소스 포트) 표에 나타납니다.

포트 미러링 세션 수정

1. **Port Mirroring(포트 미러링)** 페이지를 엽니다.
2. 필드를 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 미러링 세션 필드가 수정되고 장치가 업데이트됩니다.

포트 미러링 세션 제거

1. **Port Mirroring(포트 미러링)** 페이지를 엽니다.
2. **Reset Session(세션 재설정)** 확인란을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 미러링 세션이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 포트 미러링 세션 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. 포트 모니터 명령

흐름 기반 미러링

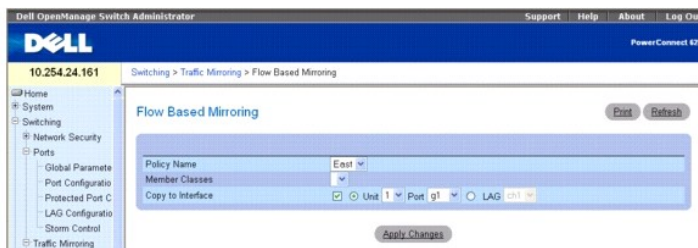
흐름 기반 미러링 기능은 QoS의 Diffserv 구성 요소에 따라 구축됩니다. QoS에서 사용자는 트래픽 클래스를 만들고 일치 조건을 정의한 다음 정책을 만들어 해당 트래픽 클래스에 수행할 동작을 정의합니다.

흐름 기반 미러링을 사용하면 특정 유형의 트래픽을 단일 대상 포트에 복사할 수 있습니다. 이는 스위치가 포트에서 모든 수신 또는 발신 트래픽을 미러링하는 대신, 해당 트래픽의 서브세트를 미러링할 수 있는 유연성을 제공합니다. 총 2, 3 및 4 정보를 기반으로 흐름을 미러링하도록 스위치를 구성할 수 있습니다.

흐름 기반 미러링 포트를 지정하려면 **Flow Based Mirroring(흐름 기반 미러링)** 페이지를 사용합니다.

Flow Based Mirroring(흐름 기반 미러링) 페이지를 표시하려면 **Switching(스위칭)** → **Traffic Mirroring(트래픽 미러링)** → **Flow Based Mirroring(흐름 기반 미러링)**을 클릭합니다.

그림 7-31. Flow Based Mirroring(흐름 기반 미러링)



Flow Based Mirroring(흐름 기반 미러링) 페이지에는 다음 필드가 포함되어 있습니다.

Policy Name(정책 이름) — 트래픽 클래스와 연결할 정책을 선택합니다. Policy Name(정책 이름)은 Diffserv "[정책 구성](#)" 웹 페이지에서 정의합니다.

Member Classes(구성원 클래스) — 이 정책과 연결할 트래픽 클래스를 선택합니다. Member Class(구성원 클래스)는 Diffserv "[클래스 구성](#)" 웹 페이지에서 정의합니다.

Copy to Interface(인터페이스로 복사) — 선택하면 패킷이 장치/포트 또는 LAG에 복사됩니다.

미러링을 대상 포트에 복사

1. **Flow Based Mirroring(흐름 기반 미러링)** 페이지를 엽니다.

2. Policy Name(정책 이름) 및 Member Class(구성원 클래스)를 지정하고 Copy to Interface(인터페이스로 복사)에서 적용할 대상 장치와 포트를 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

흐름 기반 미러링 세부사항이 지정된 포트로 복사되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 흐름 기반 미러링 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 QOS 명령

주소 표 구성

MAC 주소는 정적 또는 동적 주소 표에 저장됩니다. 정적 주소는 사용자가 정의합니다. 동적 주소는 시스템에서 탐지되며 타임아웃 후 지워집니다. 표 중 하나에 저장된 대상으로 지정된 패킷은 즉시 포트로 전달됩니다. 정적 및 동적 주소 표는 인터페이스, VLAN ID 또는 VLAN 이름별로 정렬할 수 있습니다. 또한 정적 및 동적 주소 표에 주소를 추가할 수 있습니다.

Address Tables(주소 표) 메뉴 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭) → Address Tables(주소 표)를 클릭합니다. Address Tables(주소 표) 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

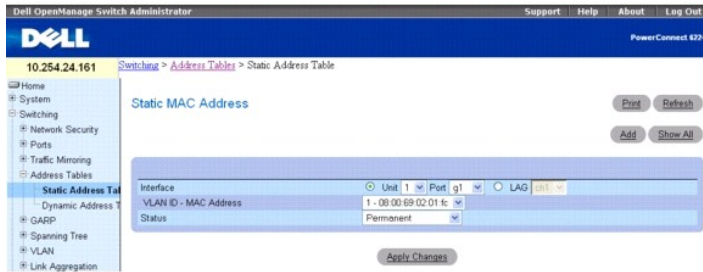
- 1 [정적 주소 표](#)
- 1 [동적 주소 표](#)

정적 주소 표

Static MAC Address(정적 MAC 주소) 페이지에는 정적 MAC 주소 목록이 포함되어 있습니다. 정적 주소는 정적 MAC 주소 표에서 제거하거나 추가할 수 있습니다.

Static MAC Address(정적 MAC 주소) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭) → Address Tables(주소 표) → Static Address Table(정적 주소 표)를 클릭합니다.

그림 7-32. Static MAC Address(정적 MAC 주소)



Static MAC Address(정적 MAC 주소) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 정적 MAC 주소가 적용되는 장치와 포트 또는 LAG를 지정합니다. 다른 장치/포트 또는 LAG의 주소를 보려면 여기에 나열된 인터페이스를 변경합니다.

VLAN ID - MAC Address(VLAN ID - MAC 주소) — 현재 정적 주소 목록에 포함된 MAC 주소에 연결된 VLAN ID를 지정합니다.

주: 지정된 인터페이스와 VLAN에 할당된 MAC 주소만 표시됩니다.

Status(상태) — MAC 주소의 상태를 지정합니다. 가능한 값은 다음과 같습니다.

- Permanent(영구) — MAC 주소는 영구적입니다.
- Secure(보안) — 장기간 포트 MAC 주소가 삭제되지 않도록 합니다.
- Delete on Reset(재설정 시 삭제) — 스위치가 재설정될 때 MAC 주소가 삭제됩니다.
- Delete on Timeout(타임아웃 시 삭제) — 타임아웃이 발생하면 MAC 주소가 삭제됩니다.

정적 MAC 주소 추가

1. Static MAC Address(정적 MAC 주소) 페이지를 엽니다.

2. Add(추가)를 클릭합니다.

Add Static MAC Address(정적 MAC 주소 추가) 페이지가 표시됩니다.

그림 7-33. Adding Static MAC Address(정적 MAC 주소 추가)

3. 필요에 따라 필드를 입력합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

새 정적 주소가 Static MAC Address Table(정적 MAC 주소 표)에 추가되고 장치가 업데이트됩니다.

정적 MAC 주소 표에서 정적 주소 수정

1. Static MAC Address(정적 MAC 주소) 페이지를 엽니다.
2. 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

정적 MAC 주소가 수정되고 장치가 업데이트됩니다.

정적 MAC 주소 표 표시

1. Static MAC Address(정적 MAC 주소) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Static MAC Address Table(정적 MAC 주소 표)에 기존 정적 MAC 주소가 모두 표시됩니다.

그림 7-34. Static MAC Address Table(정적 MAC 주소 표)

	MAC	VLAN ID	Interface	Status	Remove
1	08:00:89:02:01:FC	1	1/g1	Permanent	<input type="checkbox"/>
2	08:A6:89:02:01:28	2	1/g5	Permanent	<input type="checkbox"/>

정적 주소 표에서 정적 주소 제거

1. Static MAC Address(정적 MAC 주소) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭하여 Static MAC Address Table(정적 MAC 주소 표)을 표시합니다.
3. 제거할 주소에 대해 Remove(제거) 확인란을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

정적 주소가 삭제되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 정적 주소 매개변수 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 주소 표 명령

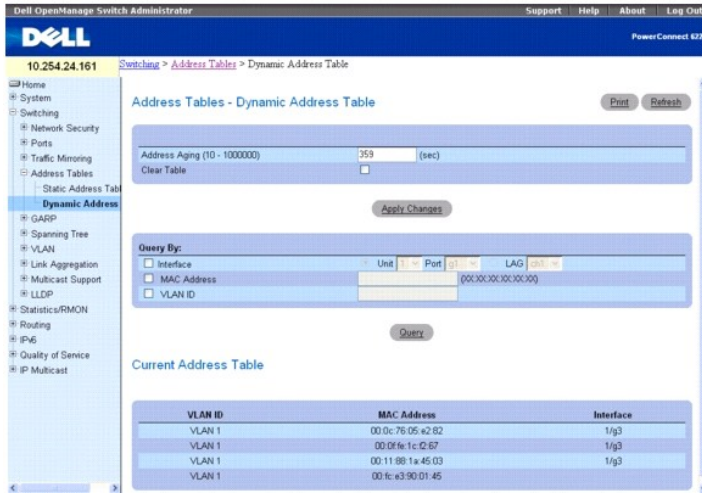
동적 주소 표

Dynamic Address Table(동적 주소 표) 페이지에는 인터페이스 유형, MAC 주소, VLAN 및 표 정렬 키를 포함하여 동적 주소 표의 정보를 질의하기 위한 필드가 포함되어 있습니다. 주소 표에 저장된 주소로 전달된 패킷은 해당 포트로 직접 전달됩니다.

Dynamic Address Table(동적 주소 표)에는 동적 MAC 주소가 표에서 제거되는 유지 시간에 대한 정보도 포함되어 있습니다.

Dynamic Address Table(동적 주소 표)을 표시하려면 디렉터리 화면에서 Switching(스위칭)→ Address Tables(주소 표)→ Dynamic Address Table(동적 주소 표)을 클릭합니다.

그림 7-35. Dynamic Address Table(동적 주소 표)



Dynamic Address Table(동적 주소 표)에는 다음 필드가 포함되어 있습니다.

Address Aging(주소 유지) (10-1000000) — 동적 MAC 주소가 지워지는 유지 시간을 초 단위로 지정합니다. 기본값은 300초입니다.

Clear Table(표 지우기) — 이 옵션을 선택하고 Apply Changes(변경사항 적용)를 클릭하는 경우 표에서 동적 MAC 주소 데이터를 모두 지웁니다.

Dynamic Address Table(동적 주소 표)은 다음을 기준으로 질의할 수 있습니다.

Interface(인터페이스) — 주소에 대해 질의된 장치와 포트를 지정합니다.

LAG — 주소에 대해 질의된 LAG를 지정합니다.

MAC Address(MAC 주소) — 주소에 대해 질의된 MAC 주소를 지정합니다.

VLAN ID — 주소에 대해 질의된 VLAN 번호(MAC 주소가 연결된)를 지정합니다.

Current Address Table(현재 주소 표)에는 패킷이 포트에 직접 전달되는 동적 주소 매개변수가 포함되어 있습니다. Current Address Table(현재 주소 표)에는 다음 필드가 포함되어 있습니다.

VLAN ID — VLAN 태그 값을 표시합니다.

MAC Address(MAC 주소) — MAC 주소를 표시합니다.

Interface(인터페이스) — 포트 번호를 표시합니다.

유지 시간 정의

1. Dynamic Address Table(동적 주소 표) 페이지를 엽니다.
2. Address Aging(주소 유지) 필드를 정의합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

유지 시간이 수정되고 장치가 업데이트됩니다.

동적 주소 표 질의

1. **Dynamic Address Table(동적 주소 표)** 페이지를 엽니다.
2. **Dynamic Address Table(동적 주소 표)**을 질의할 매개변수를 정의합니다.
항목은 **Interface(인터페이스)**, **LAG**, **MAC Address(MAC 주소)** 또는 **VLAN ID**별로 질의할 수 있습니다.
3. 동적 주소 표를 질의하려면 **Query(질의)**를 클릭합니다.

동적 주소 표에서 데이터 제거

1. **Dynamic Address Table(동적 주소 표)** 페이지를 엽니다.
2. **Clear Table(표 지우기)**을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.
Dynamic Address Table(동적 주소 표)의 모든 데이터가 지워집니다.

CLI 명령을 사용하여 동적 주소 질의 및 정렬

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 주소 표 명령

GARP 구성

GARP(Generic Attribute Registration Protocol)는 모든 네트워크 연결 또는 멤버십 유형 정보를 등록하는 일반 용도의 프로토콜입니다. GARP는 VLAN 또는 멀티캐스트 주소와 같은 주어진 네트워크 속성과 관련된 스위치 세트를 정의합니다. **GARP Timers(GARP 타이머)** 페이지는 **GARP** 메뉴 페이지에서 열 수 있습니다.

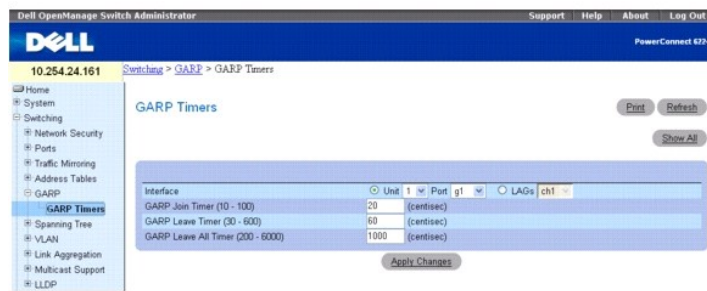
GARP 메뉴 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**GARP**를 클릭합니다.

GARP 타이머

GARP Timers(GARP 타이머) 페이지에는 스위치에 GARP를 활성화하기 위한 필드가 포함되어 있습니다.

GARP Timers(GARP 타이머) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**GARP**→**GARP Timers(GARP 타이머)**를 클릭합니다.

그림 7-36. GARP Timers(GARP 타이머)



GARP Timers(GARP 타이머) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — GARP 타이머가 활성화된 장치와 포트 또는 LAG를 지정합니다.

GARP Join Timer(GARP 연결 타이머) (10-100) — PDU가 전송되는 시간(센티초)을 표시합니다. 가능한 필드 값은 10 ~ 100이고 기본값은 100센티초입니다.

GARP Leave Timer(GARP 해제 타이머) (30-600) — 스위치가 GARP 상태에서 해제되기 전에 기다리는 시간(센티초)을 표시합니다. 해제 시간은 전송/수신된 Leave All Time (모든 해제 시간) 메시지에 의해 활성화되고, 수신되는 Join(연결) 메시지에 의해 취소됩니다. 해제 시간은 연결 시간의 세 배 이상이거나 같아야 합니다. 가능한 필드 값은 30 ~ 600이고 기본값은 60센티초입니다.

GARP Leave All Timer(GARP 모두 해제 타이머) (200-6000) — 모든 스위치가 GARP 상태에서 해제되기 전에 기다리는 시간(센티초)을 표시합니다. 모두 해제 시간은 해제 시

값보다 커야 합니다. 가능한 필드 값은 200 ~ 6000이고 기본값은 1000센티초입니다.

GARP 타이머 정의

1. GARP Timers(GARP 타이머) 페이지를 엽니다.
2. 필드를 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

매개변수가 GARP 타이머 표의 선택된 포트나 LAG로 복사되고 장치가 업데이트됩니다.

GARP 타이머 표에 매개변수 표시

1. GARP Timers(GARP 타이머) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

GARP Timers Table(GARP 타이머 표)이 표시됩니다.

그림 7-37. GARP Timers Table(GARP 타이머 표)

Interface	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	Copy To	Edit
1 1/ig1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
2 1/ig2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
3 1/ig3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
27 1/ig3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
28 1/ig4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
LAGs					
29 ch1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
30 ch2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
31 ch3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
32 ch4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
33 ch5	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
34 ch6	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
35 ch7	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
36 ch8	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>

3. 스크의 다른 장치(존재하는 경우)에 대해 GARP Timers Table(GARP 타이머 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

GARP 타이머 설정 복사

1. GARP Timers(GARP 타이머) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

GARP Timers Table(GARP 타이머 표)이 표시됩니다.

3. Copy Parameters From(매개변수 복사 위치)에서 복사할 장치와 포트를 지정합니다.
4. 이 매개변수를 수신할 각 인터페이스에 대해 Copy To(복사 위치)를 클릭합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

GARP 타이머 설정이 복사되고 장치가 업데이트됩니다.

여러 포트에 대해 GARP 타이머 설정 수정

1. **GARP Timers(GARP 타이머)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

GARP Timers Table(GARP 타이머 표)이 표시됩니다.

3. 수정할 각 인터페이스에 대해 **Edit(편집)**를 클릭합니다.

4. 필요에 따라 GARP 타이머 필드를 편집합니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

GARP 타이머 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 GARP 타이머 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 GVRP 명령

스패닝 트리 프로토콜 구성

STP(Spanning Tree Protocol)는 브리지의 모든 배열에 대한 트리 토폴로지를 제공합니다. 또한 네트워크상의 종단국 간에 하나의 경로를 제공하여 루프를 제거하기도 합니다. 지원되는 스페닝 트리 버전에는 Classic STP(클래식 STP), Multiple STP(다중 STP) 및 Rapid STP(빠른 STP) 등이 있습니다.

Classic STP(클래식 STP)는 종단국 간에 단일 경로를 제공하여 루프를 방지 및 제거합니다. Classic STP(클래식 STP) 구성에 대한 자세한 내용은 "[STP 전역 설정](#)"을 참조하십시오.

MSTP(Multiple Spanning Tree Protocol)는 VLAN 트래픽을 다른 인터페이스를 통해 효과적으로 전달하기 위해 스페닝 트리의 여러 인스턴스를 지원합니다. 스페닝 트리의 각 인스턴스는 IEEE 802.1w, RSTP(Rapid Spanning Tree)에 지정된 방식으로 작동하며, 작동 시에는 약간 수정되지만 최종 효과는 수정되지 않습니다(주요 효과 중 하나는 포트가 '전달' 상태로 빠르게 전환되는 것임). RSTP와 일반적인 STP(IEEE 802.1d) 간의 차이점은 전이중 연결과 종단국에 연결된 포트를 구성 및 인식할 수 있기 때문에 포트를 '전달' 상태로 빠르게 전환하고 Topology Change Notification(토폴로지 변경 알림)을 억제할 수 있다는 것입니다. 이러한 기능은 'pointpoint' 및 'edgeport' 매개변수로 표시됩니다. MSTP는 RSTP와 STP 모두와 호환됩니다. 이는 STP 및 RSTP 브리지에 적합하게 작동합니다. MSTP 브리지는 모두 RSTP 브리지 또는 STP 브리지로 작동하도록 구성할 수 있습니다.

Spanning Tree(스패닝 트리) 메뉴 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Spanning Tree(스패닝 트리)**를 클릭합니다. 이 **Spanning Tree(스패닝 트리)** 페이지에는 다음 STP 절차에 대한 링크가 포함되어 있습니다.

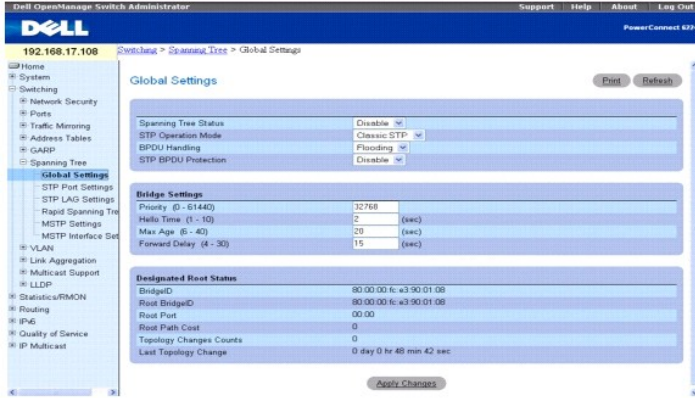
- 1 [STP 전역 설정](#)
- 1 [STP 포트 설정](#)
- 1 [STP LAG 설정](#)
- 1 [빠른 스페닝 트리](#)
- 1 [MSTP 설정](#)
- 1 [MSTP 인터페이스 설정](#)

STP 전역 설정

STP Global Settings(STP 전역 설정) 페이지에는 스위치에 STP를 활성화하기 위한 필드가 포함되어 있습니다.

STP Global Settings(STP 전역 설정) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Spanning Tree(스패닝 트리)**→**Global Settings(전역 설정)**를 클릭합니다.

그림 7-38. Spanning Tree Global Settings(스패닝 트리 전역 설정)



STP Global Settings(STP 전역 설정) 페이지에는 다음 필드가 포함되어 있습니다.

Spanning Tree Status(스패닝 트리 상태) — 스위치에서 RSTP, STP 또는 MSTP를 활성화하거나 비활성화합니다.

STP Operation Mode(STP 작동 모드) — 스위치에서 STP가 활성화된 STP 모드를 지정합니다. 가능한 필드 값은 다음과 같습니다. **Classic STP(클래식 STP)**, **Rapid STP(빠른 STP)** 및 **Multiple STP(다중 STP)**입니다.

BPDU Handling(BPDU 처리) — 인터페이스에서 스페닝 트리가 비활성화되었을 때 BPDU(Bridge Protocol Data Unit) 패킷 처리를 지정합니다. 가능한 필드 값은 Filtering(필터링) 및 Flooding(플러딩)입니다. 기본값은 Flooding(플러딩)입니다.

STP BPDU Protection(STP BPDU 보호) — 새 스위치가 STP의 기존 토폴로지에 들어가려고 할 때 포트를 비활성화합니다. 이렇게 하면 STP의 원래 부분이 아닌 스위치가 STP 토폴로지에 영향을 주는 것을 방지합니다.

Enable(활성)로 설정한 경우, BPDU가 중단 포트에 수신되면 해당 포트가 비활성화됩니다. 포트가 비활성화된 경우에는 수동으로 재활성화해야 합니다.

브리지 설정

Priority(우선 순위) (0-61440) — 브리지 우선 순위 값을 지정합니다. 스위치 또는 브리지가 STP를 실행 중인 경우 각 항목의 우선 순위가 해당됩니다. BPDU를 교환한 후에는 가장 낮은 우선 순위 값을 가진 스위치가 루트 브리지가 됩니다.

Hello Time(Hello 시간) (1-10) — 루트 브리지가 구성 메시지 간에 대기하는 시간(초)을 나타내는 스위치 Hello 시간을 지정합니다. 기본값은 2입니다.

Max Age(최대 보존 기간) (6-40) — 브리지가 토폴로지 변경을 구현하기 전에 대기하는 시간(초)을 나타내는 스위치 최대 보존 기간을 지정합니다. 기본값은 20입니다.

Forward Delay(전달 지연) (4-30) — 브리지가 패킷을 전달하기 전에 탐지 및 청취 상태를 유지하는 시간(초)을 나타내는 스위치 전달 지연 시간을 지정합니다. 기본값은 15입니다.

지정된 루트 상태

Bridge ID(브리지 ID) — 브리지 ID를 표시합니다.

Root Bridge ID(루트 브리지 ID) — 루트 브리지 ID를 지정합니다.

Root Port(루트 포트) — 이 브리지에서 루트 브리지까지 가장 낮은 비용 경로를 제공하는 포트 번호를 표시합니다. 이는 브리지가 루트가 아닌 경우 중요합니다. 기본값은 0입니다.

Root Path Cost(루트 경로 비용) — 이 브리지에서 루트까지의 경로 비용을 표시합니다.

Topology Changes Counts(토폴로지 변경 수) — 발생한 STP 상태 변경사항의 총 수를 표시합니다.

Last Topology Change(마지막 토폴로지 변경) — 마지막 토폴로그래픽이 변경된 후의 전체 시간을 표시합니다. 시간은 5시간 10분 4초와 같이 일/시/분/초 형식으로 표시됩니다.

STP 전역 매개변수 정의

1. STP Global Settings(STP 전역 설정) 페이지를 엽니다.
2. Spanning Tree Status(스패닝 트리 상태) 필드에서 **Enable(활성)**을 선택합니다.
3. STP Operation Mode(STP 작동 모드) 필드에서 STP 모드의 유형을 지정하고 나머지 설정을 정의합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

스위치에서 STP가 활성화됩니다.

STP 전역 매개변수 수정:

1. STP Global Settings(STP 전역 설정) 페이지를 엽니다.
2. 필요에 따라 이 페이지의 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

STP 매개변수가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 STP 전역 매개변수 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

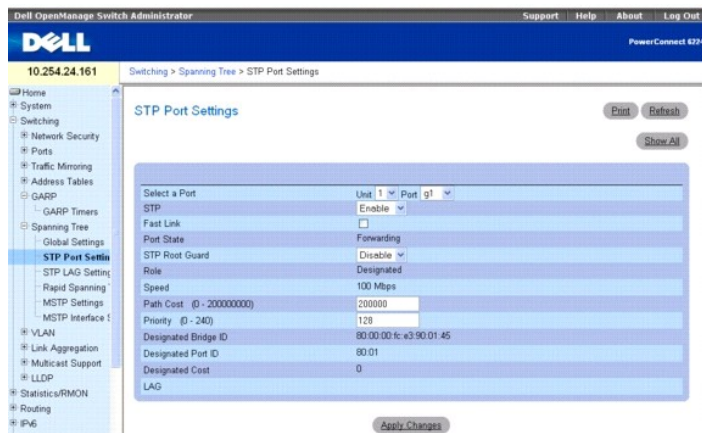
- 1 스페닝 트리 명령

STP 포트 설정

STP Port Settings(STP 포트 설정) 페이지에서 STP 속성을 개별 포트에 할당합니다.

STP Port Settings(STP 포트 설정) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치) → Spanning Tree(스패닝 트리) → STP Port Settings(STP 포트 설정)를 클릭합니다.

그림 7-39. STP Port Settings(STP 포트 설정)



STP Port Settings(STP 포트 설정) 페이지에는 다음 필드가 포함되어 있습니다.

Select a Port(포트 선택) — STP가 활성화되는 장치와 포트를 지정합니다.

STP — 포트에서 STP를 활성화하거나 비활성화합니다.

Fast Link(고속 링크) — 포트에 대한 Fast Link(고속 링크) 모드가 활성화됩니다. 포트에 대해 고속 링크 모드를 활성화한 경우 포트 링크가 가동되면 **Port State(포트 상태)**가 **Forwarding(전달)** 상태로 자동 지정됩니다. 대규모 네트워크에서는 STP 컨버전스를 수행하는 데 30~60초 정도 걸릴 수 있습니다.

Port State(포트 상태) — 포트의 현재 STP 상태를 나타냅니다. 이를 활성화하면 포트 상태에 따라 트래픽에 수행되는 전달 동작이 결정됩니다. 가능한 포트 상태는 다음과 같습니다.

Disabled(비활성) — 포트에서 STP가 현재 비활성화되어 있습니다. 포트는 MAC 주소를 탐지하면서 트래픽을 전달합니다.

Blocking(차단) — 포트가 현재 차단되어 있어 트래픽을 전달하거나 MAC 주소를 탐지하는 데 사용할 수 없습니다.

Listening(청취) — 포트가 현재 청취 모드에 있습니다. 포트는 트래픽을 전달하거나 MAC 주소를 탐지할 수 없습니다.

Learning(탐지) — 포트가 현재 탐지 모드에 있습니다. 포트는 트래픽을 전달할 수 없지만 새 MAC 주소는 탐지할 수 있습니다.

Forwarding(전달) — 포트가 현재 전달 모드에 있습니다. 포트는 트래픽을 전달하고 새 MAC 주소를 탐지할 수 있습니다.

STP Root Guard(STP 루트 보호) — 스페닝 트리 인스턴스의 트리가 예기치 않게 변경되는 것을 방지합니다. 루트 브리지의 보호가 활성화되어 있을 때 상위 BPDU가 수신되면, 해당 포트가 루트-일관성 없는 상태로 전환되어 청취 상태와 같아집니다. 루트 브리지가 강제 적용됩니다.

Role(역할) — 이 포트에서 STP 토폴로지에 있는 역할을 표시합니다.

Speed(속도) — 포트가 작동하는 속도를 표시합니다.

Path Cost(경로 비용) (1-200000000) — 루트 경로 비용에 대한 포트의 기여도를 지정합니다. 경로 비용은 더 높거나 더 낮은 값으로 조정되고 경로가 다시 지정될 때 트래픽을 전달하는 데 사용됩니다. 0은 경로 비용이 포트의 속도에 따라 설정되는 것을 의미합니다. 기본값은 0입니다.

Priority(우선 순위) (0-240) — 포트의 우선 순위 값을 지정합니다. 우선 순위 값은 루프에서 연결된 두 포트가 브리지에 있을 때 포트 선택에 영향을 줍니다. 기본값은 128입니다.

Designated Bridge ID(지정된 브리지 ID) — 지정된 브리지의 ID를 표시합니다.

Designated Port ID(지정된 포트 ID) — 선택된 포트의 ID를 표시합니다.

Designated Cost(지정된 비용) — STP 토폴로지에 포함된 포트의 비용을 표시합니다. 비용이 낮은 포트는 STP에서 루프가 감지되는 경우 차단될 확률이 더 낮습니다.

LAG — 포트가 연결된 LAG를 표시합니다.

포트에서 STP 활성화

1. **STP Port Settings(STP 포트 설정)** 페이지를 엽니다.
2. **Select a Port(포트 선택)** 필드에서 활성화할 장치와 포트를 지정합니다.
3. **STP** 필드에서 **Enable(활성)**을 선택합니다.
4. **Fast Link(고속 링크)**, **STP Root Guard(STP 루트 보호)**, **Path Cost(경로 비용)** 및 **Priority(우선 순위)**를 필요에 따라 편집합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트에서 STP가 활성화됩니다.

STP 포트 속성 수정

1. **STP Port Settings(STP 포트 설정)** 페이지를 엽니다.
2. **Fast Link(고속 링크)**, **STP Root Guard(STP 루트 보호)**, **Path Cost(경로 비용)** 및 **Priority(우선 순위)**를 필요에 따라 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

STP 포트 매개변수가 수정되고 장치가 업데이트됩니다.

STP 포트 표 표시

1. **STP Port Settings(STP 포트 설정)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.

STP Port Table(STP 포트 표)이 표시됩니다.

그림 7-40. STP Port Table(STP 포트 표)

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Lag
1 1/24	Enable	On	Manual forward Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	
2 1/24	Enable	On	Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	
3 1/24	Enable	On	Manual forward Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	
20 1/24	Enable	On	Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	
22 1/24	Enable	On	Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	
28 1/24	Enable	On	Disabled	Disabled	0	128	80:00:00:e3:90:01:45	00:00	0	

3. 스크의 다른 장치(존재하는 경우)에 대해 **STP Port Table(STP 포트 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

여러 포트에 대한 STP 포트 설정 수정

1. STP Port Settings(STP 포트 설정) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

STP Port Table(STP 포트 표)이 표시됩니다.

3. 수정할 각 포트에 대해 Edit(편집)을 클릭합니다.

4. STP 포트 설정을 필요에 따라 편집합니다.

5. Apply Changes(변경사항 적용)를 클릭합니다.

STP 포트 설정이 수정되고 장치가 업데이트됩니다.

포트에 고속 링크 적용

1. STP Port Settings(STP 포트 설정) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

STP Port Table(STP 포트 표)이 표시됩니다.

3. 수정할 각 포트에 대해 Edit(편집)을 클릭합니다.

4. 포트의 고속 링크 모드를 활성화하려면 Fast Link(고속 링크)를 선택합니다. 포트에 대해 고속 링크 모드를 활성화한 경우 포트 링크가 가동되면 Port State(포트 상태)가 Forwarding(전달) 상태로 자동 지정됩니다.

5. Apply Changes(변경사항 적용)

를 클릭합니다.

선택한 포트에 대해 STP 포트 매개변수가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 STP 포트 설정 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 스페닝 트리 명령

STP LAG 설정

STP LAG Settings(STP LAG 설정) 페이지에서 STP 포트 결함 매개변수를 할당합니다.

STP LAG Settings(STP LAG 설정) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭)→Spanning Tree(스패닝 트리)→STP LAG Settings(STP LAG 설정)를 클릭합니다.

그림 7-41. STP LAG Settings(STP LAG 설정)



STP LAG Settings(STP LAG 설정) 페이지에는 다음 필드가 포함되어 있습니다.

Select a LAG(LAG 선택) — STP 설정을 수정할 LAG 번호를 지정합니다.

STP — LAG에서 STP를 활성화하거나 비활성화합니다. 기본값은 enable(활성)입니다.

Fast Link(고속 링크) — LAG에 대한 고속 링크 모드를 활성화합니다. LAG에 대해 고속 링크 모드를 활성화한 경우 LAG가 가동되면 Port State(포트 상태)가 Forwarding(전달) 상태로 자동 지정됩니다. 고속 링크 모드는 STP 프로토콜의 컨버전스를 수행하는 데 걸리는 시간을 최적화합니다. 대규모 네트워크에서는 STP 컨버전스를 수행하는 데 30-60초 정도 걸릴 수 있습니다.

Port State(포트 상태) — LAG의 현재 STP 상태를 표시합니다. 이를 활성화하면 LAG 상태에 따라 트래픽에 수행되는 전달 동작이 결정됩니다. 브리지에서 오작동하는 LAG를 발견하면 LAG는 Broken(해제) 상태로 바뀝니다. 가능한 LAG 상태는 다음과 같습니다.

Disabled(비활성) — STP가 현재 LAG에서 비활성화되어 있습니다. LAG는 MAC 주소를 탐지하면서 트래픽을 전달합니다.

Blocking(차단) — LAG가 차단되어 있어 트래픽을 전달하거나 MAC 주소를 탐지하는 데 사용할 수 없습니다.

Listening(청취) — LAG가 청취 모드에 있고 트래픽을 전달하거나 MAC 주소를 탐지할 수 없습니다.

Learning(탐지) — LAG가 탐지 모드에 있고 트래픽을 전달할 수 없지만, 새 MAC 주소를 탐지할 수는 있습니다.

Forwarding(전달) — LAG가 현재 전달 모드에 있으며 트래픽을 전달하고 새 MAC 주소를 탐지할 수 있습니다.

Broken(해제) — LAG가 현재 오작동하고 있으며 트래픽 전달에 사용될 수 없습니다.

Role(역할) — 이 포트에서 STP 토폴로지에 있는 역할을 표시합니다.

Path Cost(경로 비용) (1-20000000) — 루트 경로 비용에 대한 LAG의 기여도를 지정합니다. 경로 비용은 더 높거나 더 낮은 값으로 조정되고 경로가 다시 지정될 때 트래픽을 전달하는 데 사용됩니다. 기본값은 0입니다.

Priority(우선 순위) (0-240) — LAG의 우선 순위 값을 지정합니다. 우선 순위 값은 브리지에 두 개의 반복된 포트가 있을 때 LAG 선택에 영향을 줍니다. 우선 순위 값은 0부터 240까지입니다.

Designated Bridge ID(지정된 브리지 ID) — 지정된 브리지 ID를 표시합니다.

Designated Port ID(지정된 포트 ID) — 지정된 포트 ID를 표시합니다.

Designated Cost(지정된 비용) — STP 토폴로지에 포함된 포트의 비용을 표시합니다. 비용이 낮은 포트는 STP에서 루프가 감지되는 경우 차단될 확률이 더 높습니다.

하나의 LAG에 대한 LAG STP 매개변수 수정

1. STP LAG Settings(STP LAG 설정) 페이지를 엽니다.
2. Select a LAG(LAG 선택) 드롭다운 메뉴에서 LAG를 선택합니다.
3. 필요에 따라 필드를 수정합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

STP LAG 매개변수가 수정되고 장치가 업데이트됩니다.

STP LAG 표 표시

1. STP LAG Settings(STP LAG 설정) 페이지를 엽니다.
2. Show All(모두 표시)를 클릭합니다.

STP LAG Table(STP LAG 표)이 표시됩니다.

그림 7-42. STP LAG Table(STP LAG 표)

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated/Designated Port ID/Cost
21	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
22	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
23	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
24	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
25	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
26	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
27	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0
28	Disable	Disable	Disable	Disabled	Disabled	0	128	80:00:00:00:00:01:45	00:00 0

3. 표에서 **Fast Link(고속 링크)**를 클릭하고 선택한 후 **Apply Changes(변경사항 적용)**를 클릭하면 개별 LAG에 대해 고속 링크 및 STP 루트 보호를 활성화하거나 비활성화할 수 있습니다.

여러 LAG에 대한 LAG STP 매개변수 수정

1. **STP LAG Settings(STP LAG 설정)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
STP LAG Table(STP LAG 표)이 표시됩니다.
3. 수정할 모든 LAG에 대해 **Edit(편집)**를 클릭합니다.
4. 필요에 따라 필드를 수정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
선택한 LAG에 대해 STP LAG 매개변수가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 STP LAG 설정 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

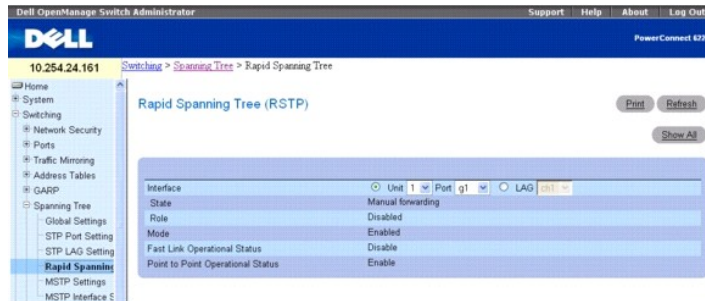
1. 스페닝 트리 명령

빠른 스페닝 트리

RSTP(Rapid Spanning Tree Protocol)는 전달 루프를 만들지 않고도 스페닝 트리의 빠른 컨버전스를 가능하게 하는 네트워크 토폴로지를 감지 및 사용합니다.

Rapid Spanning Tree(빠른 스페닝 트리) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)**→**Spanning Tree(스페닝 트리)**→**Rapid Spanning Tree(빠른 스페닝 트리)**를 클릭합니다.

그림 7-43. Rapid Spanning Tree(빠른 스페닝 트리)



Rapid Spanning Tree(빠른 스페닝 트리) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 장치/포트나 LAG에서 RSTP가 활성화되는지 여부를 결정합니다. 장치/포트나 LAG를 클릭하여 인터페이스의 유형을 지정한 다음 드롭다운 메뉴에서 구성할 장치/포트나 LAG를 선택합니다.

State(상태) — 포트에 대한 스페닝 트리 상태를 표시합니다.

Role(역할) — STP 토폴로지의 포트에 대한 스페닝 트리 역할을 표시합니다.

Mode(모드) — 관리 모드와 활성화 여부를 표시합니다.

Fast Link Operational Status(고속 링크 작동 상태) — 포트나 LAG에 대해 고속 링크가 활성화되어 있는지 여부를 나타냅니다. 포트에 대해 고속 링크가 활성화되어 있으면 포트는 자동으로 전달 상태가 됩니다. 이 설정은 "[STP 포트 설정](#)" 또는 "[STP LAG 설정](#)" 페이지에서 변경할 수 있습니다.

Point to Point Operational Status(지정간 작동 상태) — 지정간 작동 상태를 표시합니다.

지정간 링크를 통해 통신을 설정하기 위해 원래 PPP는 먼저 LCP(Link Control Protocol) 패킷을 전송하여 데이터 링크를 구성하고 테스트합니다. 링크가 설정되고 선택적 시설이 LCP의 필요에 따라 구성된 후에는 원래 PPP가 NCP(Network Control Protocols) 패킷을 전송하여 하나 이상의 네트워크 층 프로토콜을 선택하고 구성합니다. 선택된 각 네트워크 층 프로토콜이 구성되면 각 네트워크 층 프로토콜의 패킷을 링크를 통해 전송할 수 있습니다. 링크는 명시적 LCP 또는 NCP 패킷이 링크를 닫거나 일부 외부 이벤트가 발생할 때까지 통신에 대해 구성된 상태를 유지합니다. 이 유형은 실제 스위치 포트 링크 유형입니다.

RSTP(Rapid Spanning Tree) 표 표시

1. RSTP(Rapid Spanning Tree) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Rapid Spanning Tree Table(빠른 스페닝 트리 표)이 표시됩니다.

그림 7-44. Rapid Spanning Tree Table(빠른 스페닝 트리 표)

Rapid Spanning Tree Table Print Refresh

Unit: 1

Interface	Role	Fast Link Operational Status	Point to Point Operational Status
1	1/g1	Designated	Disabled
2	1/g2	Designated	Disabled
3	1/g3	Designated	Disabled
26	1/r/g2	Disabled	Disabled
27	1/r/g3	Disabled	Disabled
28	1/r/g4	Disabled	Disabled

LAGs	Role	Fast Link Operational Status	Point to Point Operational Status
29	ch1	Disabled	False
30	ch2	Disabled	False
31	ch3	Disabled	False
32	ch4	Disabled	False
33	ch5	Disabled	False
34	ch6	Disabled	False
35	ch7	Disabled	False
36	ch8	Disabled	False

Back

3. 스택의 다른 장치(존재하는 경우)에 대해 Rapid Spanning Tree Table(빠른 스페닝 트리 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

CLI 명령을 사용하여 빠른 STP 매개변수 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. 스페닝 트리 명령

MSTP 설정

MSTP(Multiple Spanning Tree Protocol)는 VLAN 트래픽을 다른 인터페이스를 통해 효과적으로 전달하기 위해 스페닝 트리의 여러 인스턴스를 지원합니다. MSTP는 RSTP 및 STP와 모두 호환됩니다. MSTP 브리지는 모두 RSTP 브리지 또는 STP 브리지로 작동하도록 구성할 수 있습니다.

MSTP Settings(MSTP 설정) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭)→Spanning Tree(스패닝 트리)→MSTP Settings(MSTP 설정)를 클릭합니다.

그림 7-45. MSTP Settings(MSTP 설정)

Dell OpenManage Switch Administrator Support Help About Log Out

DELL PowerConnect 8324

10.254.24.161 Switching > Spanning Tree > MSTP Settings

MSTP Settings Print Refresh Show All

Global Settings

Region Name (1 - 32 characters) 00-FC-E3-90-01-45

Revision (0 - 65535) 0

Max Hops (1 - 40) 20

Instance ID 80.00.00.fc:a3.90.01.45

Instance Settings

Instance ID 1

Included VLANs 1, 2

Priority (0 - 61440) 32768

BridgeID 80.00.00.fc:a3.90.01.45

Root BridgeID 80.01.00.fc:a3.90.01.45

Root Port 00.00

Root Path Cost 0

Apply Changes

MSTP Settings(MSTP 설정) 페이지에는 다음 필드가 포함되어 있으며, 이 필드는 Global Settings(전역 설정) 및 Instance Settings(인스턴스 설정)의 두 절로 구분됩니다.

Region Name(영역 이름) (1-32자) — 사용자 정의된 MST 영역 이름을 지정합니다.

Revision(개정) (0-65535) — 현재 MST 구성의 개정을 식별하는 부호 없는 16비트 숫자를 지정합니다. 개정 번호는 MST 구성의 일부로 필요합니다. 기본값은 0입니다.

Max Hops(최대 홉) (1-40) — BPDU가 삭제되기 전에 특정 영역에서 발생하는 전체 홉 수를 지정합니다. BPDU가 삭제되면 포트 정보의 보존 기간이 만료됩니다. 기본값은 20입니다.

Instance ID(인스턴스 ID) — 스페닝 트리 인스턴스의 ID를 지정합니다. 필드 범위는 1-15이고 기본값은 1입니다.

Included VLAN(포함된 VLAN) — 선택된 VLAN을 선택된 인스턴스로 매핑합니다. 모든 VLAN은 하나의 인스턴스에만 속합니다.

Priority(우선 순위) (0-61440) — 선택된 스페닝 트리 인스턴스에 대한 스위치 우선 순위를 지정합니다. 기본값은 32768입니다.

Bridge ID(브리지 ID) — 선택된 인스턴스의 브리지 ID를 지정합니다.

Root Bridge ID(루트 브리지 ID) 가장 낮은 경로 비용을 가진 루트 브리지입니다.

Root Port(루트 포트) — 선택된 인스턴스의 루트 포트를 나타냅니다.

Root Path Cost(루트 경로 비용) — 선택된 인스턴스의 경로 비용을 나타냅니다.

MSTP 설정 수정:

1. MSTP Settings(MSTP 설정) 페이지를 엽니다.
2. Global Settings(전역 설정) 및 Instance Settings(인스턴스 설정) 절의 필드를 필요에 따라 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.
MSTP 매개변수가 수정되고 장치가 업데이트됩니다.

MSTP VLAN - 인스턴스 매핑 표 표시

1. MSTP Settings(MSTP 설정) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
MSTP Settings Table(MSTP 설정 표)이 표시됩니다.

그림 7-46. MSTP Settings Table(MSTP 설정 표)

VLAN	Instance ID (# 15)	Edit
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>

3. 하나 이상의 VLAN에 대한 인스턴스 ID를 수정하려면 원하는 VLAN에 대해 Edit(편집)를 선택합니다.
4. 인스턴스 ID를 필요에 따라 변경합니다. VLAN - 인스턴스 매핑을 제거하려면 0 값을 입력합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.
선택된 VLAN에 대한 인스턴스 ID가 수정되고 장치가 업데이트됩니다.

CLS 명령을 사용하여 MST 인스턴스 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

MSTP 인터페이스 설정

MSTP Interface Settings(MSTP 인터페이스 설정) 페이지에서 MSTP 설정을 특정 인터페이스에 할당합니다.

MSTP Interface Settings(MSTP 인터페이스 설정) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)**→ **Spanning Tree(스패닝 트리)**→ **MSTP Interface Settings(MSTP 인터페이스 설정)**를 클릭합니다.

그림 7-47. MSTP Interface Settings(MSTP 인터페이스 설정)



MSTP Interface Settings(MSTP 인터페이스 설정) 페이지에는 다음 필드가 포함되어 있습니다.

Instance ID(인스턴스 ID) — 스위치에 구성된 MSTP 인스턴스를 선택합니다. 가능한 필드 범위는 1-15입니다.

Interface(인터페이스) — 이 MSTP 인터페이스에 대한 장치/포트나 LAG를 선택합니다.

Port State(포트 상태) — 특정 인스턴스에서 포트의 활성화 여부를 나타냅니다.

Port Type(포트 유형) — MSTP가 포트를 지정된 포트나 허브에 연결된 포트 중 어떤 항목으로 처리할지와, 포트가 MST 영역이나 경계 포트 중 어떤 항목에 대한 내부 포트인지 여부를 지정합니다. 포트가 경계 포트인 경우, 링크의 다른 쪽에 있는 스위치가 RSTP 및 STP 모드 중 어떤 모드인지도 나타냅니다.

Role(역할) — STP 경로에 제공하기 위해 STP 알고리즘으로 할당되는 포트 역할을 나타냅니다. 가능한 필드 값은 다음과 같습니다.

Root(루트) — 패킷을 루트 스위치로 전달하기 위해 가장 낮은 비용 경로를 제공합니다.

Designated(지정됨) — 지정된 스위치가 LAN으로 연결될 때 사용되는 포트나 LAG를 나타냅니다.

Alternate(대체) — 인터페이스에서 루트 스위치에 대한 대체 경로를 제공합니다.

Backup(백업) — 지정된 LAN에 대한 백업 경로를 제공합니다. 백업 포트는 두 포트가 지정된 링크에 의해 루트로 연결된 경우에만 발생합니다. 또한, LAN에 공유 세그먼트에 연결된 둘 이상의 연결이 있을 경우에도 발생합니다.

Disabled(비활성) — 포트가 스페닝 트리에 참여하지 않음을 나타냅니다.

Priority(우선 순위) — 지정된 인터페이스에 대한 인터페이스 우선 순위를 정의합니다. 우선 순위 범위는 16단계에서 0부터 240까지입니다. 기본값은 128입니다.

Path Cost(경로 비용)(0-200000000) — 스페닝 트리 인스턴스에 대한 포트 기여도를 나타냅니다. 범위는 항상 0 ~ 200,000,000이고 기본값은 포트의 속도에 따라 정해집니다. 기본값:

- 1 포트 채널-20,000
- 1 1000Mbps(기가)-20,000
- 1 100Mbps-200,000
- 1 10Mbps-2,000,000

Designated Bridge ID(지정된 브리지 ID) — 링크 또는 공유 LAN을 루트에 연결하는 브리지 ID 번호를 표시합니다.

Designated Port ID(지정된 포트 ID) — 링크 또는 공유된 LAN을 루트에 연결하는 지정된 브리지의 포트 ID 번호를 표시합니다.

Designated Cost(지정된 비용) — 링크 또는 공유된 LAN에서 루트까지의 경로 비용을 표시합니다.

MSTP 인터페이스 설정 할당

1. MSTP Interface Settings(MSTP 인터페이스 설정) 페이지를 엽니다.
2. 드롭다운 메뉴에서 **Instance ID(인스턴스 ID)**를 선택합니다.
3. **Port(포트)** 또는 **LAG**를 지정한 다음 관련 드롭다운 메뉴에서 인터페이스를 선택합니다.

4. **Interface Priority(인터페이스 우선 순위)** 및 **Path Cost(경로 비용)**를 지정합니다.

5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스 설정이 저장되고 장치가 업데이트됩니다.

MSTP 인터페이스 설정 표 표시

1. **MSTP Settings(MSTP 설정)** 페이지를 엽니다.

2. **Show All(모두 표시)**을 클릭합니다.

MSTP Interface Table(MSTP 인터페이스 표)이 표시됩니다.

그림 7-48. MSTP Interface Table(MSTP 인터페이스 표)

Interface	Role	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Edit
1 1/fg1	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8001	<input type="checkbox"/>
2 1/fg2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8002	<input type="checkbox"/>
3 1/fg3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8003	<input type="checkbox"/>

26 1/sg2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801A	<input type="checkbox"/>
27 1/sg3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801B	<input type="checkbox"/>
28 1/sg4	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801C	<input type="checkbox"/>

3. 스크의 다른 장치(존재하는 경우)에 대해 **MSTP Interface Table(MSTP 인터페이스 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

4. 하나 이상의 인터페이스에 대한 포트 우선 순위 또는 경로 비용을 수정하려면 원하는 인터페이스에 대한 **Edit(편집)**를 선택합니다.

5. **Port Priority(우선 순위)** 또는 **Path Cost(경로 비용)** 열의 값을 필요에 따라 변경합니다.

6. **Apply Changes(변경사항 적용)**를 클릭합니다.

선택된 인터페이스에 대해 필드가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 MSTP 인터페이스 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 스페닝 트리 명령

VLAN 구성

총 2 스위치에 VLAN(가상 LAN) 지원을 추가하면 브리징과 라우팅의 이점을 모두 얻을 수 있습니다. 브리징과 마찬가지로, VLAN 스위치는 총 2 헤더를 기준으로 트래픽을 전달하여 속도가 빨라지고, 라우터와 마찬가지로 네트워크를 논리적 세그먼트로 분할하여 관리, 보안 및 멀티캐스트 트래픽 관리를 보다 효율적으로 제공합니다.

VLAN은 종단국과 이를 연결하는 스위치 포트 세트입니다. 부서나 프로젝트 멤버십 등과 같은 논리 부서에 대해서는 여러 가지 이유가 있을 수 있습니다. 유일한 물리적 요구 사항은 종단국과 이를 연결한 포트가 동일한 VLAN에 속해야 한다는 점입니다.

네트워크의 각 VLAN에는 VLAN ID가 연결되어 있으며 이는 VLAN에서 전송되는 패킷 총 2 헤더의 IEEE 802.1Q 태그에 나타납니다. 종단국에는 태그 또는 태그의 VLAN 부분이 생략될 수 있는데, 이 경우 패킷을 수신하는 첫 번째 스위치 포트가 이를 거부하거나 기본 VLAN ID를 사용하여 태그를 삽입할 수 있습니다. 지정된 포트는 둘 이상의 VLAN에 대해 트래픽을 처리할 수 있지만 한 개의 기본 VLAN ID만 지원할 수 있습니다.

VLAN 매뉴 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)**→**VLAN**을 클릭합니다. **VLAN** 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

- 1 [VLAN 멤버십](#)
- 1 [VLAN 포트 설정](#)
- 1 [VLAN LAG 설정](#)
- 1 [MAC를 VLAN에 바인드](#)

- 1 [IP 서브네트를 VLAN에 바인드](#)
- 1 [프로토콜 그룹](#)
- 1 [GVRP 매개변수](#)

VLAN 멤버십

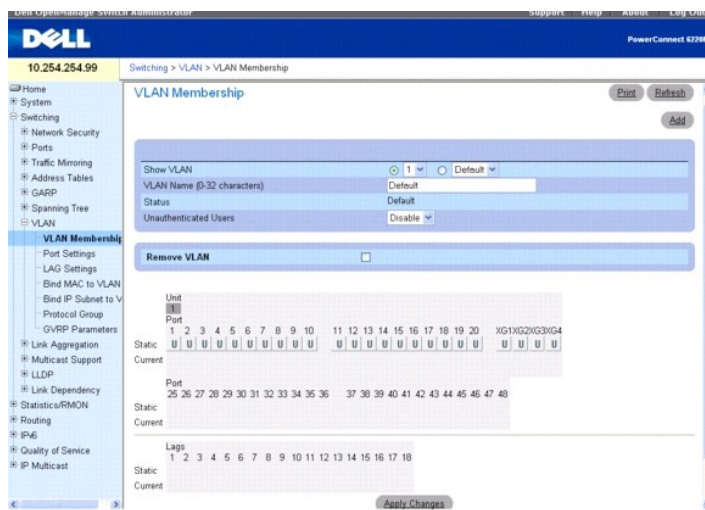
VLAN Membership(VLAN 멤버십) 페이지에서 VLAN 멤버십 표에 저장된 VLAN 그룹을 정의합니다. 스위치는 최대 4094개의 VLAN을 지원합니다. 그러나 실제로는 다음과 같은 이유로 인해 4092개의 VLAN만 만들 수 있습니다.

- 1 VLAN 1은 모든 포트가 구성원인 기본 VLAN이며,
- 1 VLAN 4095는 "Discard VLAN(VLAN 삭제)"으로 지정됩니다.

생성될 유효한 VLAN은 2-4093입니다. VLAN 4094는 예약되어 있습니다.

VLAN Membership(VLAN 멤버십) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)→VLAN→VLAN Membership(VLAN 멤버십)**을 클릭합니다.

그림 7-49. VLAN Membership(VLAN 멤버십)



VLAN Membership(VLAN 멤버십) 페이지는 두 절로 구분됩니다. 상단 절에는 전체 VLAN의 멤버십을 정의하는 필드가 포함되어 있습니다. 하단 절에는 이 VLAN의 특정 포트 및 LAG에 대한 멤버십 설정을 정의하는 표가 들어 있습니다. **VLAN Membership(VLAN 멤버십)** 필드는 다음과 같습니다.

Show VLAN(VLAN 표시) — 표시할 VLAN을 선택합니다. **VLAN ID** 또는 **VLAN Name(VLAN 이름)** 드롭다운 메뉴를 사용하여 VLAN을 선택합니다.

VLAN Name(VLAN 이름)(0-32) — 사용자 정의 VLAN 이름을 표시합니다. 이 필드는 **Add(추가)** 단추를 사용하여 정의합니다. 이름은 0-32자의 길이에서 유효합니다.

Status(상태) — VLAN 유형을 나타냅니다. 가능한 값은 다음과 같습니다.

Dynamic(동적) — VLAN이 GVRP를 통해 동적으로 만들어졌음을 나타냅니다.

Static(정적) — VLAN이 사용자 정의되었으며 수정할 수 있음을 나타냅니다.

Default(기본) — VLAN이 기본 VLAN임을 나타냅니다.

Unauthenticated Users(인증되지 않은 사용자) — Enable(활성)을 선택하면 허가되지 않은 스위치를 사용하여 이 VLAN을 액세스할 수 있습니다.

Remove VLAN(VLAN 제거) — VLAN 멤버십 표에서 표시된 VLAN을 제거합니다.

VLAN Membership(VLAN 멤버십) 표에는 어떤 포트와 LAG가 VLAN의 구성원인지와 태그가 지정되었는지(T), 태그가 해제되었는지(U) 또는 금지되었는지(F) 여부가 표시됩니다. 표에는 **Static(정적)** 및 **Current(현재)**라는 두 행이 있습니다. 이 페이지에서는 **Static(정적)** 행만 액세스할 수 있습니다. **Current(현재)** 행은 GVRP를 통해 동적으로 업데이트되거나, **Static(정적)** 행이 변경되고 **Apply Changes(변경사항 적용)**를 클릭했을 때 업데이트됩니다.

페이지의 이 절에는 다음과 같은 두 개의 표가 있습니다.

Ports(포트) — VLAN 멤버십을 포트에 할당하고 표시합니다. 멤버십을 할당하려면 특정 포트에 대해 **Static(정적)**을 클릭합니다. 클릭할 때마다 U, T 및 공백이 번갈아 표시됩니다. 정의는 다음 표를 참조하십시오.

LAGs — VLAN 멤버십을 LAG에 할당하고 표시합니다. 멤버십을 할당하려면 특정 LAG에 대해 **Static(정적)**을 클릭합니다. 클릭할 때마다 U, T 및 공백이 번갈아 표시됩니다. 정의는 다음 표를 참조하십시오.

표 7-1. VLAN Port Membership Definitions(VLAN 포트 멤버십 정의)

포트 제어	정의
T	태그 지정됨: 인터페이스가 VLAN 구성원입니다. 인터페이스에서 전달된 모든 패킷에 태그가 지정됩니다. 패킷에는 VLAN 정보가 포함됩니다.
U	태그 해제됨: 인터페이스가 VLAN 구성원입니다. 인터페이스에서 전달된 패킷의 태그가 해제됩니다.
F	금지됨: 인터페이스가 VLAN의 구성원이 될 수 없도록 금지되었음을 나타냅니다.
공백	공백: 인터페이스가 VLAN 구성원이 아닙니다. 인터페이스와 연결된 패킷이 전달되지 않습니다.

새 VLAN 추가

1. **VLAN Membership(VLAN 멤버십)** 페이지를 엽니다.
2. **Add(추가)**를 클릭합니다.

Add VLAN(VLAN 추가) 페이지가 표시됩니다.

그림 7-50. Add VLAN(VLAN 추가)

3. 새 VLAN ID와 VLAN 이름을 입력합니다.
 4. **Apply Changes(변경사항 적용)**를 클릭합니다.
- 새 VLAN이 추가되고 장치가 업데이트됩니다.

포트 또는 LAG에 VLAN 멤버십 할당

1. **VLAN Membership(VLAN 멤버십)** 페이지를 엽니다.
2. **VLAN ID** 또는 **VLAN Name(VLAN 이름)** 드롭다운 메뉴에서 VLAN을 선택합니다.
3. **VLAN Port Membership Table(VLAN 포트 멤버십 표)**에서 특정 포트/LAG에 대한 **Static(정적)** 행을 클릭하여 값을 할당합니다. 클릭할 때마다 U, T 및 공백(구성원 아님)이 번갈아 표시됩니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

포트 또는 LAG가 선택된 지정으로 VLAN에 할당되고 **Current(현재)** 행이 지정으로 업데이트되며, 장치가 업데이트됩니다.

VLAN 멤버십 그룹 수정

1. **VLAN Membership(VLAN 멤버십)** 페이지를 엽니다.
2. **VLANID** 또는 **VLAN Name(VLAN 이름)** 드롭다운 메뉴에서 VLAN을 선택합니다.
3. 필요에 따라 필드를 수정합니다.
4. **VLAN Port Membership Table(VLAN 포트 멤버십 표)**에서 해당 포트/LAG에 대한 **Static(정적)** 행을 클릭하여 포트 또는 LAG 값을 변경합니다. 클릭할 때마다 U, T 및 공백(구성원 아님)이 번갈아 표시됩니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

VLAN 멤버십 정보가 수정되고 **Current(현재)** 행이 지정한 변경사항으로 업데이트되며, 장치가 업데이트됩니다.

VLAN 제거

1. **VLAN Membership(VLAN 멤버십)** 페이지를 엽니다.
 2. **VLAN ID** 또는 **VLAN Name(VLAN 이름)** 드롭다운 메뉴에서 VLAN을 선택합니다.
 3. **Remove VLAN(VLAN 제거)** 확인란을 선택합니다.
 4. **Apply Changes(변경사항 적용)**를 클릭합니다.
- 선택된 VLAN이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 VLAN 멤버십 그룹 정의 및 포트/LAG 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. VLAN 명령

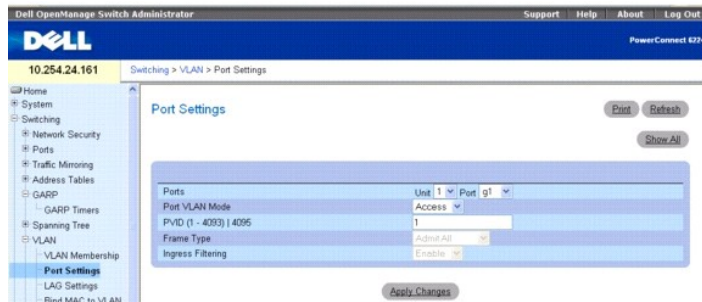
VLAN 포트 설정

포트 기반 VLAN에서 태그가 해제된 트래픽은 수신 포트 PVID를 기반으로 지정된 포트를 통해 브리지됩니다. 포트 기반 VLAN은 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트 패킷이 VLAN의 구성원인 포트에만 전송되기 때문에 네트워크 트래픽 패턴을 최적화하는 데 도움이 됩니다. VLAN 태그로 수신된 패킷은 이 VLAN ID를 전환 프로세스에 사용합니다.

VLAN Port Settings(VLAN 포트 설정) 페이지에서 VLAN 포트 매개변수를 정의 및 수정할 뿐만 아니라 포트를 VLAN의 일부로 식별합니다.

VLAN Port Settings(VLAN 포트 설정) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위칭)** → **VLAN** → **Port Settings(포트 설정)**를 클릭합니다.

그림 7-51. VLAN Port Settings(VLAN 포트 설정)



VLAN Port Settings(VLAN 포트 설정) 페이지에는 다음 필드가 포함되어 있습니다.

Ports(포트) — VLAN에 포함된 장치와 포트를 지정합니다.

Port VLAN Mode(포트 VLAN 모드) — 포트 모드를 나타냅니다. 가능한 값은 다음과 같습니다.

General(일반) — 포트가 VLAN에 속하고 각 VLAN이 tagged(태그 지정됨) 또는 untagged(태그 해제됨)로 사용자 지정되었습니다(802.1Q 전이중 모드).

Access(액세스) — 포트가 태그가 해제된 단일 VLAN에 속합니다. 포트가 액세스 모드에 있으면 포트(패킷 유형)에서 허용되는 패킷 유형을 지정할 수 없습니다. 또한 액세스 포트에서 수신 필터링을 활성화/비활성화할 수 없습니다.

Trunk(트렁크) — 포트가 둘 이상의 VLAN에 속하고 모든 포트에 태그가 지정되었습니다(선택적 단일 기본 VLAN 제외).

PVID(1-4093) | 4095 — 태그가 해제된 패킷에 VLAN ID를 할당합니다. 가능한 값은 1-4093 또는 4095입니다.

Frame Type(프레임 유형) — 포트에서 허용되는 프레임 유형을 지정합니다. 기본값은 **Admit All(모두 허용)**입니다. 가능한 값은 다음과 같습니다.

Admit Tag Only(태그만 허용) — 포트에서 태그 지정된 프레임만 허용됩니다.

Admit All(모두 허용) — 포트에서 태그 지정 및 태그 해제된 프레임이 모두 허용됩니다.

Ingress Filtering(수신 필터링) — 포트에서 수신 필터링을 활성화하거나 비활성화합니다. 수신 필터링은 VLAN 태그가 포트 VLAN 멤버십과 일치하지 않는 프레임을 삭제합니다.

포트 설정 할당

1. **VLAN Port Settings(VLAN 포트 설정)** 페이지를 엽니다.
2. **Unit(장치)** 및 **Port(포트)** 드롭다운 메뉴에서 설정을 할당할 포트를 선택합니다.

3. 페이지의 나머지 필드를 입력합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
VLAN 포트 설정이 정의되고 장치가 업데이트됩니다.

VLAN 포트 표 표시

1. **VLAN Port Settings(VLAN 포트 설정)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
VLAN Port Table(VLAN 포트 표)이 표시됩니다.

그림 7-52. VLAN Port Table(VLAN 포트 표)

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 1/1g1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 1/1g2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 1/1g3	General	3	Admit All	Enable	<input type="checkbox"/>
26 1/1g2	Access	1	Admit All	Enable	<input type="checkbox"/>
27 1/1g3	Access	1	Admit All	Enable	<input type="checkbox"/>
28 1/1g4	Access	1	Admit All	Enable	<input type="checkbox"/>

주: Access(액세스) 포트가 선택되면 포트(패킷 유형)에 허용된 패킷 유형을 지정할 수 없습니다. 또한 액세스 포트에서 수신 필터링을 활성화하거나 비활성화할 수 없습니다.

3. 스크의 다른 장치(존재하는 경우)에 대해 **VLAN Port Table(VLAN 포트 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

여러 포트의 설정 수정

1. **VLAN Port Settings(VLAN 포트 설정)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
VLAN Port Table(VLAN 포트 표)이 표시됩니다.
3. 수정할 각 포트에 대해 **Edit(편집)**를 클릭합니다.
4. 필요에 따라 필드를 편집합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
VLAN 포트 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 포트를 VLAN 그룹에 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

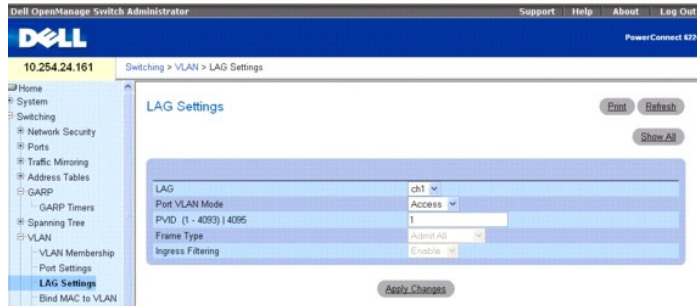
1 VLAN 명령

VLAN LAG 설정

VLAN LAG Settings(VLAN LAG 설정) 페이지에서 LAG를 VLAN에 매핑합니다. 스위치에 들어오는 태그 해제된 패킷은 PVID에서 지정된 LAG ID로 태그가 지정됩니다.

VLAN LAG Settings(VLAN LAG 설정) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**VLAN**→**LAG Settings(LAG 설정)**를 클릭합니다.

그림 7-53. VLAN LAG Settings(VLAN LAG 설정)



VLAN LAG Settings(VLAN LAG 설정) 페이지에는 다음 필드가 포함되어 있습니다.

LAG — VLAN에 포함된 LAG 번호를 지정합니다.

Port VLAN Mode(포트 VLAN 모드) — LAG에 대한 포트 VLAN 모드를 나타냅니다. 가능한 값은 다음과 같습니다.

General(일반) — LAG가 VLAN에 속하고 각 VLAN이 tagged(태그 지정됨) 또는 untagged(태그 해제됨)로 사용자 지정되었습니다(802.1Q 전이종 모드).

Access(액세스) — LAG가 태그가 해제된 단일 VLAN에 속합니다.

Trunk(트렁크) — LAG가 둘 이상의 VLAN에 속하고 모든 포트에 태그가 지정되었습니다(선택적 단일 기본 VLAN 제외).

PVID(1~4093) | 4095 — 태그가 해제된 패킷에 VLAN ID를 할당합니다. 가능한 값은 1~4093 또는 4095입니다.

Frame Type(프레임 유형) — LAG에 허용되는 패킷 유형을 지정합니다. 기본값은 Admit Tag Only(태그만 허용)입니다. 가능한 값은 다음과 같습니다.

Admit Tag Only(태그만 허용) — 태그 지정된 패킷만 LAG에 허용됩니다.

Admit All(모두 허용) — 태그 지정 및 태그 해제된 패킷이 모두 LAG에 허용됩니다.

Ingress Filtering(수신 필터링) — LAG별로 수신 필터링을 활성화하거나 비활성화합니다. 수신 필터링은 VLAN 태그가 LAG VLAN 멤버십과 일치하지 않는 패킷을 삭제합니다.

VLAN LAG 설정 할당

1. VLAN LAG Settings(VLAN LAG 설정) 페이지를 엽니다.
2. LAG 드롭다운 메뉴에서 LAG를 선택합니다.
3. 페이지의 나머지 필드를 입력합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

VLAN LAG 매개변수가 정의되고 장치가 업데이트됩니다.

VLAN LAG 표 표시

1. VLAN LAG Settings(VLAN LAG 설정) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

VLAN LAG Table(VLAN LAG 표)이 표시됩니다.

그림 7-54. VLAN LAG Table(VLAN LAG 표)

VLAN LAG Table Exit Edit

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 ch1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 ch2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 ch3	Access	1	Admit All	Enable	<input type="checkbox"/>
4 ch4	Access	1	Admit All	Enable	<input type="checkbox"/>
5 ch5	Access	1	Admit All	Enable	<input type="checkbox"/>
6 ch6	Access	1	Admit All	Enable	<input type="checkbox"/>
7 ch7	Access	1	Admit All	Enable	<input type="checkbox"/>
8 ch8	Access	1	Admit All	Enable	<input type="checkbox"/>

여러 LAG의 설정 수정

1. VLAN LAG Settings(VLAN LAG 설정) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
VLAN LAG Table(VLAN LAG 표)이 표시됩니다.
3. 수정할 각 LAG에 대해 Edit(편집)를 클릭합니다.
4. 필요에 따라 필드를 편집합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.
VLAN LAG 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 LAG를 VLAN 그룹에 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. VLAN 명령

MAC를 VLAN에 바인드

Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지에서 MAC 항목을 VLAN 표에 매핑합니다. 소스 MAC 주소와 VLAN ID가 지정된 후에는 MAC - VLAN 구성이 스위치의 모든 포트에서 공유됩니다. MAC - VLAN 표는 최대 128개의 항목을 지원합니다.

Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭)→VLAN→Bind MAC to VLAN(MAC를 VLAN에 바인드)을 클릭합니다.

그림 7-55. Bind MAC to VLAN(MAC를 VLAN에 바인드)



Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지에는 다음 필드가 포함되어 있습니다.

MAC Address(MAC 주소) — VLAN에 대한 MAC 주소를 지정합니다.

Bind to VLAN(VLAN에 바인드) (1-4093) — MAC를 연결할 VLAN을 지정합니다.

MAC를 VLAN에 바인드 설정 할당

1. Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지를 엽니다.
2. VLAN에 연결할 MAC 주소를 입력합니다.
3. MAC 주소를 연결할 VLAN을 입력합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
이제 나열된 MAC 주소와 VLAN이 연결되고 장치가 업데이트됩니다.

VLAN LAG 표 표시

1. Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
MAC - VLAN Bind Table(MAC - VLAN 바인드 표)이 표시됩니다.

그림 7-56. MAC - VLAN Bind Table(MAC - VLAN 바인드 표)

	MAC Address	Bind to VLAN	Remove	Edit
1	0800 4012 01FC	2	<input type="checkbox"/>	<input type="checkbox"/>
2	0800 4012 012F	118	<input type="checkbox"/>	<input type="checkbox"/>

여러 MAC 주소에 대한 VLAN 수정

1. Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
MAC - VLAN Bind Table(MAC - VLAN 바인드 표)이 표시됩니다.
3. 수정할 VLAN이 있는 각 MAC 주소에 대해 Edit(편집)를 클릭합니다.
4. Bind to VLAN(VLAN에 바인드) 필드를 편집합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.
MAC - VLAN 설정이 수정되고 장치가 업데이트됩니다.

MAC - VLAN 항목 제거

1. Bind MAC to VLAN(MAC를 VLAN에 바인드) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.
MAC - VLAN Bind Table(MAC - VLAN 바인드 표)이 표시됩니다.
3. 제거할 각 항목에 대해 Remove(제거)를 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 MAC를 VLAN에 바인딩

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 VLAN 명령

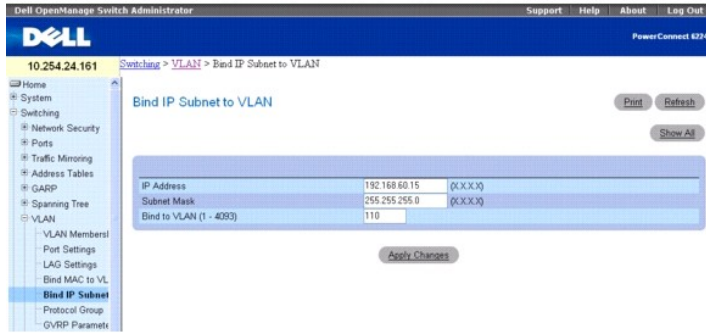
IP 서브네트를 VLAN에 바인드

IP 서브네트 - VLAN 매핑은 IP 서브네트 - VLAN 표에서 항목을 구성하여 정의합니다. 항목은 소스 IP 주소, 네트워크 마스크 및 원하는 VLAN ID를 통해 지정됩니다. IP 서브네트 - VLAN 구성은 스위치의 모든 포트에서 공유됩니다. 이 표에는 최대 64개의 항목을 구성할 수 있습니다.

Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지에서 IP 서브네트를 VLAN에 할당합니다.

Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치) → VLAN → Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드)을 클릭합니다.

그림 7-57. Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드)



Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지에는 다음 필드가 포함되어 있습니다.

IP Address(IP 주소) — 패킷 소스 IP 주소를 지정합니다.

Subnet Mask(서브네트 마스크) — 패킷 소스 IP 서브네트 마스크를 지정합니다.

Bind to VLAN(VLAN에 바인드) (1-4093) — IP 주소가 할당된 VLAN을 지정합니다.

IP 서브네트를 VLAN에 바인딩

1. Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지를 엽니다.
2. VLAN에 바인드할 IP 주소를 입력합니다.
3. IP 주소와 연결된 IP 서브네트를 입력합니다.
4. IP 주소와 서브네트 마스크가 할당된 VLAN ID를 입력합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.

이제 나열된 VLAN과 IP 서브네트가 연결되고 장치가 업데이트됩니다.

IP 서브네트 - VLAN 바인드 표 표시

1. Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
3. **IP Subnet - VLAN Bind Table(IP 서브네트 - VLAN 바인드 표)**이 표시됩니다.

그림 7-58. IP Subnet - VLAN Bind Table(IP 서브네트 - VLAN 바인드 표)

	IP Address	Subnet Mask	Bind to VLAN	Remove	Edit
1	192.168.12.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.13.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.60.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>

여러 IP 주소에 대한 VLAN 바인드 수정

1. Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드) 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
IP Subnet - VLAN Bind Table(IP 서브네트 - VLAN 바인드 표)이 표시됩니다.
3. 수정할 각 항목에 대해 **Edit(편집)**를 클릭합니다.

- 필요에 따라 필드를 편집합니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.
VLAN에 바인드 설정이 수정되고 장치가 업데이트됩니다.

MAC - IP 서브네트 항목 제거

- Bind IP Subnet to VLAN(IP 서브네트를 VLAN에 바인드)** 페이지를 엽니다.
- Show All(모두 표시)**를 클릭합니다.
IP Subnet - VLAN Bind Table(IP 서브네트 - VLAN 바인드 표)이 표시됩니다.
- 제거할 각 항목에 대해 **Remove(제거)**를 선택합니다.
- Apply Changes(변경사항 적용)**를 클릭합니다.
항목이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IP 서브네트를 VLAN에 바인딩

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- VLAN 명령

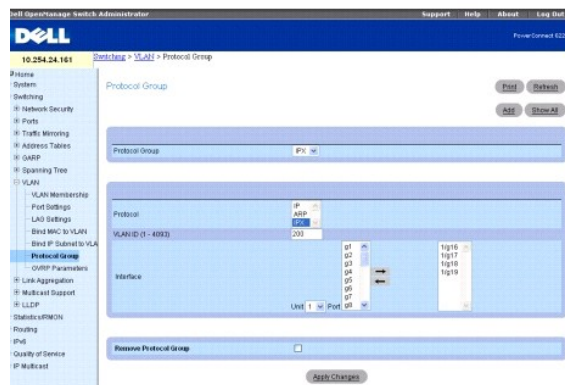
프로토콜 그룹

프로토콜 기반 VLAN에서는 트래픽이 VLAN의 프로토콜을 기준으로 특정 포트를 통해 브리지됩니다. 사용자 정의 패킷 필터는 특정 패킷이 특정 VLAN에 속하는지 여부를 결정합니다. 프로토콜 기반 VLAN은 네트워크 세그먼트에 여러 프로토콜을 실행 중인 호스트가 있는 경우 가장 많이 사용됩니다.

Protocol Group(프로토콜 그룹) 페이지에서 EtherTypes가 속할 VLAN을 구성한 다음 이 설정을 사용하도록 특정 포트를 활성화합니다.

Protocol Group(프로토콜 그룹) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치) → VLAN → Protocol Group(프로토콜 그룹)**을 클릭합니다.

그림 7-59. Protocol Group(프로토콜 그룹)



Protocol Group(프로토콜 그룹) 페이지에는 다음 필드가 포함되어 있습니다.

Protocol Group(프로토콜 그룹) — 프로토콜 그룹 ID와 연결된 이름을 표시합니다. **Add(추가)** 단추를 클릭하여 새 그룹을 만듭니다.

Protocol(프로토콜) — 이 그룹과 연결된 프로토콜을 지정합니다.

VLAN ID(1-4093) — 이 그룹과 연결된 VLAN ID를 지정합니다.

Interface(인터페이스) — 이 그룹에서 제거하거나 추가할 인터페이스를 선택합니다. 프로토콜 그룹에 속할 인터페이스를 지정하고 오른쪽 화살표를 클릭합니다. 오른쪽 옆에 표시되는 인터페이스는 프로토콜 그룹의 일부입니다.

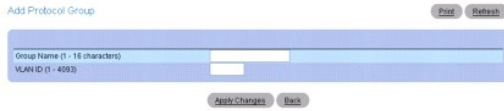
Remove Protocol Group(프로토콜 그룹 제거) — 이 옵션을 선택하고 **Apply Changes(변경사항 적용)**를 클릭하면 화면에 표시된 프로토콜 그룹이 제거됩니다. 동시에 여러 그룹을 제거하려면 **Show All(모두 표시)**를 클릭하고 **Protocol Group Table(프로토콜 그룹 표)**에서 **Remove(제거)** 확인란을 사용합니다.

프로토콜 그룹 추가

1. Protocol Group(프로토콜 그룹) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add Protocol Group(프로토콜 그룹 추가) 페이지가 표시됩니다.

그림 7-60. Add Protocol Group(프로토콜 그룹 추가)



3. 새 프로토콜 그룹 이름과 이 그룹에 연결할 VLAN ID를 입력합니다.
4. Protocol Group(프로토콜 그룹) 페이지로 돌아갑니다.
5. 추가한 프로토콜 그룹을 선택한 다음 프로토콜을 선택합니다.
6. 첫 번째 인터페이스 열에서 프로토콜 그룹에 추가할 인터페이스를 클릭하여 지정합니다. 여러 인터페이스를 선택하려면 Shift 키(연속하는 여러 인터페이스 선택) 또는 Ctrl 키(연속하지 않는 여러 인터페이스 선택)를 누른 상태에서 클릭합니다.

7. 오른쪽 화살표를 클릭합니다.

선택된 인터페이스가 두 번째 열로 이동합니다. 이 열의 모든 인터페이스는 프로토콜 그룹의 일부입니다.

8. Apply Changes(변경사항 적용)를 클릭합니다.

프로토콜 그룹이 추가되고 장치가 업데이트됩니다.

VLAN 프로토콜 그룹 설정 수정

1. Protocol Group(프로토콜 그룹) 페이지를 엽니다.
2. 프로토콜 그룹 ID 드롭다운 메뉴에서 수정할 프로토콜을 지정합니다.
3. 필요에 따라 프로토콜 또는 VLAN ID를 변경합니다.
4. 그룹에 인터페이스를 추가하려면 첫 번째 열에서 원하는 인터페이스를 클릭하여 지정합니다. 여러 인터페이스를 선택하려면 Shift 키(연속하는 여러 인터페이스 선택) 또는 Ctrl 키(연속하지 않는 여러 인터페이스 선택)를 누른 상태에서 클릭합니다.

5. 오른쪽 화살표를 클릭합니다.

선택된 인터페이스가 두 번째 열로 이동합니다. 이 열의 모든 인터페이스는 프로토콜 그룹의 일부입니다.

6. 그룹에서 인터페이스를 제거하려면 두 번째 열에서 원하는 인터페이스를 클릭하여 지정합니다.

7. 왼쪽 화살표를 클릭합니다.

선택된 인터페이스가 두 번째 열에서 제거됩니다.

8. Apply Changes(변경사항 적용)를 클릭합니다.

VLAN 프로토콜 그룹 매개변수가 수정되고 장치가 업데이트됩니다.

프로토콜 그룹 표에서 여러 프로토콜 제거

1. Protocol Group(프로토콜 그룹) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

Protocol Group(프로토콜 그룹) 표가 표시됩니다.

그림 7-61. Protocol Group Table(프로토콜 그룹 표)

Group Name	Protocol	VLAN ID	Interface	Remove
1	IPX	200	1/16 1/17 1/18 1/19	<input type="checkbox"/> 삭제
2	IPV2	110	1/21 1/22 1/23 1/24	<input type="checkbox"/> 삭제

3. 제거할 프로토콜 그룹에 대해 Remove(제거)를 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

프로토콜이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 프로토콜 그룹 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. VLAN 명령

GVRP 매개변수

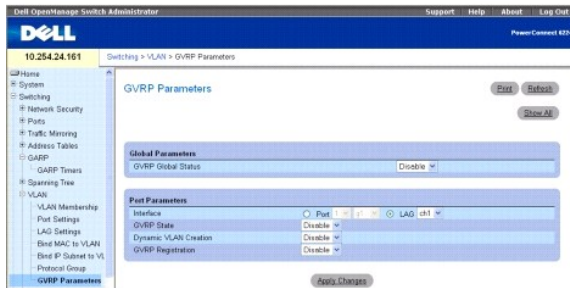
GARP VLAN 등록 프로토콜은 네트워크 스위치가 VLAN 멤버십 정보를 동일한 세그먼트에 연결된 MAC 네트워크 스위치에 동적으로 등록(및 등록 해제)할 수 있도록 하고, 이 정보가 GVRP를 지원하는 브리지된 모든 LAN 네트워크 스위치에 유포되도록 하는 메커니즘을 제공합니다.

GVRP의 작동은 GARP(Generic Attribute Registration Protocol)에서 제공되는 서비스에 의존합니다. GVRP는 최대 1024개의 VLAN을 만들 수 있습니다.

GVRP를 전역으로 활성화하려면 GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 사용합니다. 인터페이스별로 GVRP를 활성화할 수도 있습니다.

GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치) → VLAN → GVRP Parameters(GVRP 매개변수)를 클릭합니다.

그림 7-62. GVRP Global Parameters(GVRP 전역 매개변수)



GVRP Global Parameters(GVRP 전역 매개변수) 페이지에는 다음 필드가 포함되어 있습니다.

GVRP Global Status(GVRP 전역 상태) — 스위치에서 GVRP를 활성화하거나 비활성화합니다. GVRP는 기본적으로 비활성화되어 있습니다.

Interface(인터페이스) — GVRP가 활성화된 장치와 포트 또는 LAG를 지정합니다.

GVRP State(GVRP 상태) — 지정된 인터페이스에서 GVRP를 활성화하거나 비활성화합니다.

Dynamic VLAN Creation(동적 VLAN 만들기) — GVRP를 통해 VLAN 만들기를 활성화하거나 비활성화합니다.

GVRP Registration(GVRP 등록) — GVRP 등록을 활성화하거나 비활성화합니다.

스위치에서 GVRP 활성화

1. GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 엽니다.
2. GVRP Global Status(GVRP 전역 상태) 필드에서 Enable(활성)을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

스위치에서 GVRP가 활성화됩니다.

GVRP를 통해 VLAN 등록 활성화

1. GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 엽니다.
2. 원하는 인터페이스에 대한 GVRP Global Status(GVRP 전역 상태) 필드에서 Enable(활성)을 선택합니다.
3. GVRP Registration(GVRP 등록) 필드에서 Enable(활성)을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

포트에서 GVRP VLAN 등록이 활성화되고 장치가 업데이트됩니다.

GVRP 포트 매개변수 표 표시

1. GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 엽니다.
 2. Show All(모두 표시)을 클릭합니다.
- GVRP Port Parameters Table(GVRP 포트 매개변수 표)이 표시됩니다.

그림 7-63. GVRP Port Parameters Table(GVRP 포트 매개변수 표)

Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Copy To	Edit
1	1/1	Disable	Disable	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	1/2	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
3	1/3	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>

26	1/26	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
27	1/27	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
28	1/28	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>

LAGs					
29	lag1	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
30	lag2	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
31	lag3	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
32	lag4	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
33	lag5	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
34	lag6	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
35	lag7	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
36	lag8	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>

3. 스왑의 다른 장치(존재하는 경우)에 대해 GVRP Port Parameters Table(GVRP 포트 매개변수 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

GVRP 매개변수 복사

1. GVRP Global Parameters(GVRP 전역 매개변수) 페이지를 엽니다.
 2. Show All(모두 표시)을 클릭합니다.
- GVRP Port Parameters Table(GVRP 포트 매개변수 표)이 표시됩니다.
3. Copy Parameters From(매개변수 복사 위치)에서 복사할 포트 또는 LAG를 지정합니다.
 4. 이 매개변수를 수신할 각 인터페이스/LAG에 대해 Copy To(복사 위치)를 클릭합니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

GVRP 포트 매개변수 설정이 복사되고 장치가 업데이트됩니다.

여러 포트에 대해 GVRP 매개변수 수정

1. **GVRP Global Parameters(GVRP 전역 매개변수)** 페이지를 엽니다.

2. **Show All(모두 표시)**을 클릭합니다.

GVRP Port Parameters Table(GVRP 포트 매개변수 표)이 표시됩니다.

3. 수정할 각 인터페이스/LAG에 대해 **Edit(편집)**를 클릭합니다.

4. GVRP 포트 매개변수 필드를 필요에 따라 편집합니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

GVRP 포트 매개변수 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 GVRP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. GVRP 명령

포트 결합

링크 결합을 사용하면 하나 이상의 전이중(FDX) 이더넷 링크를 함께 결합하여 LAG(Link Aggregation Group)를 만들 수 있습니다. 따라서 네트워크 스위치는 LAG를 단일 링크로 취급할 수 있습니다.

정적 LAG가 지원됩니다. 포트가 LAG에 정적 구성원으로 추가되면 LACPDU를 전송하거나 수신하지 않습니다.

Link Aggregation(링크 결합) 메뉴 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Link Aggregation(링크 결합)**을 클릭합니다. **Link Aggregation(링크 결합)** 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

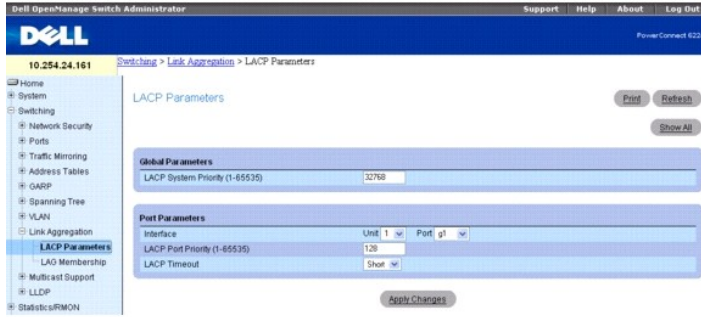
1. [LACP 매개변수](#)
1. [LAG 멤버십](#)
1. [LAG 해시 구성](#)
1. [LAG 해시 요약](#)

LACP 매개변수

링크 결합은 LACPDU의 주기적 교환으로 초기화 및 유지 관리됩니다. **LACP Parameters(LACP 매개변수)** 페이지에서 LACP LAG를 구성합니다.

LACP Parameters(LACP 매개변수) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Link Aggregation(링크 결합)**→**LACP Parameters(LACP 매개변수)**를 클릭합니다.

그림 7-64. LACP Parameters(LACP 매개변수)



LACP Parameters(LACP 매개변수) 페이지는 전역 매개변수와 포트 매개변수의 두 절로 구분됩니다. 이 페이지의 필드는 다음과 같습니다.

전역 매개변수

LACP System Priority(LACP 시스템 우선 순위) (1-65535) — 전역 설정에 대한 LACP 우선 순위 값을 나타냅니다. 기본값은 1입니다.

포트 매개변수

Interface(인터페이스) — 타임아웃 및 우선 순위 값이 할당되는 장치와 포트 번호를 지정합니다.

LACP Port Priority(LACP 포트 우선 순위) (1-65535) — 지정된 포트에 대한 LACP 우선 순위 값을 지정합니다. 기본값은 1입니다.

LACP Timeout(LACP 타임아웃) — 관리 LACP 타임아웃을 지정합니다. 가능한 값은 다음과 같습니다.

Short(짧은) — 짧은 타임아웃 값을 지정합니다.

Long(긴) — 긴 타임아웃 값을 지정합니다. 기본 설정입니다.

링크 결합 매개변수 정의

1. **LACP Parameters(LACP 매개변수)** 페이지를 엽니다.
2. 필요에 따라 필드를 입력합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

매개변수가 정의되고 장치가 업데이트됩니다.

LACP 매개변수 표 표시

1. **LACP Parameters(LACP 매개변수)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.

LACP Parameters Table(LACP 매개변수 표)이 표시됩니다.

그림 7-65. LACP Parameters Table(LACP 매개변수 표)

LACP Parameters Table Print Refresh

Unit: 1

Port	Port Priority	LACP Timeout	Edit
1	128	Long	<input checked="" type="checkbox"/>
2	128	Long	<input type="checkbox"/>
3	128	Long	<input type="checkbox"/>

26	128	Long	<input type="checkbox"/>
27	128	Long	<input type="checkbox"/>
28	128	Long	<input type="checkbox"/>

Apply Changes Back

3. 스크의 다른 장치(존재하는 경우)에 대해 **LACP Parameters Table(LACP 매개변수 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

여러 포트에 대한 LACP 매개변수 수정

1. **LACP Parameters(LACP 매개변수)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.
LACP Parameters Table(LACP 매개변수 표)이 표시됩니다.
3. 수정할 각 포트에 대해 **Edit(편집)**를 클릭합니다.
4. 필요에 따라 필드를 편집합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
LACP 매개변수 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 LACP 매개변수 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

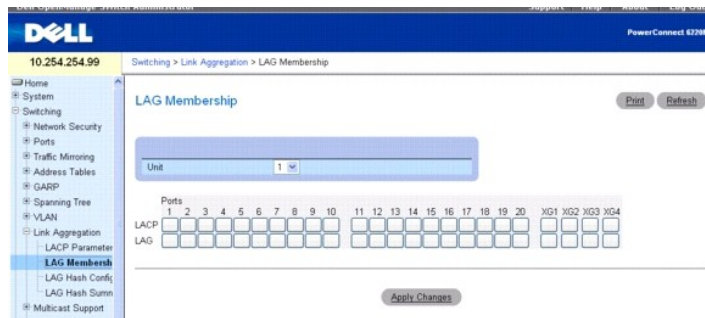
- 1 LACP 명령

LAG 멤버십

스위치는 시스템당 18개의 LAG, LAG당 8개의 포트를 지원합니다. **LAG Membership(LAG 멤버십)** 페이지에서 LAG와 LACP에 포트를 할당합니다.

LAG Membership(LAG 멤버십) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Link Aggregation(링크 결합)** → **LAG Membership(LAG 멤버십)**을 클릭합니다.

그림 7-66. LAG Membership(LAG 멤버십)



LAG Membership(LAG 멤버십) 페이지에는 다음 필드가 있는 표가 포함되어 있습니다.

LACP — LAG 포트를 LACP 멤버십으로 결합합니다. LAG 행에 번호가 있는 포트의 경우 **LACP** 행에서 클릭하여 LACP를 "on"으로 전환할 수 있습니다. 클릭할 때마다 L(LACP)과 공백(LACP 없음) 간에 전환됩니다.

LAG — 포트를 LAG에 추가하고, 포트가 속할 특정 LAG를 나타냅니다. 클릭할 때마다 LAG 번호가 1부터 8까지 전환된 다음 공백(할당된 LAG 없음)으로 돌아갑니다.


포트를 LAG에 추가

1. **LAG Membership(LAG 멤버십)** 페이지를 엽니다.
2. **LAG** 행을 클릭하여 포트를 원하는 LAG로 전환합니다.
해당 포트에 대해 LAG 번호가 표시됩니다. LAG 번호는 클릭할 때마다 18에 도달할 때까지 증가한 후에 공백(할당된 LAG 없음)으로 돌아갑니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.

선택한 LAG에 포트가 할당되고 장치가 업데이트됩니다.

LAG 포트를 LACP에 추가

1. LAG Membership(LAG 멤버십) 페이지를 엽니다.
2. LACP 행을 클릭하여 원하는 LAG 포트를 L로 전환합니다.

 **주:** 포트를 LACP로 결합하려면 먼저 LAG에 할당해야 합니다.

3. Apply Changes(변경사항 적용)를 클릭합니다.

LAG 포트가 LACP로 결합되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 포트를 LAG 및 LACP에 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

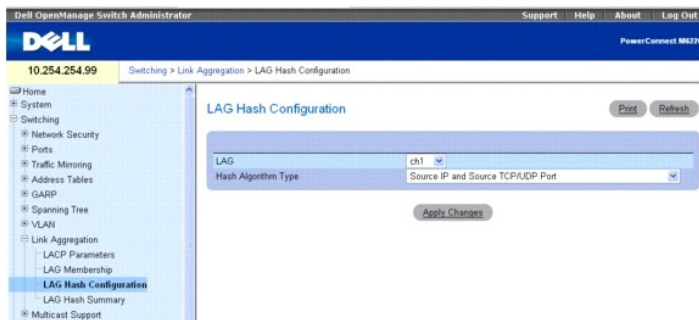
- 1 포트 채널 명령

LAG 해시 구성

결함자 링크의 트래픽 분배 모드를 설정하려면 LAG 해시 알고리즘을 사용합니다. 각 트렁크의 해시 유형을 설정할 수 있습니다.

LAG Hash Configuration(LAG 해시 구성) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치)→ Link Aggregation(링크 결합)→ LAG Hash Configuration(LAG 해시 구성)을 클릭합니다.

그림 7-67. LAG Hash Configuration(LAG 해시 구성)



LAG Hash Configuration(LAG 해시 구성) 페이지에는 다음 필드가 포함되어 있습니다.

LAG — 드롭다운 메뉴에 LAG 번호가 나열됩니다.

Hash Algorithm Type(해시 알고리즘 유형) — 유니캐스트 트래픽용 해시 알고리즘은 다음 중 하나입니다.

- 1 소스 MAC, VLAN, EtherType, SourceModule 및 포트 ID
- 1 대상 MAC, VLAN, EtherType, SourceModule 및 포트 ID
- 1 소스 IP 및 소스 TCP/UDP 포트(기본값)
- 1 대상 IP 및 대상 TCP/UDP 포트
- 1 소스/대상 MAC, VLAN, EtherType, 소스 MODID/포트
- 1 소스/대상 IP 및 소스/대상 TCP/UDP 포트

LAG 해시 구성

1. LAG Hash Configuration(LAG 해시 구성) 페이지를 엽니다.
2. 구성할 LAG 및 LAG를 할당할 해시 알고리즘을 할당합니다.

3. **Apply Changes(변경사항 적용)**를 클릭합니다.

매개변수가 수정되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 LAG 해시 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

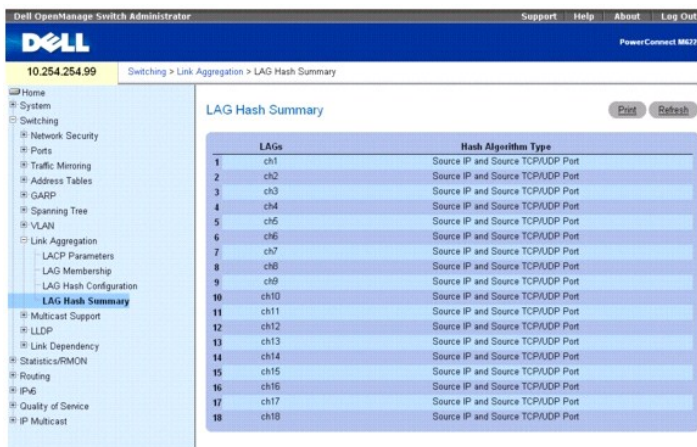
- 1 포트 채널 명령

LAG 해시 요약

LAG Hash Summary(LAG 해시 요약) 페이지에 시스템의 채널 및 그 채널에 할당된 해시 알고리즘 유형이 나열됩니다.

LAG Hash Summary(LAG 해시 요약) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Link Aggregation(링크 결합)** → **LAG Hash Summary(LAG 해시 요약)**를 클릭합니다.

그림 7-68. LAG Hash Summary(LAG 해시 요약)



LAG Hash Summary(LAG 해시 요약) 페이지에는 다음 필드가 있는 표가 포함되어 있습니다.

LAG — LAG 구성원이 나열됩니다.

Hash Algorithm Type(해시 알고리즘 유형) — LAG와 연결된 유니캐스트 트래픽 흐름용 해시 알고리즘 유형을 표시합니다.

CLI 명령을 사용하여 LAG 해시 알고리즘 요약 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 포트 채널 명령

멀티캐스트 지원 관리

스위치는 총 2 멀티캐스트 전달 데이터베이스를 사용하여 멀티캐스트 대상 MAC 주소로 수신된 패킷에 대한 전달 결정을 내립니다. 멀티캐스트를 스위치의 특정 포트로만 제한하면 트래픽이 불필요한 네트워크의 일부로 가는 것을 방지할 수 있습니다.

패킷이 스위치에 들어오면 대상 MAC 주소가 VLAN ID와 결합되고 총 2 전달 데이터베이스에서 검색이 수행됩니다. 일치하는 항목이 없으면 패킷은 스위치 구성에 따라 VLAN의 모든 포트에 플러딩되거나 삭제됩니다. 일치하는 항목이 있으면 패킷은 해당 멀티캐스트 그룹의 구성원인 포트만 전달됩니다.

Multicast Support(멀티캐스트 지원) *메뉴* 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Multicast Support(멀티캐스트 지원)**를 클릭합니다. 이 **Multicast Support(멀티캐스트 지원)** 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

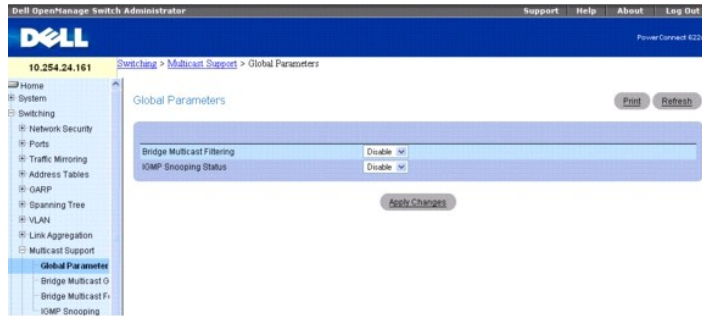
- 1 [멀티캐스트 전역 매개변수](#)
- 1 [브리지 멀티캐스트 그룹](#)
- 1 [브리지 멀티캐스트 전달](#)
- 1 [IGMP 스누핑](#)

멀티캐스트 전역 매개변수

Multicast Global Parameters(멀티캐스트 전역 매개변수) 페이지에서 스위치에 대한 브리지 멀티캐스트 필터링 또는 IGMP 스누핑을 활성화합니다. 이 기능에 대한 매개변수는 [브리지 멀티캐스트 전달 및 IGMP 스누핑](#) 웹 페이지에서 수정할 수 있습니다.

Multicast Global Parameters(멀티캐스트 전역 매개변수) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Multicast Support(멀티캐스트 지원)**→**Global Parameters(전역 매개변수)**를 클릭합니다.

그림 7-69. Multicast Global Parameters(멀티캐스트 전역 매개변수)



Multicast Global Parameters(멀티캐스트 전역 매개변수) 페이지에는 다음 필드가 포함되어 있습니다.

Bridge Multicast Filtering(브리지 멀티캐스트 필터링) — 브리지 멀티캐스트 필터링을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

IGMP Snooping Status(IGMP 스누핑 상태) — IGMP 스누핑을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

스위치에서 브리지 멀티캐스트 필터링 활성화

1. Multicast Global Parameters(멀티캐스트 전역 매개변수) 페이지를 엽니다.
2. Bridge Multicast Filtering(브리지 멀티캐스트 필터링) 필드에서 **Enable(활성)**을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

스위치에서 브리지 멀티캐스트가 활성화됩니다.

CLI 명령을 사용하여 멀티캐스트 전달 및/또는 IGMP 스누핑 활성화

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

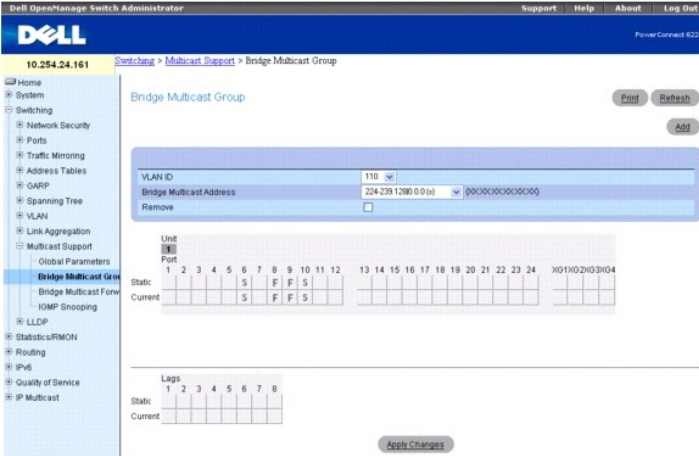
- 1 주소 표 명령

브리지 멀티캐스트 그룹

Bridge Multicast Group(브리지 멀티캐스트 그룹) 페이지에서 새 멀티캐스트 서비스 그룹을 만들거나 기존 멀티캐스트 서비스 그룹에 할당된 포트와 LAG를 수정합니다. 연결된 인터페이스는 **Port(포트)** 및 **LAG** 표에 표시되고 각 항목이 멀티캐스트 그룹에 연결된 방식이 반영됩니다.

Bridge Multicast Group(브리지 멀티캐스트 그룹) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**Multicast Support(멀티캐스트 지원)**→**Bridge Multicast Group(브리지 멀티캐스트 그룹)**을 클릭합니다.

그림 7-70. Bridge Multicast Group(브리지 멀티캐스트 그룹)



Bridge Multicast Group(브리지 멀티캐스트 그룹) 페이지에는 다음 필드가 포함되어 있습니다.

VLAN ID — 멀티캐스트 그룹을 추가하거나 기존 멀티캐스트 그룹에서 포트를 수정하려면 VLAN을 선택합니다.

Bridge Multicast Address(브리지 멀티캐스트 주소) — 선택된 VLAN ID와 연결된 멀티캐스트 그룹 MAC 주소/IP 주소를 식별합니다. **Add(추가)** 단추를 사용하여 새 주소를 VLAN ID와 연결합니다.

Remove(제거) — 브리지 멀티캐스트 주소를 제거합니다.

포트 및 LAG 구성원 표

Bridge Multicast Group(브리지 멀티캐스트 그룹) 표에는 어떤 포트와 LAG가 멀티캐스트 그룹의 구성원인지와, 이를 상태가 정적인지(S), 동적인지(D) 또는 금지되었는지(F) 여부 가 표시됩니다. 표에는 **Static(정적)** 및 **Current(현재)** 라는 두 행이 있습니다. 이 페이지에서는 **Static(정적)** 행만 액세스할 수 있습니다. **Static(정적)** 행을 변경하고 **Apply Changes(변경사항 적용)** 를 클릭하면 **Current(현재)** 행이 업데이트됩니다.

Bridge Multicast Group(브리지 멀티캐스트 그룹) 페이지에는 두 개의 편집 가능한 표가 포함되어 있습니다.

Unit and Ports(장치 및 포트) — 멀티캐스트 그룹 멤버십을 포트에 할당하고 표시합니다. 멤버십을 할당하려면 특정 포트에 대해 **Static(정적)** 을 클릭합니다. 클릭할 때마다 S, F 및 공백(멤버가 아님)이 번갈아 정의는 다음 표를 참조하십시오.

LAGs — 멀티캐스트 그룹 멤버십을 LAG에 할당하고 표시합니다. 멤버십을 할당하려면 특정 LAG에 대해 **Static(정적)** 을 클릭합니다. 클릭할 때마다 S, F 및 공백(멤버가 아님)이 번갈아 정의는 다음 표를 참조하십시오.

다음 표에는 포트/LAG IGMP 관리 설정에 대한 정의가 포함되어 있습니다.

표 7-2. /LAG IGMP 관리 설정

포트 제어	정의
D	동적: 포트/LAG가 멀티캐스트 그룹에 동적으로 연결되었음을 나타냅니다(<i>Current(현재)</i> 행에 표시).
S	정적: <i>Static(정적)</i> 행에서 포트를 멀티캐스트 그룹에 정적 구성원으로 연결합니다. Apply Changes(변경사항 적용) 를 클릭하면 <i>Current(현재)</i> 행에 표시됩니다.
공백	공백: 포트가 멀티캐스트 그룹에 연결되지 않았음을 나타냅니다.

브리지 멀티캐스트 주소 추가

1. Bridge Multicast Group(브리지 멀티캐스트 그룹) 페이지를 엽니다.
 2. **Add(추가)** 를 클릭합니다.
- Add Bridge Multicast Group(브리지 멀티캐스트 그룹 추가) 페이지가 표시됩니다.

그림 7-71. Add Bridge Multicast Group(브리지 멀티캐스트 그룹 추가)

3. 드롭다운 메뉴에서 **VLAN ID**를 선택합니다.
4. **새 브리지 멀티캐스트 IP 또는 MAC** 주소를 정의합니다.
5. **Bridge Multicast Group(브리지 멀티캐스트 그룹)** 표에서 특정 포트/LAG의 **Static(정적)** 행을 클릭하여 설정을 할당합니다. 클릭할 때마다 S, F 및 공백(멤버가 아님)이 번갈아 표시됩니다.
6. **Apply Changes(변경사항 적용)**를 클릭합니다.

브리지 멀티캐스트 주소가 멀티캐스트 그룹에 할당되고 포트/LAG가 그룹(**Current(현재)** 행이 **Static(정적)** 설정으로 업데이트됨)에 할당되며, 장치가 업데이트됩니다.

인터페이스를 기존 멀티캐스트 그룹에 할당

1. **Bridge Multicast Group(브리지 멀티캐스트 그룹)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 **VLAN ID**를 선택합니다.
연결된 **Bridge Multicast Address(브리지 멀티캐스트 주소)**가 표시됩니다.
3. **Bridge Multicast Group(브리지 멀티캐스트 그룹)** 표에서 특정 포트/LAG의 **Static(정적)** 행을 클릭하여 설정을 할당합니다. 클릭할 때마다 S, F 및 공백(구성원 아님)이 번갈아 표시됩니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

인터페이스가 멀티캐스트 그룹에 할당되고 **Current(현재)** 행이 **Static(정적)** 설정으로 업데이트되며, 장치가 업데이트됩니다.

브리지 멀티캐스트 그룹 제거

1. **Bridge Multicast Group(브리지 멀티캐스트 그룹)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 제거할 브리지 멀티캐스트 그룹과 연결된 **VLAN ID**를 선택합니다.
Bridge Multicast Address(브리지 멀티캐스트 주소) 및 할당된 포트/LAG가 표시됩니다.
3. **Remove(제거)** 확인란을 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

선택된 브리지 멀티캐스트 그룹이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 멀티캐스트 서비스 구성원 관리

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

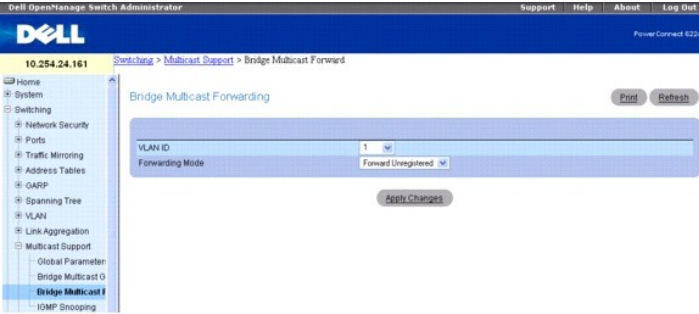
- 1 주소 표 명령

브리지 멀티캐스트 전달

Bridge Multicast Forward(브리지 멀티캐스트 전달) 페이지에서 포트나 LAG를 인접한 멀티캐스트 스위치에 연결할 수 있도록 합니다. IGMP 스누핑이 활성화되면 멀티캐스트 패킷이 적절한 포트 또는 VLAN에 전달됩니다.

Bridge Multicast Forward(브리지 멀티캐스트 전달) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Multicast Support(멀티캐스트 지원)** → **Bridge Multicast Forward(브리지 멀티캐스트 전달)**를 클릭합니다.

그림 7-72. Bridge Multicast Forward(브리지 멀티캐스트 전달)



Bridge Multicast Forward(브리지 멀티캐스트 전달) 페이지에는 다음 필드와 두 개의 편집 가능한 표가 포함되어 있습니다.

VLAN ID — 적용할 VLAN을 선택합니다.

Forwarding Mode(전달 모드) — 선택된 VLAN에 대한 멀티캐스트 전달 모드를 지정합니다. 가능한 값은 다음과 같습니다.

Forward Unregistered(미등록 전달) — 이전 IGMP 멤버십 보고서에서 발표된 그룹과 일치하지 않는 대상 주소를 가진 IPv4 멀티캐스트 패킷의 전달을 허용합니다.

Forward All(모두 전달) — 등록 및 등록되지 않은 멀티캐스트 패킷의 전달을 허용합니다.

Filter Unregistered(미등록 필터) — 이전 IGMP 멤버십 보고서에서 발표된 그룹과 일치하지 않는 대상 주소를 가진 IPv4 멀티캐스트 패킷의 전달을 금지합니다.

브리지 멀티캐스트 전달 모드 변경

1. **Bridge Multicast Forward(브리지 멀티캐스트 전달)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 **VLAN ID**를 선택합니다.
3. 드롭다운 메뉴에서 VLAN을 할당할 **Forwarding Mode(전달 모드)**를 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

VLAN이 **Forwarding Mode(전달 모드)** 설정으로 업데이트되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 멀티캐스트 라우터에 연결된 LAG 및 포트 관리

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

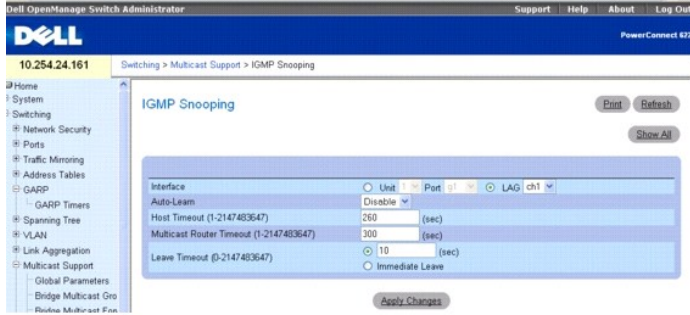
- 1 주소 표 명령

IGMP 스누핑

IGMP Snooping(IGMP 스누핑) 페이지에서 IGMP 구성원을 추가합니다.

IGMP Snooping(IGMP 스누핑) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)** → **Multicast Support(멀티캐스트 지원)** → **IGMP Snooping(IGMP 스누핑)**을 클릭합니다.

그림 7-73. IGMP Snooping(IGMP 스누핑)



IGMP Snooping(IGMP 스누핑) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 적용할 장치와 포트를 선택합니다.

Auto-Learn(자동 탐색) — 스위치에서 자동 탐색을 활성화하거나 비활성화합니다.

Host Timeout(호스트 타임아웃) — IGMP 스누핑 항목의 보존 기간이 만료되는 시간을 지정합니다. 기본 시간은 260초입니다.

Multicast Router Timeout(멀티캐스트 라우터 타임아웃) — 멀티캐스트 라우터 항목의 보존 기간이 만료되는 시간을 지정합니다. 기본값은 300초입니다.

Leave Timeout(해제 타임아웃) — 포트 해제 메시지가 수신된 후 항목 보존 기간이 만료되는 시간을 초 단위로 지정합니다. 타임아웃 기간에 대한 시간을 입력하거나 **Immediate Leave(즉시 해제)**를 클릭하여 즉시 타임아웃을 지정합니다. 기본 타임아웃은 10초입니다.

스위치에서 IGMP 스누핑 활성화

1. IGMP Snooping(IGMP 스누핑) 페이지를 엽니다.
2. Interface(인터페이스) 필드에서 구성할 장치와 포트를 선택합니다.
3. 필요에 따라 페이지의 필드를 완료합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

IGMP 스누핑이 스위치에서 활성화됩니다.

IGMP 스누핑 표 표시

1. IGMP Snooping(IGMP 스누핑) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

IGMP Snooping Table(IGMP 스누핑 표)이 표시됩니다.

그림 7-74. IGMP Snooping Table(IGMP 스누핑 표)

Port	Auto Learn Enable	Host Timeout	Multicast Router Timeout	Leave Timeout	Copy To	Edit
1	1/g1	Disable	260	300	10	
2	1/g2	Disable	260	300	10	
3	1/g3	Disable	260	300	10	

LAGs	Auto Learn Enable	Host Timeout	Multicast Router Timeout	Leave Timeout	Copy To	Edit
29	ch1	Disable	260	300	10	
30	ch2	Disable	260	300	10	
31	ch3	Disable	260	300	10	
32	ch4	Disable	260	300	10	
33	ch5	Disable	260	300	10	
34	ch6	Disable	260	300	10	
35	ch7	Disable	260	300	10	
36	ch8	Disable	260	300	10	

3. 스택의 다른 장치(존재하는 경우)에 대해 **IGMP Snooping Table(IGMP 스누핑 표)**을 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

여러 포트 또는 LAG의 IGMP 스누핑 설정 수정

1. **IGMP Snooping(IGMP 스누핑)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.
IGMP Snooping Table(IGMP 스누핑 표)이 표시됩니다.
3. 수정할 각 포트 또는 LAG에 대해 **Edit(편집)**를 클릭합니다.
4. 필요에 따라 IGMP 스누핑 필드를 편집합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
IGMP 스누핑 설정이 수정되고 장치가 업데이트됩니다.

여러 포트 또는 LAG에 IGMP 스누핑 설정 복사

1. **IGMP Snooping(IGMP 스누핑)** 페이지를 엽니다.
2. **Show All(모두 표시)**을 클릭합니다.
IGMP Snooping Table(IGMP 스누핑 표)이 표시됩니다.
3. **Copy Parameters From(매개변수 복사 위치)**을 클릭합니다.
4. 원하는 매개변수의 소스로 사용할 장치/포트 또는 LAG를 선택합니다.
5. 이 매개변수가 복사될 장치/포트 또는 LAG에 대해 **Copy To(복사 위치)**를 클릭합니다.
6. **Apply Changes(변경사항 적용)**를 클릭합니다.
IGMP 스누핑 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령으로 IGMP 스누핑 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. IGMP 스누핑 명령

LLDP(Link Layer Discovery Protocol) 구성

IEEE 802.1AB 정의 표준인 LLDP(Link Layer Discovery Protocol)를 사용하면 802 LAN에 상주하는 스테이션은 주요 기능 및 물리적 설명을 알릴 수 있습니다. 네트워크 관리자는 이 정보를 보고 시스템 토폴로지를 식별하여 LAN의 잘못된 구성을 감지합니다.

LLDP는 단방향 프로토콜이므로 요청/응답 순서가 없습니다. 정보는 전송 기능을 구현하는 스테이션에 의해 알려지며, 수신 기능을 구현하는 스테이션에 의해 수신 및 처리됩니다. 전송 및 수신 기능은 포트마다 별도로 활성화/비활성화할 수 있습니다. 기본적으로 전송/수신 기능은 둘 다 모든 포트에서 비활성화되어 있습니다. 응용 프로그램은 구성된 상태와 포트의 작동 상태를 기반으로 각 전송 및 수신 상태 시스템을 적절하게 시작합니다.

LLDP 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

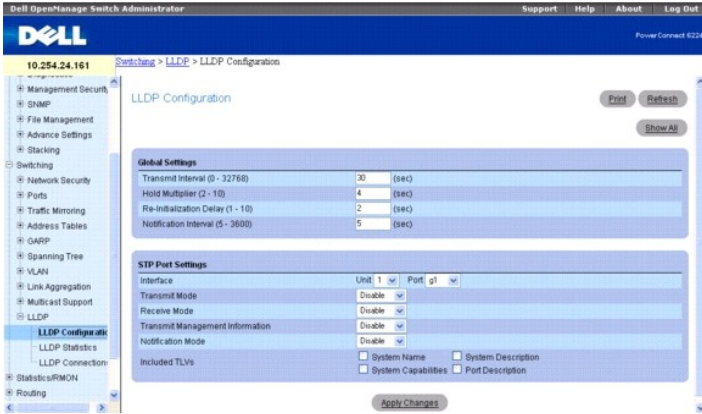
1. [LLDP 구성](#)
1. [LLDP 통계](#)
1. [LLDP 연결](#)

LLDP 구성

LLDP 구성 페이지에서 LLDP 매개변수를 지정합니다. 전체 시스템과 특정 인터페이스에 적용되는 매개변수는 여기에서 지정할 수 있습니다.

LLDP Configuration(LLDP 구성) 페이지를 표시하려면 디렉터리 화면에서 **Switching(스위치)**→**LLDP**→**LLDP Configuration(LLDP 구성)**을 클릭합니다.

그림 7-75. LLDP Configuration(LLDP 구성)



LLDP Configuration(LLDP 구성) 페이지에는 다음 필드가 포함되어 있습니다.

전역 설정

Transmit Interval(전송 간격) (1-32768) — 프레임이 전송되는 간격을 지정합니다. 기본값은 30초입니다.

Hold Multiplier(유지 승수) (2-10) — TTL에 할당할 전송 간격의 승수를 지정합니다. 기본값은 4입니다.

Re-Initialization Delay(재초기화 지연) (1-10) — 재초기화 전의 지연을 지정합니다. 기본값은 2초입니다.

Notification Interval(알림 간격) (5-3600) — 알림 전송을 제한합니다. 기본값은 5초입니다.

포트 설정

Interface(인터페이스) — 이 매개변수에서 적용할 포트를 지정합니다.

Transmit Mode(전송 모드) — 전송 기능을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

Receive Mode(수신 모드) — 수신 기능을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

Transmit Management Information(전송 관리 정보) — 관리 주소 인스턴스의 전송을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

Notification Mode(알림 모드) — 원격 변경 알림을 활성화하거나 비활성화합니다. 기본값은 Disabled(비활성)입니다.

Included TLVs(포함된 TLV) — 전송할 TLV 정보를 선택합니다. 시스템 이름, 시스템 기능, 시스템 설명 및 포트 설명 등을 선택할 수 있습니다.

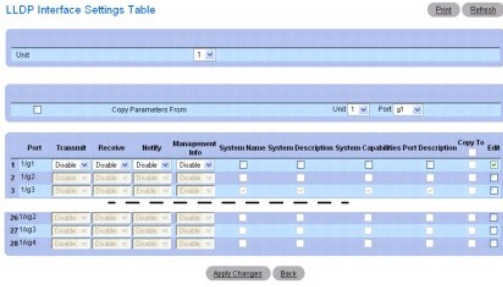
LLDP 구성 수정

1. **LLDP Configuration(LLDP 구성)** 페이지를 엽니다.
2. 필요에 따라 필드를 정의합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.
LLDP 매개변수가 스위치에 저장됩니다.

LLDP 인터페이스 설정 표 표시

1. **LLDP Configuration(LLDP 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
LLDP Interface Settings Table(LLDP 인터페이스 설정 표)이 표시됩니다.

그림 7-76. LLDP Interface Settings Table(LLDP 인터페이스 설정 표)



3. 스택의 다른 장치(존재하는 경우)에 대해 LLDP Interface Settings Table(LLDP 인터페이스 설정 표)을 보려면 Unit(장치) 드롭다운 메뉴를 사용합니다.

LLDP 인터페이스 설정 복사

1. LLDP Configuration(LLDP 구성) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

LLDP Interface Settings Table(LLDP 인터페이스 설정 표)이 표시됩니다.

3. Copy Parameters From(매개변수 복사 위치)에서 복사할 장치와 포트를 지정합니다.

4. 이 매개변수를 수신할 각 장치/포트에 대해 Copy To(복사 위치)를 클릭합니다.

5. Apply Changes(변경사항 적용)를 클릭합니다.

LLDP 인터페이스 설정이 복사되고 장치가 업데이트됩니다.

여러 포트의 LLDP 인터페이스 설정 수정

1. LLDP Configuration(LLDP 구성) 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

LLDP Interface Settings Table(LLDP 인터페이스 설정 표)이 표시됩니다.

3. 수정할 각 장치/포트에 대해 Edit(편집)를 클릭합니다.

4. 필요에 따라 LLDP 인터페이스 필드를 편집합니다.

5. Apply Changes(변경사항 적용)를 클릭합니다.

LLDP 인터페이스 설정이 수정되고 장치가 업데이트됩니다.

CLI 명령으로 LLDP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

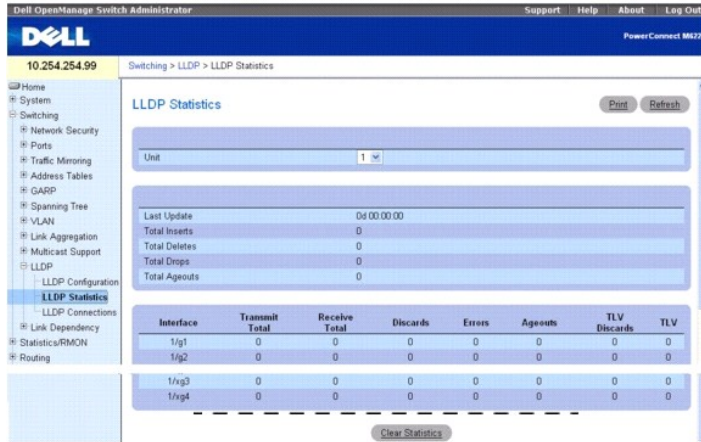
1 LLDP 명령

LLDP 통계

LLDP 통계 페이지에서 LLDP 관련 통계를 확인합니다.

LLDP Statistics(LLDP 통계) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치)→LLDP→LLDP Statistics(LLDP 통계)를 클릭합니다.

그림 7-77. LLDP Statistics(LLDP 통계)



LLDP Statistics(LLDP 통계) 페이지에는 다음 통계가 표시됩니다.

전체 시스템 통계

Last Update(마지막 업데이트) — 원격 데이터 항목이 작성, 수정 또는 삭제된 마지막 시스템 가동 시간 값을 표시합니다.

Total Inserts(전체 삽입) — 원격 스위치에서 알려진 전체 정보 집합이 표에 삽입된 횟수를 표시합니다.

Total Deletes(전체 삭제) — 원격 스위치에서 알려진 전체 정보 집합이 표에서 삭제된 횟수를 표시합니다.

Total Drops(전체 삭제) — 자원 부족으로 인해 원격 스위치에서 알려진 전체 정보 집합을 삽입하지 못한 횟수를 표시합니다.

Total Ageouts(전체 만료) — TTL(Time-to-Live) 만료로 인해 원격 데이터 항목이 삭제된 횟수를 표시합니다.

포트 통계

Interface(인터페이스) — 해당 라인의 통계가 적용되는 장치와 포트를 표시합니다.

Transmit Total(전체 전송) — 표시된 포트에 전송된 LLDP 프레임의 전체 수를 표시합니다.

Receive Total(전체 수신) — 표시된 포트에 수신된 유효한 LLDP 프레임의 전체 수를 표시합니다.

Discards(삭제) — 표시된 포트에 수신된 LLDP 프레임의 수와 삭제된 횟수를 표시합니다.

Errors(오류) — 표시된 포트에 수신된 유효하지 않은 LLDP 프레임의 수를 표시합니다.

Ageouts(만료) — TTL 만료로 인해 표시된 포트의 원격 데이터 항목이 삭제된 횟수를 표시합니다.

TLV Discards(TLV 삭제) — 표시된 포트에 수신된 LLDP TLV(Type(유형), Length(길이), Value(값) 집합)의 수와 LLDP 에이전트에 의해 삭제된 횟수를 표시합니다.

TLV Unknowns(TLV 알 수 없음) — 표시된 포트에 수신된 LLDP TLV 중 LLDP 에이전트에 의해 인식되지 않은 유형의 수를 표시합니다.

스택의 다른 장치(존재하는 경우)에 대해 **LLDP Statistics(LLDP 통계)**를 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

Clear Statistics(통계 지우기) 단추를 사용하여 모든 LLDP 통계를 0으로 재설정합니다.

CLI 명령으로 LLDP 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

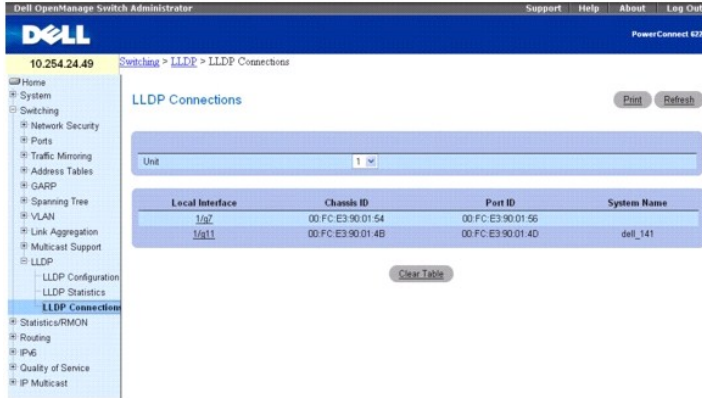
1 LLDP 명령

LLDP 연결

LLDP Connections(LLDP 연결) 페이지에서 LLDP가 활성화된 포트 목록을 확인합니다. 기본 연결 세부사항이 표시됩니다.

LLDP Connections(LLDP 연결) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위치)→LLDP→LLDP Connections(LLDP 연결)를 클릭합니다.

그림 7-78. LLDP Connections Table(LLDP 연결 표)



LLDP Connections(LLDP 연결) 페이지에 다음 포트 세부사항이 표시됩니다.

Local Interface(로컬 인터페이스) — 스택의 장치와 포트를 지정합니다.

Chassis ID(채시 ID) — 802 LAN 장치의 채시를 식별합니다.

Port ID(포트 ID) — LLDPU가 전송된 포트 번호를 식별합니다.

System Name(시스템 이름) — 원격 장치와 연결된 시스템 이름을 식별합니다.

스택의 다른 장치(존재하는 경우)에 대해 LLDP Connections(LLDP 연결)를 보려면 **Unit(장치)** 드롭다운 메뉴를 사용합니다.

Clear Table(표 지우기) 단추를 사용하여 LLDP Connections(LLDP 연결) 표에서 모든 정보를 삭제합니다.

LLDP 연결에 대한 세부사항 보기

1. LLDP Connections(LLDP 연결) 페이지를 엽니다.
2. 해당 장치에 대한 세부사항을 보려면 **Local Interface(로컬 인터페이스)** 필드에서 인터페이스를 클릭합니다.

장치의 LLDP Connections - Detailed(LLDP 연결 - 세부사항) 페이지가 표시됩니다.

그림 7-79. Detailed LLDP Connections(세부 LLDP 연결)



3. **Back(뒤로)** 단추를 사용하여 LLDP Connections(LLDP 연결) 페이지로 돌아갑니다.

CLI 명령으로 LLDP 연결 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. LLDP 명령

[목차 페이지로 돌아가기](#)

라우팅 구성

Dell™ PowerConnect™ M6220 사용 설명서

- [ARP](#)
- [IP](#)
- [OSPF](#)
- [BOOTP/DHCP 릴레이 에이전트](#)
- [RIP](#)
- [라우터 검색](#)
- [라우터](#)
- [VLAN 라우팅](#)
- [VRRP](#)
- [터널](#)
- [루프백](#)

6200 시리즈는 IP 라우팅 기능을 지원합니다. **Routing(라우팅)** 메뉴 페이지를 사용하여 VLAN의 라우팅을 구성할 수 있습니다.

패킷이 스위치에 들어오면 대상 MAC 주소가 구성된 라우팅 인터페이스와 일치하는지 확인됩니다. 일치하는 경우 장치가 호스트 표에서 일치하는 대상 IP 주소를 검색합니다. 항목이 있으면 패킷이 호스트로 라우팅됩니다. 일치하는 항목이 없는 경우 스위치는 대상 IP 주소에 대해 가장 긴 접두어 일치룰 수행합니다. 항목이 있으면 패킷이 다음 홉으로 라우팅됩니다. 일치하는 항목이 없는 경우 패킷이 기본 경로에 지정된 다음 홉으로 라우팅됩니다. 기본 경로가 구성되어 있지 않으면 패킷이 제대로 처리되도록 6200 시리즈 소프트웨어로 전달됩니다.

라우팅 표에는 관리자가 정적으로 추가한 항목이나 RIP 또는 OSPF를 통해 동적으로 추가된 항목이 포함될 수 있습니다. 호스트 표에는 관리자가 정적으로 추가한 항목이나 ARP를 통해 동적으로 추가된 항목이 포함될 수 있습니다.

Routing(라우팅) 메뉴 페이지에는 다음 기능에 대한 링크가 있습니다.

- 1 [ARP](#)
- 1 [IP](#)
- 1 [OSPF](#)
- 1 [BOOTP/DHCP 릴레이 에이전트](#)
- 1 [RIP](#)
- 1 [라우터 검색](#)
- 1 [라우터](#)
- 1 [VLAN 라우팅](#)
- 1 [VRRP](#)
- 1 [터널](#)
- 1 [루프백](#)

 **주:** 모든 라우팅 페이지에 대해 CLI 명령을 사용할 수 있는 것은 아닙니다.

ARP

6200 시리즈는 ARP 프로토콜을 사용하여 레이어 2 MAC 주소를 레이어 3 IPv4 주소와 연결합니다. 또한 관리자는 정적으로 ARP 표에 항목을 추가할 수 있습니다.

ARP는 인터넷 프로토콜(IP)의 필수 부분으로, IP 주소를 이더넷 등 LAN에서 정의된 미디어(MAC) 주소로 변환하는 데 사용됩니다. IP 패킷을 보낼 필요가 있는 스테이션은 대상이 같은 서브네트에 없는 경우 IP 대상 또는 다음 홉 라우터의 MAC 주소를 알아야 합니다. 이렇게 하려면 ARP 요청 패킷을 브로드캐스팅하면 됩니다. 해당 수신자는 MAC 주소가 포함된 ARP 응답을 유니캐스팅하여 이에 응답합니다. 확인된 MAC 주소는 IP 패킷 앞에 추가되는 레이어 2 헤더의 대상 주소 필드에 사용됩니다.

ARP 캐시는 네트워크의 각 스테이션에서 로컬로 유지 관리되는 표입니다. 이 캐시의 생성 또는 유지 관리와 관련하여 특정 요구 사항은 없지만, 적어도 0x0806 EtherType(이더넷 유형) 필드에서 이더넷에 대해 표시하는 ARP 프로토콜 패킷을 처리하는 동안 알게 된 정보를 포함해야 합니다. ARP 캐시 항목은 ARP 요청 또는 응답인지에 관계없이 ARP 패킷 페이로드 필드의 소스 정보를 검사하여 확인됩니다. 따라서 LAN 세그먼트 또는 가상 LAN(VLAN)의 모든 스테이션에 ARP 요청이 브로드캐스팅되는 경우 모든 수신자가 해당 ARP 캐시에 발신자의 IP 및 MAC 주소를 저장할 수 있습니다. 유니캐스팅되는 ARP 응답은 일반적으로 요청자에게만 표시되며, 요청자는 해당 ARP 캐시에 발신자 정보를 저장합니다. 항상 최신 정보가 ARP 캐시에 있는 기존 내용을 교체합니다.

ARP 캐시는 896개 항목을 지원할 수 있지만 사용자가 이 크기를 256과 896 사이의 임의의 값으로 구성할 수 있습니다. 라우터에서 일반적인 경우처럼 장치가 여러 개의 네트워크 인터페이스를 지원하는 경우 모든 인스턴스에 대해 하나의 ARP 캐시가 사용되거나 인스턴스별로 개별 캐시가 유지 관리됩니다. 두 번째 방법은 인스턴스별로 네트워크 주소 지정이 고유하지 않을 때 유용하지만 이더넷 MAC 주소 지정에는 해당되지 않으므로 하나의 ARP 캐시가 사용됩니다.

네트워크에서 장치를 이동할 수 있으므로 한때 특정 MAC 주소와 연결된 IP 주소가 이제 다른 MAC를 사용하거나 네트워크에서 완전히 사라질 수도 있습니다(재구성되거나 연결이 끊어졌거나 전원이 꺼짐). 이 때문에 네트워크에서 확인된 새 정보에 따라 항목을 업데이트하거나, 정기적으로 재생하여 주소가 있는지 여부를 확인하거나, 일반적으로 구성 중에 지정된 보존 기간 간격 중에 ARP 패킷의 발신자로 확인되지 않은 항목을 캐시에서 제거하지 않으면 ARP 캐시에 잘못된 정보가 유지됩니다.

ARP 메뉴 페이지에는 ARP 세부사항을 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **ARP**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

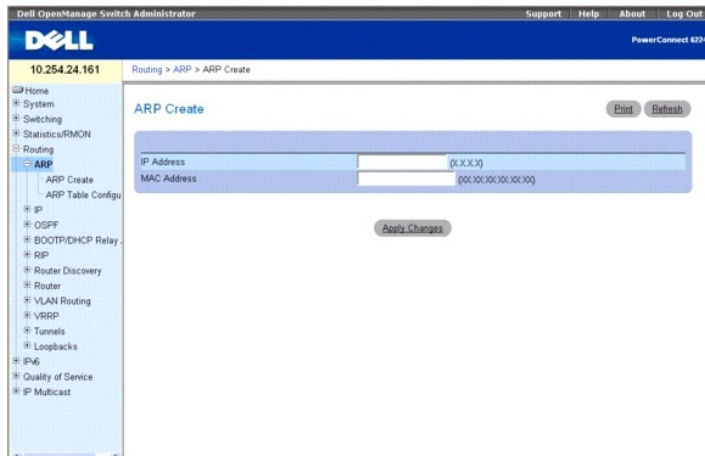
- 1 [ARP 만들기](#)
- 1 [ARP 표 구성](#)

ARP 만들기

ARP Create(ARP 만들기) 페이지를 사용하여 ARP 표에 항목을 추가할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **ARP** → **ARP Create(ARP 만들기)** 를 클릭합니다.

그림 10-1. ARP Create(ARP 만들기)



ARP Create(ARP 만들기) 페이지에는 다음 필드가 있습니다.

IP Address(IP 주소) — 추가할 IP 주소를 입력합니다. 스위치의 기존 라우팅 인터페이스 중 하나에 연결된 서브네트에 있는 장치의 IP 주소여야 합니다.

MAC Address(MAC 주소) — 장치의 유니캐스트 MAC 주소입니다. 콜론으로 구분된 6개의 두 자리 16진수로 주소를 입력합니다(예: 00:06:29:32:81:40).

ARP 표에 항목 추가

1. **ARP Create(ARP 만들기)** 페이지를 엽니다.
2. 연결할 주소를 지정합니다.
3. **Apply Changes(변경사항 적용)** 를 클릭하십시오.

주소가 이제 ARP 캐시에 있습니다.

CLI 명령을 사용하여 ARP 표에 항목 추가

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서* 의 다음 장을 참조하십시오.

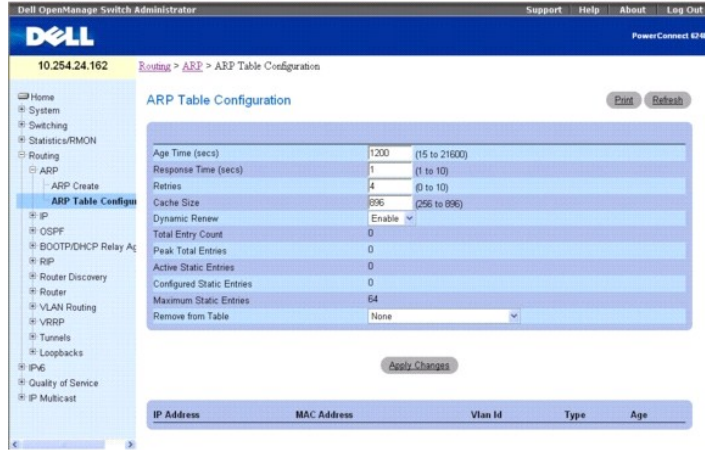
1. ARP 명령

ARP 표 구성

이 페이지를 사용하여 ARP 표에 대한 구성 매개변수를 변경할 수 있습니다. 이 화면에 표 내용을 표시할 수도 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **ARP** → **ARP Table Configuration(ARP 표 구성)** 을 클릭합니다.

그림 10-2. ARP Table Configuration(ARP 표 구성)



ARP Table Configuration(ARP 표 구성) 페이지에는 다음 필드가 있습니다.

Age Time (secs)(보존 시간(초)) — 스위치에서 ARP 항목 보존 시간으로 사용할 값을 입력합니다. ARP 항목의 보존 기간이 만료되기까지의 시간(초)을 나타내는 유효한 정수를 입력해야 합니다. 이 필드의 범위는 15 ~ 21600초입니다. Age Time(보존 시간)의 기본값은 1200초입니다.

Response Time (secs)(응답 시간(초)) — 스위치에서 ARP 응답 타임아웃으로 사용할 값을 입력합니다. 스위치가 ARP 요청에 대한 응답을 기다리는 시간(초)을 나타내는 유효한 정수를 입력해야 합니다. 이 필드의 범위는 1 ~ 10초입니다. Response Time(응답 시간)의 기본값은 1초입니다.

Retries(재시도 횟수) — ARP 요청이 재시도되는 최대 횟수를 지정하는 정수를 입력합니다. 이 필드의 범위는 0 ~ 10입니다. Retries(재시도 횟수)의 기본값은 4입니다.

Cache Size(캐시 크기) — ARP 캐시에 대한 최대 항목 수를 지정하는 정수를 입력합니다. 이 필드의 범위는 256 ~ 896입니다. Cache Size(캐시 크기)의 기본값은 896입니다.

Dynamic Renew(동적 갱신) — Dynamic(동적) 유형의 ARP 항목의 보존 기간이 만료될 때 ARP 구성 요소에서 자동으로 갱신할지 여부를 제어합니다. 기본 설정은 Enable(활성)입니다.

Total Entry Count(총 항목 수) — ARP 표에 있는 총 항목 수입니다.

Peak Total Entries(최대 총 항목 수) — Total Entry Count(총 항목 수)의 최대값입니다. 이 카운터 값은 ARP 표 Cache Size(캐시 크기) 값을 변경할 때마다 다시 시작됩니다.

Active Static Entries(활성 정적 항목 수) — ARP 표에 있는 총 활성 정적 항목 수입니다.

Configured Static Entries(구성된 정적 항목 수) — ARP 표에 있는 총 구성된 정적 항목 수입니다.

Maximum Static Entries(최대 정적 항목 수) — 정의할 수 있는 최대 정적 항목 수입니다.

Remove from Table(표에서 제거) — ARP 표에서 특정 항목을 제거할 수 있습니다. 나열된 선택 항목은 삭제할 ARP 항목 유형을 지정합니다.

- 1 All Dynamic Entries(모든 동적 항목)
- 1 All Dynamic and Gateway Entries(모든 동적 및 게이트웨이 항목)
- 1 Specific Dynamic Gateway Entry(특정 동적 게이트웨이 항목)
- 1 Specific Static Entry(특정 정적 항목)

페이지의 맨 아래에 표시되는 ARP 표에는 다음 필드가 있습니다.

IP Address(IP 주소) — 스위치의 라우팅 인터페이스 중 하나에 연결된 서브네트에 있는 장치의 IP 주소입니다.

MAC Address(MAC 주소) — 장치의 유니캐스트 MAC 주소입니다. 형식은 콜론으로 구분된 6개의 두 자리 16진수입니다(예: 00:06:29:32:81:40).

VLAN ID — ARP 항목과 연관된 라우팅 인터페이스입니다.

Type(유형) — ARP 항목의 유형입니다.

Age(보존 기간) — ARP 표에서 항목이 마지막으로 재생된 이후의 보존 기간입니다. 형식은 hh:mm:ss입니다.

ARP 표 구성

1. ARP Table Configuration(ARP 표 구성) 페이지를 엽니다.
2. 필요에 따라 매개변수를 변경합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

변경사항이 저장되고 ARP 표가 업데이트됩니다.

CLI 명령을 사용하여 ARP 표 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 ARP 명령

IP

IP 메뉴 페이지에는 IP 라우팅 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **IP**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

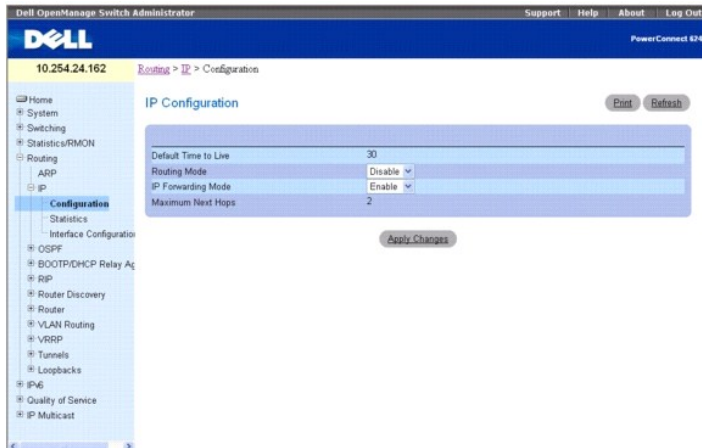
- 1 [IP 구성](#)
- 1 [IP 통계](#)
- 1 [IP 인터페이스 구성](#)

IP 구성

인터페이스와 달리 **Configuration(구성)** 페이지를 사용하여 스위치에 대한 라우팅 매개변수를 구성할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **IP** → **Configuration(구성)**를 클릭합니다.

그림 10-3. IP Configuration(IP 구성)



IP Configuration(IP 구성) 페이지에는 다음과 같은 필드가 있습니다.

Default Time to Live(기본 TTL) — 전송 레이어 프로토콜에서 TTL 값을 제공하지 않은 경우 스위치에서 발생한 데이터그램 IP 헤더의 Time-To-Live(TTL) 필드에 삽입되는 기본값입니다.

Routing Mode(라우팅 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. 인터페이스를 라우팅하려면 스위치에 대해 라우팅을 활성화해야 합니다. 또한 라우팅은 VLAN 인터페이스별로 활성화되거나 비활성화됩니다. 기본값은 Disable(비활성)입니다.

IP Forwarding Mode(IP 전달 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. IP 프레임 전달을 활성화하거나 비활성화합니다. 기본값은 Enable(활성)입니다.

Maximum Next Hops(최대 다음 홉) — 스위치에서 지원하는 최대 홉 수입니다. 이 값은 컴파일시 상수입니다.

IP 라우팅 매개변수 구성

1. IP Configuration(IP 구성) 페이지를 엽니다.
2. 필요에 따라 매개변수를 변경합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

변경사항이 저장되고 라우팅 매개변수가 업데이트됩니다.

CLI 명령을 사용하여 IP 라우팅 매개변수 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 IP 라우팅 명령
- 1 VLAN 명령

IP 통계

IP Statistics(IP 통계) 페이지는 RFC 1213에 지정된 대로 통계를 보고합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **IP** → **Statistics(통계)**를 클릭합니다.

그림 10-4. IP Statistics(IP 통계)

Metric	Value
IpInReceives	520
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	479
IpOutRequests	699
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpMigs	0
IcmpErrors	0

IP Statistics(IP 통계) 페이지에는 다음과 같은 필드가 있습니다.

IpInReceives — 잘못 받은 입력 데이터그램을 포함하여 인터페이스에서 받은 총 입력 데이터그램 수입니다.

IpInHdrErrors — 잘못된 검사 합, 버전 번호 불일치, 기타 형식 오류, TTL 초과, IP 옵션 처리 중에 발견된 오류 등 IP 헤더의 오류로 인해 삭제된 입력 데이터그램 수입니다.

IpInAddrErrors — IP 헤더의 대상 필드에 있는 IP 주소가 이 엔터티에서 수신되는 유효한 주소가 아니어서 삭제된 입력 데이터그램 수입니다. 이 개수에는 잘못된 주소(예: 0.0.0.0) 및 지원되지 않는 클래스 E(예: 클래스 E)의 주소가 포함됩니다. IP 게이트웨이가 아니므로 데이터그램을 전달하지 않는 엔터티의 경우 이 카운터에 대상 주소가 로컬 주소가 아니어서 삭제된 데이터그램이 포함됩니다.

IpForwDatagrams — 이 엔터티가 최종 IP 대상이 아니어서 최종 대상으로 전달할 경로를 찾으려고 시도된 입력 데이터그램 수입니다. IP 게이트웨이 역할을 하지 않는 엔터티의 경우 이 엔터티를 통해 소스 라우팅되었으며 Source-Route(소스 라우팅) 옵션 처리에 성공한 패킷만 이 카운터에 포함됩니다.

IpInUnknownProtos — 성공적으로 수신되었지만 알 수 없거나 지원되지 않는 프로토콜로 인해 삭제된 로컬 주소 지정 데이터그램 수입니다.

IpInDiscards — 처리를 계속할 수 없도록 하는 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 삭제된 입력 IP 데이터그램 수입니다. 재조립을 기다리는 동안 삭제되는 데이터그램은 이 카운터에 포함되지 않습니다.

IpInDelivers — 성공적으로 IP 사용자 프로토콜(ICMP 포함)로 전달된 총 입력 데이터그램 수입니다.

IpOutRequests — 로컬 IP 사용자 프로토콜(ICMP 포함)이 전송 요청에서 IP에 제공한 총 IP 데이터그램 수입니다. ipForwDatagrams에 의해 계산되는 데이터그램은 이 카운터에 포함되지 않습니다.

IpOutDiscards — 대상으로 전송할 수 없도록 하는 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 삭제된 출력 IP 데이터그램 수입니다. 패킷이 해당 삭제 기준에 맞을 경우 ipForwDatagrams에 의해 계산되는 데이터그램이 이 카운터에 포함됩니다.

IpOutNoRoutes — 대상으로 전송할 경로를 찾을 수 없어 삭제된 IP 데이터그램 수입니다. 이 '경로 없음' 기준에 맞을 경우 ipForwDatagrams 및 기본 게이트웨이가 모두 다운되어 호스트가 라우팅할 수 없는 모든 데이터그램에 의해 계산되는 모든 패킷이 이 카운터에 포함됩니다.

IpReasmTimeout — 이 엔터티에서 재조립을 기다리는 동안 수신된 조각이 보관되는 최대 시간(초)입니다.

IpReasmReqds — 이 엔터티에서 재조립해야 하는 수신된 IP 조각 수입니다.

IpReasmOKs — 성공적으로 재조립된 IP 데이터그램 수입니다.

IpReasmFails — IP 재조립 알고리즘에서 감지된, 타임아웃, 오류 등으로 인한 실패 수입니다. 일부 알고리즘에서 조각을 받을 때 결함하여 조각 수를 추적하지 못할 수 있으므로 이 개

수가 반드시 삭제된 IP 조각 수가 되는 것은 아닙니다.

IpFragOKs — 이 엔터티에서 성공적으로 조각화된 IP 데이터그램 수입니다.

IpFragFails — 이 엔터티에서 조각화해야 하지만 Don't Fragment(조각화 안 함) 플래그 설정 등의 이유로 조각화할 수 없어서 삭제된 IP 데이터그램 수입니다.

IpFragCreates — 이 엔터티에서의 조각화로 인해 생성된 IP 데이터그램 조각 수입니다.

IpRoutingDiscards — 유효하지만 삭제하도록 선택된 라우팅 항목 수입니다. 다른 라우팅 항목에 사용할 버퍼 공간 확보 등의 이유로 이러한 항목을 삭제할 수 있습니다.

IcmpInMsgs — 엔터티에서 받은 총 ICMP 메시지 수입니다. icmpInErrors에 의해 계산되는 모든 항목이 이 카운터에 포함됩니다.

IcmpInErrors — 엔터티에서 받았지만 ICMP 관련 오류(잘못된 ICMP 검사 함, 잘못된 길이 등)가 있는 것으로 확인된 ICMP 메시지 수입니다.

IcmpInDestUnreachs — 수신된 ICMP Destination Unreachable(대상에 접근할 수 없음) 메시지 수입니다.

IcmpInTimeExcds — 수신된 ICMP Time Exceeded(시간 초과됨) 메시지 수입니다.

IcmpInParmProbs — 수신된 ICMP Parameter Problem(매개변수 문제) 메시지 수입니다.

IcmpInSrcQuenchs — 수신된 ICMP Source Quench(소스 억제) 메시지 수입니다.

IcmpInRedirects — 수신된 ICMP Redirect(리디렉션) 메시지 수입니다.

IcmpInEchos — 수신된 ICMP Echo Request(Echo 요청) 메시지 수입니다.

IcmpInEchoReps — 수신된 ICMP Echo Reply(Echo 응답) 메시지 수입니다.

IcmpInTimestamps — 수신된 ICMP Timestamp Request(타임 스탬프 요청) 메시지 수입니다.

IcmpInTimestampReps — 수신된 ICMP Timestamp Reply(타임 스탬프 응답) 메시지 수입니다.

IcmpInAddrMasks — 수신된 ICMP Address Mask Request(주소 마스크 요청) 메시지 수입니다.

IcmpInAddrMaskReps — 수신된 ICMP Address Mask Reply(주소 마스크 응답) 메시지 수입니다.

IcmpOutMsgs — 이 엔터티에서 보내려고 한 총 ICMP 메시지 수입니다. icmpOutErrors에 의해 계산되는 모든 항목이 이 카운터에 포함됩니다.

IcmpOutErrors — 버퍼 부족 등 ICMP 내에서 발견된 문제로 인해 이 엔터티에서 보내지 못한 ICMP 메시지 수입니다. IP에서 결과 데이터그램을 라우팅할 수 없는 경우 등 ICMP 레이어 외부에서 발견된 오류는 이 값에 포함되지 않습니다. 구현에 따라 이 카운터 값에 적용되는 오류 유형이 없는 경우도 있습니다.

IcmpOutDestUnreachs — 전송된 ICMP Destination Unreachable(대상에 접근할 수 없음) 메시지 수입니다.

IcmpOutTimeExcds — 전송된 ICMP Time Exceeded(시간 초과됨) 메시지 수입니다.

IcmpOutParmProbs — 전송된 ICMP Parameter Problem(매개변수 문제) 메시지 수입니다.

IcmpOutSrcQuenchs — 전송된 ICMP Source Quench(소스 억제) 메시지 수입니다.

IcmpOutRedirects — 전송된 ICMP Redirect(리디렉션) 메시지 수입니다. 호스트는 리디렉션을 보내지 않으므로 호스트에 대한 이 개체는 항상 0입니다.

IcmpOutEchos — 전송된 ICMP Echo Request(Echo 요청) 메시지 수입니다.

IcmpOutEchoReps — 전송된 ICMP Echo Reply(Echo 응답) 메시지 수입니다.

IcmpOutTimestamps — ICMP Timestamp Request(타임 스탬프 요청) 메시지 수입니다.

IcmpOutTimestampReps — 전송된 ICMP Timestamp Reply(타임 스탬프 응답) 메시지 수입니다.

IcmpOutAddrMasks — 전송된 ICMP Address Mask Request(주소 마스크 요청) 메시지 수입니다.

IcmpOutAddrMaskReps — 전송된 ICMP Address Mask Reply(주소 마스크 응답) 메시지 수입니다.

IP 통계 재생

1. **IP Statistics(IP 통계)** 페이지를 엽니다.
2. **Refresh(재생)**를 클릭합니다.

화면에 스위치에 있는 데이터의 현재 상태가 표시됩니다.

CLI 명령을 사용하여 IP 통계 표시

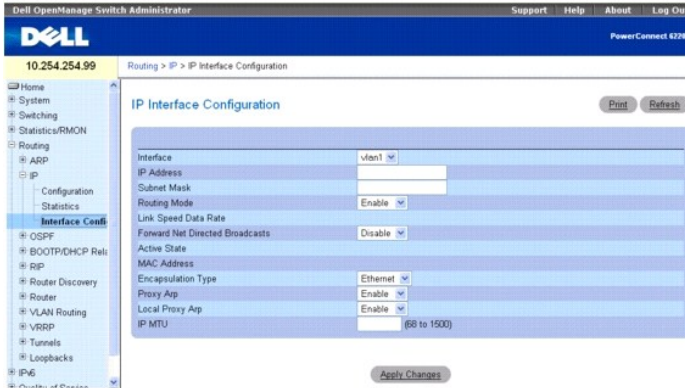
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

IP 인터페이스 구성

IP Interface Configuration(IP 인터페이스 구성) 페이지를 사용하여 이 스위치에 대한 IP 인터페이스 데이터를 업데이트할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → IP → Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 10-5. IP Interface Configuration(IP 인터페이스 구성)



IP Interface Configuration(IP 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 구성할 인터페이스를 선택합니다. 드롭다운 메뉴에는 **Switching(전환) → VLAN → VLAN Membership(VLAN 멤버십) → Add(추가)** 페이지에서 만든 VLAN 및 루프백 인터페이스가 있습니다.

IP Address(IP 주소) — 인터페이스의 IP 주소를 입력합니다.

Subnet Mask(서브네트 마스크) — 인터페이스의 서브네트 마스크를 입력합니다. 서브네트/네트워크 마스크라고도 하며, 연결된 네트워크를 식별하는 데 사용되는 인터페이스의 IP 주소 부분을 정의합니다.

Routing Mode(라우팅 모드) — 이 값을 설정하면 인터페이스에 대한 라우팅이 활성화되거나 비활성화됩니다. 기본값은 Enable(활성)입니다.

Link Speed Data Rate(링크 속도 데이터 전송 속도) — 지정된 인터페이스의 물리적 링크 데이터 전송 속도를 나타내는 정수입니다. 이 데이터는 물리적 인터페이스에만 유효하며 Mbps 단위로 측정됩니다.

Forward Net Directed Broadcasts(네트워크상의 브로드캐스트 전달) — 네트워크상의 브로드캐스트 패킷 처리 방법을 선택합니다. 드롭다운 메뉴에서 Enable(활성)을 선택하면 네트워크상의 브로드캐스트가 전달됩니다. Disable(비활성)을 선택한 경우에는 삭제됩니다. 기본값은 Disable(비활성)입니다.

Active State(활성 상태) — 지정된 인터페이스의 상태가 Active(활성) 또는 Inactive(비활성)입니다. 링크가 작동하고 전달 상태에 있으면 인터페이스가 활성화된 것으로 간주됩니다.

MAC Address(MAC 주소) — 지정된 인터페이스의 내장된 물리적 주소입니다. 형식은 콜론으로 구분된 6개의 두 자리 16진수입니다(예: 00:06:29:32:81:40). 이 값은 물리적 인터페이스에 유효합니다. VLAN 라우팅 인터페이스 등 논리적 인터페이스의 경우 이 필드가 시스템 MAC 주소가 표시됩니다.

Encapsulation Type(캡슐화 유형) — 지정된 인터페이스에서 전송된 패킷에 대한 링크 레이어 캡슐화 유형을 드롭다운 메뉴에서 선택합니다. 가능한 값은 Ethernet(이더넷)과 SNAP입니다. 기본값은 Ethernet(이더넷)입니다.

Proxy ARP(프록시 ARP) — 드롭다운 메뉴에서 Disable(비활성) 또는 Enable(활성)을 선택하여 지정된 인터페이스에 대해 프록시 ARP를 비활성화하거나 활성화합니다.

Local Proxy ARP(로컬 프록시 ARP) — 드롭다운 메뉴에서 Disable(비활성) 또는 Enable(활성)을 선택하여 지정된 인터페이스에 대해 로컬 프록시 ARP를 비활성화하거나 활성화합니다.

IP MTU — 인터페이스에서 전송되는 IP 패킷의 최대 전송 단위(MTU) 크기를 지정합니다. 유효한 범위는 68 ~ 1500입니다. 기본값은 1500입니다.

IP 인터페이스 수정

1. IP Interface Configuration(IP 인터페이스 구성) 페이지를 엽니다.

2. 필요에 따라 값을 변경합니다.

3. Apply Changes(변경사항 적용)를 클릭하십시오.

변경사항이 저장되고 IP 인터페이스가 업데이트됩니다.

IP 인터페이스 구성 CLI 명령

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 [CLI 참조 안내서](#)의 다음 장을 참조하십시오.

- 1 IP 주소 지정 명령
- 1 IP 라우팅 명령
- 1 ARP 명령

OSPF

OSPF(Open Shortest Path First) 라우팅 프로토콜은 내부 게이트웨이 프로토콜(IGP)입니다. 각 OSPF 라우터는 도메인에 있는 모든 라우터 및 네트워크의 최단 경로 트리를 구축합니다. 라우팅 정보는 정기적으로 및 네트워크 토폴로지 변경시 Link State Update(링크 상태 업데이트) 패킷에 포함되어 전파됩니다. 이 정보는 수신 및 흡수되어 개별 라우터의 OSPF 데이터베이스에 저장됩니다. 데이터베이스 교환에서 정보의 핵심 부분은 라우터와 연관된 인터페이스 수와 IP 주소입니다. OSPF는 보조 IP 주소를 라우터에 연결된 스텝 네트워크로 간주합니다. 따라서 OSPF 라우팅 도메인에서 이러한 네트워크가 알려지긴 하지만 보조 주소에는 인접 관계가 설정되지 않습니다. 또한 OSPF에 의해 알려지려면 모든 보조 IP 주소가 주 IP 주소와 같은 영역에 있어야 합니다. 영역 구성이 네트워크 단위가 아닌 인터페이스 단위로 이루어지는 6200 시리즈 구현의 경우에는 항상 유효합니다.

OSPF 메뉴 페이지에는 OSPF 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→ OSPF**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

- 1 [OSPF 구성](#)
- 1 [영역 구성](#)
- 1 [스텝 영역 요약](#)
- 1 [영역 범위 구성](#)
- 1 [인터페이스 통계](#)
- 1 [인터페이스 구성](#)
- 1 [인접 항목 표](#)
- 1 [인접 구성](#)
- 1 [링크 상태 데이터베이스](#)
- 1 [가상 링크 구성](#)
- 1 [가상 링크 요약](#)
- 1 [경로 재배포 구성](#)
- 1 [경로 재배포 요약](#)

OSPF 구성

OSPF Configuration(OSPF 구성) 페이지를 사용하여 라우터에 대해 OSPF를 활성화하고 관련 OSPF 설정을 구성할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→ OSPF→ Configuration(구성)**을 클릭합니다.


그림 10-6. OSPF Configuration(OSPF 구성)



OSPF Configuration(OSPF 구성) 페이지에는 다음 필드가 있습니다.

Router ID(라우터 ID) — 자치 시스템(AS)에서 라우터를 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다. 라우터 ID를 변경하려면 먼저 OSPF를 비활성화해야 합니다. 새 라우터 ID를 설정한 후 OSPF를 다시 활성화하여 변경사항을 적용해야 합니다. 유효한 라우터 ID는 아니지만 기본값은 0.0.0.0입니다.

OSPF Admin Mode(OSPF 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 스위치에 대해 OSPF가 활성화됩니다. 기본값은 Disable(비활성)입니다. OSPF가 작동하려면 라우터 ID를 구성해야 합니다.

 **주:** OSPF가 라우터에서 초기화되면 라우터가 재설정될 때까지 초기화된 상태로 유지됩니다.

ASBR Mode(ASBR 모드) — ASBR 모드가 활성화되었는지 또는 비활성화되었는지 나타냅니다. 활성화된 경우에는 라우터가 자치 시스템의 경계 라우터입니다. 라우터는 다른 프로토콜로부터 알게 된 경로를 재배포하도록 구성된 경우 자동으로 ASBR이 됩니다.

RFC 1583 Compatibility(RFC 1583 호환성) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 동일한 대상을 알리는 여러 개의 AS-External-LSA 중 하나를 선택할 때 사용되는 기본 설정 규칙을 지정합니다. Enable(활성)을 선택하면 RFC 1583에 의해 정의된 항목이 기본 설정 규칙이 됩니다. Disable(비활성)을 선택하면 동일한 대상에 대한 AS-External-LSA가 서로 다른 영역에서 발생한 경우 라우팅 루프를 방지하는 OSPF-2 표준(RFC 2328)의 16.4.1절에서 정의된 항목이 기본 설정 규칙이 됩니다. 기본값은 Enable(활성)입니다. 라우팅 루프를 방지하려면 Disable(비활성)을 선택해야 하지만, 이는 라우팅 도메인의 모든 OSPF 라우터가 RFC 2328에 따라 작동할 수 있는 경우에만 적용됩니다.

ABR Status(ABR 상태) — 값은 Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다. 활성화된 경우에는 라우터가 영역 경계 라우터입니다. 비활성화된 경우에는 라우터가 영역 경계 라우터가 아닙니다.

Exit Overflow Interval (sec)(종료 오버플로 간격(초)) — 오버플로 상태가 된 이후 라우터가 오버플로 상태를 벗어나려고 시도하기까지 기다려야 하는 시간(초)을 입력합니다. 이 값을 사용하면 라우터에서 기본값이 아닌 AS-External-LSA를 다시 발생할 수 있습니다. 0을 입력한 경우 라우터를 다시 시작해야 오버플로 상태에서 벗어납니다. 범위는 0 ~ 2147483647초입니다.

SPF DelayTime (secs)(SPF 지연 시간(초)) — 시간(초)을 입력합니다. 지연 시간(초)은 OSPF가 토폴로지 변경을 수신한 시간과 SPF 계산을 시작한 시간의 차이입니다. 이 값은 0 ~ 65535 사이의 정수일 수 있습니다. 기본 시간은 5초입니다. 값이 0이면 지연이 없습니다. 즉, SPF 계산이 즉시 시작됩니다.

SPF HoldTime(secs)(SPF 보류 시간(초)) — 두 개의 연속 SPF 계산 사이의 최소 시간(초)을 입력합니다. 이 값은 0 ~ 65535 사이의 정수일 수 있습니다. 기본 시간은 10초입니다. 값이 0이면 지연이 없습니다. 즉, 두 개의 SPF 계산이 연속해서 수행될 수 있습니다.

External LSA Count(외부 LSA 수) — 링크 상태 데이터베이스의 외부(LS 유형 5) LSA(Link State Advertisements) 수입니다.

External LSA Checksum(외부 LSA 검사 합계) — 링크 상태 데이터베이스에 포함되어 있는 외부 LSA(Link State Advertisements)의 LS 검사 합계입니다. 이 합계를 사용하면 라우터의 링크 상태 데이터베이스가 변경되었는지 여부를 확인하고 두 라우터의 링크 상태 데이터베이스를 비교할 수 있습니다. 이 값은 16진수입니다.

New LSAs Originated(발생한 새 LSA) — 지정된 OSPF 영역에서 라우터는 여러 개의 LSA를 발생시킵니다. 각 라우터는 라우터-LSA를 발생시킵니다. 라우터가 특정 영역 네트워크에 대해 지정된 라우터인 경우 해당 네트워크에 대한 네트워크-LSA를 발생시킵니다. 이 값은 이 라우터에서 발생하는 LSA 수를 나타냅니다.

LSAs Received(수신된 LSA 수) — 새 인스턴스화를 위해 결정된 LSA(링크 상태 알림) 수입니다. 자체 생성된 LSA의 최신 인스턴스화는 이 수에 포함되지 않습니다.

Default Metric(기본 메트릭) — 재배포된 경로의 메트릭에 대한 기본값을 설정합니다. 설정된 경우 이 필드에 기본 메트릭이 표시되고 이전에 구성되지 않은 경우에는 공백이 표시됩니다. 유효한 값은 1 ~ 16,777,214입니다.

Maximum Paths(최대 경로) — OSPF가 지정된 대상에 보고할 수 있는 최대 경로 수를 구성합니다. 유효한 값은 1 ~ 2입니다.

Default Route Advertise(기본 경로 알림)

Default Information Originate(기본 정보 발생) — Default Route Advertise(기본 경로 알림)를 활성화하거나 비활성화합니다.

Always(항상) — True로 설정된 경우 라우터 알림 0.0.0.0/0.0.0.0을 설정합니다.

Metric(메트릭) — 기본 경로 메트릭을 지정합니다. 유효한 값은 1 ~ 16,777,214입니다.

Metric Type(메트릭 유형) — 기본 경로의 메트릭 유형을 설정합니다. 옵션은 External Type 1(외부 유형 1)과 External Type 2(외부 유형 2)입니다. External Type 2(외부 유형 2)가 기본값입니다.

OSPF 구성 수정

1. **OSPF Configuration(OSPF 구성)** 페이지를 엽니다.
2. 필요에 따라 값을 변경합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

변경사항이 저장되고 OSPF 인터페이스가 업데이트됩니다.

OSPF 구성 CLI 명령

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

영역 구성

Routing(라우팅)→ OSPF→ Interface Configuration(인터페이스 구성)을 통해 인터페이스에 대해 OSPF를 활성화한 경우 OSPF Area Configuration(OSPF 영역 구성) 페이지를 사용하여 스태 영역 구성과 NSSA를 만들 수 있습니다. 이 웹 페이지가 표시되려면 OSPF가 활성화된 라우터가 하나 이상 있어야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 Routing(라우팅)→ OSPF→ Area Configuration(영역 구성)을 클릭합니다.

그림 10-7. OSPF Area Configuration(OSPF 영역 구성)



OSPF Area Configuration(OSPF 영역 구성) 페이지에는 다음 필드가 있습니다.

Area(영역) — 드롭다운 메뉴에서 표시할 영역을 선택합니다. 영역을 선택하면 Stub Area Information(스태 영역 정보)의 필드가 표시됩니다.

Area ID(영역 ID) — OSPF 영역입니다. 영역 ID는 라우터 인터페이스가 연결되는 영역을 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다.

External Routing(외부 라우팅) — AS 외부 LSA가 영역을 플러딩하는지 여부를 포함하여 영역에 대한 라우터의 기능 정의입니다. 스태 영역인 경우에는 이러한 옵션에 대해 외부 라우팅 기능을 구성할 수 있지만, 스태 영역이 아닌 경우에는 Import External LSA(외부 LSA 가져오기) 옵션만 사용할 수 있습니다.

SPF Runs(SPF 실행 횟수) — 이 영역의 링크 상태 데이터베이스를 사용하여 내부 영역 경로를 계산한 횟수입니다. 일반적으로 Dijkstra 알고리즘을 사용하여 수행됩니다.

Area Border Router Count(영역 경계 라우터 수) — 이 영역에서 연결 가능한 총 영역 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

Area LSA Count(영역 LSA 수) — AS 외부 LSA를 제외한 이 영역의 링크 상태 데이터베이스에 있는 총 링크 상태 알람 수입니다.

Area LSA Checksum(영역 LSA 검사 합계) — 이 영역의 링크 상태 데이터베이스에 포함된 링크 상태 알람 LS 검사 합계의 부호 없는 32비트 합계입니다. 외부(LS 유형 5) 링크 상태 알람은 이 합계에서 제외됩니다. 이 합계를 사용하면 라우터의 링크 상태 데이터베이스가 변경되었는지 여부를 확인하고 두 라우터의 링크 상태 데이터베이스를 비교할 수 있습니다. 이 값은 16진수입니다.

Stub Area Information(스태 영역 정보)

Import Summary LSAs(요약 LSA 가져오기) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 요약 LSA를 스태 영역으로 가져옵니다.

Metric Value(메트릭 값) — 스태 영역에 알려진 기본 경로에 대해 적용할 메트릭 값을 입력합니다. 유효한 값 범위는 1 ~ 16,777,215입니다.

Metric Type(메트릭 유형) — Metric Value(메트릭 값) 필드에 지정된 메트릭 유형을 선택합니다.

Translator Role(변환기 역할) — NSSA Translator Role(변환기 역할)을 always/candidate(항상/후보)로 구성합니다.

Translator Stability Interval(변환기 안정성 간격) — 선택된 NSSA에 대한 Translator Stability Interval(변환기 안정성 간격)을 구성합니다.

No-Redistribute Mode(재배포 안 함 모드) — 선택된 NSSA에 대한 경로 재배포를 구성합니다.

Translator State(변환기 상태) — 변환기의 현재 상태를 표시합니다.

OSPF 영역 구성

1. OSPF Area Configuration(OSPF 영역 구성) 페이지를 엽니다.
2. 구성할 영역을 지정합니다.
3. 필요에 따라 나머지 필드의 값을 지정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

OSPF 영역이 정의 및 구성됩니다.

OSPF 영역 구성 표시

1. **OSPF Area Configuration(OSPF 영역 구성)** 페이지를 엽니다.

2. 드롭다운 메뉴에서 표시할 OSPF Area(영역)를 선택합니다.

이 영역에 대한 OSPF 영역 구성이 표시됩니다.

OSPF 영역 구성 삭제

다음 단계를 사용하여 NSSA 구성 또는 스템 영역 구성을 삭제할 수 있습니다.

1. **OSPF Area Configuration(OSPF 영역 구성)** 페이지를 엽니다.

2. 드롭다운 메뉴에서 삭제할 OSPF Area configuration(영역 구성)을 선택합니다.

구성이 표시됩니다.

3. **Delete(삭제)**를 클릭합니다.

OSPF 영역 구성이 제거됩니다.

OSPF 영역 구성 CLI 명령

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

스템 영역 요약

OSPF Stub Area Summary(OSPF 스템 영역 요약) 페이지를 사용하여 OSPF 스템 영역 세부사항을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **OSPF** → **Stub Area Summary(스템 영역 요약)**를 클릭합니다.

그림 10-8. OSPF Area Summary(OSPF 영역 요약)

Area ID	Type of Service	Metric Value	Metric Type	Import Summary LSAs
0.0.0.1	Normal	1	OSPF Metric	Enable

OSPF Stub Area Summary(OSPF 스템 영역 요약) 페이지에는 다음 필드가 있습니다.

Area ID(영역 ID) — 스템 영역의 영역 ID입니다.

Type of Service(서비스 종류) — 스템 메트릭과 연관된 서비스 종류입니다. 스위치는 Normal(일반)만 지원합니다.

Metric Value(메트릭 값) — 구성된 메트릭 값을 표시합니다.

Metric Type(메트릭 유형) — 스템 영역에 대한 메트릭 유형으로, 유효한 유형은 다음과 같습니다.

- 1 OSPF Metric(OSPF 메트릭) — 일반 OSPF 메트릭
- 1 Comparable Cost(유사한 비용) — OSPF 메트릭과 유사한 External Type 1(외부 유형 1) 메트릭
- 1 Non-comparable Cost(유사하지 않은 비용) — OSPF 메트릭의 비용보다 크다고 가정되는 External Type 2(외부 유형 2) 메트릭

Import Summary LSAs(요약 LSA 가져오기) — 요약 LSA 가져오기가 활성화되었는지 또는 비활성화되었는지 나타냅니다.

OSPF 스텝 영역 표시 CLI 명령

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 OSPF 명령

영역 범위 구성

OSPF Area Range Configuration(OSPF 영역 범위 구성) 페이지를 사용하여 지정된 NSSA에 대한 영역 범위를 구성하고 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **OSPF** → **Area Range Configuration(영역 범위 구성)**을 클릭합니다.

그림 10-9. OSPF Area Range Configuration(OSPF 영역 범위 구성)



OSPF Area Range Configuration(OSPF 영역 범위 구성) 페이지에는 다음 필드가 있습니다.

Area ID(영역 ID) — 드롭다운 메뉴에서 데이터를 구성할 영역을 선택합니다.

IP Address(IP 주소) — 선택된 영역에 대한 주소 범위의 IP 주소를 입력합니다.

Subnet Mask(서브네트 마스크) — 선택된 영역에 대한 주소 범위의 서브네트 마스크를 입력합니다.

LSDB Type(LSDB 유형) — 지정된 영역 및 주소 범위와 연관된 링크 알림 유형을 선택합니다. 기본 유형은 'Network Summary(네트워크 요약)'입니다.

Advertisement(알림) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 네트워크 요약 LSA를 통해 주소 범위가 영역 외부에 알려집니다. 기본값은 Enable(활성)입니다.

Add(추가) — 영역 범위를 추가하려면 Add(추가) 확인란을 선택합니다.

OSPF Area Range Table(OSPF 영역 범위 표)

Area ID(영역 ID) — OSPF 영역을 표시합니다.

IP Address(IP 주소) — 영역에 대한 주소 범위의 IP 주소를 표시합니다.

Subnet Mask(서브네트 마스크) — 영역에 대한 주소 범위의 서브네트 마스크를 표시합니다.

LSDB Type(LSDB 유형) — 주소 범위 및 영역에 대한 링크 알림 유형을 표시합니다.

Advertisement(알림) — 주소 범위 및 영역에 대한 알림 모드를 표시합니다.

Remove(제거) — 지정된 영역 항목을 제거합니다.

OSPF 영역 범위 정의

1. OSPF Area Range Configuration(OSPF 영역 범위 구성) 페이지를 엽니다.
2. Area ID(영역 ID), IP Address(IP 주소), Subnet Mask(서브넷 마스크), LSDB Type(LSDB 유형) 및 Advertisement(알림)을 입력합니다.
3. Add(추가) 확인란을 클릭합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

OSPF 영역 범위가 정의 및 구성됩니다. 구성된 모든 OSPF 영역 범위는 OSPF Area Range Configuration(OSPF 영역 범위 구성) 페이지의 표에 표시됩니다.

OSPF 영역 범위 구성 제거

1. OSPF Area Range Configuration(OSPF 영역 범위 구성) 페이지를 엽니다.
2. Area ID to be deleted(삭제할 영역 ID) 행의 Remove(제거) 확인란을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

주소 범위가 영역 구성에서 제거됩니다.

OSPF 영역 범위 구성 CLI 명령

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. OSPF 명령

인터페이스 통계

OSPF Interface Statistics(OSPF 인터페이스 통계) 페이지를 사용하여 선택된 인터페이스에 대한 통계를 표시할 수 있습니다. OSPF가 활성화된 경우에만 정보가 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 Routing(라우팅) → OSPF → Interface Statistics(인터페이스 통계)를 클릭합니다.

그림 10-10. OSPF Interface Statistics(OSPF 인터페이스 통계)

Interface	OSPF Area ID	Area Border Router Count	AS Border Router Count	Area LSA Count	IP Address	Interface Events	Virtual Events	Neighbor Events	External LSA Count
0/4/1	0.0.0	1	0	6	13.1.1.1	2	0	6	0

OSPF Interface Statistics(OSPF 인터페이스 통계) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 표시할 인터페이스를 선택합니다.

OSPF Area ID(OSPF 영역 ID) — 선택된 라우터 인터페이스가 속하는 OSPF 영역입니다. OSPF 영역 ID는 인터페이스가 연결되는 영역을 고유하게 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다.

Area Border Router Count(영역 경계 라우터 수) — 이 영역에서 연결 가능한 총 영역 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

AS Border Router Count(AS 경계 라우터 수) — 이 영역에서 연결 가능한 총 자치 시스템 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

Area LSA Count(영역 LSA 수) — AS 외부 LSA를 제외한 이 영역의 링크 상태 데이터베이스에 있는 총 링크 상태 알림 수입니다.

IP Address(IP 주소) — 인터페이스의 IP 주소입니다.

Interface Events(인터페이스 이벤트 수) — 지정된 OSPF 인터페이스의 상태가 변경되었거나 오류가 발생한 횟수입니다.

Virtual Events(가상 이벤트 수) — 이 가상 링크에서 발생한 상태 변경 또는 오류 수입니다.

Neighbor Events(인접 이벤트 수) — 이 인접 관계의 상태가 변경되었거나 오류가 발생한 횟수입니다.

External LSA Count(외부 LSA 수) — 링크 상태 데이터베이스의 외부(LS 유형 5) 링크 상태 알림 수입니다.

OSPF 인터페이스 통계 표시

1. OSPF Interface Statistics(OSPF 인터페이스 통계) 페이지를 엽니다.

2. 드롭다운 메뉴에서 데이터를 표시할 인터페이스를 선택합니다.

이 인터페이스에 대한 통계가 표시됩니다.

CLI 명령을 사용하여 OSPF 인터페이스 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

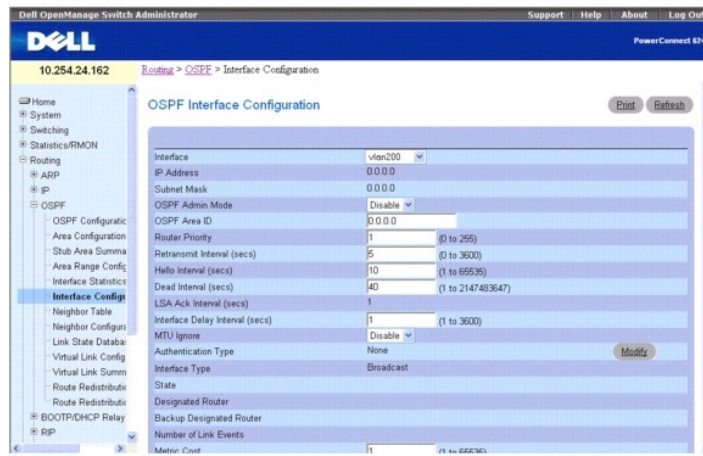
1. OSPF 명령

인터페이스 구성

OSPF Interface Configuration(OSPF 인터페이스 구성) 페이지를 사용하여 OSPF 인터페이스를 구성할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **OSPF** → **Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 10-11. OSPF Interface Configuration(OSPF 인터페이스 구성)



OSPF Interface Configuration(OSPF 인터페이스 구성) 페이지에는 다음 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 표시 또는 구성할 인터페이스를 선택합니다.

IP Address(IP 주소) — VLAN 인터페이스의 주소를 표시합니다.

Subnet Mask(서브넷 마스크) — VLAN 인터페이스의 서브넷 마스크를 표시합니다.

OSPF Admin Mode(OSPF 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택할 수 있습니다. 기본값은 Disable(비활성)입니다. OSPF Admin Mode(OSPF 관리 모드)를 활성화하지 않고 OSPF 매개변수를 구성할 수 있지만, 이러한 매개변수는 Admin Mode(관리 모드)를 활성화해야만 적용됩니다. 다음 정보는 관리 모드가 활성화된 경우에만 표시됩니다. 상태, 지정된 라우터, 지정된 백업 라우터, 링크 이벤트 수, LSA 승인 간격 및 메트릭 비용. OSPF가 완전히 작동하려면 Interface IP Configuration(인터페이스 IP 구성) 페이지를 통해 유효한 IP 주소와 서브넷 마스크를 입력해야 합니다.

 **주:** OSPF가 라우터에서 초기화되면 라우터가 재설정될 때까지 초기화된 상태로 유지됩니다.

OSPF Area ID(OSPF 영역 ID) — 선택된 라우터 인터페이스가 연결되는 OSPF 영역을 고유하게 식별하는, 정으로 된 10진수 형식의 32비트 정수를 입력합니다. 존재하지 않는 영역 ID를 할당하면 해당 영역이 기본값으로 생성됩니다.

Router Priority(라우터 우선 순위) — 선택된 인터페이스에 대한 OSPF 우선 순위를 입력합니다. 인터페이스의 우선 순위는 0부터 255 사이의 정수로 지정됩니다. 기본값은 1이며 가장 높은 라우터 우선 순위를 나타냅니다. 값이 0인 경우 이 네트워크에서 해당 라우터를 지정된 라우터로 사용할 수 없습니다.

Retransmit Interval (secs)(재전송 간격(초)) — 지정된 인터페이스에 대한 OSPF 재전송 간격을 입력합니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)입니다. 이 값은 데이터베이스 설정 및 링크 상태 요청 패킷을 재전송할 때도 사용됩니다. 유효한 값의 범위는 0 ~ 3600초(1시간)입니다. 기본값은 5초입니다.

Hello Interval (secs)(Hello 간격(초)) — 지정된 인터페이스에 대한 OSPF Hello 간격(초)을 입력합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 유효한 값의 범위는 1 ~ 65,535이고 기본값은 10초입니다.

Dead Interval (secs)(작동 중단 간격(초)) — 지정된 인터페이스에 대한 OSPF 작동 중단 간격(초)을 입력합니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 이 값은 Hello 간격의 배수(예: 4)여야 합니다. 유효한 값의 범위는 1 ~ 2,147,483,647이고 기본값은 40입니다.

LSA Ack Interval(LSA 승인 간격) — LSA 승인 패킷 전송 간격(초)으로, Retransmit Interval(재전송 간격)보다 작아야 합니다.

Interface Delay Interval (secs)(인터페이스 지연 간격(초)) — 지정된 인터페이스에 대한 OSPF 운송 지연을 입력합니다. 선택된 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 지정합니다. 유효한 값의 범위는 1 ~ 3600초(1시간)입니다. 기본값은 1초입니다.

MTU Ignore(MTU 무시) — 패킷을 받을 때 OSPF MTU 불일치 감지를 비활성화합니다. 기본값은 Disable(비활성)입니다.

Authentication Type(인증 유형) — Modify(수정) 단추를 클릭하여 None(없음) 이외의 인증 유형을 선택할 수 있습니다. 그러면 드롭다운 메뉴에서 인증 유형을 선택할 수 있는 새 웹 페이지가 표시됩니다. 가능한 값은 다음과 같습니다.

- 1 **None(없음)** — 초기 인터페이스 상태입니다. 두 번째 화면의 드롭다운 메뉴에서 이 옵션을 선택하고 **Apply Changes(변경사항 적용)**를 클릭하면 첫 번째 화면으로 돌아가고 인증 프로토콜이 실행되지 않습니다.
- 1 **Simple(단순)** — Simple(단순)을 선택하면 인증 키를 입력하라는 메시지가 표시됩니다. 이 키는 네트워크에서 전송되는 모든 패킷의 OSPF 헤더에 일반 텍스트 형식으로 포함됩니다. 네트워크상의 모든 라우터는 동일한 키로 구성되어야 합니다.
- 1 **Encrypt(암호화)** — Encrypt(암호화)를 선택하면 인증 키와 인증 ID를 모두 입력하라는 메시지가 표시됩니다. 암호화에서는 MD5 Message-Digest 알고리즘을 사용합니다. 네트워크상의 모든 라우터는 동일한 키 및 ID로 구성되어야 합니다.

Interface Type(인터페이스 유형) — 항상 브로드캐스팅되는 OSPF 인터페이스 유형입니다.

State(상태) — 선택된 라우터 인터페이스의 현재 상태입니다. 가능한 값은 다음과 같습니다.

- 1 **Down(다운)** — 초기 인터페이스 상태입니다. 이 상태인 경우에는 하위 레벨 프로토콜에서 인터페이스를 사용할 수 없습니다. 또한 인터페이스 매개변수가 해당 초기 값으로 설정됩니다. 모든 인터페이스 타이머가 비활성화되고 인터페이스와 관련된 인접 항목이 없습니다.
- 1 **Loopback(루프백)** — 이 상태에서는 라우터의 네트워크 인터페이스가 하드웨어 또는 소프트웨어에서 순환됩니다. 따라서 인터페이스를 일반 데이터 트래픽에 사용할 수 없습니다. 그렇더라도, 인터페이스에 ICMP 핑을 보내거나 비트 오류 테스트 등을 수행하여 이 인터페이스의 상태와 관련한 정보를 수집하는 것이 좋습니다. 따라서 IP 패킷의 주소가 루프백 상태의 인터페이스로 지정될 수도 있습니다. 이 과정이 용이하게 진행되도록 라우터 LSA에서 이러한 인터페이스를 대상이 IP 인터페이스 주소인 단일 호스트 경로로 알립니다.
- 1 **Waiting(대기)** — 라우터가 수신된 Hello 패킷을 모니터링하여 네트워크에 대한 지정된 (백업) 라우터 ID를 확인하려고 합니다. 라우터를 지정된 백업 라우터 또는 지정된 라우터로 선택하려면 라우터가 대기 상태에서 벗어나야 합니다. 그러면 지정된 (백업) 라우터가 불필요하게 변경되지 않습니다.
- 1 **Designated Router(지정된 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 라우터가 됩니다. 인접 항목은 네트워크에 연결된 모든 다른 라우터로 설정됩니다. 또한 라우터가 네트워크 노드에 대한 네트워크 LSA를 발생해야 합니다. 네트워크 LSA에는 네트워크에 연결되는 모든 라우터(지정된 라우터 포함)에 대한 링크가 포함되어 있습니다.
- 1 **Backup Designated Router(지정된 백업 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 백업 라우터가 됩니다. 현재의 지정된 라우터가 실패하면 이 라우터가 지정된 라우터로 승격됩니다. 라우터는 인접 항목을 네트워크에 연결된 모든 다른 라우터로 설정합니다. 지정된 백업 라우터는 플러딩 절차 중에는 지정된 라우터와 약간 다른 기능을 수행합니다.
- 1 **Other Designated Router(기타 지정된 라우터)** — 다른 라우터를 지정된 라우터 및 지정된 백업 라우터로 선택한 브로드캐스트 또는 NBMA 네트워크에 인터페이스가 연결됩니다. 라우터가 지정된 라우터와 지정된 백업 라우터 모두에 대한 인접 항목을 생성하려고 시도합니다.

State(상태)는 OSPF 관리 모드가 활성화된 경우에만 표시됩니다.

Designated Router(지정된 라우터) — 알림을 보내는 라우터의 관점에서 이 네트워크에 대한 지정된 라우터의 ID입니다. 여기서 지정된 라우터는 해당 라우터 ID를 기준으로 식별됩니다. 값이 0.0.0.0이면 지정된 라우터가 없는 것입니다. 이 필드는 OSPF 관리 모드가 활성화된 경우에만 표시됩니다.

Backup Designated Router(지정된 백업 라우터) — 알림을 보내는 라우터의 관점에서 이 네트워크에 대한 지정된 백업 라우터의 ID입니다. 여기서 지정된 백업 라우터는 해당 라우터 ID를 기준으로 식별됩니다. 지정된 백업 라우터가 없으면 0.0.0.0으로 설정합니다. 이 필드는 OSPF 관리 모드가 활성화된 경우에만 표시됩니다.

Number of Link Events(링크 이벤트 수) — 지정된 OSPF 인터페이스가 해당 상태를 변경한 횟수입니다. 이 필드는 OSPF 관리 모드가 활성화된 경우에만 표시됩니다.

Metric Cost(메트릭 비용) — 이 인터페이스에 대한 TOS(서비스 종류) 비용 값을 입력합니다. 메트릭 비용 범위는 1 ~ 65,535입니다. Metric Cost(메트릭 비용)은 인터페이스에 대해 OSPF가 초기화된 경우에만 구성할 수 있고 표시됩니다.

OSPF 인터페이스 구성 설정

1. **OSPF Interface Configuration(OSPF 인터페이스 구성)** 페이지를 엽니다.
2. 구성할 인터페이스를 지정합니다.
3. 필요에 따라 나머지 필드의 값을 지정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

OSPF 인터페이스가 구성됩니다.

OSPF 인터페이스 구성 표시

1. **OSPF Interface Configuration(OSPF 인터페이스 구성)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 데이터를 표시할 VLAN 인터페이스를 선택합니다.

이 인터페이스에 대한 구성 데이터가 표시됩니다.

CLI 명령을 사용하여 OSPF 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

인접 항목 표

OSPF Neighbor Table(OSPF 인접 항목 표) 페이지를 사용하여 OSPF 인접 항목 표 목록을 표시할 수 있습니다. 특정 인접 ID를 지정하면 해당 인접 항목에 대한 자세한 정보가 제공됩니다. OSPF가 활성화된 경우에만 아래 정보가 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → OSPF → Neighbor Table(인접 항목 표)**을 클릭합니다.

그림 10-12. OSPF Neighbor Table(OSPF 인접 항목 표)



OSPF Neighbor Table(OSPF 인접 항목 표) 페이지에는 다음 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 표시할 인터페이스를 선택합니다.

Router ID(라우터 ID) — 인접 인터페이스를 나타내는, 점으로 된 10진수 형식의 32비트 정수입니다.

IP Address(IP 주소) — 연결된 네트워크에 대한 인접 라우터 인터페이스의 IP 주소입니다. 이 주소는 인접 관계를 따라 프로토콜 패킷이 유니캐스트로 전송될 때 대상 IP 주소로 사용됩니다. 또한 인접 라우터가 지정된 라우터로 선택된 경우 라우터-LSA에서 연결된 네트워크에 대한 링크 ID로 사용됩니다. 인접 항목 IP 주소는 인접 항목에서 Hello 패킷을 받을 때 확인됩니다. 가상 링크의 경우에는 라우팅 표 구축 프로세스 중에 인접 항목 IP 주소가 확인됩니다.

Neighbor Interface Index(인접 인터페이스 색인) — 인접 인터페이스 색인을 식별하는 인터페이스입니다.

CLI 명령을 사용하여 OSPF 인접 항목 표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

인접 구성

OSPF Neighbor Configuration(OSPF 인접 항목 구성) 페이지를 사용하여 선택된 인접 항목 ID에 대한 OSPF 인접 항목 구성을 표시할 수 있습니다. 특정 인접 항목 ID를 지정하면 인접 항목에 대한 자세한 정보가 제공됩니다. OSPF가 활성화되어 있고 인터페이스에 인접 항목이 있는 경우에만 아래 정보가 표시됩니다. IP 주소는 인접 항목의 IP 주소입니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → OSPF → Neighbor Configuration(인접 항목 구성)**을 클릭합니다.

그림 10-13. OSPF Neighbor Configuration(OSPF 인접 항목 구성)



OSPF Neighbor Configuration(OSPF 인접 항목 구성) 페이지에는 다음 필드가 있습니다.

Interface — 드롭다운 메뉴에서 라우팅이 활성화된 VLAN 인터페이스를 선택합니다.

Neighbor IP Address(인접 항목 IP 주소) — 데이터를 표시할 인접 항목의 IP 주소를 선택합니다.

Router ID(라우터 ID) — 인접 라우터를 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다.

Options(옵션) — 인접 항목이 지원하는 선택적 OSPF 기능입니다. OSPF Options(옵션) 필드는 OSPF Hello 패킷, Database Description(데이터베이스 설명) 패킷 및 모든 링크 상태 알림에 있습니다. Options(옵션) 필드를 사용하면 OSPF 라우터가 선택적 기능을 지원하거나 지원하지 않을 수 있으며, 가능 수준을 다른 OSPF 라우터에 알릴 수 있습니다. 이 예제니즘을 통해 서로 기능이 다른 라우터를 OSPF 라우팅 도메인 내에 혼합해서 사용할 수 있습니다. Options(옵션) 값은 비트맵이며, 인접 항목의 기능을 나타냅니다.

Router Priority(라우터 우선 순위) — 지정된 인접 항목에 대한 OSPF 우선 순위를 표시합니다. 인접 항목의 우선 순위는 0부터 255 사이의 정수 값으로 지정됩니다. 값이 0이면 라우터를 이 네트워크의 지정된 라우터로 지정할 수 없습니다.

State(상태) — 인접 항목의 상태는 다음 중 하나입니다.

- 1 **Down(다운)** — 인접 통신의 초기 상태입니다. 인접 항목으로부터 최근에 수신된 정보가 없음을 나타냅니다. 빈도는 높지 않지만 NBMA 네트워크에서 Hello 패킷이 다운 상태인 인접 항목으로 전송되는 경우도 있습니다.
- 1 **Attempt(시도)** — 이 상태는 NBMA 네트워크에 연결된 인접 항목에만 유효합니다. 인접 항목으로부터 최근에 수신된 정보는 없지만 인접 항목에 연결하기 위해 보다 효율적인 노력이 필요함을 나타냅니다. 이를 위해 인접 항목에 Hello 간격으로 Hello 패킷을 보냅니다.
- 1 **Init(초기화)** — 이 상태는 인접 항목으로부터 Hello 패킷이 최근에 표시된 적이 있음을 나타냅니다. 아직은 인접 항목과의 양방향 통신이 설정되지 않습니다. 즉, 라우터가 인접 항목의 Hello 패킷에 표시되지 않습니다. 이 상태 이상에 해당하는 모든 인접 항목은 연관된 인터페이스에서 보낸 Hello 패킷에 나열됩니다.
- 1 **2-Way(양방향)** — 이 상태에서는 두 라우터 간에 양방향으로 통신합니다. 양방향 통신은 Hello 프로토콜 작업을 통해 보장됩니다. 이 상태는 시작 인접 관계 설정이 없는 가장 높은 상태입니다. 지정된 (백업) 라우터는 상태가 양방향 이상에 해당하는 인접 항목 집합 중에서 선택됩니다.
- 1 **Exchange Start(교환 시작)** — 인접하는 두 라우터 간의 인접 관계를 생성하는 첫 번째 단계입니다. 이 단계의 목적은 마스터로 사용할 라우터를 결정하고 초기 DD 순번을 결정하는 데 있습니다. 이 상태 이상에서 수행되는 인접 통신을 인접 관계라고 합니다.
- 1 **Exchange(교환)** — 이 상태의 라우터는 인접 항목에 Database Description(데이터베이스 설명) 패킷을 보내 전체 링크 상태를 설명합니다. 이 상태에서는 인접 항목의 최신 LSA를 요청하는 링크 상태 요청 패킷이 전송될 수도 있습니다. 교환 상태 이상에 해당하는 모든 인접 관계는 플래딩 절차에 사용됩니다. 이러한 인접 관계에서는 모든 유형의 OSPF 라우팅 프로토콜 패킷을 완벽하게 전송하고 수신할 수 있습니다.
- 1 **Loading(로드 중)** — 이 상태에서는 교환 상태에서 검색되었지만 아직 수신되지 않은 최신 LSA를 요청하는 링크 상태 요청 패킷이 인접 항목에 전송됩니다.
- 1 **Full(전체)** — 이 상태에서는 인접하는 라우터가 서로 완벽하게 접합니다. 이러한 인접 관계는 라우터-LSA 및 네트워크-LSA에 나타납니다.

Events(이벤트 수) — 이 인접 관계의 상태가 변경되었거나 오류가 발생한 횟수입니다.

Permanence(영구) — 이 변수는 항목의 상태를 표시합니다. Dynamic(동적) 및 permanent(영구적)은 인접 항목이 알려진 방법을 나타냅니다.

Hello Suppressed(Hello 표시 안 함) — 이 상태는 인접 항목에 Hello가 표시되는지 여부를 나타냅니다.

Retransmission Queue Length(재전송 대기열 길이) — 재전송 대기열의 현재 길이입니다.

OSPF 인접 항목 구성 표시

1. OSPF Neighbor Configuration(OSPF 인접 항목 구성) 페이지를 엽니다.

2. 표시할 인터페이스 및 IP 주소를 선택합니다.

인접 항목 구성이 표시됩니다.

CLI 명령을 사용하여 OSPF 인접 항목 구성 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

링크 상태 데이터베이스

OSPF Link State Database(OSPF 링크 상태 데이터베이스) 페이지를 사용하여 OSPF 링크 상태 정보를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **OSPF** → **Link State Database(링크 상태 데이터베이스)**를 클릭합니다.

그림 10-14. OSPF Link State Database(OSPF 링크 상태 데이터베이스)

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
1.1.1.1	0.0.0.0	Router Links	1.1.1.1	336	-2147483641	0x8958	E --
2.2.2.2	0.0.0.0	Router Links	2.2.2.2	340	-2147483640	0xac41	E --
2.2.2.2	0.0.0.0	Network Links	13.1.1.2	460	-2147483647	0xa64e	E --
1.1.1.1	0.0.0.0	Network Summary	17.1.1.0	355	-2147483646	0xba80	E --
2.2.2.2	0.0.0.0	Network Summary	17.1.1.0	351	-2147483646	0x426a	E --
2.2.2.2	0.0.0.0	Summary ASBR	1.1.1.1	351	-2147483647	0x652	E --
1.1.1.1	0.0.0.1	Router Links	1.1.1.1	340	-2147483644	0xb25c	E --
2.2.2.2	0.0.0.1	Router Links	2.2.2.2	341	-2147483643	0xc946	E --
2.2.2.2	0.0.0.1	Network Links	17.1.1.2	366	-2147483647	0xb27e	E --
1.1.1.1	0.0.0.1	Network Summary	13.1.1.0	365	-2147483646	0xae60	E --
2.2.2.2	0.0.0.1	Network Summary	13.1.1.0	445	-2147483645	0x74ce	E --

OSPF Link State Database(OSPF 링크 상태 데이터베이스) 페이지에는 다음 필드가 있습니다.

Router ID(라우터 ID) — 자치 시스템(AS)에서 라우터를 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다. 라우터 ID는 IP Configuration(IP 구성) 페이지에서 설정됩니다. 라우터 ID를 변경하려면 먼저 OSPF를 비활성화해야 합니다. 새 라우터 ID를 설정한 후 OSPF를 다시 활성화하여 변경사항을 적용해야 합니다. 유효한 라우터 ID는 아니지만 기본 값은 0.0.0.0입니다.

Area ID(영역 ID) — 라우터 인터페이스 중 하나가 연결되는 OSPF 영역의 ID입니다. 영역 ID는 인터페이스가 연결되는 영역을 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다.

LSA Type(LSA 유형) — 링크 상태 알람의 형식과 기능입니다. 가능한 값은 다음과 같습니다.

1. Router Links(라우터 링크)
1. Network Links(네트워크 링크)
1. Network Summary(네트워크 요약)
1. ASBR Summary(ASBR 요약)
1. AS-external(AS 외부)

LS ID — Link State ID(링크 상태 ID)는 알람에서 설명하는 라우팅 도메인 부분을 식별합니다. LS ID 값은 알람의 LS 유형에 따라 다릅니다.

Age(보존 기간) — 링크 상태 알람이 처음 발생된 이후에 경과한 시간(초)입니다.

Sequence(순서) — 순서 번호 필드는 부호 있는 32비트 정수입니다. 오래되었거나 중복된 링크 상태 알람을 검색하는 데 사용됩니다. 순서 번호가 클수록 최신 알람입니다.

Checksum(검사 합계) — 검사 합은 알람의 데이터 손실을 검색하는 데 사용됩니다. 데이터 손실은 알람이 플러딩되는 동안이나 라우터의 메모리에 유지된 상태에서 발생할 수 있습니다. 이 필드는 LS 보존 기간 필드를 제외한 전체 알람 내용의 검사 합입니다.

Options(옵션) — 링크 상태 알람 헤더의 Options(옵션) 필드는 알람과 관련된 선택적 기능을 나타냅니다. 가능한 값은 다음과 같습니다.

1. **Q** — OoS 트래픽 엔지니어링 지원을 활성화합니다.
1. **E** — AS 외부 LSA가 플러딩되는 방식을 설명합니다.
1. **MC** — IP 멀티캐스트 데이터그램이 표준 사양에 따라 전달되는 방식을 설명합니다.

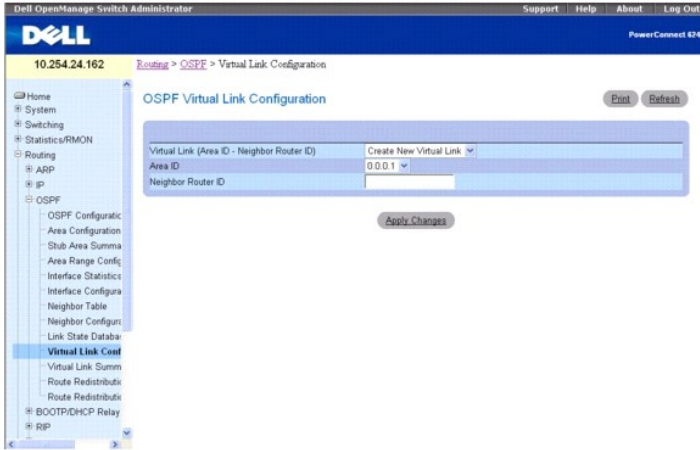
- 1 — 불투명 LSA가 지원되는지 여부를 설명합니다.
- 1 — VPN/COS에 대한 OSPF++ 확장이 지원되는지 여부를 설명합니다.

가상 링크 구성

OSPF Virtual Link Configuration (OSPF 가상 링크 구성) 페이지를 사용하여 특정 영역과 인접 항목에 대한 가상 인터페이스 정보를 만들거나 구성할 수 있습니다. 이 페이지를 표시하려면 유효한 OSPF 영역을 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → OSPF → Virtual Link Configuration(가상 링크 구성)**을 클릭합니다.

그림 10-15. OSPF Virtual Link Configuration - Create (OSPF 가상 링크 구성 - 만들기)



OSPF Virtual Link Configuration (OSPF 가상 링크 구성) 페이지에는 다음 필드가 있습니다.

Virtual Link (Area ID - Neighbor Router ID) (가상 링크(영역 ID - 인접 라우터 ID)) — 데이터를 표시 또는 구성할 가상 링크를 선택합니다. Area ID(영역 ID) 및 Neighbor Router ID(인접 라우터 ID)로 구성되어 있습니다. 새 가상 링크를 만들려면 드롭다운 메뉴에서 **Create New Virtual Link(새 가상 링크 만들기)**를 선택하여 새 가상 링크를 정의합니다. **Create New Virtual Link(새 가상 링크 만들기)**가 선택되어 있으면 다음 필드가 나타납니다.

Area ID(영역 ID) — 라우터 인터페이스가 연결되는 영역을 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다.

Neighbor Router ID(인접 라우터 ID) — 가상 링크의 일부인 인접 라우터를 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다.

Hello Interval (secs) (Hello 간격(초)) — 지정된 인터페이스에 대한 OSPF Hello 간격(초)을 입력합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 유효한 값의 범위는 1 ~ 65535이고 기본값은 10초입니다.

Dead Interval (secs) (작동 중단 간격(초)) — 지정된 인터페이스에 대한 OSPF 작동 중단 간격(초)을 입력합니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 이 값은 Hello 간격의 배수(예: 4)여야 합니다. 유효한 값의 범위는 1 ~ 65535이고 기본값은 40초입니다.

Interface Delay Interval (secs) (인터페이스 지연 간격(초)) — 가상 링크에 대한 OSPF 운송 지연(초)을 입력합니다. 이 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 지정합니다.

State(상태) — 선택된 가상 링크의 현재 상태입니다. 상태는 다음 중 하나입니다.

- 1 **Down(다운)** — 초기 인터페이스 상태입니다. 이 상태인 경우에는 하위 레벨 프로토콜에서 인터페이스를 사용할 수 없습니다. 또한 인터페이스 매개변수가 해당 초기 값으로 설정됩니다. 모든 인터페이스 타이머가 비활성화되고 인터페이스와 연관된 인접 항목이 없습니다.
- 1 **Waiting(대기)** — 라우터가 수신된 Hello 패킷을 모니터링하여 지정된 (백업) 라우터 ID를 확인하려고 합니다. 라우터를 지정된 백업 라우터 또는 지정된 라우터로 선택하려면 라우터가 대기 상태에서 벗어나야 합니다. 그러면 지정된 (백업) 라우터가 불필요하게 변경되지 않습니다.
- 1 **Point-to-Point(지점 대 지점)** — 인터페이스가 작동 상태이고 가상 링크에 연결되어 있습니다. 이 상태에서 라우터는 인접하는 라우터에 인접 관계를 생성하려고 시도합니다. Hello 패킷이 Hello 간격(초)으로 인접 항목에 전송됩니다.
- 1 **Designated Router(지정된 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 라우터가 됩니다. 인접 항목은 네트워크에 연결된 모든 다른 라우터로 설정됩니다. 또한 라우터가 네트워크 노드에 대한 네트워크 LSA를 발생해야 합니다. 네트워크 LSA에는 네트워크에 연결되는 모든 라우터(지정된 라우터 포함)에 대한 링크가 포함되어 있습니다.
- 1 **Backup Designated Router(지정된 백업 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 백업 라우터가 됩니다. 현재의 지정된 라우터가 실패하면 이 라우터가 지정된 라우터로 승격됩니다. 라우터는 인접 항목을 네트워크에 연결된 모든 다른 라우터로 설정합니다. 지정된 백업 라우터는 플러딩 절차 중에는 지정된 라우터와 약간 다른 기능을 수행합니다.
- 1 **Other Designated Router(기타 지정된 라우터)** — 다른 라우터를 지정된 라우터 및 지정된 백업 라우터로 선택한 브로드캐스트 또는 NBMA 네트워크에 인터페이스가 연결됩니다. 라우터가 지정된 라우터와 지정된 백업 라우터 모두에 대한 인접 항목을 생성하려고 시도합니다.

Neighbor State(인접 상태) — 가상 인접 관계의 상태입니다.

Retransmit Interval(재전송 간격) — 지정된 인터페이스에 대한 OSPF 재전송 간격을 입력합니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)입니다.

이 값은 데이터베이스 설정 및 링크 상태 요청 패킷을 재전송할 때도 사용됩니다. 유효한 값의 범위는 0 ~ 3600초(1시간)입니다. 기본값은 5초입니다.

Authentication Type(인증 유형) — Configure Authentication(인증 구성) 단추를 클릭하여 None(없음) 이외의 인증 유형을 선택할 수 있습니다. 그러면 드롭다운 메뉴에서 인증 유형을 선택할 수 있는 새 화면이 표시됩니다. 선택 항목은 다음과 같습니다:

1. **None(없음)** — 초기 인터페이스 상태입니다. 두 번째 화면의 드롭다운 메뉴에서 이 옵션을 선택하고 **Apply Changes(변경사항 적용)**를 클릭하면 첫 번째 화면으로 돌아갑니다.
1. **Simple(단순)** — Simple(단순)을 선택하면 인증 키를 입력하라는 메시지가 표시됩니다. 이 키는 네트워크에서 전송되는 모든 패킷의 OSPF 헤더에 일반 텍스트 형식으로 포함됩니다. 네트워크상의 모든 라우터는 동일한 키로 구성되어야 합니다.
1. **Encrypt(암호화)** — Encrypt(암호화)를 선택하면 인증 키와 인증 ID를 모두 입력하라는 메시지가 표시됩니다. 암호화에서는 MD5 Message-Digest 알고리즘을 사용합니다. 네트워크상의 모든 라우터는 동일한 키 및 ID로 구성되어야 합니다.

Authentication Key(인증 키) — 지정된 인터페이스에 대한 OSPF 인증 키를 입력합니다. 인증을 사용하도록 선택하지 않으면 키를 입력하라는 메시지가 표시되지 않습니다. Simple(단순) 인증을 선택하면 8자보다 긴 키를 사용할 수 없습니다. Encrypt(암호화)를 선택하면 키 길이는 최대 16자가 될 수 있습니다. 키 값은 Read/Write(읽기/쓰기) 권한으로 로그인한 경우에만 표시되며 그렇지 않은 경우 별표로 표시됩니다.

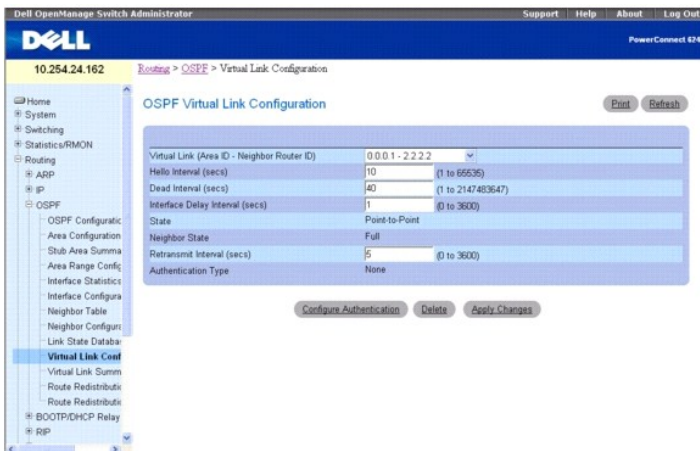
Authentication ID(인증 ID) — 인증에 사용할 ID를 입력합니다. 인증 유형으로 Encrypt(암호화)를 선택한 경우에만 ID를 입력하라는 메시지가 표시됩니다. ID는 0 ~ 255(포함) 사이의 숫자입니다.

새 가상 링크 정의

1. **OSPF Virtual Link Configuration(OSPF 가상 링크 구성)** 페이지를 엽니다.
2. **Virtual Link (Area ID - Neighbor Router ID)(가상 링크(영역 ID - 인접 라우터 ID))** 드롭다운 메뉴에서 **Create New Virtual Link(새 가상 링크 만들기)**를 선택합니다.
3. 새 가상 링크에 대한 Neighbor Router ID(인접 라우터 ID)를 지정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

나머지 필드는 Virtual Link(가상 링크)가 생성되었을 때 표시됩니다.

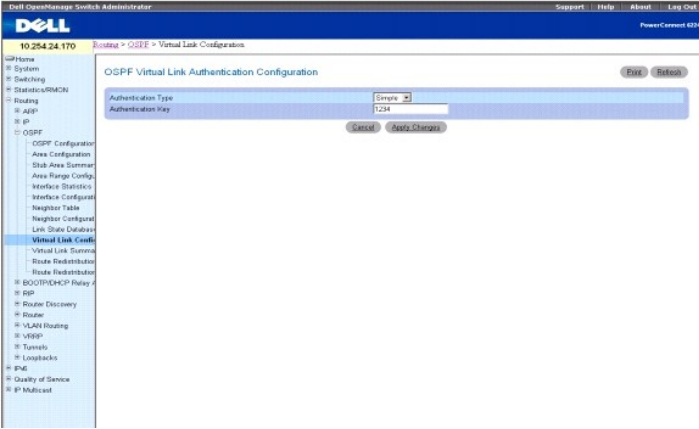
그림 10-16. OSPF Virtual Link Configuration - Create(OSPF 가상 링크 구성)



5. **Configure Authentication(인증 구성)**를 클릭하여 인증을 수정합니다.

다음 페이지가 나타납니다.

그림 10-17. OSPF Virtual Link Authentication Configuration(OSPF 가상 링크 인증 구성)



6. **Authentication Type(인증 유형)** 및 **Authentication Key(인증 키)** 값을 선택합니다.
7. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

가상 링크 데이터 구성

1. **OSPF Virtual Link Configuration(OSPF 가상 링크 구성)** 페이지를 엽니다.
 2. 구성할 Area ID(영역 ID) 및 Neighbor Router ID(인접 라우터 ID)를 지정합니다.
 3. 필요에 따라 필드에 데이터를 입력합니다.
 4. **Configure Authentication(인증 구성)**을 클릭하여 인증을 수정합니다.
 5. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.
- 지정된 ID에 대한 가상 링크 데이터가 구성되고 장치가 업데이트됩니다.

가상 링크 데이터 표시

1. **OSPF Virtual Link Configuration(OSPF 가상 링크 구성)** 페이지를 엽니다.
 2. 표시할 Area ID(영역 ID) 및 Neighbor Router ID(인접 라우터 ID)를 지정합니다.
- 해당 ID에 대한 가상 링크 데이터가 표시됩니다.

가상 링크 제거

1. **OSPF Virtual Link Configuration(OSPF 가상 링크 구성)** 페이지를 엽니다.
 2. 제거할 가상 링크와 연관된 Area ID(영역 ID) 및 Neighbor Router ID(인접 라우터 ID)를 지정합니다.
- 관련 가상 링크 데이터가 표시됩니다.
3. **Delete(삭제)**를 클릭합니다.
- 가상 링크가 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 가상 링크 데이터 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

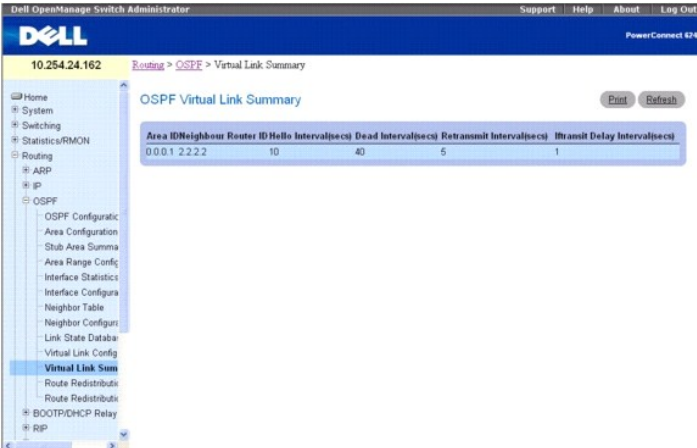
1. OSPF 명령

가상 링크 요약

OSPF Virtual Link Summary(OSPF 가상 링크 요약) 페이지를 사용하여 구성된 모든 가상 링크를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**OSPF**→**Virtual Link Summary(가상 링크 요약)**을 클릭합니다.

그림 10-18. OSPF Virtual Link Configuration(OSPF 가상 링크 구성)



OSPF Virtual Link Summary(OSPF 가상 링크 요약) 페이지에는 다음 필드가 있습니다.

Area ID(영역 ID) — 배포할 데이터에 대한 가상 링크 식별자의 영역 ID 부분입니다. 영역 ID와 인접 라우터 ID가 결합하여 가상 링크를 정의합니다.

Neighbor Router ID(인접 라우터 ID) — 가상 링크 식별의 인접 항목 부분입니다. 인터페이스가 공통(백본이 아님) 영역을 갖도록 영역 경계 라우터 쌍 간에 가상 링크를 구성할 수 있습니다.

Hello Interval (secs)(Hello 간격(초)) — 가상 링크에 대한 OSPF Hello 간격(초)입니다. Hello 간격 값은 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다.

Dead Interval (secs)(작동 중단 간격(초)) — 가상 링크에 대한 OSPF 작동 중단 간격(초)입니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 공통 네트워크에 연결된 모든 라우터에 대해 동일해야 하며, Hello 간격의 배수(예: 4)여야 합니다.

Retransmit Interval (secs)(재전송 간격(초)) — 가상 링크에 대한 OSPF 재전송 간격(초)입니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)을 지정합니다. 이 값은 데이터베이스 설명 및 링크 상태 요청 패킷을 재전송할 때도 사용됩니다.

Ifransit Delay Interval (secs)(Ifransit 지연 간격(초)) — 가상 링크에 대한 OSPF 운송 지연(초)을 입력합니다. 이 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 지정합니다.

CLI 명령을 사용하여 가상 링크 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

경로 재배포 구성

OSPF Route Redistribution Configuration(OSPF 경로 재배포 구성) 페이지를 사용하여 Static(정적), Connected(연결됨) 및 RIP를 통해 확인된 경로에 대한 재배포를 OSPF에서 구성할 수 있습니다. 모든 항목 또는 선택된 항목에서 확인된 경로를 재배포하도록 선택할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**OSPF**→**Route Redistribution Configuration(경로 재배포 구성)**을 클릭합니다.

그림 10-19. OSPF Route Redistribution Configuration(OSPF 경로 재배포 구성)



OSPF Route Redistribution Configuration(OSPF 경로 재배포 구성) 페이지에는 다음 필드가 있습니다.

Configured Source(구성된 소스) — 이 프로토콜을 통해 확인된 경로를 재배포하도록 OSPF에 대해 구성된 프로토콜입니다. OSPF에서 재배포하도록 구성된 소스 경로만 사용할 수 있습니다. Create(만들기)를 사용하면 새 소스 경로를 구성할 수 있습니다.

Available Source(사용 가능한 소스) — 경로를 재배포하도록 OSPF에 대해 구성할 수 있는 프로토콜입니다. 이 확인란은 Configured Source(구성된 소스)로 Create(만들기)를 선택한 경우에만 표시됩니다. 가능한 값은 Static(정적), Connected(연결됨) 및 RIP(RIP)입니다.

Metric(메트릭) — 재배포된 경로에 대한 메트릭 값을 설정합니다. 소스가 미리 구성된 경우 이 필드에 메트릭 값이 표시됩니다. 유효한 값은 0 ~ 16,777,214입니다.

Metric Type(메트릭 유형) — 드롭다운 메뉴에서 재배포된 경로의 OSPF 메트릭 유형을 선택합니다.

Tag(태그) — 재배포된 경로의 태그 필드를 설정합니다. 소스가 미리 구성된 경우 이 필드에 태그 값이 표시되며 그렇지 않은 경우 0이 표시됩니다. 유효한 값은 0 ~ 4294967295입니다.

Subnets(서브넷) — 드롭다운 메뉴에서 서브넷 경로를 재배포할지 여부를 선택합니다.

Distribute List(배포 목록) — 대상 프로토콜에서 재배포할 경로를 필터링하는 Access List(액세스 목록)를 선택합니다. 허용된 경로만 재배포됩니다. 이 명령이 존재하지 않는 액세스 목록을 참조하는 경우에는 모든 경로가 허용됩니다. 드롭다운 메뉴에서 **Switching(전환) → Network Security(네트워크 보안) → Access Control Lists(액세스 제어 목록) → IP Access Control Lists(IP 액세스 제어 목록)** 페이지에서 구성된 ACL이 나열됩니다. 경로 필터링에서는 액세스 목록의 다음 필드만 사용됩니다.

- 1 소스 IP 주소 및 넷마스크
- 1 대상 IP 주소 및 넷마스크
- 1 작업(허용 또는 거부)

모든 다른 필드(소스 및 대상 포트, 우선 순위, ToS 등)는 무시됩니다.

소스 IP 주소는 경로의 대상 IP 주소와 비교됩니다. 액세스 목록 규칙의 소스 IP 넷마스크는 와일드카드 마스크로 처리되며, 소스 IP 주소의 어느 비트가 경로의 대상 주소와 일치해야 하는지를 나타냅니다. 마스크의 1은 해당 주소 비트와 관계 없음을 나타냅니다.

액세스 목록 규칙에 대상 IP 주소와 넷마스크가 포함된 경우 (확장 액세스 목록) 대상 IP 주소는 경로 대상의 네트워크 마스크와 비교됩니다. 액세스 목록의 대상 넷마스크는 와일드카드 마스크로 작동하며 경로 대상 마스크의 어느 비트가 필터링 작업에 중요한지를 나타냅니다.

OSPF 경로 재배포 소스 만들기

재배포가 구성되어 있지 않으면 Configured Source(구성된 소스) 필드의 Create(만들기)와 Available Source(사용 가능한 소스) 필드의 가능한 소스만 표시됩니다. Available Source(사용 가능한 소스)를 선택한 경우 구성 데이터를 입력하고 **Apply Changes(변경사항 적용)**를 클릭합니다. Configure Source(소스 구성) 드롭다운 목록에 항목이 표시되고 Available Source(사용 가능한 소스) 드롭다운 목록에서 제거됩니다.

1. OSPF Route Redistribution Configuration(OSPF 경로 재배포 구성) 페이지를 엽니다.
2. Configured Source(구성된 소스) 필드에서 **Create(만들기)**를 지정합니다.
3. Available Source(사용 가능한 소스) 필드에서 Static(정적), Connected(연결됨) 또는 RIP를 선택합니다.
4. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

경로 재배포 데이터가 구성되고 장치가 업데이트됩니다.

OSPF 경로 재배포 데이터 수정

1. OSPF Route Redistribution Configuration(OSPF 경로 재배포 구성) 페이지를 엽니다.
2. Configured Source(구성된 소스) 드롭다운에서 소스를 선택합니다.
3. 필요에 따라 필드에 데이터를 입력합니다.
4. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

경로 재배포 데이터가 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPF 경로 재배포 데이터 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

경로 재배포 요약

OSPF Route Redistribution Summary(OSPF 경로 재배포 요약) 페이지를 사용하여 OSPF 경로 재배포 구성을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**OSPF**→**Route Redistribution Summary(경로 재배포 요약)**을 클릭합니다.

그림 10-20. OSPF Route Redistribution Summary(OSPF 경로 재배포 요약)

Source	Metric	Metric Type	Tag	Subnets	Distribute List
RIP	10	External Type 2	21	Disable	15
BGP	1	External Type 2	10	Disable	1

OSPF Route Redistribution Summary(OSPF 경로 재배포 요약) 페이지에는 다음 필드가 있습니다.

Source(소스) — OSPF가 재배포할 소스 경로입니다.

Metric(메트릭) — 지정된 소스 경로에 대해 재배포된 경로의 메트릭입니다. 구성되지 않은 경우 Unconfigured(구성 안 됨)를 표시합니다.

Metric Type(메트릭 유형) — 재배포된 경로의 OSPF 메트릭 유형입니다.

Tag(태그) — 재배포된 경로의 태그 필드입니다. 소스가 미리 구성된 경우 이 필드에 태그 값이 표시되며 그렇지 않은 경우 0이 표시됩니다.

Subnets(서브네트) — 서브네트 경로를 재배포할지 여부를 지정합니다.

Distribute List(배포 목록) — 대상 프로토콜에서 재배포할 경로를 필터링하는 Access List(액세스 목록)입니다.

CLI 명령을 사용하여 경로 재배포 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

BOOTP/DHCP 릴레이 에이전트

BOOTP/DHCP 릴레이 에이전트를 사용하면 BOOTP/DHCP 클라이언트와 서버가 서로 다른 서브네트 간에 BOOTP/DHCP 메시지를 교환할 수 있습니다. 릴레이 에이전트는 클라이언트로부터 요청을 받아 유효한 홉과 giaddr 필드를 확인합니다. 홉 수가 구성된 값보다 크면 에이전트는 패킷이 에이전트를 루핑하고 있다고 가정하고 패킷을 삭제합니다. giaddr 필드가 0이면 에이전트는 이 필드에 요청이 수신된 인터페이스의 IP 주소를 입력해야 합니다. 에이전트는 유효한 패킷을 다음 구성된 대상으로 유니캐스팅합니다. 서버는 giaddr 필드에 표시된 대로 클라이언트에 가장 가까운 릴레이 에이전트의 주소가 지정한 유니캐스트 BOOTREPLY로 응답합니다. 서버로부터 BOOTREPLY가 수신되면 에이전트는 BOOTREQUEST가 전송된 인터페이스에서 브로드캐스트 또는 유니캐스트로 이 응답을 전달합니다. 이 인터페이스는 giaddr 필드로 식별할 수 있습니다.

또한 6200 시리즈 DHCP 구성 요소는 고객이 고속 모뎀을 통해 인터넷에 연결되어 있을 때 소스 회로를 식별하는 DHCP 릴레이 에이전트 옵션을 지원합니다. 릴레이 에이전트는 서버로 요청을 전달할 때 이러한 옵션을 삽입하고 클라이언트로 응답을 보낼 때 제거합니다.

인터페이스에 IP 주소가 여러 개 있을 경우 릴레이 에이전트는 릴레이 에이전트 IP 주소로 구성된 기본 IP 주소를 사용해야 합니다.

BOOTP/DHCP Relay Agent(BOOTP/DHCP 릴레이 에이전트) 메뉴 페이지에는 BOOTP/DHCP 릴레이 에이전트를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→BOOTP/DHCP Relay Agent(BOOTP/DHCP 릴레이 에이전트)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

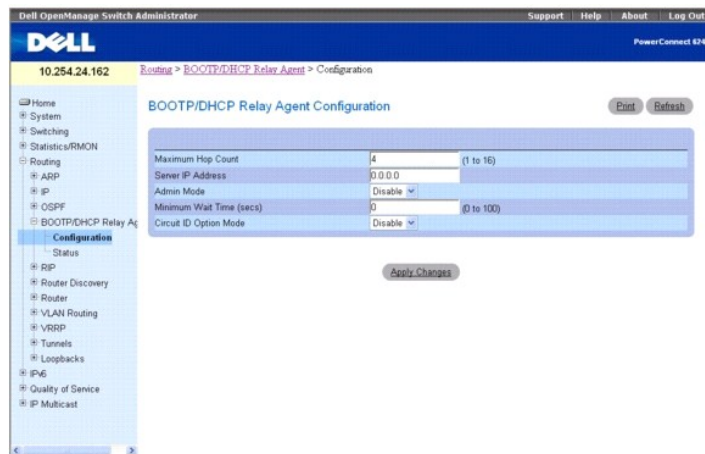
- 1. [BOOTP/DHCP 릴레이 에이전트 구성](#)
- 1. [BOOTP/DHCP 릴레이 에이전트 상태](#)

BOOTP/DHCP 릴레이 에이전트 구성

BOOTP/DHCP Relay Agent Configuration(BOOTP/DHCP 릴레이 에이전트 구성) 페이지를 사용하여 BOOTP/DHCP 릴레이 에이전트를 구성 및 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→BOOTP/DHCP Relay Agent(BOOTP/DHCP 릴레이 에이전트)→Configuration(구성)**를 클릭합니다.

그림 10-21. BOOTP/DHCP BOOTP/DHCP 릴레이 에이전트 구성



BOOTP/DHCP Relay Agent Configuration(BOOTP/DHCP 릴레이 에이전트 구성) 페이지에는 다음 필드가 있습니다.

Maximum Hop Count(최대 홉 수) — 클라이언트 요청이 삭제되기까지 수행할 수 있는 최대 홉 수를 입력합니다.

Server IP Address(서버 IP 주소) — BOOTP/DHCP 서버의 IP 주소 또는 다음 BOOTP/DHCP 릴레이 에이전트의 IP 주소를 입력합니다.

Admin Mode(관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 BOOTP/DHCP 요청이 Server IP address(서버 IP 주소) 필드에 입력한 IP 주소로 전달됩니다.

Minimum Wait Time(secs)(최소 대기 시간(초)) — 시간(초)을 입력합니다. 이 값은 클라이언트의 전원을 켜 이후에 경과한 시간을 나타내는 클라이언트 요청 패킷의 타임 스탬프와 비교됩니다. 타임 스탬프가 최대 대기 시간을 초과하는 경우에만 패킷이 전달됩니다.

Circuit ID Option Mode(회로 ID 옵션 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 릴레이 에이전트가 패킷을 서버에 전달하기 전에 Option 82 헤더 패킷을 DHCP 요청 패킷에 추가한 다음 클라이언트에 응답을 전달하는 동안 해당 패킷을 스트라이핑합니다.

BOOTP/DHCP 구성

1. **BOOTP/DHCP Configuration(BOOTP/DHCP 구성)** 페이지를 엽니다.
2. 필요에 따라 필드에 데이터를 입력합니다.
3. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

BOOTP/DHCP 데이터가 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 BOOTP/DHCP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

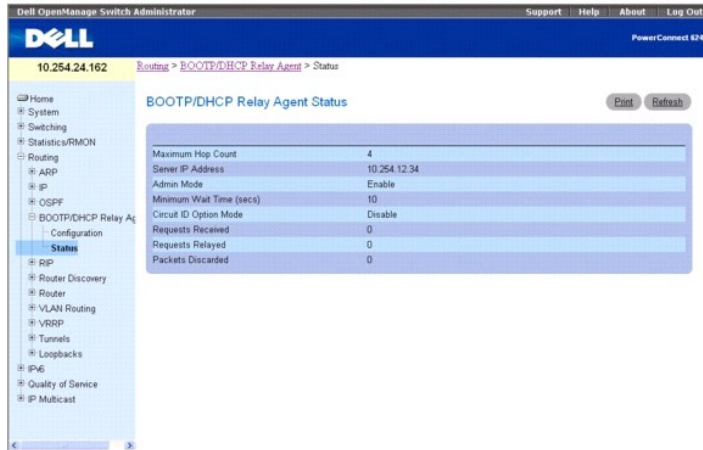
- 1 DHCP 및 BOOTP 릴레이 명령

BOOTP/DHCP 릴레이 에이전트 상태

BOOTP/DHCP Relay Agent Status(BOOTP/DHCP 릴레이 에이전트 상태) 페이지를 사용하여 BOOTP/DHCP 릴레이 에이전트 구성 및 상태 정보를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→ **BOOTP/DHCP Relay Agent(BOOTP/DHCP 릴레이 에이전트)**→ **Status(상태)**를 클릭합니다.

그림 10-22. BOOTP/DHCP Relay Agent Status(BOOTP/DHCP 릴레이 에이전트 상태)



BOOTP/DHCP Status(BOOTP/DHCP 상태) 페이지에는 다음 필드가 있습니다.

Maximum Hop Count(최대 홉 수) — 클라이언트 요청이 삭제되지 않고 수행할 수 있는 최대 홉 수입니다.

Server IP Address(서버 IP 주소) — BOOTP/DHCP 서버의 IP 주소 또는 다음 BOOTP/DHCP 릴레이 에이전트의 IP 주소입니다.

Admin Mode(관리 모드) — 릴레이의 Administrative Mode(관리 모드)입니다. 구성 페이지에서 Enable(활성)을 선택하면 BOOTP/DHCP 요청이 Server IP address(서버 IP 주소) 필드에 입력한 IP 주소로 전달됩니다.

Minimum Wait Time(secs)(최소 대기 시간(초)) — 최소 시간(초)입니다. 이 값은 클라이언트의 전원을 켜 이후에 경과한 시간을 나타내는 클라이언트 요청 패킷의 타임 스탬프와 비교됩니다. 타임 스탬프가 최대 대기 시간을 초과하는 경우에만 패킷이 전달됩니다.

Circuit ID Option Mode(회로 ID 옵션 모드) — 릴레이 에이전트 옵션으로, Enabled(활성화됨) 또는 Disabled(비활성화됨)가 될 수 있습니다. Enable(활성)을 선택하면 릴레이 에이전트가 패킷을 서버에 전달하기 전에 Option 82 헤더 패킷을 DHCP 요청 패킷에 추가한 다음 클라이언트에 응답을 전달하는 동안 해당 패킷을 스트라이핑합니다.

Requests Received(수신된 요청) — 마지막으로 스위치를 재설정된 이후 모든 클라이언트로부터 수신된 총 BOOTP/DHCP 요청 수입니다.

Requests Relayed(릴레이된 요청) — 마지막으로 스위치를 재설정된 이후 서버로 전달된 총 BOOTP/DHCP 요청 수입니다.

Packets Discarded(삭제된 패킷) — 마지막으로 스위치를 재설정된 이후 이 릴레이 에이전트가 삭제한 총 BOOTP/DHCP 패킷 수입니다.

CLI 명령을 사용하여 BOOTP/DHCP 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 DHCP 및 BOOTP 릴레이 명령

RIP

RIP는 Bellman-Ford 알고리즘을 기반으로 하고 소규모 네트워크(네트워크 지름이 15개 홉보다 크지 않음)를 대상으로 하는 IGP(Interior Gateway Protocol)입니다. 라우팅 정보는 정기적으로 및 네트워크 토폴로지 변경시 전송되는 RIP 업데이트 패킷에 포함되어 전파됩니다. RIP 업데이트가 수신될 때 지정된 경로가 있는지 여부에 따라 라우터에서 경로를 수정 또는 삭제하거나 경로 표에 추가할 수 있습니다. 경로 기본 설정은 각 대상에 대한 거리를 나타내는 구성 가능한 메트릭을 통해 전달됩니다.

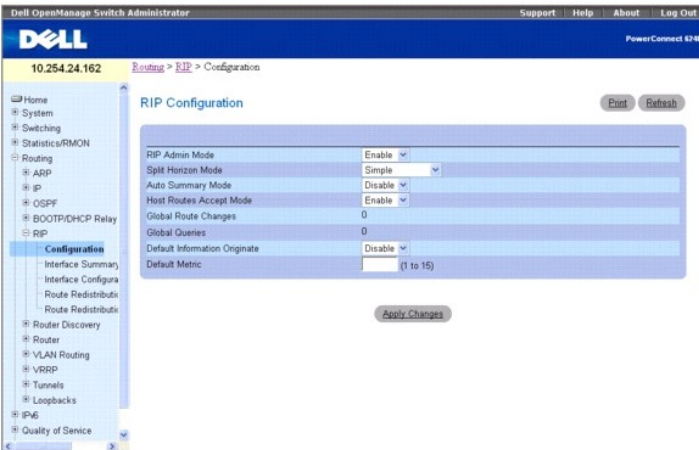
RIP 메뉴 페이지에는 RIP 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→ **RIP**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

- 1 [RIP 구성](#)
- 1 [RIP 인터페이스 요약](#)
- 1 [RIP 인터페이스 구성](#)
- 1 [RIP 경로 재배포 구성](#)
- 1 [RIP 경로 재배포 요약](#)

RIP 구성

RIP Configuration(RIP 구성) 페이지를 사용하여 RIP를 전역 모드로 활성화 및 구성하거나 비활성화할 수 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **RIP** → **Configuration(구성)**을 클릭합니다.

그림 10-23. RIP Configuration(RIP 구성)



RIP Configuration(RIP 구성) 페이지에는 다음과 같은 필드가 있습니다.

RIP Admin Mode(RIP 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면

스위치에 대해 RIP가 활성화됩니다. 기본값은 Disable(비활성)입니다.

Split Horizon Mode(분할 가로 모드) — 드롭다운 메뉴에서 None(없음), Simple(단순) 또는 Poison Reverse(포이즌 리버스)를 선택합니다. 기본값은 Simple(단순)입니다. 분할 가로는 경로가 원래 확인된 라우터로 전송된 업데이트에 경로가 포함된 경우 발생하는 문제를 방지하는 기법입니다. 옵션은 다음과 같습니다.

- 1 **None(없음)** — 이 경우에 대해 특별한 처리가 수행되지 않습니다.
- 1 **Simple(단순)** — 경로가 확인된 라우터로 전송되는 업데이트에 포함되지 않습니다.
- 1 **Poison Reverse(포이즌 리버스)** — 경로가 확인된 라우터로 전송되는 업데이트에 포함되지만 메트릭이 무한대로 설정됩니다.

Auto Summary Mode(자동 요약 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 총 항목 수를 줄이기 위해 인접 경로 그룹이 하나의 항목으로 요약됩니다. 기본값은 Enable(활성)입니다.

Host Routes Accept Mode(호스트 경로 승인 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 라우터가 호스트 경로를 승인합니다. 기본값은 Enable(활성)입니다.

Global Route Changes(전역 경로 변경) — IP 경로 데이터베이스에 대한 RIP의 경로 변경 수를 표시합니다. 경로의 보존 기간 재생은 포함되지 않습니다.

Global Queries(전역 쿼리) — 다른 시스템에서 RIP 쿼리로 전송된 응답 수를 표시합니다.

Default Information Originate(기본 정보 발생) — Default Route Advertise(기본 경로 알람)를 활성화하거나 비활성화합니다.

Default Metric(기본 메트릭) — 재배포된 경로의 메트릭에 대한 기본값을 설정합니다. 설정된 경우 이 필드에 기본 메트릭이 표시되고 이전에 구성되지 않은 경우에는 공백이 표시됩니다. 유효한 값은 1 ~ 15입니다.

RIP 구성

1. **RIP Configuration(RIP 구성)** 페이지를 엽니다.
2. 필요에 따라 필드에 데이터를 입력합니다.
3. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

RIP가 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 RIP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

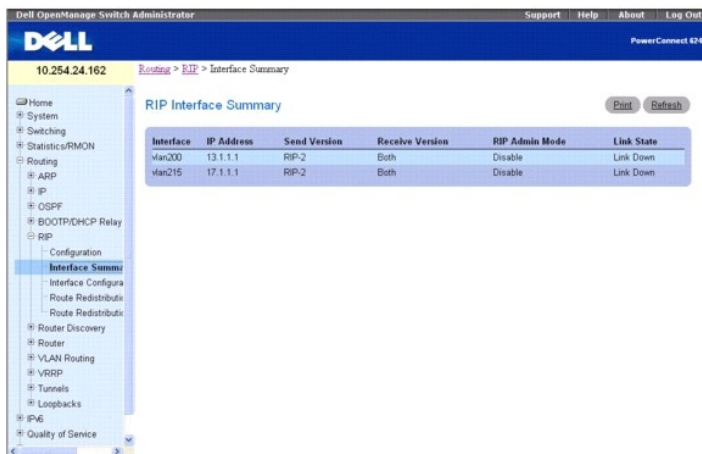
- 1 RIP(Routing Information Protocol) 명령

RIP 인터페이스 요약

RIP Interface Summary(RIP 인터페이스 요약) 페이지를 사용하여 인터페이스의 RIP 구성 상태를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → RIP → Interface Summary(인터페이스 요약)**를 클릭합니다.

그림 10-24. RIP Interface Summary(RIP 인터페이스 요약)



Interface	IP Address	Send Version	Receive Version	RIP Admin Mode	Link State
Vlan200	13.1.1.1	RIP-2	Both	Disable	Link Down
Vlan215	17.1.1.1	RIP-2	Both	Disable	Link Down

RIP Interface Summary(RIP 인터페이스 요약) 페이지에는 다음 필드가 있습니다.

Interface(인터페이스) — RIP가 활성화된 라우팅 가능 VLAN 등의 인터페이스입니다.

IP Address(IP 주소) — 라우터 인터페이스의 IP 주소입니다.

Send Version(전송 버전) — 인터페이스에서 전송된 RIP 제어 패킷이 준수하는 RIP 버전을 지정합니다. 기본값은 RIP-2이고 가능한 값은 다음과 같습니다.

- 1 **RIP-1** — RIP 버전 1 패킷이 브로드캐스트를 사용하여 전송됩니다.
- 1 **RIP-1c** — RIP 버전 1 호환 모드입니다. RIP 버전 2 형식 패킷이 브로드캐스트를 사용하여 전송됩니다.
- 1 **RIP-2** — RIP 버전 2 패킷이 멀티캐스트를 사용하여 전송됩니다.
- 1 **None(없음)** — RIP 제어 패킷이 전송되지 않습니다.

Receive Version(수신 버전) — 인터페이스에서 승인하는 RIP 버전 제어 패킷을 지정합니다. 기본값은 Both(모두)입니다. 가능한 값은 다음과 같습니다.

- 1 **RIP-1** — RIP 버전 1 형식 패킷만 수신됩니다.
- 1 **RIP-2** — RIP 버전 2 형식 패킷만 수신됩니다.
- 1 **Both(모두)** — 두 형식의 패킷이 모두 수신됩니다.
- 1 **None(없음)** — RIP 제어 패킷이 수신되지 않습니다.

RIP Admin Mode(RIP 관리 모드) — 인터페이스에서 RIP를 활성화할지 또는 비활성화할지 지정합니다.

Link State(링크 상태) — RIP 인터페이스가 작동하는지 또는 다운되었는지 지정합니다.

CLI 명령을 사용하여 RIP 인터페이스 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

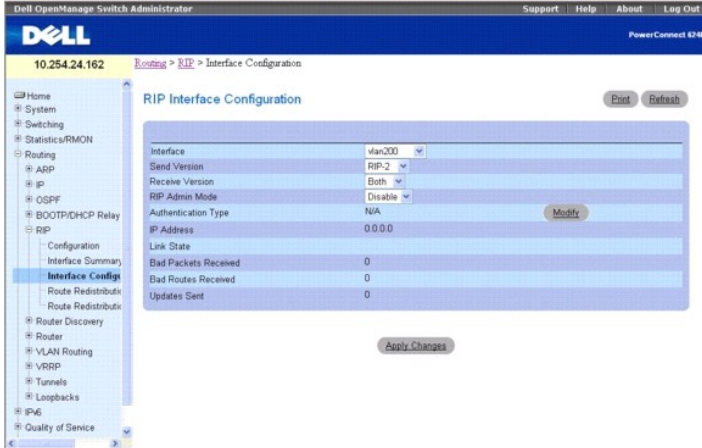
- 1 RIP(Routing Information Protocol) 명령

RIP 인터페이스 구성

RIP Interface Configuration(RIP 인터페이스 구성) 페이지를 사용하여 특정 인터페이스에서 RIP를 활성화 및 구성하거나 비활성화할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**RIP**→**Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 10-25. RIP Interface Configuration(RIP 인터페이스 구성)



RIP Interface Configuration(RIP 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 구성할 인터페이스를 선택합니다.

Send Version(전송 버전) — 라우터가 라우팅 업데이트와 함께 보내는 RIP 버전입니다. 기본값은 RIP-2이고 가능한 값은 다음과 같습니다.

- 1 **RIP-1** — 브로드캐스트를 통해 RIP 버전 1 형식 패킷만 보냅니다.
- 1 **RIP-1c** — RIP 버전 1 호환 모드입니다. 브로드캐스트를 통해 RIP 버전 2 형식 패킷을 보냅니다.
- 1 **RIP-2** — 멀티캐스트를 사용하여 RIP 버전 2 패킷을 보냅니다.
- 1 **None(없음)** — RIP 제어 패킷이 전송되지 않습니다.

Receive Version(수신 버전) — 라우터가 승인해야 하는 라우팅 업데이트의 RIP 버전입니다. 기본값은 Both(모두)입니다. 가능한 값은 다음과 같습니다.

- 1 **RIP-1** — RIP 버전 1 형식 패킷만 승인합니다.
- 1 **RIP-2** — RIP 버전 2 형식 패킷만 승인합니다.
- 1 **Both(모두)** — 두 형식의 패킷을 모두 승인합니다.
- 1 **None(없음)** — RIP 제어 패킷이 승인되지 않습니다.

RIP Admin Mode(RIP 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. 인터페이스에서 RIP 버전 1 또는 버전 1c를 활성화하기 전에 먼저 해당 인터페이스에서 네트워크상의 브로드캐스트 모드를 활성화해야 합니다. 기본값은 Disable(비활성)입니다.

Authentication Type(인증 유형) — **Modify(수정)** 단추를 클릭하여 None(없음) 이외의 인증 유형을 선택할 수 있습니다. 그러면 드롭다운 메뉴에서 인증 유형을 선택할 수 있는 새 화면이 표시됩니다. 가능한 값은 다음과 같습니다.

- 1 **None(없음)** — 초기 인터페이스 상태입니다. 두 번째 화면의 드롭다운 메뉴에서 이 옵션을 선택하고 **Apply Changes(변경사항 적용)**를 클릭하면 첫 번째 화면으로 돌아가고 인증 프로토콜이 실행되지 않습니다.
- 1 **Simple(단순)** — Simple(단순)을 선택하면 인증 키를 입력하라는 메시지가 표시됩니다. 이 키는 네트워크에서 전송되는 모든 패킷의 RIP 헤더에 일반 텍스트 형식으로 포함됩니다. 네트워크상의 모든 라우터는 동일한 키로 구성되어야 합니다.
- 1 **Encrypt(암호화)** — Encrypt(암호화)를 선택하면 인증 키와 인증 ID를 모두 입력하라는 메시지가 표시됩니다. 암호화에서는 MD5 Message-Digest 알고리즘을 사용합니다. 네트워크상의 모든 라우터는 동일한 키 및 ID로 구성되어야 합니다.

IP Address(IP 주소) — 라우터 인터페이스의 IP 주소를 표시합니다.

Link State(링크 상태) — RIP 인터페이스가 작동하는지 또는 다운되었는지 지정합니다.

Bad Packets Received(수신된 잘못된 패킷 수) — 잘못되었거나 손상된 RIP 패킷 수를 표시합니다. 이 값에서는 새 정보를 포함하여 전송되는 전체 업데이트를 명시적으로 포함하지 않습니다.

Bad Routes Received(수신된 잘못된 경로 수) — 어떤 이유로든 무시된, 유효한 RIP 패킷의 경로 수를 표시합니다(예: 이 인터페이스에서 실제로 전송된 트리거된 RIP 업데이트 수). 이 값에서는 새 정보를 포함하여 전송되는 전체 업데이트를 명시적으로 포함하지 않습니다.

Updates Sent(전송된 업데이트) — 전송된 경로 업데이트 수를 표시합니다.

RIP 인터페이스 구성

1. RIP Interface Configuration(RIP 인터페이스 구성) 페이지를 엽니다.

2. 데이터를 구성할 인터페이스를 지정합니다.

3. 필요에 따라 필드에 데이터를 입력합니다.

Send Version(전송 버전) — 드롭다운 상자에서 **None(없음)**, **RIP-1**, **RIP-1c** 또는 **RIP2**를 선택합니다.

Receive Version(수신 버전) — 드롭다운 상자에서 **None(없음)**, **RIP-1**, **RIP-2** 또는 **Both(모두)**를 선택합니다.

RIP Admin Mode(RIP 관리 모드) — **Enable(활성)** 또는 **Disable(비활성)**을 선택합니다.

Authentication Type(인증 유형) — 다른 인증 유형을 구성하려면 **Modify(수정)** 단추를 클릭합니다.

4. 끝나면 **Apply Changes(변경사항 적용)**를 클릭합니다.

RIP 인터페이스 구성이 구성되고 장치가 업데이트됩니다.

인증 방법 선택

1. RIP Interface Configuration(RIP 인터페이스 구성) 페이지를 엽니다.

2. 인증 방법을 구성할 인터페이스를 지정합니다.

3. **Modify(수정)**를 클릭합니다.

Authentication Method(인증 방법) 페이지가 표시됩니다.

4. 드롭다운 메뉴에서 Authentication Type(인증 유형)으로 **None(없음)**, **Simple(단순)** 또는 **Encrypt(암호화)**를 지정합니다.

5. Authentication Type(인증 유형)으로 **Simple(단순)** 또는 **Encrypt(암호화)**를 지정하면 추가 필드가 나타납니다. **Simple(단순)** 또는 **Encrypt(암호화)**를 입력하고 Authentication Key ID(인증 키 ID)로 **Encrypt(암호화)**를 입력합니다.

6. **Apply Changes(변경사항 적용)**를 클릭하십시오.

7. 인증 방법이 업데이트되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 RIP 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

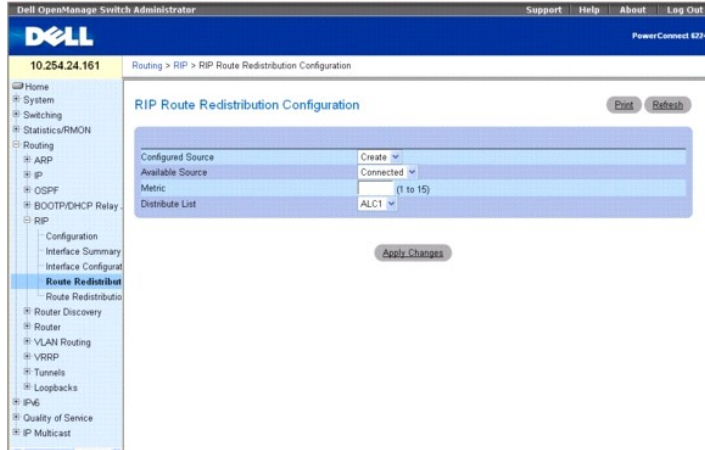
1. RIP(Routing Information Protocol) 명령

RIP 경로 재배포 구성

RIP Route Redistribution Configuration(RIP 경로 재배포 구성) 페이지를 사용하여 RIP 경로 재배포 매개변수를 구성할 수 있습니다. 각 필드 옆에는 해당 필드에 허용되는 값이 표시됩니다. 유효하지 않은 값을 입력하면 모든 유효값 목록과 함께 경고 메시지가 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**RIP**→**Route Redistribution Configuration(경로 재배포 구성)**을 클릭합니다.

그림 10-26. RIP Route Redistribution Configuration(RIP 경로 재배포 구성)



RIP Route Redistribution Configuration(RIP 경로 재배포 구성) 페이지에는 다음 필드가 있습니다.

Configured Source(구성된 소스) — 이 선택 상자는 동적 선택 항목으로, RIP에서 재배포하도록 구성된 소스 경로에 의해서만 채워집니다. Create(만들기)를 사용하면 사용 가능한 소스 경로를 구성할 수 있습니다.

Available Source(사용 가능한 소스) — 이 선택 상자는 동적 선택 항목으로, RIP에서 재배포하도록 구성하지 않은 소스 경로에 의해서만 채워집니다. 이 선택 상자는 Configured Source(구성된 소스)로 Create(만들기) 옵션을 선택한 경우에만 표시됩니다. 가능한 값은 다음과 같습니다.

- 1 Static(정적)
- 1 Connected(연결됨)
- 1 OSPF

Metric(메트릭) — 재배포된 경로의 메트릭으로 사용할 메트릭 값을 설정합니다. 소스가 미리 구성되어 있고 수정 가능한 경우에 이 필드에 메트릭이 표시됩니다. 유효한 값은 1 ~ 15입니다.

Distribute List(배포 목록) — 이 선택 상자는 대상 프로토콜에서 재배포할 경로를 필터링하는 Access List(액세스 목록)를 설정합니다. 허용된 경로만 재배포됩니다.

드롭다운 메뉴에서 **Switching(전환)→ Network Security(네트워크 보안)→ Access Control Lists(액세스 제어 목록)→ IP Access Control Lists(IP 액세스 제어 목록)** 페이지에서 구성된 ACL이 나열됩니다. 경로 필터링에서는 액세스 목록의 다음 필드만 사용됩니다.

- 1 소스 IP 주소 및 넷마스크
- 1 대상 IP 주소 및 넷마스크
- 1 작업(허용 또는 거부)

모든 다른 필드(소스 및 대상 포트, 우선 순위, ToS 등)는 무시됩니다.

소스 IP 주소는 경로의 대상 IP 주소와 비교됩니다. 액세스 목록 규칙의 소스 IP 넷마스크는 와일드카드 마스크로 처리되며, 소스 IP 주소의 어느 비트가 경로의 대상 주소와 일치해야 하는지를 나타냅니다. 마스크의 1은 해당 주소 비트와 관계 없음을 나타냅니다.

액세스 목록 규칙에 대상 IP 주소와 넷마스크가 포함된 경우(확장 액세스 목록) 대상 IP 주소는 경로 대상의 네트워크 마스크와 비교됩니다. 액세스 목록의 대상 넷마스크는 와일드카드 마스크로 작동하며 경로 대상 마스크의 어느 비트가 필터링 작업에 중요한지를 나타냅니다.

구성된 소스 만들기

1. RIP Route Redistribution Configuration(RIP 경로 재배포 구성) 페이지를 엽니다.
2. 구성할 Available Source(사용 가능한 소스)를 선택합니다.
3. 나머지 필드의 값을 지정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

이제 지정된 소스가 구성되고 장치가 업데이트됩니다.

구성된 소스 수정

1. RIP Route Redistribution Configuration(RIP 경로 재배포 구성) 페이지를 엽니다.

- 수정할 Configured Source(구성된 소스)를 선택합니다.
- 필요에 따라 이 화면의 값을 변경합니다.
- Apply Changes(변경사항 적용)**를 클릭하십시오.
지정된 변경 내용이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 RIP 경로 재배포 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

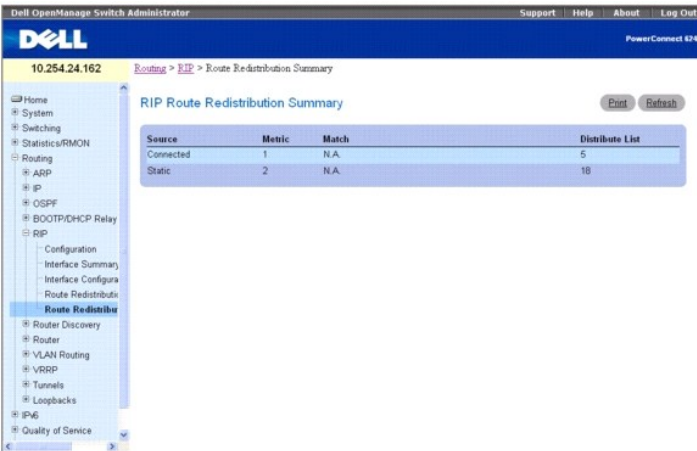
- RIP(Routing Information Protocol) 명령

RIP 경로 재배포 요약

RIP Route Redistribution Summary(RIP 경로 재배포 요약) 페이지를 사용하여 경로 재배포 구성을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **RIP** → **Route Redistribution Summary(경로 재배포 요약)**를 클릭합니다.

그림 10-27. RIP Route Redistribution Summary(RIP 경로 재배포 요약)



RIP Route Redistribution Summary(RIP 경로 재배포 요약) 페이지에는 다음 필드가 있습니다.

Source(소스) — RIP가 재배포할 소스 경로입니다.

Metric(메트릭) — 지정된 소스 경로에 대해 재배포된 경로의 메트릭입니다. 구성되지 않은 경우 Unconfigured(구성 안 됨)를 표시합니다.

Match(일치) — Source(소스)로 OSPF를 선택한 경우 재배포되는 경로 목록입니다. 이 목록에는 다음이 하나 이상 포함될 수 있습니다.

- 내부
- External 1
- External 2
- NSSA-External 1
- NSSA-External 2
- 해당 없음(OSPF가 아닐 경우)

Distribute List(배포 목록) — 대상 프로토콜에서 재배포할 경로를 필터링하는 Access List(액세스 목록)입니다. Distribute List(배포 목록)를 구성하지 않은 경우 이 필드가 비어 있습니다.

CLI 명령을 사용하여 RIP 경로 재배포 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- RIP(Routing Information Protocol) 명령

라우터 검색

라우터 검색 프로토콜은 호스트에서 서브네트의 작업 라우터를 식별하는 데 사용됩니다. 라우터 검색 메시지의 두 가지 유형은 "Router Advertisements(라우터 알림)" 및 "Router Solicitations(라우터 요청)"입니다. 이 프로토콜에서는 모든 라우터가 연관된 IP 주소를 주기적으로 알려야 합니다. 호스트는 이러한 알림을 수신하고 인접 라우터의 IP 주소를 검색합니다.

Router Discovery(라우터 검색) 메뉴 페이지에는 라우터 검색 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 메뉴를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router Discovery(라우터 검색)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

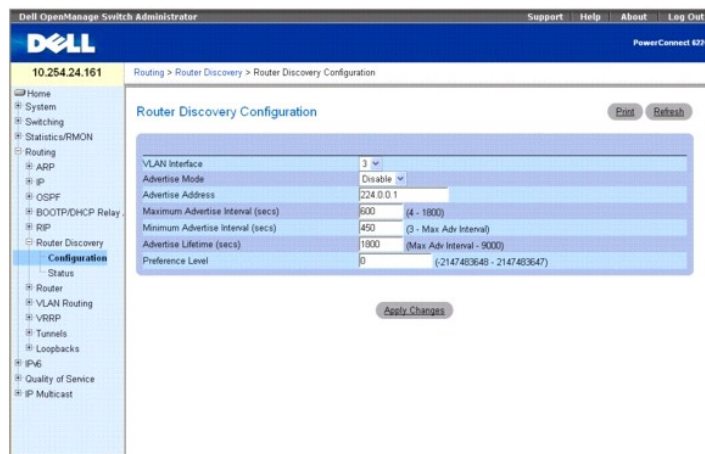
- 1 [라우터 검색 구성](#)
- 1 [라우터 검색 상태](#)

라우터 검색 구성

Router Discovery Configuration(라우터 검색 구성) 페이지를 사용하여 라우터 검색 매개변수를 입력하거나 변경할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router Discovery(라우터 검색)** → **Configuration(구성)**를 클릭합니다.

그림 10-28. Router Discovery Configuration(라우터 검색 구성)



Router Discovery Configuration(라우터 검색 구성) 페이지에는 다음 필드가 있습니다.

VLAN Interface(VLAN 인터페이스) — 데이터를 구성할 라우터 인터페이스를 선택합니다.

Advertise Mode(알림 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 라우터 알림이 선택된 인터페이스에서 전송됩니다.

Advertise Address(알림 주소) — 라우터를 알리는 데 사용할 IP 주소를 입력합니다.

Maximum Advertise Interval(secs)(최대 알림 간격(초)) — 인터페이스에서 전송되는 라우터 알림 간의 최대 허용 간격(초)을 입력합니다.

Minimum Advertise Interval(secs)(최소 알림 간격(초)) — 인터페이스에서 전송되는 라우터 알림 간의 최소 허용 간격(초)을 입력합니다.

Advertise Lifetime(secs)(알림 수명(초)) — 인터페이스에서 전송되는 라우터 알림의 수명 필드로 사용할 값(초)을 입력합니다. 호스트가 알림으로 받은 주소를 유효한 라우터 주소로 간주할 최대 시간입니다.

Preference Level(기본 설정 레벨) — 라우터의 기본 설정 레벨을 같은 서브네트의 다른 라우터에 대한 기본 라우터로 지정합니다. 주소의 번호가 높을수록 우선합니다. 정수를 입력해야 합니다.

라우터 검색 구성

1. **Router Discovery Configuration(라우터 검색 구성)** 페이지를 엽니다.
2. 구성할 라우터 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드의 데이터를 구성합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

지정된 구성 변경 내용이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 라우터 검색 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

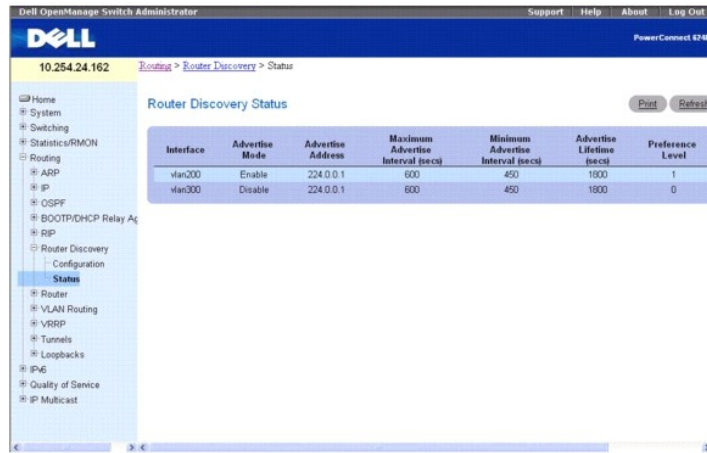
- 1 라우터 검색 프로토콜 명령

라우터 검색 상태

Router Discovery Status(라우터 검색 상태) 페이지를 사용하여 각 포트에 대한 라우터 검색 데이터를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router Discovery(라우터 검색)** → **Status(상태)**를 클릭합니다.

그림 10-29. Router Discovery Status(라우터 검색 상태)



Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
vlan200	Enable	224.0.0.1	600	450	1800	1
vlan300	Disable	224.0.0.1	600	450	1800	0

Router Discovery Status(라우터 검색 상태) 페이지에는 다음 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시할 라우터 인터페이스입니다.

Advertise Mode(알림 모드) — 값은 Enable(활성) 또는 Disable(비활성)입니다. Enable(활성)을 선택하면 해당 인터페이스에 대해 라우터 검색이 활성화됩니다.

Advertise Address(알림 주소) — 라우터를 알리는 데 사용할 IP 주소입니다.

Maximum Advertise Interval(secs)(최대 알림 간격(초)) — 인터페이스에서 전송되는 라우터 알림 간의 최대 허용 간격(초)입니다.

Minimum Advertise Interval(secs)(최소 알림 간격(초)) — 인터페이스에서 전송되는 라우터 알림 간의 최소 허용 간격(초)입니다.

Advertise Lifetime(secs)(알림 수명(초)) — 인터페이스에서 전송되는 라우터 알림의 수명 필드로 사용할 값(초)입니다. 호스트가 알림으로 받은 주소를 유효한 라우터 주소로 간주할 최대 시간입니다.

Preference Level(기본 설정 레벨) — 같은 서브네트의 다른 라우터에 대한 기본 라우터로서의 라우터의 기본 설정 레벨입니다. 주소의 번호가 높을수록 우선합니다.

CLI 명령을 사용하여 라우터 검색 상태 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 라우터 검색 프로토콜 명령

라우터

Router(라우터) 메뉴 페이지에는 경로표를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router(라우터)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

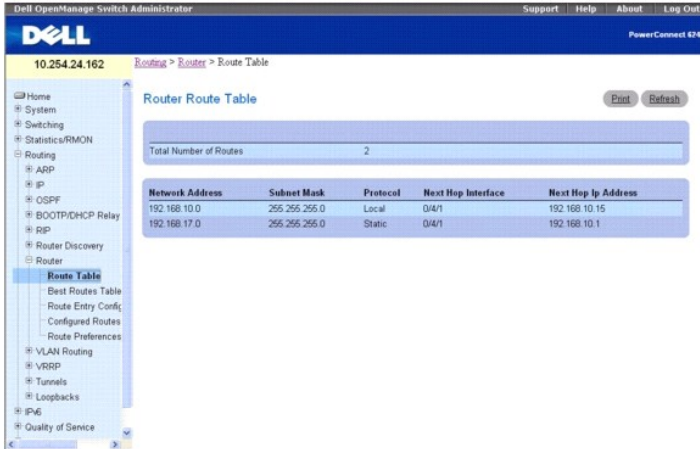
- 1 [경로표](#)
- 1 [최적의 경로표](#)
- 1 [경로 항목 구성](#)
- 1 [구성된 경로](#)

경로표

Router Route Table(라우터 경로표) 페이지를 사용하여 경로표 구성을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router(라우터)** → **Router Table(라우터 표)**를 클릭합니다.

그림 10-30. Router Route Table(라우터 경로표)



Router Route Table(라우터 경로표) 페이지에는 다음과 같은 필드가 있습니다.

Total Number of Routes(총 경로 수) — 경로표에 있는 총 경로 수입니다.

Network Address(네트워크 주소) — 대상의 IP 경로 점두어입니다.

Subnet Mask(서브네트 마스크) — 서브네트/네트워크 마스크라고도 하며, 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

Protocol(프로토콜) — 이 필드는 지정된 경로를 생성한 프로토콜을 나타냅니다. 다음 중 하나를 사용할 수 있습니다.

- 1 지역
- 1 Static
- 1 기본값
- 1 OSPF Intra
- 1 OSPF Inter
- 1 OSPF Type-1
- 1 OSPF Type-2
- 1 RIP

Next Hop Interface(다음 홉 인터페이스) — 대상에 트래픽을 전달하는 데 사용할 전송 라우터 인터페이스입니다.

Next Hop IP Address(다음 홉 IP 주소) — 대상 경로의 다음 라우터(있는 경우)에 트래픽을 전달할 때 사용할 전송 라우터 IP 주소입니다. 다음 라우터는 항상 직접 연결된 네트워크의 로컬 인터페이스 IP 주소 또는 인접 항목 중 하나입니다.

CLI 명령을 사용하여 라우터 경로표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

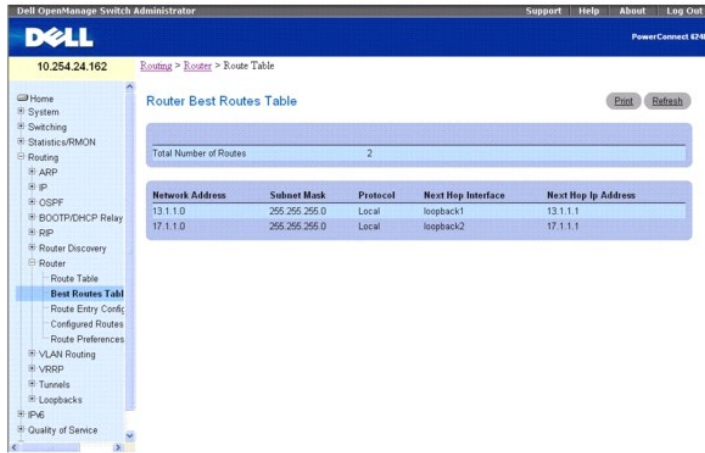
- 1 IP 라우팅 명령

최적의 경로표

Router Best Routes Table(최적의 라우터 경로표) 페이지를 사용하여 경로표에서 최적의 경로를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router(라우터)** → **Best Router Table(최적의 라우터 표)**를 클릭합니다.

그림 10-31. Router Best Route Table(최적의 라우터 경로표)



Router Best Route Table(최적의 라우터 경로표) 페이지에는 다음과 같은 필드가 있습니다.

Total Number of Routes(총 경로 수) — 경로표에 있는 총 경로 수입니다.

Network Address(네트워크 주소) — 대상의 IP 경로 점두어입니다.

Subnet Mask(서브네트 마스크) — 서브네트/네트워크 마스크라고도 하며, 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

Protocol(프로토콜) — 이 필드는 지정된 경로를 생성한 프로토콜을 나타냅니다. 다음 중 하나를 사용할 수 있습니다.

- 1 지역
- 1 Static
- 1 기본값
- 1 OSPF Intra
- 1 OSPF Inter
- 1 OSPF Type-1
- 1 OSPF Type-2
- 1 RIP

Next Hop Interface(다음 홉 인터페이스) — 대상에 트래픽을 전달하는 데 사용할 전송 라우터 인터페이스입니다.

Next Hop IP Address(다음 홉 IP 주소) — 대상 경로의 다음 라우터(있는 경우)에 트래픽을 전달할 때 사용할 전송 라우터 IP 주소입니다. 다음 라우터는 항상 직접 연결된 네트워크의 로컬 인터페이스 IP 주소 또는 인접 항목 중 하나입니다.

CLI 명령을 사용하여 최적의 경로표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

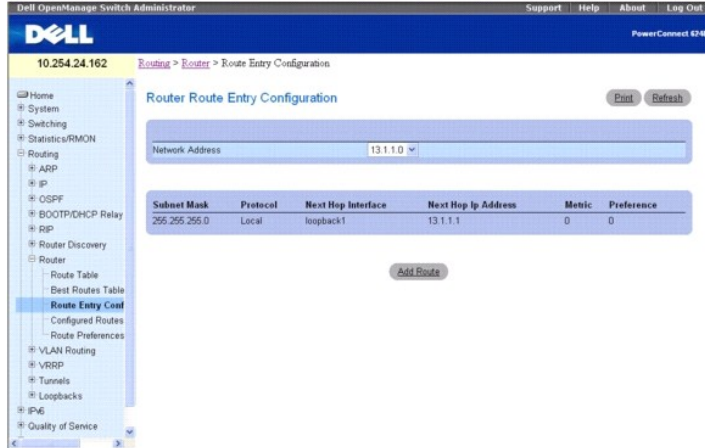
- 1 IP 라우팅 명령

경로 항목 구성

Router Route Entry Configuration(라우터 경로 항목 구성) 페이지를 사용하여 새 라우터 경로를 추가하고 라우터 경로를 구성할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router(라우터)** → **Router Entry Configuration(라우터 항목 구성)**을 클릭합니다.

그림 10-32. Router Route Entry Configuration(라우터 경로 항목 구성)



Router Route Entry Configuration(라우터 경로 항목 구성) 페이지에는 다음 필드가 있습니다.

Network Address(네트워크 주소) — 드롭다운 메뉴에서 대상의 IP 경로 접두어를 지정합니다. 경로를 만들려면 유효한 라우팅 인터페이스가 있어야 하며 다음 홉 IP 주소가 라우팅 인터페이스와 같은 네트워크에 있어야 합니다. 라우팅 인터페이스는 **IP Interface Configuration(IP 인터페이스 구성)** 페이지에서 생성됩니다. 유효한 다음 홉 IP 주소는 **Route Table(경로표)** 페이지에서 볼 수 있습니다.

Subnet Mask(서브네트 마스크) — 서브네트/네트워크 마스크라고도 하며, 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

Protocol(프로토콜) — 이 필드는 지정된 경로를 생성한 프로토콜을 나타냅니다. 가능한 값은 다음과 같습니다.

- 1 지역
- 1 Static
- 1 기본값
- 1 OSPF Intra
- 1 OSPF Inter
- 1 OSPF Type-1
- 1 OSPF Type-2
- 1 RIP

Next Hop Interface(다음 홉 인터페이스) — 대상에 트래픽을 전달하는 데 사용할 전송 라우터 인터페이스입니다.

Next Hop IP Address(다음 홉 IP 주소) — 대상 경로의 다음 라우터(있는 경우)에 트래픽을 전달할 때 사용할 전송 라우터 IP 주소입니다. 다음 라우터는 항상 직접 연결된 네트워크의 로컬 인터페이스 IP 주소 또는 인접 항목 중 하나입니다. 경로를 만들 때 다음 홉 IP는 라우팅 인터페이스와 같은 네트워크에 있어야 합니다. 유효한 다음 홉 IP 주소는 'Route Table(경로표)' 페이지에서 볼 수 있습니다.

Metric(메트릭) — 대상에 대한 경로의 관리 비용입니다. 값을 입력하지 않은 경우 기본값은 1입니다. 범위는 0~255입니다. 이 필드는 정적 경로를 만드는 경우에만 표시됩니다.

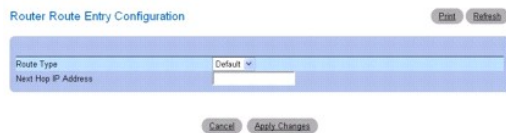
Preference(기본 설정) — 구성된 다음 홉에 대한 기본 설정 값을 지정합니다.

라우터 경로 추가

1. Router Route Entry Configuration(라우터 경로 항목 구성) 페이지를 엽니다.
2. Add Route(경로 추가)를 클릭합니다.

화면이 새로 고쳐지고 Router Route Entry Configuration(라우터 경로 항목 구성) 페이지가 [그림 10-33](#)에 표시된 대로 새 필드를 표시합니다.

그림 10-33. Add Route - Default Route Type(경로 추가 - 기본 경로 유형)



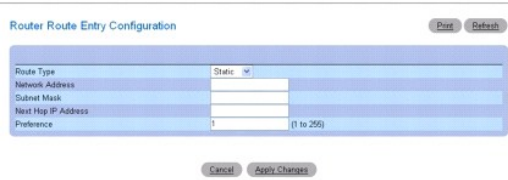
3. Route Type(경로 유형) 옆에 있는 드롭다운 상자를 사용하여 Default(기본) 경로 또는 Static(정적) 경로를 추가합니다.

Static(정적)을 선택할 경우 페이지가 새로 고쳐지고 [그림 10-34](#)에 표시된 대로 새 필드가 나타납니다.

Default(기본) — Next Hop IP Address(다음 홉 IP 주소) 필드에 기본 게이트웨이 주소를 입력합니다.

Static(정적) — Network Address(네트워크 주소), Subnet Mask(서브넷 마스크), Next Hop IP Address(다음 홉 IP 주소) 및 Preference(기본 설정)에 대한 값을 입력합니다.

그림 10-34. Route Entry Configuration - Add Static Route Type(경로 항목 구성 - 정적 경로 유형 추가)



4. Apply Changes(변경사항 적용)를 클릭하십시오.

새 경로가 추가되고 Configured Routes(구성된 경로) 페이지로 리디렉션됩니다.

CLI 명령을 사용하여 라우터 경로 추가

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

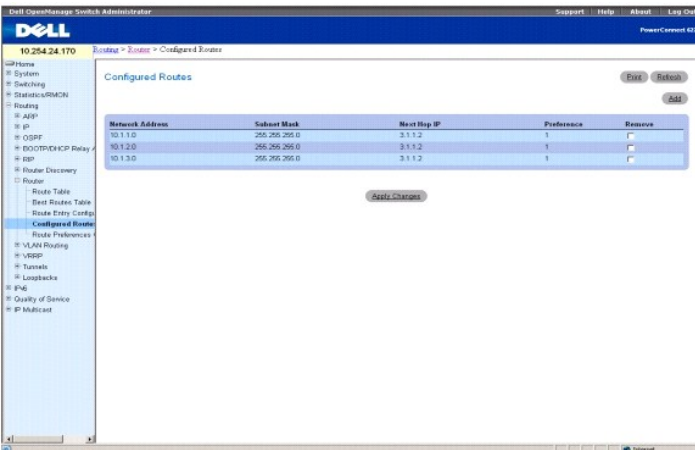
- 1 IP 라우팅 명령

구성된 경로

Configured Routes(구성된 경로) 페이지를 사용하여 구성된 경로를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 Routing(라우팅) → Router(라우터) → Configured Routes(구성된 경로)를 클릭합니다.

그림 10-35. Configured Routes(구성된 경로)



Configured Routes(구성된 경로) 페이지에는 다음 필드가 있습니다.

Network Address(네트워크 주소) — 대상의 IP 경로 점두어입니다.

Subnet Mask(서브넷 마스크) — 서브넷/네트워크 마스크라고도 하며, 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

Next Hop IP(다음 홉 IP) — 대상에 트래픽을 전달하는 데 사용할 전송 라우터 인터페이스입니다.

Preference(기본 설정) — 추가한 경로에 대해 구성된 기본 설정을 표시합니다.

Remove(제거) — 구성된 경로를 제거하려면 이 확인란을 사용합니다.

라우터 경로 추가

1. Configured Routes(구성된 경로) 페이지를 엽니다.

2. Add(추가)를 클릭합니다.

Router Route Entry Configuration(라우터 경로 항목 구성) 페이지가 [그림 10-33](#)처럼 표시됩니다.

3. Route Type(경로 유형) 옆에 있는 드롭다운 상자를 사용하여 Default(기본) 경로 또는 Static(정적) 경로를 추가합니다.

Default(기본) — Next Hop IP Address(다음 홉 IP 주소) 필드에 기본 게이트웨이 주소를 입력합니다. [그림 10-33](#)은 Route Type(경로 유형) 값이 Default(기본)일 때의 화면을 보여줍니다.

Static(정적) — Network Address(네트워크 주소), Subnet Mask(서브넷 마스크), Next Hop IP Address(다음 홉 IP 주소) 및 Preference(기본 설정)에 대한 값을 입력합니다. [그림 10-34](#)은 Route Type(경로 유형) 값이 Static(정적)일 때의 화면을 보여줍니다.

4. Apply Changes(변경사항 적용)를 클릭하십시오.

새 경로가 추가되고 Configured Routes(구성된 경로) 페이지로 돌아갑니다.

CLI 명령을 사용하여 구성된 경로 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 [CLI 참조 안내서](#)의 다음 장을 참조하십시오.

- 1 IP 라우팅 명령

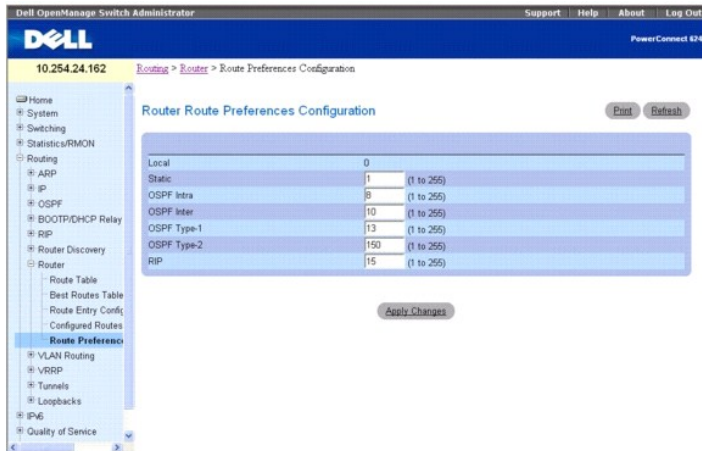
경로 기본 설정 구성

Router Route Preferences Configuration(라우터 경로 기본 설정 구성) 페이지를 사용하여 각 프로토콜에 대한 기본 설정(예: 정적 경로의 경우 60)을 구성할 수 있습니다. 이러한 값은 1 ~ 255 범위의 임의의 값으로, 경로 메트릭과 관계가 없습니다. 대부분의 라우팅 프로토콜은 경로 메트릭을 사용하여 다른 프로토콜에 관계 없이 프로토콜에 알려진 최단 경로를 결정합니다.

기본 설정 값이 가장 낮은 경로를 선택하여 대상에 대한 최단 경로를 선택합니다. 대상에 대한 경로가 여러 개 있는 경우 기본 설정 값을 사용하여 기본 경로를 결정합니다. 기본 설정 값이 동일한 경로가 있는 경우 최단 경로 메트릭을 가진 경로가 선택됩니다. 메트릭 불일치(예: RIP 및 OSPF 메트릭을 직접 비교할 수 없음) 문제를 방지하려면 각 프로토콜에 대해 다른 기본 설정 값을 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Router(라우터)** → **Route Preferences Configuration(경로 기본 설정 구성)**을 클릭합니다.

그림 10-36. Router Route Preferences Configuration(라우터 경로 기본 설정 구성)



Router Route Preferences Configuration(라우터 경로 기본 설정 구성) 페이지에는 다음 필드가 있습니다.

Local(로컬) — 이 필드에는 로컬 경로 기본 설정 값이 표시됩니다.

Static(정적) — 라우터의 정적 경로 기본 설정 값입니다. 기본값은 1이고 범위는 1 ~ 255입니다.

OSPF Intra — 라우터의 OSPF intra 경로 기본 설정 값입니다. 기본값은 8이고 범위는 1 ~ 255입니다. OSPF 사양(RFC 2328)에서는 OSPF를 통해 전달되는 경로에 대한 기본 설정을 다음과 같은 순서로 지정해야 합니다. intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPF Inter — 라우터의 OSPF inter 경로 기본 설정 값입니다. 기본값은 10이고 범위는 1 ~ 255입니다. OSPF 사양(RFC 2328)에서는 OSPF를 통해 전달되는 경로에 대한 기본 설정을 다음과 같은 순서로 지정해야 합니다. intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPF Type-1 — 라우터의 OSPF type-1 경로 기본 설정 값입니다. 기본값은 13이고 범위는 1 ~ 255입니다. OSPF 사양(RFC 2328)에서는 OSPF를 통해 전달되는 경로에 대한 기본 설정을 다음과 같은 순서로 지정해야 합니다. intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPF Type-2 — 라우터의 OSPF type-2 경로 기본 설정 값입니다. 기본값은 150이고 범위는 1 ~ 255입니다. OSPF 사양(RFC 2328)에서는 OSPF를 통해 전달되는 경로에 대한 기본 설정을 다음과 같은 순서로 지정해야 합니다. intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

RIP — 라우터의 RIP 경로 기본 설정 값입니다. 기본값은 15이고 범위는 1 ~ 255입니다.

경로 기본 설정 구성

1. **Route Preferences Configuration(경로 기본 설정 구성)** 페이지를 엽니다.
2. 페이지에서 관련 필드를 정의합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

경로 기본 설정이 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 경로 기본 설정 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. OSPF 명령

VLAN 라우팅

라우팅을 지원하는 일부 VLAN으로 6200 시리즈 소프트웨어를 구성할 수 있습니다. VLAN이 라우터 포트인 것처럼 VLAN의 트래픽을 처리하도록 소프트웨어를 구성할 수도 있습니다.

라우팅 대신 브리징(기본값)에 대해 포트를 활성화하면 인바운드 패킷에 대해 모든 정상적인 브리징 처리가 수행됩니다. 그런 후에 이 패킷은 VLAN과 연결됩니다. MAC Destination Address (MAC DA)(MAC 대상 주소(MAC DA)) 및 VLAN ID는 MAC 주소 표를 검색하는 데 사용됩니다. VLAN에 대해 라우팅이 활성화되고 인바운드 유니캐스트 패킷의 MAC DA가 외부 브리징-라우터 인터페이스의 것이면 패킷이 라우팅됩니다. 인바운드 멀티캐스트 패킷이 라우팅된 VLAN에서 수신된 경우에는 VLAN의 모든 포트 및 내부 브리징-라우터 인터페이스로 전달됩니다.

여러 VLAN에 속하도록 포트를 구성할 수 있으므로 포트의 모든 VLAN 또는 일부에 대해 VLAN 라우팅이 활성화될 수도 있습니다. VLAN 라우팅을 사용하면 여러 개의 물리적 포트가 같은 서브네트에 위치할 수 있습니다. VLAN이 여러 개의 물리적 네트워크에 걸쳐 있거나 추가 세그멘테이션 또는 보안이 필요한 경우에도 VLAN 라우팅을 사용할 수 있습니다. 이 절에서는 VLAN 라우팅을 지원하도록 6200 시리즈 소프트웨어를 구성하는 방법에 대해 설명합니다. 포트는 VLAN 포트 또는 라우터 포트가 될 수 있지만 둘 다일 수는 없습니다. 하지만 그 자체가 라우터 포트인 VLAN에 VLAN 포트가 포함될 수 있습니다.

VLAN Routing(VLAN 라우팅) 메뉴 페이지에는 VLAN 라우팅 매개변수 및 데이터를 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→VLAN Routing(VLAN 라우팅)**을 클릭합니다. 다음 웹 페이지는 이 메뉴 페이지에서 액세스할 수 있습니다.

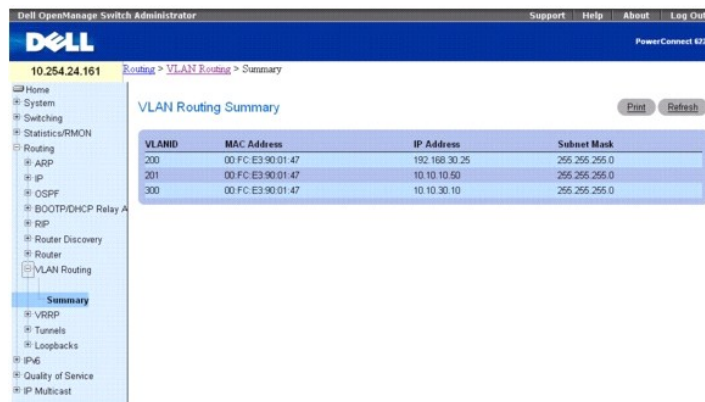
1. [VLAN 라우팅 요약](#)

VLAN 라우팅 요약

VLAN Routing Summary(VLAN 라우팅 요약) 페이지를 사용하여 시스템에 구성된 VLAN 라우팅 인터페이스에 대한 정보를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→VLAN Routing(VLAN 라우팅)→Summary(요약)**를 클릭합니다.

그림 10-37. VLAN Routing Summary(VLAN 라우팅 요약)



VLANID	MAC Address	IP Address	Subnet Mask
200	00 FC E3 90 01 47	192.168.30.25	255.255.255.0
201	00 FC E3 90 01 47	10.10.10.50	255.255.255.0
300	00 FC E3 90 01 47	10.10.30.10	255.255.255.0

VLAN Routing Summary(VLAN 라우팅 요약) 페이지에는 다음 필드가 있습니다.

VLAN ID — 데이터가 현재 표 행에 표시되는 VLAN의 ID입니다.

MAC Address(MAC 주소) — VLAN 라우팅 인터페이스에 지정된 MAC 주소입니다.

IP Address(IP 주소) — VLAN 라우팅 인터페이스의 구성된 IP 주소입니다. VLAN이 생성되었으며 IP 주소가 구성되지 않은 경우 기본적으로 이 페이지에 IP 주소 0.0.0.0이 표시됩니다. IP 주소를 구성하려면 **IP→ Interface Configuration(인터페이스 구성)**으로 이동합니다.

Subnet Mask(서브네트 마스크) — VLAN 라우팅 인터페이스의 구성된 서브네트 마스크입니다. VLAN 라우팅 인터페이스를 처음 구성한 경우 이 값은 0.0.0.0이며 IP Interface Configuration(IP 인터페이스 구성) 페이지에서 입력해야 합니다.

CLI 명령을 사용하여 VLAN 라우팅 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 IP 주소 지정 명령
- 1 VLAN(가상 LAN) 라우팅 명령

VRRP

가상 라우터 중복 프로토콜(VRRP)은 백업 라우터를 동적으로 선택하는 체계를 제공하여 기본 라우터 실패를 처리합니다. 이 프로토콜의 주 목적은 기본 게이트웨이 라우터 실패로 인해 실패가 감지될 때까지 이 라우터로 전달된 모든 트래픽이 손실되는 "블랙홀" 기간을 최소화하는 것입니다. 기본 경로의 정적 구성이 일반적이지만 이 방법은 기본 라우터 실패시 단일 실패 지점을 발생시키는 단점이 있습니다. VRRP는 기본 게이트웨이 역할을 하는 여러 개의 IP 주소와 연관된 "가상 라우터"의 개념을 사용합니다. 이러한 IP 주소를 제어하는 VRRP 라우터(이전의 마스크)가 실패하면 백업 VRRP 라우터가 IP 주소 및 기본 전달 역할 그룹을 처리합니다.

VRRP 메뉴 페이지에는 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→ VRRP**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

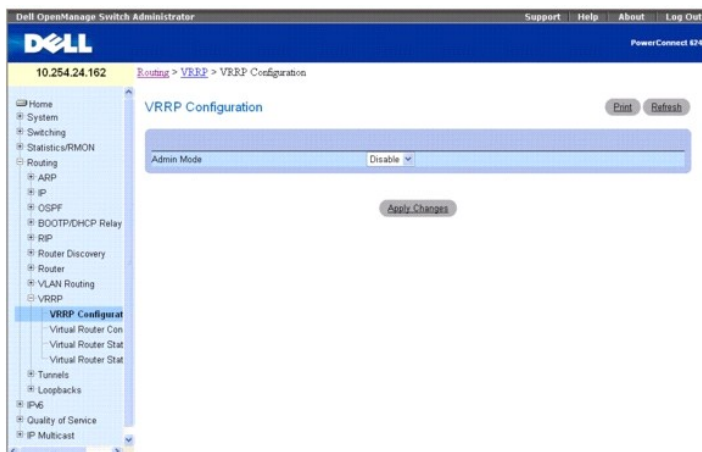
- 1 [VRRP 구성](#)
- 1 [가상 라우터 구성](#)
- 1 [가상 라우터 상태](#)
- 1 [가상 라우터 통계](#)

VRRP 구성

VRRP Configuration(VRRP 구성) 페이지를 사용하여 가상 라우터의 관리 상태를 활성화하거나 비활성화할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)→ VRRP→ VRRP Configuration(VRRP 구성)**을 클릭합니다.

그림 10-38. VRRP Configuration(VRRP 구성)



VRRP Configuration(VRRP 구성) 페이지에는 다음 필드가 있습니다.

Admin Mode(관리 모드) — 라우터의 VRRP 관리 상태를 활성 또는 비활성으로 설정합니다. 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하십시오. 기본값은 Disable(비활성)입니다.

CLI 명령을 사용하여 VRRP 상태 변경

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

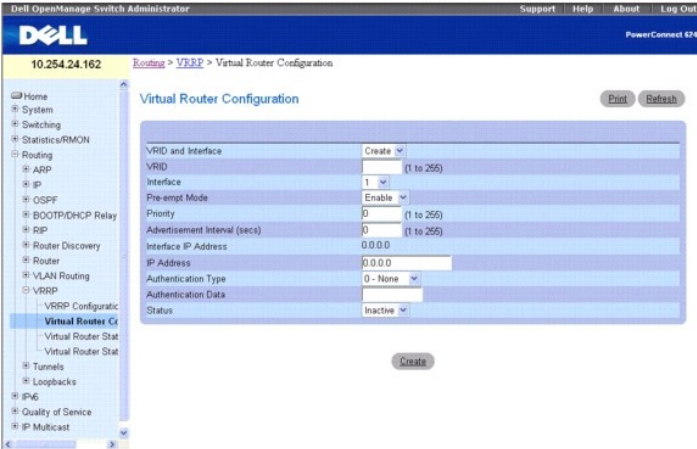
- 1 가상 라우터 중복 프로토콜 명령

가상 라우터 구성

Virtual Router Configuration(가상 라우터 구성) 페이지를 사용하여 새 가상 라우터를 만들거나 기존 가상 라우터를 구성할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅) → VRRP → Virtual Router Configuration(가상 라우터 구성)**을 클릭합니다.

그림 10-39. Virtual Router Configuration(가상 라우터 구성)



Virtual Router Configuration(가상 라우터 구성) 페이지에는 다음 필드가 있습니다.

VRID and Interface(VRID 및 인터페이스) — 드롭다운 메뉴에서 Create(만들기)를 선택하여 새 가상 라우터를 구성하거나 인터페이스 번호 및 VRID별로 나열된 기존 가상 라우터 중 하나를 선택합니다.

VRID — 이 필드는 새 가상 라우터를 만드는 경우에만 구성할 수 있으며, 1 ~ 255 범위의 VRID를 입력합니다.

Interface(인터페이스) — 이 필드는 새 가상 라우터를 만드는 경우에만 구성할 수 있으며, 드롭다운 메뉴에서 새 가상 라우터에 대한 인터페이스를 선택합니다.

Pre-empt Mode(예방 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택한 경우 마스터가 가상 라우터 IP 주소의 소유자가 아니고 백업 라우터의 우선 순위가 마스터 가상 라우터의 우선 순위보다 크면 백업 라우터가 마스터 라우터를 예방합니다. 기본값은 Enable(활성)입니다.

Priority(우선 순위) — 마스터 가상 라우터를 선택할 때 VRRP 라우터에서 사용할 우선 순위 값을 입력합니다. 가상 IP 주소가 인터페이스 IP 주소와 같으면 어떤 값을 입력하든 관계없이 우선 순위는 255로 설정됩니다. 가상 IP 주소와 인터페이스 IP 주소가 같지 않을 때 우선 순위를 255로 입력하면 우선 순위가 기본값인 100으로 설정됩니다.

Advertisement Interval(secs)(알림 간격(초)) — 이 가상 라우터의 알림 패킷 전송 간격(초)을 입력합니다. 1 ~ 255 사이의 숫자를 입력합니다. 기본값은 1초입니다.

Interface IP Address(인터페이스 IP 주소) — 선택된 인터페이스와 연관된 IP 주소를 나타냅니다.

IP Address(IP 주소) — 가상 라우터와 연관된 IP 주소를 입력합니다. 기본값은 0.0.0.0으로, **Create(만들기)**를 누르기 전에 이 값을 변경해야 합니다.

Authentication Type(인증 유형) — 드롭다운 메뉴에서 가상 라우터에 대한 인증 유형을 선택합니다. 기본값은 None(없음)입니다. 선택 항목은 다음과 같습니다:

- 1 **0-None(0-없음)** — 인증이 수행되지 않습니다.
- 1 **1-Simple(1-단순)** — 텍스트 암호를 사용하여 인증이 수행됩니다.

Authentication Data(인증 데이터) — 단순 인증을 선택한 경우 암호를 입력합니다.

Status(상태) — 가상 라우터의 작업을 시작하거나 중지하려면 드롭다운 메뉴에서 Active(활성) 또는 Inactive(비활성)를 선택합니다. 기본값은 Inactive(비활성)입니다.

보조 VRRP 주소를 구성하려면 먼저 VR에 대해 하나의 IP 주소(기본 주소)를 구성합니다. 그런 다음 해당 인터페이스에 여러 개의 보조 주소를 추가할 수 있습니다.

새 가상 라우터 만들기

1. **Virtual Router Configuration(가상 라우터 구성)** 페이지를 엽니다.
2. VRID and Interface(VRID 및 인터페이스) 드롭다운 메뉴에서 **Create(만들기)**를 선택합니다.

3. 새 가상 라우터에 대한 VRID 및 인터페이스를 지정합니다.
 4. 필요에 따라 나머지 필드를 정의합니다.
 5. **Create(만들기)**를 클릭합니다.
- 새 가상 라우터가 저장되고 장치가 업데이트됩니다.

가상 라우터 구성

1. **Virtual Router Configuration(가상 라우터 구성)** 페이지를 엽니다.
 2. 구성할 가상 라우터의 VRID 및 인터페이스를 선택합니다.
 3. 필요에 따라 필드를 변경합니다.
 4. **Apply Changes(변경사항 적용)**를 클릭하십시오.
- 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 가상 라우터 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 가상 라우터 중복 프로토콜 명령

가상 라우터 상태

Virtual Router Status(가상 라우터 상태) 페이지를 사용하여 가상 라우터 상태를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**VRPP**→**Virtual Router Status(가상 라우터 상태)**를 클릭합니다.

그림 10-40. Virtual Router Status(가상 라우터 상태)

VRID	VLANID	Priority	Preempt Mode	Advertisement Interval(sec)	Virtual Ip Address	Interface Ip Address	Owner	VMAC Address
20	vlan200	4	Enable	1	10.50.50.50	192.168.30.15	False	00:00:5E:00:01:01
110	vlan300	80	Disable	30	10.90.90.52	0.0.0.0	False	00:00:5E:00:01:01

Virtual Router Status(가상 라우터 상태) 페이지에는 다음 필드가 있습니다.

VRID — 가상 라우터 식별자입니다.

VLANID - VRID와 연관된 인터페이스를 나타냅니다.

Priority(우선 순위) — 마스터 가상 라우터를 선택할 때 VRRP 라우터에서 사용할 우선 순위 값입니다.

Pre-empt Mode(예방 모드)

- 1 **Enable(활성)** — 가상 라우터에 백업 라우터가 있는 경우 마스터가 가상 라우터 IP 주소의 소유자가 아니고 백업 라우터의 우선 순위가 마스터 가상 라우터의 우선 순위보다 크면 백업 라우터가 마스터 라우터를 예방합니다.
- 1 **Disable(비활성)** — 가상 라우터에 백업 라우터가 있는 경우 가상 라우터의 우선 순위가 더 커도 마스터 라우터를 예방하지 않습니다.

Advertisement Interval(secs)(알림 간격(초)) — 이 가상 라우터의 알림 패킷 전송 간격(초)입니다.

Virtual IP Address(가상 IP 주소) — 가상 라우터와 연관된 IP 주소입니다.

Interface IP Address(인터페이스 IP 주소) — 가상 라우터에서 사용할 인터페이스와 연관된 실제 IP 주소입니다.

Owner(소유자) — 가상 IP 주소와 인터페이스 IP 주소가 같으면 True로 설정되고 그렇지 않으면 False로 설정됩니다. 이 매개 변수가 True로 설정되면 가상 라우터는 가상 IP 주소의 소유자가 되고 활성화된 경우 항상 마스터 라우터로 선택됩니다.

VMAC Address(VMAC 주소) — 가상 라우터와 연관된 가상 MAC 주소로, 조직에서 고유한 24비트 식별자, VRRP 주소 블록을 식별하는 16비트 상수 및 8비트 VRID로 구성됩니다. 가상 MAC 주소는 00:00:5e:00:01:XX이고, 여기서 XX는 VRID입니다.

Auth Type(인증 유형) — 가상 라우터에 사용되는 인증 유형입니다.

- 1 None(없음) — 인증 유형을 None(없음)으로 지정합니다.
- 1 Simple(단순) — 인증 유형을 단순 텍스트 암호로 지정합니다.

State(상태) — 가상 라우터의 현재 상태입니다.

- 1 Initialize(초기화)
- 1 Master(마스터)
- 1 Backup(백업)

Status(상태) — 가상 라우터의 현재 상태입니다.

- 1 Inactive(비활성)
- 1 Active

Secondary IP Address(보조 IP 주소) — 기본 VRRP에 대해 구성된 보조 VRRP 주소입니다.

CLI 명령을 사용하여 가상 라우터 상태 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 가상 라우터 중복 프로토콜 명령

가상 라우터 통계

Virtual Router Statistics(가상 라우터 통계) 페이지를 사용하여 지정된 가상 라우터에 대한 통계를 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **VRRP** → **Virtual Router Statistics(가상 라우터 통계)**를 클릭합니다.

그림 10-41. Virtual Router Statistics(가상 라우터 통계)

Statistic	Value
Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
VRID and VLAN	20 - vlan200
VRID	20
VLAN	vlan200
Up Time	0 days 0 hrs 32 mins 40 secs
State Transitioned to Master	1
Advertisement Received	1834
Advertisement Interval Errors	0
Authentication Failure	0
IP TTL Errors	0
Zero Priority Packets Received	0
Zero Priority Packets Sent	0
Invalid Type Packets Received	0
Address List Errors	0
Invalid Authentication Type	0
Authentication Type Mismatch	0
Packet Length Errors	0

Virtual Router Statistics(가상 라우터 통계) 페이지에는 다음 필드가 있습니다. 이러한 필드는 대부분 유효한 VRRP 구성이 있는 경우에만 표시됩니다.

Router Checksum Errors(라우터 검사 합 오류) — VRRP 검사 합 값이 유효하지 않은, 수신된 총 VRRP 패킷 수입니다.

Router Version Errors(라우터 버전 오류) — 버전 번호가 알 수 없거나 지원되지 않는, 수신된 총 VRRP 패킷 수입니다.

Router VRID Errors(라우터 VRID 오류) — VRID가 이 가상 라우터에 유효하지 않은, 수신된 총 VRRP 패킷 수입니다.

VRID and VLAN ID(VRID 및 VLAN ID) — 인터페이스 번호 및 VRID별로 나열된 기존 가상 라우터 중에서 통계 정보를 표시할 가상 라우터를 선택합니다.

VRID — 선택된 가상 라우터에 대한 VRID입니다.

VLAN ID — 선택된 가상 라우터에 대한 인터페이스입니다.

Up Time(작동 시간) — 가상 라우터가 초기화된 상태로 전환되기까지의 경과 시간(일, 시간, 분 및 초)입니다.

State Transitioned to Master(상태가 마스터로 전환된 횟수) — 이 가상 라우터의 상태가 마스터로 전환된 총 횟수입니다.

Advertisement Received(수신된 알람) — 이 가상 라우터에 수신된 총 VRRP 알람 수입니다.

Advertisement Interval Errors(알람 간격 오류) — 알람 간격이 로컬 가상 라우터에 대해 구성된 간격과 다른, 수신된 총 VRRP 알람 패킷 수입니다.

Authentication Failure(알림 실패) — 인증 검사를 통과하지 못한, 수신된 총 VRRP 패킷 수입니다.

IP TTL Errors(IP TTL 오류) — IP TTL(Time-To-Live)이 255와 같지 않은, 가상 라우터에 수신된 총 VRRP 패킷 수입니다.

Zero Priority Packets Received(수신된 우선 순위 0 패킷) — 우선 순위가 0인, 가상 라우터에 수신된 총 VRRP 패킷 수입니다.

Zero Priority Packets Sent(전송된 우선 순위 0 패킷) — 우선 순위가 0인, 가상 라우터에서 전송된 총 VRRP 패킷 수입니다.

Invalid Type Packets Received(수신된 유효하지 않은 유형 패킷) — Type(유형) 필드 값이 유효하지 않은, 가상 라우터에 수신된 총 VRRP 패킷 수입니다.

Address List Errors(주소 목록 오류) — 주소 목록이 가상 라우터에 대해 로컬에서 구성된 목록과 일치하지 않는, 수신된 총 패킷 수입니다.

Invalid Authentication Type(유효하지 않은 인증 유형) — 인증 유형을 알 수 없는, 수신된 총 패킷 수입니다.

Authentication Type Mismatch(인증 유형 불일치) — 인증 유형이 로컬에서 구성된 인증 방법과 다른, 수신된 총 패킷 수입니다.

Packet Length Errors(패킷 길이 오류) — 패킷 길이가 VRRP 헤더 길이보다 작은, 수신된 총 패킷 수입니다.

가상 라우터 통계 표시

1. **Virtual Router Statistics(가상 라우터 통계)** 페이지를 엽니다.
2. **VRID** 및 **VLANID** 필드에서 통계 정보를 표시할 가상 라우터를 선택합니다. 이 정보는 유효한 VRRP 구성이 있는 경우에만 표시됩니다.

CLI 명령을 사용하여 가상 라우터 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 가상 라우터 중복 프로토콜 명령

터널

6200 시리즈는 터널 인터페이스의 생성, 삭제 및 관리 기능을 제공합니다. 이러한 기능은 사용자 구성을 통해 생성 및 삭제되는 동적 인터페이스입니다.

IPv4 네트워크를 IPv6 네트워크로 쉽게 전환할 수 있도록 하는 구성형 및 자동 터널 클래스가 있습니다. 두 클래스의 차이점은 구성된 터널은 터널의 대상 또는 종단점을 사용하여 명시적으로 구성되는 반면 자동 터널은 터널로 라우팅된 패킷의 대상 주소에서 터널의 종단점을 유추한다는 것입니다.

6200 시리즈는 지정대 지정 터널을 지원합니다. 지정대 지정 인터페이스는 인터페이스만 기준으로 라우팅을 제공하며(다음 홉 주소를 명시적으로 지정할 필요가 없음) 번호가 지정되지 않은 인터페이스 정의를 허용합니다.

Tunnels(터널) 메뉴 페이지에는 터널 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**Tunnels(터널)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

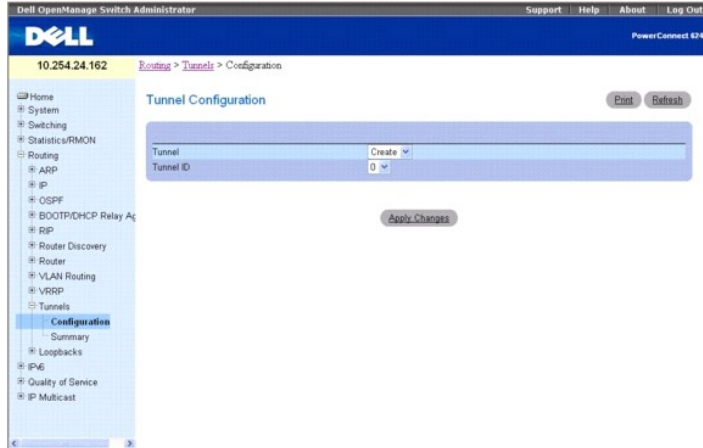
- 1 [터널 구성](#)
- 1 [터널 요약](#)

터널 구성

Tunnels Configuration(터널 구성) 페이지를 사용하여 터널을 생성, 구성 또는 삭제할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)**→**Tunnels(터널)**→**Configuration(구성)**을 클릭합니다.

그림 10-42. Tunnels Configuration(터널 구성)



Tunnels Configuration(터널 구성) 페이지에는 다음 필드가 있습니다.

Tunnel(터널) — 드롭다운 메뉴를 사용하여 현재 구성된 터널 ID 목록에서 선택합니다. 최대 터널 인터페이스 수가 생성되지 않은 경우에는 Create(만들기) 작업을 수행할 수도 있습니다.

Tunnel ID(터널 ID) — 터널 선택 항목에서 Create(만들기)를 선택하면 사용 가능한 터널 ID 목록이 표시됩니다. 페이지의 나머지 필드를 표시하려면 새 터널과 연결할 터널 ID를 선택하고 **Apply Changes(변경사항 적용)**를 클릭해야 합니다.

Mode(모드) — 터널 모드에 대한 선택 항목입니다. 지원되는 모드는 IPv6-in-IPv4(IPv4 내의 IPv6)뿐입니다.

Link Local Only Mode(링크 로컬 전용 모드) — 링크 로컬 주소를 사용하여 이 인터페이스에서 IPv6을 활성화합니다. 이 옵션은 명시적 IPv6 주소를 지정하기 전에만 구성할 수 있습니다.

IPv6 Address(IPv6 주소) — 선택된 터널 인터페이스의 IPv6 주소를 선택합니다. 최대 주소 수가 구성되어 있지 않은 경우에는 추가 작업을 수행할 수도 있습니다.

IPv6 Address(IPv6 주소) — IPv6 Address(IPv6 주소) 선택 항목에서 Add(추가)를 선택하면 이 IPv6 주소 입력 필드가 표시됩니다. 주소는 점두어/길이 형식으로 입력해야 합니다.

64비트 확장 고유 식별자(EUI-64)를 지정할 수도 있습니다.

Source(소스) — IPv4 Address(IPv4 주소) 또는 Interface(인터페이스) 중에서 원하는 소스를 선택합니다. Address(주소)를 선택한 경우 이 터널의 소스 주소를 정으로 된 10진수 표기법으로 입력해야 합니다. Interface(인터페이스)를 선택한 경우 이 터널의 소스 인터페이스를 선택해야 합니다. 선택된 인터페이스와 연관된 주소가 소스 주소로 사용됩니다.

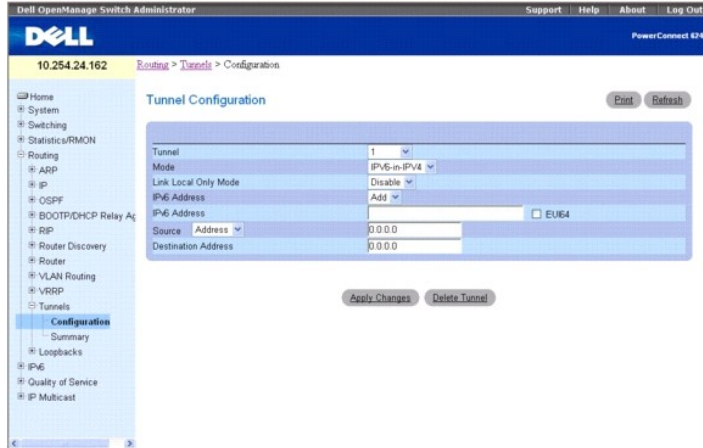
Destination Address(대상 주소) — 정으로 된 10진수 표기법을 사용한 이 터널의 IPv4 대상 주소입니다.

새 터널 만들기

1. Tunnels Configuration(터널 구성) 페이지를 엽니다.
2. Tunnel(터널) 드롭다운 메뉴에서 Create(만들기)를 선택합니다.
3. Tunnel ID(터널 ID) 필드에서 사용할 ID를 지정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

터널 ID(터널 ID) 필드가 제거되고 나머지 터널 필드가 표시됩니다.

그림 10-43. Tunnels Configuration - Entry(터널 구성 - 항목)



5. 필요에 따라 필드를 구성합니다.
6. 나머지 필드에 원하는 값을 입력합니다.
7. **Apply Changes(변경사항 적용)**를 클릭하십시오.
새 터널이 저장되고 장치가 업데이트됩니다.

기존 터널 수정

1. **Tunnels Configuration(터널 구성)** 페이지를 엽니다.
2. **Tunnel(터널)** 드롭다운 메뉴에서 수정할 터널을 지정합니다.
3. 나머지 필드에서 필드 값을 원하는 대로 변경합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.
새 구성이 저장되고 장치가 업데이트됩니다.

터널 제거

1. **Tunnels Configuration(터널 구성)** 페이지를 엽니다.
2. **Tunnel(터널)** 드롭다운 메뉴에서 제거할 터널을 지정합니다.
3. **Delete Tunnel(터널 삭제)**을 클릭합니다.
터널이 삭제되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 터널 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

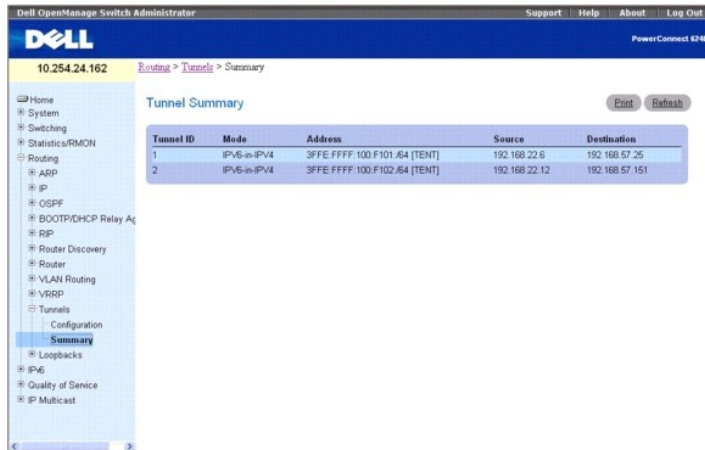
1. 터널 인터페이스 명령

터널 요약

Tunnels Summary(터널 요약) 페이지를 사용하여 구성된 터널 요약을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Tunnels(터널)** → **Summary(요약)**를 클릭합니다.

그림 10-44. Tunnels Summary(터널 요약)



Tunnels Summary(터널 요약) 페이지에는 다음 필드가 있습니다.

Tunnel ID(터널 ID) — 터널 ID입니다.

Mode(모드) — 해당하는 터널 모드입니다.

Address(주소) — 터널의 IPv6 주소입니다.

Source(소스) — 해당하는 터널 소스 주소입니다. 인터페이스를 구성한 경우 인터페이스와 주소가 모두 표시됩니다. 소스 인터페이스에 주소가 구성되어 있지 않으면 주소 대신 'unconfigured(구성 안 됨)'라는 텍스트가 표시됩니다.

Destination(대상) — 해당하는 터널 대상 주소입니다.

CLI 명령을 사용하여 터널 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 터널 인터페이스 명령

루프백

6200 시리즈는 루프백 인터페이스의 생성, 삭제 및 관리 기능을 제공합니다. 이러한 기능은 사용자 구성을 통해 생성 및 삭제되는 동적 인터페이스입니다. 6200 시리즈는 여러 개의 루프백 인터페이스를 지원합니다.

루프백 인터페이스는 항상 작동합니다. 따라서 다른 스위치에서 참조할 수 있는 안정적인 IP 주소를 장치에 구성하는 옵션을 제공합니다. 이 인터페이스는 전송된 패킷의 소스 주소를 제공하며 로컬 패킷과 원격 패킷을 모두 수신할 수 있습니다. 일반적으로 라우팅 프로토콜에서 이 인터페이스를 사용합니다.

루프백은 스위치 시스템의 네트워크 포트와 다른 방식으로 동작합니다. 특히 루프백 인터페이스에는 인접 항목이 없습니다. 이 주소로 라우터와 통신할 수 있도록 로컬 주소를 지정하는 의사 장치이므로 항상 작동하며 기존의 모든 활성 인터페이스에서 트래픽을 수신할 수 있습니다. 원격 클라이언트에서 접근할 수 있는 경우 루프백 주소를 사용하여 텔넷 및 ssh 같은 다양한 서비스를 통해 라우터와 통신할 수 있습니다. 이런 방식으로 루프백 주소는 수신되는 패킷 처리와 관련해서 라우터의 로컬 주소와 동일하게 동작합니다.

Loopbacks(루프백) 메뉴 페이지에는 루프백 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Loopbacks(루프백)**을 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

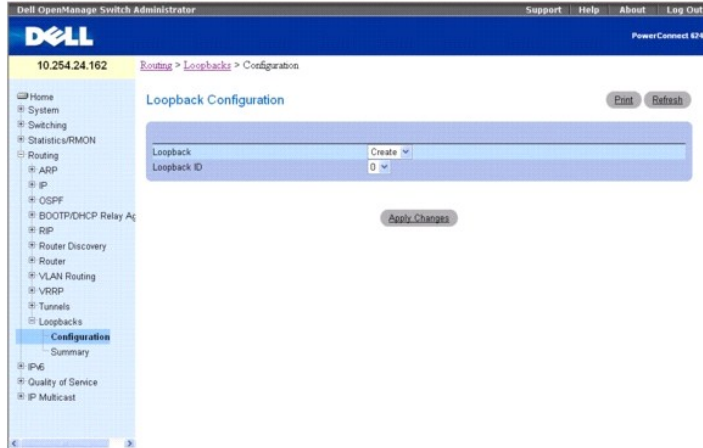
- 1 루프백 구성
- 1 루프백 요약

루프백 구성

Loopbacks Configuration(루프백 구성) 페이지를 사용하여 루프백 인터페이스를 생성, 구성 또는 제거할 수 있습니다. 루프백의 보조 주소를 설정하거나 삭제할 수도 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Loopbacks(루프백)** → **Configuration(구성)**을 클릭합니다.

그림 10-45. Loopback Configuration(루프백 구성)



Loopback Configuration(루프백 구성) 페이지에는 다음 필드가 있습니다.

Loopback(루프백) — 드롭다운 메뉴를 사용하여 현재 구성된 루프백 인터페이스 목록에서 선택합니다. 최대 루프백 인터페이스 수가 생성되지 않은 경우에는 Create(만들기) 작업을 수행할 수도 있습니다.

Loopback ID(루프백 ID) — Loopback(루프백) 필드에서 Create(만들기)를 선택하면 사용 가능한 루프백 ID 목록이 표시됩니다.

Protocol(프로토콜) — IPv4 또는 IPv6을 선택하여 루프백 인터페이스에 해당 속성을 구성합니다. 선택된 프로토콜에 따라 이 페이지에 표시되는 필드가 달라집니다.

Link Local Only Mode(링크 로컬 전용 모드) — 링크 로컬 주소를 사용하여 이 인터페이스에서 IPv6을 활성화합니다. 이 옵션은 지정된 프로토콜이 IPv6인 경우에만 표시되며 명시적 IPv6 주소를 지정하기 전에만 구성할 수 있습니다.

IPv6 Address(IPv6 주소) — 선택된 루프백 인터페이스에 대해 구성된 IPv6 주소 목록을 선택합니다. 최대 주소 수가 구성되어 있지 않은 경우에는 추가 작업을 수행할 수도 있습니다. 이 옵션은 지정된 프로토콜이 IPv6인 경우에만 표시됩니다.

IPv6 Address(IPv6 주소) — IPv6 Address(IPv6 주소) 선택 항목에서 Add(추가)를 선택하면 이 IPv6 주소 입력 필드가 표시됩니다. 점두어/길어 형식으로 주소를 입력하십시오. 이 옵션은 지정된 프로토콜이 IPv6인 경우에만 표시됩니다.

EU164 — 64비트 확장 고유 식별자(EUI-64)를 지정할 수도 있습니다. 이 옵션은 지정된 프로토콜이 IPv6인 경우에만 표시됩니다.

IPv4 Address(IPv4 주소) — 점으로 된 10진수 표기법을 사용한 이 인터페이스의 기본 IPv4 주소입니다. 이 옵션은 지정된 프로토콜이 IPv4인 경우에만 표시됩니다.

IPv4 Subnet Mask(IPv4 서브네트 마스크) — 점으로 된 10진수 표기법을 사용한 이 인터페이스의 기본 IPv4 서브네트 마스크입니다. 이 옵션은 지정된 프로토콜이 IPv4인 경우에만 표시됩니다.

다음 필드는 기본 주소를 구성한 경우에 표시됩니다. 여러 개의 보조 주소를 구성할 수 있습니다.

Secondary Address(보조 주소) — 드롭다운 메뉴에서 선택된 루프백 인터페이스에 대해 구성된 IPv4 보조 주소를 선택합니다. 최대 보조 주소 수가 구성되지 않은 경우 여기서 Add Secondary IP Address(보조 IP 주소 추가)를 선택하면 Secondary IP Address(보조 IP 주소) 필드에 새 주소를 입력할 수 있습니다. 보조 주소를 추가하려면 먼저 기본 주소를 구성해야 합니다.

Secondary IP Address(보조 IP 주소) — 점으로 된 10진수 표기법을 사용한 이 인터페이스의 보조 IP 주소입니다. 이 입력 필드는 Add Secondary(보조 항목 추가)를 선택한 경우에만 표시됩니다.

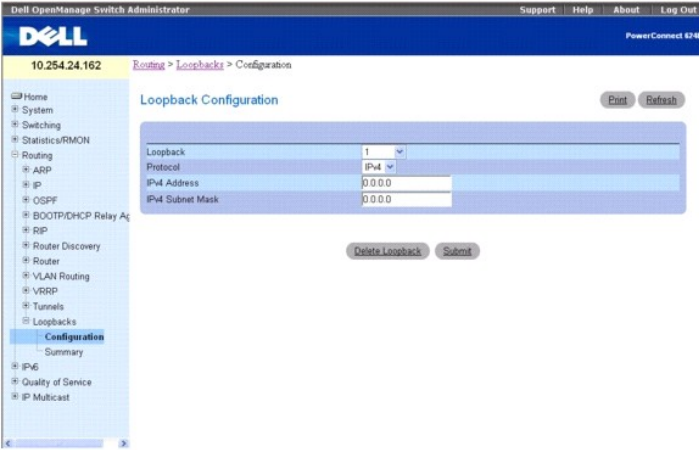
Secondary Subnet Mask(보조 서브네트 마스크) — 점으로 된 10진수 표기법을 사용한 이 인터페이스의 보조 서브네트 마스크입니다. 이 입력 필드는 Add Secondary(보조 항목 추가)를 선택한 경우에만 표시됩니다.

새 루프백 만들기(IPv4)

1. Loopbacks Configuration(루프백 구성) 페이지를 엽니다.
2. Loopback(루프백) 드롭다운 메뉴에서 Create(만들기)를 선택합니다.
3. Loopback ID(루프백 ID) 필드에서 사용할 ID를 지정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

Loopback ID(루프백 ID) 필드가 사라지고 나머지 루프백 필드가 표시됩니다.

그림 10-46. Loopbacks Configuration - IPv4 Entry(루프백 구성 - IPv4 항목)



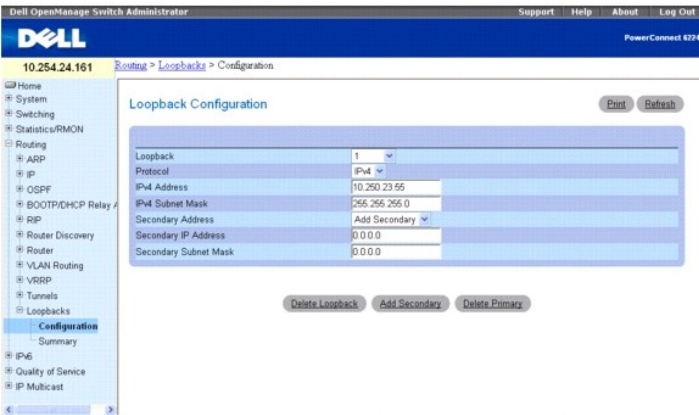
5. Protocol(프로토콜) 필드에 IPv4를 입력합니다.

6. 나머지 필드에 원하는 값을 입력합니다.

7. Submit(제출)를 클릭합니다.

새 루프백이 저장되고 보조 주소 구성 필드를 표시하는 웹 페이지가 다시 나타납니다.

그림 10-47. Loopback Configuration - Add Secondary Address(루프백 구성 - 보조 주소 추가)



8. Secondary Address(보조 주소), Secondary IP Address(보조 IP 주소) 및 Secondary Subnet Mask(보조 서브넷 마스크) 필드를 입력합니다.

9. Add Secondary(보조 주소 추가) 단추를 클릭합니다. 보조 주소가 저장되고 기본 및 보조 루프백 주소를 표시하는 웹 페이지가 다시 나타납니다.

새 루프백 만들기(IPv6)

1. Loopbacks Configuration(루프백 구성) 페이지를 엽니다.

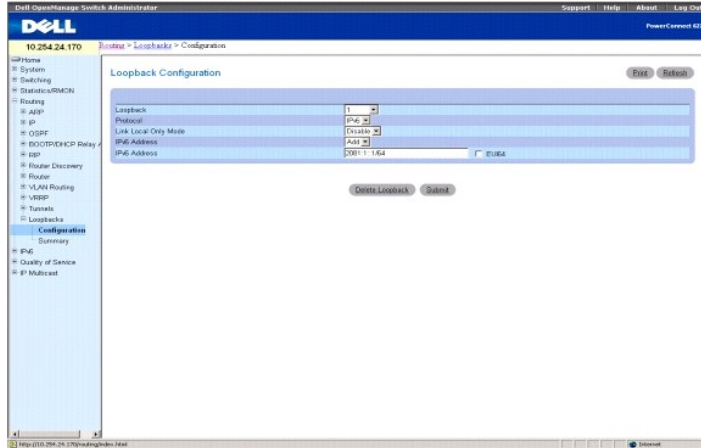
2. Loopback(루프백) 드롭다운 메뉴에서 Create(만들기)를 선택합니다.

3. Loopback ID(루프백 ID) 필드에서 사용할 ID를 지정합니다.

4. Apply Changes(변경사항 적용)를 클릭합니다.

Loopback ID(루프백 ID) 필드가 사라지고 나머지 루프백 필드가 표시됩니다.

그림 10-48. Loopbacks Configuration - IPv6 Entry(루프백 구성 - IPv6 항목)



5. Protocol(프로토콜) 필드의 드롭다운 상자에서 IPv6을 선택합니다.
6. IPv6 Address(IPv6 주소)를 추가합니다.
7. 나머지 필드에 원하는 값을 입력합니다.
8. Submit(제출)를 클릭합니다.

새 루프백이 저장되고 장치가 업데이트됩니다.

기존 루프백 구성

1. Loopback Configuration(루프백 구성) 페이지를 엽니다.
2. Loopback(루프백) 드롭다운 메뉴에서 구성할 루프백을 지정합니다.
3. 나머지 필드에서 필드 값을 원하는 대로 변경합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

새 구성이 저장되고 장치가 업데이트됩니다.

루프백 제거

1. Loopback Configuration(루프백 구성) 페이지를 엽니다.
2. Loopback(루프백) 드롭다운 메뉴에서 제거할 루프백을 지정합니다.
3. Delete Loopback(루프백 삭제)를 클릭합니다.

루프백이 삭제되고 장치가 업데이트됩니다.

보조 주소 제거

1. Loopback Configuration(루프백 구성) 페이지를 엽니다.
2. 영향을 받을 루프백을 지정합니다.
3. 제거할 보조 주소를 지정합니다.
4. Delete Selected Secondary(선택된 보조 주소 삭제)를 클릭합니다.

보조 주소가 삭제되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 루프백 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

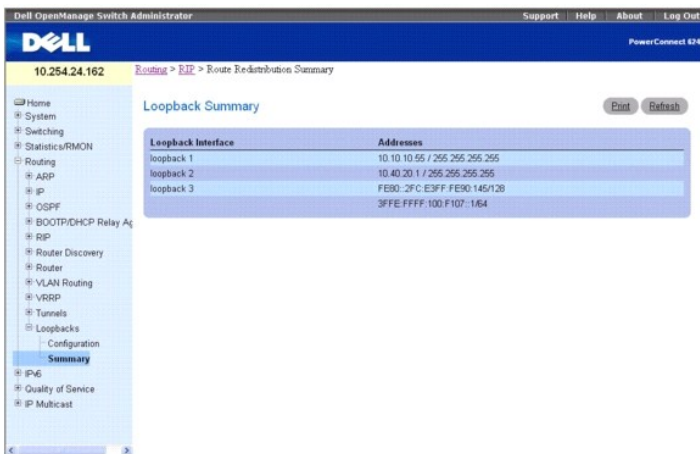
- 1 루프백 인터페이스 명령
- 1 IP 주소 지정 명령
- 1 IPv6 라우팅 명령

루프백 요약

Loopbacks Summary(루프백 요약) 페이지를 사용하여 구성된 루프백 요약을 표시할 수 있습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Routing(라우팅)** → **Loopbacks(루프백)** → **Summary(요약)**를 클릭합니다.

그림 10-49. Loopbacks Summary(루프백 요약)



Loopbacks Summary(루프백 요약) 페이지에는 다음 필드가 있습니다.

Loopback Interface(루프백 인터페이스) — 구성된 루프백 인터페이스의 ID입니다.

Addresses(주소) — 루프백 인터페이스에 구성된 주소 목록입니다.

CLI 명령을 사용하여 루프백 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 루프백 인터페이스 명령

[목차 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

IPv6 구성

Dell™ PowerConnect™ M6220 사용 설명서

- [전역 구성](#)
- [인터페이스 구성](#)
- [인터페이스 요약](#)
- [IPv6 통계](#)
- [IPv6 인접 항목 표](#)
- [DHCPv6](#)
- [OSPFv3](#)
- [IPv6 경로](#)

IPv6은 차세대 인터넷 프로토콜입니다. 32비트 주소를 사용하는 IPv4와 달리 IPv6은 128비트 주소를 지원함으로써 IPv4에서 겪은 주소 부족 문제를 해결하고, 지정된 네트워크에 필요한 전역 고유 IP 주소의 수를 줄이기 위해 IPv4 네트워크에서 사용된 NAT(네트워크 주소 변환)에 대한 필요성을 제거했습니다. 집계 주소는 잘 알려진 주소 조합을 통해 전역 라우팅표의 크기를 현저히 줄일 수 있습니다. 보안이 훨씬 통합되고 네트워크 구성이 단순화된 반면 유연성이 향상되었습니다.

6200 시리즈는 IPv6과 IPv4를 동시에 지원합니다. IPv4와 마찬가지로 루프백 및 VLAN 인터페이스에서 IPv6 라우팅을 사용할 수 있으며, IPv4, IPv6 또는 둘 모두에 대해 각 L3 라우팅 인터페이스를 사용할 수 있습니다. L3를 통해 유입되는 IP 프로토콜(예: UDP 및 TCP)은 IPv6에서 변경되지 않습니다. 이러한 이유로 IPv4 및 IPv6의 전송에 단일 CPU 스택이 사용되며 단일 소켓 인터페이스가 IPv4 및 IPv6 모두에 대한 액세스를 제공합니다. 라우팅 프로토콜은 하나 또는 두 개의 IP 버전에 대해 경로를 계산할 수 있습니다.

IPv6 *메뉴* 페이지에는 다음 기능에 대한 링크가 있습니다.

- 1 [전역 구성](#)
- 1 [인터페이스 구성](#)
- 1 [인터페이스 요약](#)
- 1 [IPv6 통계](#)
- 1 [IPv6 인접 항목 표](#)
- 1 [DHCPv6](#)
- 1 [OSPFv3](#)
- 1 [IPv6 경로](#)

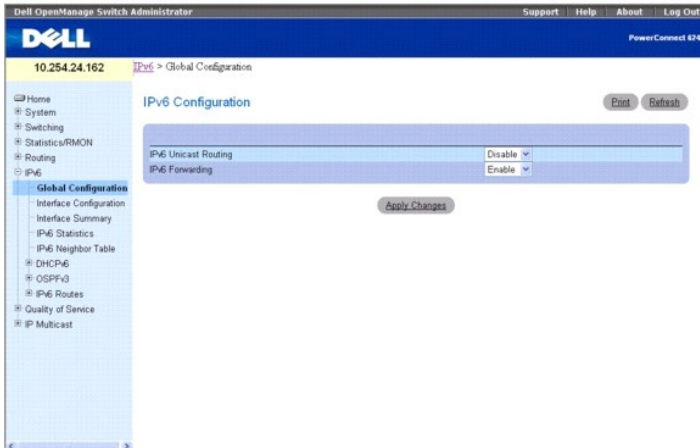
 **주:** 일부 IPv6 페이지에서는 CLI 명령을 사용할 수 없습니다.

전역 구성

Global Configuration(전역 구성) 페이지를 사용하여 라우터에서 IPv6 전달을 사용하도록 설정하고 IPv6 유니캐스트 데이터그램의 전달을 활성화합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **Global Configuration(전역 구성)**을 클릭합니다.

그림 11-1. IPv6 Global Settings(IPv6 전역 구성)



IPv6 Global Configuration(IPv6 전역 구성) 페이지에는 다음과 같은 필드가 있습니다.

IPv6 Unicast Routing(IPv6 유니캐스트 라우팅) — 라우터에서 IPv6 유니캐스트 라우팅을 전역으로 활성화하거나 비활성화합니다. 기본값은 Disable(비활성)입니다.

IPv6 Forwarding(IPv6 전달) — 라우터에서 IPv6 프레임의 전달을 활성화하거나 비활성화합니다. 기본값은 Enable(활성)입니다.

IPv6 매개변수 구성

1. **IPv6 Global Configuration(IPv6 전역 구성)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 유니캐스트 라우팅을 활성화하거나 비활성화합니다.
3. 드롭다운 메뉴에서 IPv6 프레임 전달을 활성화하거나 비활성화합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

설정이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IPv6 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. IPv6 라우팅 명령

인터페이스 구성

Interface Configuration(인터페이스 구성) 페이지를 사용하여 IPv6 인터페이스 매개변수를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→ Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 11-2. IPv6 Interface Configuration(IPv6 인터페이스 구성)



IPv6 Interface Configuration(IPv6 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 구성할 인터페이스를 선택합니다. 선택을 변경하면 화면이 재생되어 새로 선택된 포트에 대해 모든 필드가 업데이트됩니다. 라우팅을 사용하는 인터페이스와 터널만 표시됩니다.

IPv6 Mode(IPv6 모드) — IPv6 모드를 활성화하면 인터페이스에서 전역 주소 없이 IPv6를 작동할 수 있습니다. 이 경우 EUI-64 기반의 링크 로컬 주소가 사용됩니다. 이 선택기에는 IPv6 모드에 대해 Enable(활성) 및 Disable(비활성)의 두 가지 옵션이 제공됩니다. 기본값은 Disable(비활성)입니다.

IPv6 Prefix(IPv6 접두어) — 이 인터페이스에서 IPv6 접두어를 추가하거나 삭제하도록 선택합니다. 접두어를 추가하려면 다음 IPv6 Prefix(IPv6 접두어) 필드에 접두어를 지정합니다. **Delete(삭제)**를 클릭하면 표시된 IPv6 접두어가 삭제됩니다.

IPv6 Prefix(IPv6 접두어) — 인터페이스의 접두어 길이에 맞게 IPv6 접두어를 지정합니다. 선택 항목을 변경하면 화면이 새로 고쳐지고 선택한 IPv6 주소에 대한 유효 수명, 기본 수명, 온링크 플래그 및 자치 플래그가 업데이트됩니다.

EUI-64 — 이 확인란을 선택하면 64비트 유니캐스트 접두어를 지정합니다.

Valid Lifetime by Prefix(접두어별 유효 수명) — 라우터 알림에서 **Prefix Information(접두어 정보)** 옵션의 **Valid Lifetime(유효 수명)** 필드에 지정할 값(초)입니다. 접두어는 이러한 시간 길이에 대한 온링크 확인에 유효합니다. 상태 비저장 주소 자동 구성을 사용하여 이러한 접두어에서 주소를 생성하는 호스트는 시간 길이에 이러한 주소를 사용할 수 있습니다. 기본 수명보다 오래되었지만 유효 수명보다 짧은 자동 구성 주소는 "반대 주소"로 간주됩니다. RFC 2462에서 정의된 대로 반대 주소는 "사용을 권하지 않는 인터페이스에 할당되었지만 금지되지 않은 주소입니다. 반대 주소는 더 이상 새 통신에서 소스로 사용하지 않아야 하지만 반대 주소에서 전송된 패킷은 그대로 전달됩니다. 기본 주소로 전환하여 특정 상위 레이어 동작이 부족해질 수 있는 통신에서 소스 주소로 반대 주소를 계속 사용할 수 있습니다(예: 기존 TCP 연결)." 유효 범위는 0 ~ 4,294,967,295초입니다.

Preferred Lifetime by Prefix(접두어별 기본 수명) — 라우터 알림에서 **Prefix Information(접두어 정보)** 옵션의 **Preferred Lifetime(기본 수명)** 필드에 지정할 값(초)입니다. 상태 비저장 자동 구성을 사용하여 접두어에서 생성한 주소는 이 시간 길이에 "기본"으로 남습니다. RFC 2462에서 정의된 대로 기본 주소는 "상단 레이어 프로토콜 사용이 제한되지 않는 인터페이스에 할당된 주소입니다. 인터페이스에서 전송한 패킷의 소스(또는 대상) 주소로 기본 주소를 사용할 수 있습니다. 범위는 0 ~ 4,294,967,295초입니다.

Onlink Flag by Prefix(접두어별 온링크 플래그) — 온링크 확인을 위해 선택한 접두어를 지정합니다. 기본값은 Enable(활성)입니다. 이 선택기에는 온링크 플래그에 대해 Enable(활성) 및 Disable(비활성)의 두 가지 옵션이 제공됩니다.

Autonomous Flag by Prefix(접두어별 자치 플래그) — 자치 주소 구성을 위해 선택한 접두어를 지정합니다. 기본값은 Disable(비활성)입니다. 이 선택기에는 자치 플래그에 대해 Enable(활성) 및 Disable(비활성)의 두 가지 옵션이 제공됩니다.

Current State by Prefix(접두어별 현재 상태) — 선택한 IPv6 접두어에 대한 인터페이스 작동 상태입니다.

Routing Mode(라우팅 모드) — 인터페이스의 라우팅 모드를 지정합니다. 이 선택기에는 라우팅 모드에 대해 Enable(활성) 및 Disable(비활성)의 두 가지 옵션이 제공됩니다. 기본값은 Disable(비활성)입니다.

IPv6 Routing Operational Mode(IPv6 라우팅 작동 모드) — 인터페이스의 작동 상태를 지정합니다. 기본값은 Disable(비활성)입니다.

Interface Maximum Transmit Unit(인터페이스 최대 전송 단위) — 인터페이스의 최대 전송 단위를 지정합니다. 이 값이 0이면 인터페이스를 라우팅에 사용할 수 없습니다. 라우팅이 활성화되어 있으면 이 값을 0으로 설정할 수 없습니다. MTU의 유효한 범위는 1280 - 1500입니다.

Router Duplicate Address Detection Transmits(라우터 주소 중복 검사 전송) — 인터페이스의 주소 중복 검사 전송 횟수를 지정합니다. DAD 전송 값은 0 - 600 범위 내에 있어야 합니다.

Router Advertisement NS Interval(라우터 알림 NS 간격) — 인터페이스에서 전송된 라우터 알림의 재전송 시간 필드를 지정합니다. 값을 0으로 지정하면 이 라우터에 대해 간격이 지정되지 않았음을 의미합니다. 인접 간청 간격의 범위는 1000 - 4294967295입니다.

Router Lifetime Interval(라우터 수명 간격) — 인터페이스에서 전송된 라우터 알림 수명 필드를 지정합니다. 이 값은 최대 알림 간격보다 크거나 같아야 합니다. 값을 0으로 지정하면 라우터를 기본 라우터로 사용하지 않음을 의미합니다. 라우터 수명 범위는 0 - 9000입니다.

Router Advertisement Reachable Time(라우터 알림 연결 가능 시간) — ND 확인 후 연결 가능한 인접 항목을 고려하기 위한 라우터 알림 시간을 지정합니다. 연결 가능 시간 범위는 0 - 3600000입니다.

Router Advertisement Interval(라우터 알림 간격) — 인터페이스에서 전송되는 라우터 알림 간에 허용된 최대 시간을 지정합니다. 기본값은 600입니다. 최대 알림 간격 범위는 4 - 1800입니다.

Router Advertisement Managed Config Flag(라우터 알림 관리 주소 구성 플래그) — 라우터 알림 관리 주소 구성 플래그를 지정합니다. 활성화되면 최종 노드에서 DHCPv6를 사용합니다. 비활성이면 최종 노드에서 주소를 자동으로 구성합니다. 관리 플래그의 기본값은 Disable(비활성)입니다.

Router Advertisement Other Config Flag(라우터 알림 기타 구성 플래그) — 라우터 알림 기타 상태 구성 플래그를 지정합니다. 기타 구성 플래그의 기본값은 Disable(비활성)입니다.

Router Advertisement Suppress Flag(라우터 알림 표시 안 함 플래그) — 인터페이스의 라우터 알림 표시 안 함을 지정합니다. 표시 안 함 플래그의 기본값은 Disable(비활성)입니다.

IPv6 인터페이스 구성

1. **IPv6 Interface Configuration(IPv6 인터페이스 구성)** 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

IPv6 인터페이스 수정 사항이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IPv6 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. IPv6 라우팅 명령

인터페이스 요약

Interface Summary(인터페이스 요약) 페이지를 사용하여 모든 IPv6 인터페이스의 설정을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **Interface Summary(인터페이스 요약)**을 클릭합니다.

그림 11-3. IPv6 Interface Summary(IPv6 인터페이스 요약)

Interface	Routing Mode	Admin Mode	Operational Mode	IPv6 Prefix/Prefix Length	State	IPv6 Address	State
1/g1	Disabled	Enabled	Disabled				
1/g2	Disabled	Enabled	Disabled				
1/g3	Disabled	Enabled	Disabled				
1/g4	Disabled	Enabled	Disabled				
1/g5	Disabled	Enabled	Disabled				
1/g6	Disabled	Enabled	Disabled				
1/g7	Disabled	Enabled	Disabled				
1/g8	Disabled	Enabled	Disabled				
1/g9	Disabled	Enabled	Disabled				
1/g10	Disabled	Enabled	Disabled				
1/g11	Disabled	Enabled	Disabled				
1/g12	Disabled	Enabled	Disabled				
1/g13	Disabled	Enabled	Disabled				
1/g14	Disabled	Enabled	Disabled				
1/g15	Disabled	Enabled	Disabled				
1/g16	Disabled	Enabled	Disabled				
1/g17	Disabled	Enabled	Disabled				
1/g18	Disabled	Enabled	Disabled				
1/g19	Disabled	Enabled	Disabled				
1/g20	Disabled	Enabled	Disabled				

IPv6 Interface Summary(IPv6 인터페이스 요약) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 현재 표 행에 설정이 표시되는 인터페이스를 지정합니다.

Routing Mode(라우팅 모드) — 인터페이스의 라우팅 모드를 지정합니다.

Admin Mode(관리 모드) — 인터페이스의 관리 모드를 지정합니다.

Operational Mode(작동 모드) — 인터페이스의 작동 모드를 지정합니다.

IPv6 Prefix/PrefixLength(IPv6 접두어/접두어 길이) — 인터페이스에서 구성된 IPv6 주소를 지정합니다.

State(상태) — 인터페이스의 활성 여부를 지정합니다.

CLI 명령을 사용하여 IPv6 인터페이스 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 IPv6 라우팅 명령

IPv6 통계

IPv6 Statistics(IPv6 통계) 페이지를 사용하여 하나 또는 모든 인터페이스의 IPv6 트래픽 통계를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **IPv6 Statistics(IPv6 통계)**를 클릭합니다.

그림 11-4. IPv6 Statistics(IP 통계)

Interface	IPv6 Statistics	Value
All	Total Datagrams Received	0
All	Received Datagrams Locally Delivered	0
All	Received Datagrams Discarded Due To Header Errors	0
All	Received Datagrams Discarded Due To MTU	0
All	Received Datagrams Discarded Due To No Route	0
All	Received Datagrams With Unknown Protocol	0
All	Received Datagrams Discarded Due To Invalid Address	0
All	Received Datagrams Discarded Due To Truncated Data	0
All	Received Datagrams Discarded Other	0
All	Received Datagrams Reassembly Required	0
All	Datagrams Successfully Reassembled	0
All	Datagrams Failed To Reassemble	0
All	Datagrams Forwarded	0
All	Datagrams Locally Transmitted	0
All	Datagrams Transmit Failed	0

IPv6 Statistics(IPv6 통계) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 통계를 표시할 인터페이스를 선택합니다. 선택을 변경하면 화면이 재생되어 새로 선택된 인터페이스에 대해 모든 필드가 업데이트됩니다.

IPv6 통계

Total Datagrams Received(수신된 총 데이터그램 수) — 오류로 수신된 데이터그램을 포함하여 인터페이스에 수신된 총 입력 데이터그램 수입니다.

Received Datagrams Locally Delivered(로컬로 전달된 수신 데이터그램 수) — IPv6 사용자 프로토콜에 성공적으로 전달된 총 데이터그램 수(ICMP 포함)입니다. 이 카운터는 이러한 데이터그램이 전송된 인터페이스에서 증분되며 일부 데이터그램의 경우 입력 인터페이스가 아닐 수 있습니다.

Received Datagrams Discarded Due To Header Errors(헤더 오류로 인해 삭제된 수신 데이터그램 수) — 버전 번호 불일치, 기타 형식 오류, 초과된 홉 수, IPv6 옵션 처리 중 검색된 오류 등을 포함하여 IPv6 헤더의 오류로 인해 삭제된 입력 데이터그램 수입니다.

Received Datagrams Discarded Due To MTU(MTU로 인해 삭제된 수신 데이터그램 수) — 입력 데이터그램의 크기가 보내는 인터페이스의 링크 MTU를 초과했기 때문에 전송할 수 없는 입력 데이터그램 수입니다.

Received Datagrams Discarded Due To No Route(경로가 없어서 삭제된 수신 데이터그램 수) — 입력 데이터그램을 대상으로 전송할 경로가 없기 때문에 삭제된 입력 데이터그램 수입니다.

Received Datagrams With Unknown Protocol(알 수 없는 프로토콜로 수신된 데이터그램 수) — 성공적으로 수신되었지만 알 수 없거나 지원되지 않는 프로토콜로 인해 삭제된 로컬 수신 데이터그램 수입니다. 이 카운터는 이러한 데이터그램이 전송된 인터페이스에서 증분되며 일부 데이터그램의 경우 입력 인터페이스가 아닐 수 있습니다.

Received Datagrams Discarded Due To Invalid Address(잘못된 주소로 인해 삭제된 수신 데이터그램 수) — IPv6 헤더의 대상 필드에 있는 IPv6 주소가 이 엔티티에서 수신할 수 없는 잘못된 주소이기 때문에 삭제된 입력 데이터그램 수입니다. 이 카운터에는 잘못된 주소(예: ::0) 및 지원되지 않는 주소(예: 지정되지 않은 점두어를 가진 주소)가 포함됩니다. IPv6 라우터가 아니기 때문에 데이터그램을 전달할 수 없는 엔티티의 경우 이 카운터에는 대상 주소가 로컬 주소가 아니기 때문에 삭제된 데이터그램이 포함됩니다.

Received Datagrams Discarded Due To Truncated Data(잘린 데이터로 인해 삭제된 수신 데이터그램 수) — 데이터그램 프레임이 데이터를 충분히 전달하지 못했기 때문에 삭제된 입력 데이터그램 수입니다.

Received Datagrams Discarded Other(기타 이유로 삭제된 수신 데이터그램 수) — 프로세스를 중단할 만한 문제가 없지만 삭제된(예: 버퍼 공간 부족) 입력 IPv6 데이터그램 수입니다. 재조립을 기다리는 동안 삭제되는 데이터그램은 이 카운터에 포함되지 않습니다.

Received Datagrams Reassembly Required(재조립이 필요한 수신 데이터그램 수) — 이 인터페이스에서 재조립해야 하는 수신 IPv6 조각 수입니다. 이 카운터는 이러한 조각이 전송된 인터페이스에서 증분되며 일부 조각의 경우 입력 인터페이스가 아닐 수 있습니다.

Datagrams Successfully Reassembled(성공적으로 재조립된 데이터그램 수) — 성공적으로 재조립된 IPv6 데이터그램 수입니다. 이 카운터는 이러한 데이터그램이 전송된 인터페이스에서 증분되며 일부 조각의 경우 입력 인터페이스가 아닐 수 있습니다.

Datagrams Failed To Reassemble(재조립에 실패한 데이터그램 수) — IPv6 재조립 알고리즘에 의해 감지된 실패 수입니다(예: 타임 아웃, 오류 등). 일부 알고리즘(예: RFC 815 알고리즘)에서는 조각을 수신하는 대로 조합하여 조각 수 추적에 실패할 수 있기 때문에 삭제된 IPv6 조각 수를 반드시 계산하지는 않습니다. 이 카운터는 이러한 조각이 전송된 인터페이스에서 증분되며 일부 조각의 경우 입력 인터페이스가 아닐 수 있습니다.

Datagrams Forwarded(전달된 데이터그램 수) — 최종 대상에 대해 이 엔티티가 수신 및 전송한 출력 데이터그램 수입니다. IPv6 라우터 역할을 수행하지 않는 엔티티의 경우 이 카운터에는 이 엔티티를 통해 소스 라우팅되고 소스 라우팅이 성공적으로 처리된 패킷만 포함됩니다. 성공적으로 전송된 데이터그램의 경우 보내는 인터페이스의 카운터가 증분됩니다.

Datagrams Locally Transmitted(로컬로 전송된 데이터그램 수) — 이 엔티티가 이 출력 인터페이스에서 성공적으로 전송된 데이터그램 수입니다.

Datagrams Transmit Failed(전송에 실패한 데이터그램 수) — 이 엔티티가 성공적으로 전송하지 못한 데이터그램 수입니다.

Datagrams Successfully Fragmented(성공적으로 조각난 데이터그램 수) — 이 출력 인터페이스에서 성공적으로 조각난 IPv6 데이터그램 수입니다.

Datagrams Failed To Fragment(조각화에 실패한 데이터그램 수) — 이 인터페이스에서 조각화할 수 없는 출력 데이터그램 수입니다.

Datagrams Fragments Created(생성된 데이터그램 조각 수) — 이 출력 인터페이스에서 조각화의 결과로 생성된 출력 데이터그램 조각 수입니다.

Multicast Datagrams Received(수신된 멀티캐스트 데이터그램 수) — 인터페이스에 의해 수신된 멀티캐스트 패킷 수입니다.

Multicast Datagrams Transmitted(전송된 멀티캐스트 데이터그램 수) — 인터페이스에 의해 전송된 멀티캐스트 패킷 수입니다.

ICMPv6 통계

Total ICMPv6 Messages Received(수신된 총 ICMPv6 메시지 수) — ipv6IcmpInErrors에 의해 계산된 모든 메시지가 포함된, 인터페이스에 의해 수신된 총 ICMP 메시지 수입니다. 이 인터페이스는 ICMP 메시지가 전송된 인터페이스이며 메시지에 대해 입력 인터페이스가 아닐 수 있습니다.

ICMPv6 Messages With Errors Received(오류와 함께 수신된 ICMPv6 메시지 수) — 인터페이스가 수신했지만 ICMP 특정 오류(불량 ICMP 검사 함, 잘못된 길이 등)를 가진 것으로 확인된 ICMP 메시지 수입니다.

ICMPv6 Destination Unreachable Messages Received(수신된 ICMPv6 대상 접근불가능 메시지 수) — 인터페이스에 의해 수신된 ICMP 대상 접근불가능 메시지 수입니다.

ICMPv6 Messages Prohibited Administratively Received(수신된 ICMPv6 관리 금지 메시지 수) — 인터페이스에 의해 수신된 ICMP 대상 접근불가능/통신 관리 금지 메시지 수입니다.

ICMPv6 Time Exceeded Messages Received(수신된 ICMPv6 시간 초과 메시지 수) — 인터페이스에 의해 수신된 ICMP 시간 초과 메시지 수입니다.

ICMPv6 Parameter Problem Messages Received(수신된 ICMPv6 매개변수 문제 메시지 수) — 인터페이스에 의해 수신된 ICMPv6 매개변수 문제 메시지 수입니다.

ICMPv6 Packet Too Big Messages Received(수신된 ICMPv6 패킷 너무 큰 메시지 수) — 인터페이스에 의해 수신된 ICMP 패킷 너무 큰 메시지 수입니다.

ICMPv6 Echo Request Messages Received(수신된 ICMPv6 에코 요청 메시지 수) — 인터페이스에 의해 수신된 ICMP 에코 (요청) 메시지 수입니다.

ICMPv6 Echo Reply Messages Received(수신된 ICMPv6 에코 응답 메시지 수) — 인터페이스에 의해 수신된 ICMP 에코 응답 메시지 수입니다.

ICMPv6 Router Solicit Messages Received(수신된 ICMPv6 라우터 간청 메시지 수) — 인터페이스에 의해 수신된 ICMP 라우터 간청 메시지 수입니다.

ICMPv6 Router Advertisement Messages Received(수신된 ICMPv6 라우터 알림 메시지 수) — 인터페이스에 의해 수신된 ICMP 라우터 알림 메시지 수입니다.

ICMPv6 Neighbor Solicit Messages Received(수신된 ICMPv6 인접 간청 메시지 수) — 인터페이스에 의해 수신된 ICMP 인접 간청 메시지 수입니다.

ICMPv6 Neighbor Advertisement Messages Received(수신된 ICMPv6 인접 알림 메시지 수) — 인터페이스에 의해 수신된 ICMP 인접 알림 메시지 수입니다.

ICMPv6 Redirect Messages Received(수신된 ICMPv6 재지정 메시지 수) — 인터페이스에 의해 수신된 ICMPv6 재지정 메시지 수입니다.

ICMPv6 Group Membership Query Messages Received(수신된 ICMPv6 그룹 멤버십 쿼리 메시지 수) — 인터페이스에 의해 수신된 ICMPv6 그룹 멤버십 쿼리 메시지 수입니다.

ICMPv6 Group Membership Response Messages Received(수신된 ICMPv6 그룹 멤버십 응답 메시지 수) — 인터페이스에 의해 수신된 ICMPv6 그룹 멤버십 응답 메시지 수입니다.

ICMPv6 Group Membership Reduction Messages Received(수신된 ICMPv6 그룹 멤버십 감소 메시지 수) — 인터페이스에 의해 수신된 ICMPv6 그룹 멤버십 감소 메시지 수입니다.

Total ICMPv6 Messages Transmitted(전송된 총 ICMPv6 메시지 수) — 이 인터페이스가 전송을 시도한 총 ICMP 메시지 수입니다. icmpOutErrors에 의해 계산되는 모든 항목이 이 카운터에 포함됩니다.

ICMPv6 Messages Not Transmitted Due To Error(오류로 인해 전송되지 않은 ICMPv6 메시지 수) — 버퍼 부족과 같이 ICMP 내에서 발생한 문제로 인해 이 인터페이스가 전송하지 못한 ICMP 메시지 수입니다. IPv6가 결과 데이터그램을 라우팅할 수 없는 것과 같이 ICMP 계층 외부에서 발생한 오류는 이 값에서 제외되어야 합니다. 구현에 따라 이 카운터 값에 적용되는 오류 유형이 없는 경우도 있습니다.

ICMPv6 Destination Unreachable Messages Transmitted(전송된 ICMPv6 대상 접근불가능 메시지 수) — 인터페이스에 의해 전송된 ICMP 대상 접근불가능 메시지 수입니다.

ICMPv6 Messages Prohibited Administratively Transmitted(전송된 ICMPv6 관리 금지 메시지 수) — 전송된 ICMP 대상 접근불가능/통신 관리 금지 메시지 수입니다.

ICMPv6 Time Exceeded Messages Transmitted(전송된 ICMPv6 시간 초과 메시지 수) — 인터페이스에 의해 전송된 ICMP 시간 초과 메시지 수입니다.

ICMPv6 Parameter Problem Messages Transmitted(전송된 ICMPv6 매개변수 문제 메시지 수) — 인터페이스에 의해 전송된 ICMP 매개변수 문제 메시지 수입니다.

ICMPv6 Packet Too Big Messages Transmitted(전송된 ICMPv6 패킷 너무 큰 메시지 수) — 인터페이스에 의해 전송된 ICMP 패킷 너무 큰 메시지 수입니다.

ICMPv6 Echo Request Messages Transmitted(전송된 ICMPv6 에코 요청 메시지 수) — 인터페이스에 의해 전송된 ICMP 에코(요청) 메시지 수입니다.

ICMPv6 Echo Reply Messages Transmitted(전송된 ICMPv6 에코 응답 메시지 수) — 인터페이스에 의해 전송된 ICMP 에코 응답 메시지 수입니다.

ICMPv6 Router Solicit Messages Transmitted(수신된 ICMPv6 라우터 간청 메시지 수) — 인터페이스에 의해 전송된 ICMP 라우터 간청 메시지 수입니다.

ICMPv6 Router Advertisement Messages Transmitted(전송된 ICMPv6 라우터 알림 메시지 수) — 인터페이스에 의해 전송된 ICMP 라우터 알림 메시지 수입니다.

ICMPv6 Neighbor Solicit Messages Transmitted(전송된 ICMPv6 인접 간청 메시지 수) — 인터페이스에 의해 전송된 ICMP 인접 간청 메시지 수입니다.

ICMPv6 Neighbor Advertisement Messages Transmitted(전송된 ICMPv6 인접 알림 메시지 수) — 인터페이스에 의해 전송된 ICMP 인접 알림 메시지 수입니다.

ICMPv6 Redirect Messages Transmitted(전송된 ICMPv6 재지정 메시지 수) — 전송된 재지정 메시지 수입니다.

ICMPv6 Group Membership Query Messages Transmitted(전송된 ICMPv6 그룹 멤버십 쿼리 메시지 수) — 전송된 ICMPv6 그룹 멤버십 쿼리 메시지 수입니다.

ICMPv6 Group Membership Response Messages Transmitted(전송된 ICMPv6 그룹 멤버십 응답 메시지 수) — 전송된 ICMPv6 그룹 멤버십 응답 메시지 수입니다.

ICMPv6 Group Membership Reduction Messages Transmitted(전송된 ICMPv6 그룹 멤버십 감소 메시지 수) — 전송된 ICMPv6 그룹 멤버십 감소 메시지 수입니다.

ICMPv6 Duplicate Address Detects(ICMPv6 주소 중복 검사) — 인터페이스에 의해 감지된 중복 주소 수입니다.

IPv6 통계 표시

1. **IPv6 Statistics(IPv6 통계)** 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

선택된 인터페이스에 대한 통계가 표시됩니다.

CLI 명령을 사용하여 IPv6 및 ICMPv6 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

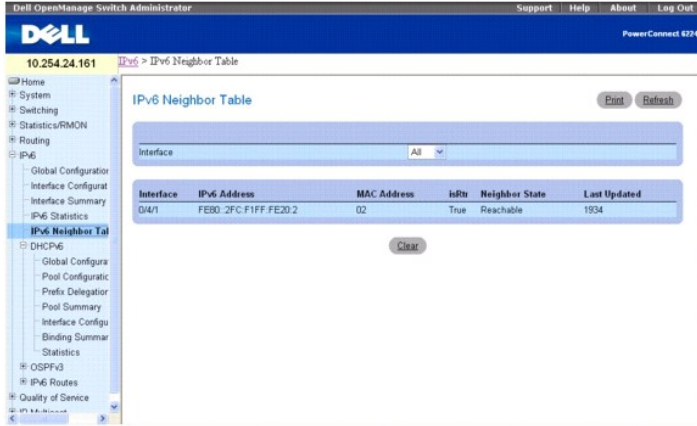
1 IPv6 라우팅 명령

IPv6 인접 항목 표

IPv6 Neighbor Table(IPv6 인접 항목 표) 페이지를 사용하여 지정된 인터페이스의 IPv6 인접 항목 세부 사항을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6→ IPv6 Neighbor Table(IPv6 인접 항목 표)을 클릭합니다.

그림 11-5. IPv6 Neighbor Table(IPv6 인접 항목 표)



IPv6 Neighbor Table(IPv6 인접 항목 표) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 인접 항목 상태 정보가 표시되는 인터페이스를 선택합니다.

Interface(인터페이스) — 현재 표 행에 설정이 표시되는 인터페이스를 지정합니다.

IPv6 Address(IPv6 주소) — 인접 항목 또는 인터페이스의 IPv6 주소를 지정합니다.

MAC Address(MAC 주소) — 인터페이스와 연결된 MAC 주소를 지정합니다.

IsRtr — 인접 항목이 라우터인지 여부를 표시합니다. 인접 항목이 라우터인 경우 값은 TRUE입니다. 인접 항목이 라우터가 아닌 경우 값은 FALSE입니다.

Neighbor State(인접 항목 상태) — 인접 항목 개시 항목의 상태를 지정합니다. 다음은 IPv6 인접 항목 검색 개시의 동적 항목 상태입니다.

- 1 **Incmp** — 항목에 대해 주소 확인이 수행됩니다. 인접 간청 메시지가 대상의 간청 노드 멀티캐스트 주소로 전송되었지만 해당 인접 알림 메시지를 아직 수신하지 못했습니다.
- 1 **Reachable(연결 가능)** — 인접 항목에 대한 전송 경로가 제대로 작동 중이었던 마지막 연결 가능 시간(밀리초) 내에 포지티브 확인을 수신했습니다. REACH(연결) 상태 동안 패킷이 전송될 때 장치는 특별한 작업을 수행하지 않습니다.
- 1 **Stale(스테일)** — 전송 경로가 제대로 작동 중이었던 마지막 포지티브 확인을 수신한 이후 연결 가능 시간(밀리초)이 경과되었습니다. STALE(스테일) 상태 동안 패킷이 전송될 때까지 장치가 어떠한 작업도 수행하지 않습니다.
- 1 **Delay(지연)** — 전송 경로가 제대로 작동 중이었던 마지막 포지티브 확인을 수신한 이후 연결 가능 시간(밀리초)이 경과되었습니다. 패킷이 마지막 DELAY_FIRST_PROBE_TIME초 내에 전송되었습니다. DELAY(지연) 상태로 전환되는 DELAY_FIRST_PROBE_TIME초 내에 연결 가능 확인을 수신하지 않은 경우 인접 간청 메시지를 전송하고 상태를 PROBE(프로브)로 변경합니다.
- 1 **Probe(프로브)** — 연결 가능 확인을 수신할 때까지 재전송 타이머 시간(밀리초)마다 인접 간청 메시지를 재전송하여 연결 가능 확인을 실제로 확인합니다.

Last Updated(최신 업데이트) — 주소가 연결 가능한 상태임을 확인한 이후 시간입니다.

IPv6 인접 항목 표 표시

1. **IPv6 Neighbor Table(IPv6 인접 항목 표)** 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

선택된 인터페이스에 대한 인접 항목 세부 사항이 표시됩니다.

CLI 명령을 사용하여 IPv6 인접 항목 표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

DHCPv6

DHCP는 일반적으로 IP 주소, 게이트웨이 및 DNS, NTP 및/또는 SIP(Session Initiation Protocol) 매개변수와 같은 기타 네트워킹 정보의 지정을 위해 클라이언트(예: 호스트) 및 서버(예: 라우터) 간에 사용됩니다. 그러나 IPv6는 IPv6 NDP(Neighbor Discovery Protocol)를 통한 IP 주소 자동 구성 및 라우터 알림 메시지 사용을 제공합니다. 따라서 네트워크 내의 DHCPv6 역할은 IP 주소 지정에 사용하지 않는 DHCPv4 역할과는 다릅니다.

일반적으로 DHCPv4에 의해 지원되고 DHCPv6에 의해서도 지원되고 구성되어야 하는 DHCP 옵션 목록이 있습니다.

주: 이러한 옵션 중 가장 중요한 옵션은 **IPv6→DHCPv6→Pool Configuration(풀 구성)** 웹 페이지에서 구성되는 DNS 서버 옵션입니다.

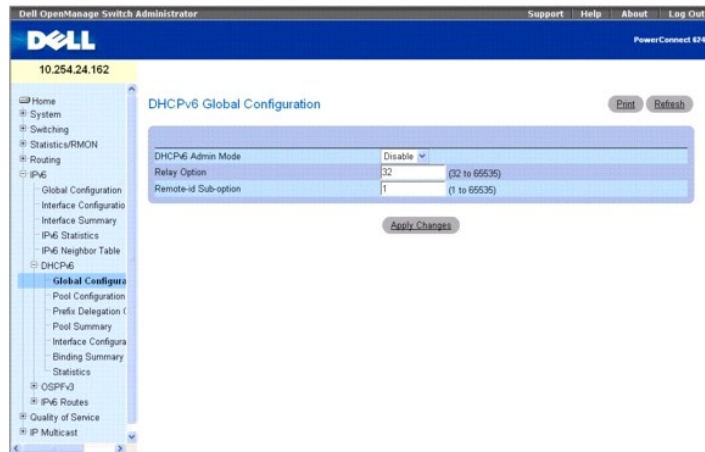
DHCPv6 메뉴 페이지에는 DHCPv6 매개변수 및 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→DHCPv6**을 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

- 1. [DHCPv6 전역 구성](#)
- 1. [DHCPv6 풀 구성](#)
- 1. [접두어 위임 구성](#)
- 1. [DHCPv6 풀 요약](#)
- 1. [DHCPv6 인터페이스 구성](#)
- 1. [DHCPv6 서버 바인딩 요약](#)
- 1. [DHCPv6 통계](#)

DHCPv6 전역 구성

DHCPv6 Global Configuration(DHCPv6 전역 구성) 페이지를 사용하여 DHCPv6 전역 매개변수를 구성합니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→DHCPv6→Global Configuration(전역 구성)**을 클릭합니다.

그림 11-6. DHCPv6 Global Settings(DHCPv6 전역 구성)



DHCPv6 Global Configuration(DHCPv6 전역 구성) 페이지에는 다음과 같은 필드가 있습니다.

DHCPv6 Admin Mode(DHCPv6 관리 모드) — 스위치의 DHCPv6 작동을 지정합니다. 가능한 값은 Enable(활성) 및 Disable(비활성)이고 기본값은 Disable(비활성)입니다.

Relay Option(릴레이 옵션) — 릴레이 에이전트 정보 옵션 값을 지정합니다. 허용되는 값은 32 - 65535이고 릴레이 에이전트 및 서버 간에 교환된 값을 표시합니다. 각 값마다 서로 다른 의미를 가지며 1-39 값은 표준화되어 있습니다. 기본값은 32이며 OPTION_INFORMATION_REFRESH_TIME을 의미합니다.

Remote-id Sub-option(원격 ID 하위 옵션) — 릴레이 에이전트 정보 옵션 원격 ID 하위 옵션 유형을 표시할 번호를 지정할 수 있습니다. 허용되는 값은 1 - 65535이고 기본값은 1입니다.

DHCPv6 전역 매개변수 구성

1. DHCPv6 Global Configuration(DHCPv6 전역 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

DHCPv6 매개변수 수정 사항이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DHCPv6 전역 매개변수 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1 DHCPv6 명령

DHCPv6 풀 구성

IPv6 클라이언트용 DHCP는 설치한 풀에서 매개변수를 사용하도록 구성된 서버에 연결됩니다. 풀은 풀 이름을 통해 식별되고 DNS 서버의 IPv6 주소 및 도메인 이름이 포함되어 있습니다.

Pool Configuration(풀 구성) 페이지를 사용하여 풀을 생성하고 풀 매개변수를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **DHCPv6** → **Pool Configuration(풀 구성)** 을 클릭합니다.

그림 11-7. Pool Configuration - Create(풀 구성 - 생성)

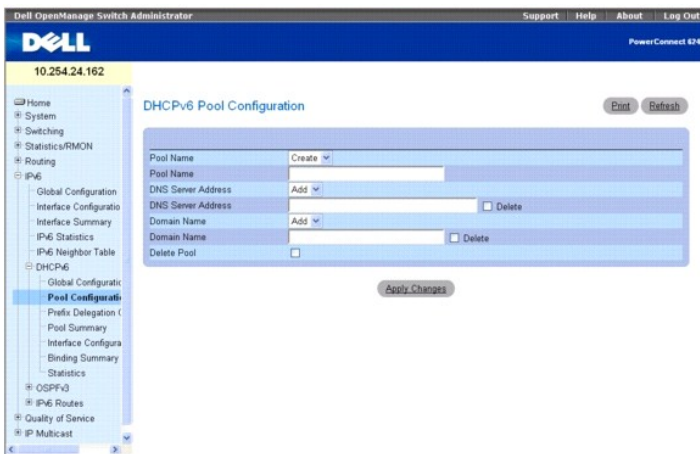
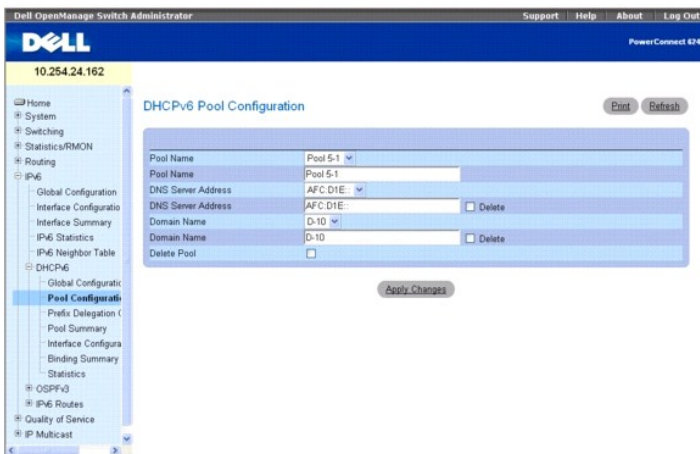


그림 11-8. Pool Configuration - Display(풀 구성 - 표시)



Pool Configuration(풀 구성) 페이지에는 다음과 같은 필드가 있습니다.

Pool Name(풀 이름) — 모든 풀 이름이 구성된 드롭다운 메뉴입니다. **Create(생성)**를 선택하면 새 풀 정보 준비 시 페이지의 필드에 있는 데이터가 삭제됩니다.

Pool Name(풀 이름) — 이전 필드에서 선택한 풀을 표시하거나 Create(생성)를 선택한 경우 DHCPv6 풀에 대한 고유 이름 항목을 제공합니다. 최대 31자의 영숫자를 입력할 수 있습니다.

DNS Server Address(DNS 서버 주소) — 특정 DHCPv6 풀 내에서 DNS 서버의 IPv6 주소를 지정하는 드롭다운 메뉴입니다. 메뉴에서 **Add(추가)**를 선택하면 새 주소 준비 시 다음 필드에 있는 데이터가 삭제됩니다.

DNS Server Address(DNS 서버 주소) — 이전 필드에서 선택한 DNS 서버 주소를 표시합니다. 이전 필드에서 Add(추가)를 선택한 경우 여기서 새 DNS 서버 주소를 입력합니다. 이

풀에서 주소를 제거하려면 **Delete(삭제)**를 클릭합니다. **Apply Changes(변경사항 적용)**를 클릭하면 주소가 삭제됩니다.

Domain Name(도메인 이름) — 특정 DHCPv6 풀 내에서 구성된 도메인 이름 목록을 지정한 드롭다운 메뉴입니다. 메뉴에서 **Add(추가)**를 선택하면 새 이름 준비 시 다음 필드에 있는 데이터가 삭제됩니다.

Domain Name(도메인 이름) — 이전 필드에서 선택한 DNS 도메인 이름을 표시합니다. 이전 필드에서 Add(추가)를 선택한 경우 여기서 새 DNS 도메인 이름을 입력합니다. 최대 255자의 영숫자를 입력할 수 있습니다. 이 풀에서 도메인 이름을 제거하려면 **Delete(삭제)**를 클릭합니다. **Apply Changes(변경사항 적용)**를 클릭하면 이름이 삭제됩니다.

Delete Pool(풀 삭제) — 표시된 풀을 삭제하려면 이 상자를 선택합니다. **Apply Changes(변경사항 적용)**를 클릭하면 풀이 삭제됩니다.

DHCPv6 풀 생성

1. **Pool Configuration(풀 구성)** 페이지를 엽니다.
2. Pool Name(풀 이름) 드롭다운 메뉴에서 Create(생성)를 선택합니다.
3. Pool Name(풀 이름) 필드에 새 이름을 입력합니다.
4. 이 풀에 연결할 기존 DNS 서버 주소를 지정하거나 새 주소를 생성합니다.
5. 이 풀에 연결할 기존 도메인 이름을 지정하거나 새 도메인 이름을 생성합니다.
6. **Apply Changes(변경사항 적용)**를 클릭하십시오.

새 풀이 저장되고 장치가 업데이트됩니다. 새 DNS 서버 주소 또는 도메인 이름이 지정된 경우에도 저장됩니다.

DHCPv6 풀 매개변수 수정

1. **Pool Configuration(풀 구성)** 페이지를 엽니다.
2. Pool Name(풀 이름) 드롭다운 메뉴에서 매개변수를 변경할 풀을 선택합니다.
3. 지정한 풀에 대해 새 DNS 서버 주소를 변경하거나 설정합니다.
4. 지정한 풀에 대해 새 도메인 이름을 변경하거나 설정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

DHCPv6 풀 매개변수 수정 사항이 저장되고 장치가 업데이트됩니다.

DHCPv6 풀 또는 매개변수 삭제

1. **Pool Configuration(풀 구성)** 페이지를 엽니다.
2. Pool Name(풀 이름) 드롭다운 메뉴에서 적용할 풀을 선택합니다.
3. 이 풀의 DNS 서버 주소를 삭제하려면 Delete(삭제) 상자를 클릭합니다.
4. 이 풀의 도메인 이름을 삭제하려면 Delete(삭제) 상자를 클릭합니다.
5. 전체 풀을 삭제하려면 Delete Pool(풀 삭제) 상자를 클릭합니다.
6. **Apply Changes(변경사항 적용)**를 클릭하십시오.

풀 또는 매개변수 설정이 삭제되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DHCPv6 풀 매개변수 구성

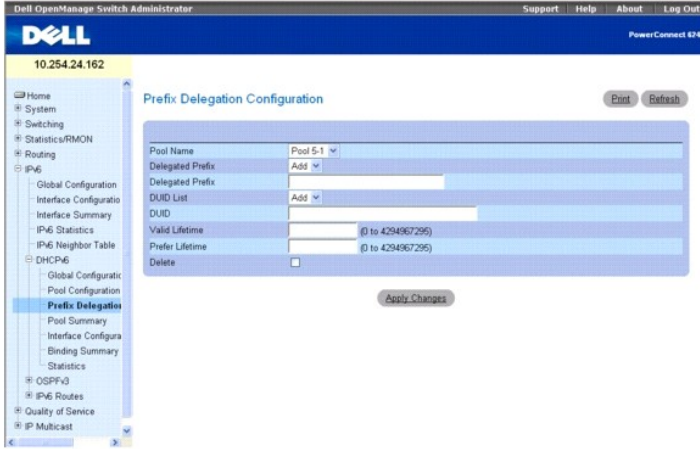
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

접두어 위임 구성

Prefix Delegation Configuration(접두어 위임 구성) 페이지를 사용하여 위임된 풀 접두어를 구성합니다. 위임된 접두어를 구성하기 전에 [DHCPv6 풀 구성](#)을 사용하여 최소 하나의 풀을 생성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → DHCPv6 → Prefix Delegation Configuration(접두어 위임 구성)을 클릭합니다.

그림 11-9. Prefix Delegation Configuration(접두어 위임 구성)



Prefix Delegation Configuration(접두어 위임 구성) 페이지에는 다음과 같은 필드가 있습니다.

Pool Name(풀 이름) — 구성된 모든 풀 이름을 지정합니다. 구성할 풀을 선택합니다.

Delegated Prefix(위임된 접두어) — 지정한 풀에 연결할 위임된 IPv6 접두어를 지정하는 드롭다운 메뉴입니다. 이 풀에 대해 새 위임된 접두어를 정의하려면 **Add(추가)**를 선택합니다.

Delegated Prefix(위임된 접두어) — 선택한 위임된 접두어를 표시하거나 새 접두어를 입력할 수 있습니다.

DUID List(DUID 목록) - 클라이언트 고유 DUID 값을 선택하는 드롭다운 메뉴입니다. 이 풀에 대해 새 DUID 값을 정의하려면 **Add(추가)**를 선택합니다.

DUID - 선택한 DUID 값을 표시하거나 새 값을 입력할 수 있습니다.

Valid Lifetime(유효 수명) — 위임된 접두어에 대해 유효한 수명(초)을 지정합니다.

Prefer Lifetime(기본 수명) — 위임된 접두어에 대해 기본 설정 수명(초)을 지정합니다.

Delete(삭제) — 이 확인란을 선택한 후 **Apply Changes(변경사항 적용)**를 클릭하면 표시된 풀 접두어 위임 구성을 삭제합니다.

풀에 위임된 접두어 구성

1. **Prefix Delegation Configuration(접두어 위임 구성)** 페이지를 엽니다.
2. 구성할 풀을 선택합니다.
3. 위임된 접두어를 지정합니다.
4. 필요에 따라 나머지 필드를 수정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

위임된 접두어 및 매개변수가 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 위임된 접두어 구성

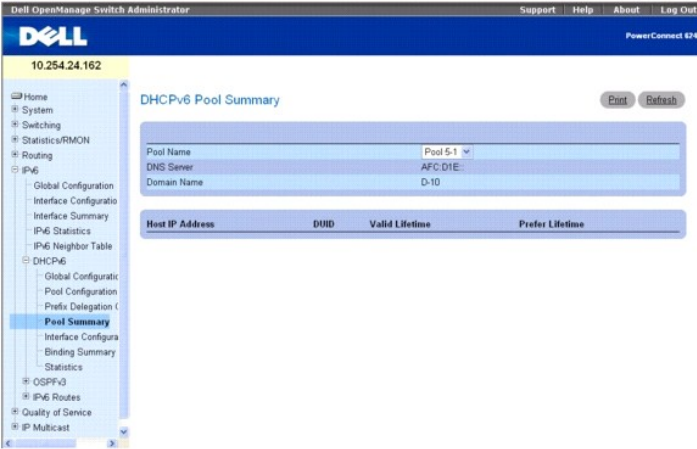
이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

DHCPv6 풀 요약

Pool Summary(풀 요약) 페이지를 사용하여 모든 DHCPv6 풀에 대한 설정을 표시합니다. Pool Summary(풀 요약)를 표시하기 전에 [DHCPv6 풀 구성](#)을 사용하여 최소 하나의 풀을 생성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **DHCPv6** → **Pool Summary(풀 요약)**을 클릭합니다.

그림 11-10. Pool Summary(풀 요약)



Pool Summary(풀 요약) 페이지에는 다음과 같은 필드가 있습니다.

Pool Name(풀 이름) — 표시할 풀을 선택합니다.

DNS Server(DNS 서버) — 연결된 DNS 서버의 IPv6 주소를 표시합니다.

Domain Name(도메인 이름) — DNS 도메인 이름을 표시합니다.

Host IP Address(호스트 IP 주소) — 위임된 점두어의 IPv6 주소 및 마스크 길이를 표시합니다.

DUID — 클라이언트의 고유 DUID 값을 식별하는데 사용되는 식별자입니다.

Valid Lifetime(유효 수명) — 위임된 점두어에 대해 유효한 수명(초)을 표시합니다.

Prefer Lifetime(기본 수명) — 위임된 점두어에 대해 기본 설정 수명(초)을 표시합니다.

CLI 명령을 사용하여 풀 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

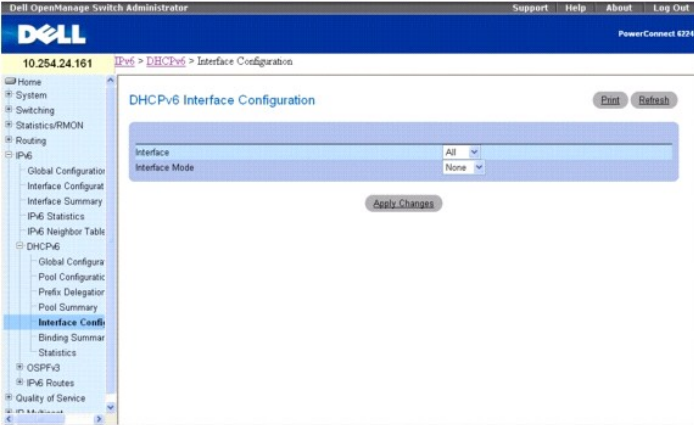
- 1 DHCPv6 명령

DHCPv6 인터페이스 구성

DHCPv6 Interface Configuration(DHCPv6 인터페이스 구성) 페이지를 사용하여 DHCPv6 인터페이스를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **DHCPv6** → **Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 11-11. DHCPv6 Interface Configuration(DHCPv6 인터페이스 구성)



DHCPv6 Interface Configuration(DHCPv6 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — DHCPv6 서버 기능을 구성할 인터페이스를 선택합니다.

Interface Mode(인터페이스 모드) — DHCPv6 모드를 서버 또는 릴레이로 구성합니다. DHCPv6 서버 및 DHCPv6 릴레이 기능은 서로 간에 배타적입니다.

Pool Name(풀 이름) — 상태 비저장 및/또는 점두어 위임 매개변수가 포함된 DHCPv6 풀을 선택합니다. 이 필드는 인터페이스 모드가 서버인 경우에 표시됩니다.

Rapid Commit(빠른 커밋) — 빠른 커밋은 옵션 매개변수입니다. 지정하면 클라이언트 및 서버 간에 간략하게 교환할 수 있습니다. 이 필드는 인터페이스 모드가 서버인 경우에 표시됩니다.

Preference(기본 설정) — 여러 DHCPv6 서버 간의 기본 설정을 결정하기 위해 클라이언트에 의해 사용된 기본 설정 값을 선택합니다. 허용되는 값은 0 - 4294967295입니다. 이 필드는 Interface Mode(인터페이스 모드)가 Server(서버)인 경우 표시됩니다.

Delete(삭제) — 이 구성을 삭제하려면 이 상자를 선택하고 **Apply Changes(변경사항 적용)**를 클릭합니다. 이 필드는 인터페이스 모드가 서버 또는 릴레이일 경우에 표시됩니다.

Relay Interface(릴레이 인터페이스) — 릴레이 서버에 연결할 인터페이스를 선택합니다. 이 필드는 인터페이스 모드가 릴레이인 경우에 표시됩니다.

Destination IP Address(대상 IP 주소) — DHCPv6 릴레이 서버의 IPv6 주소를 선택합니다. 이 필드는 인터페이스 모드가 릴레이인 경우에 표시됩니다.

Remote ID(원격 ID) — 릴레이 에이전트 정보 옵션을 선택합니다. 원격 ID는 DHCPv6 서버 DUID 및 릴레이 인터페이스 번호에서 파생되며 사용자 정의 문자열로 지정할 수 있습니다. 이 필드는 인터페이스 모드가 릴레이인 경우에 표시됩니다.

릴레이 인터페이스 모드에 대한 DHCPv6 인터페이스 구성

1. DHCPv6 Interface Configuration(DHCPv6 인터페이스 구성) 페이지를 엽니다.
2. 원하는 인터페이스를 지정하고 **Interface Mode(인터페이스 모드)** 드롭다운 메뉴에서 **Relay(릴레이)**를 선택합니다.

다음과 같은 화면이 나타납니다.

그림 11-12. DHCPv6 Interface Configuration - Relay(DHCPv6 인터페이스 구성 - 릴레이)



3. 필요에 따라 필드를 수정합니다.

4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

DHCPv6 인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DHCPv6 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 DHCPv6 명령

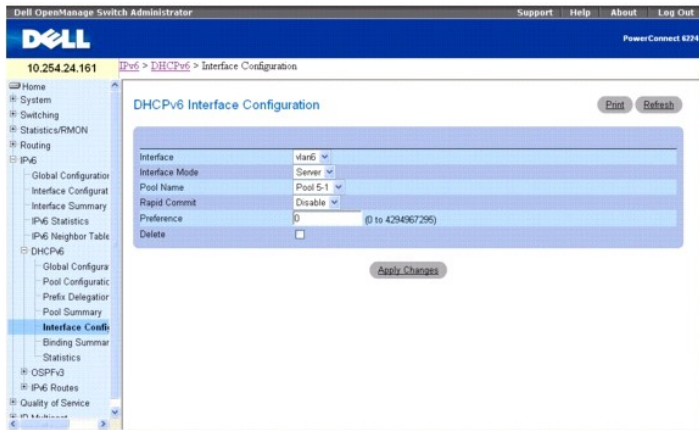
서버 인터페이스 모드에 대한 DHCPv6 인터페이스 구성

1. **DHCPv6 Interface Configuration(DHCPv6 인터페이스 구성)** 페이지를 엽니다.

2. 원하는 인터페이스를 지정하고 **Interface Mode(인터페이스 모드)** 드롭다운 메뉴에서 **Server(서버)**를 선택합니다.

다음과 같은 화면이 나타납니다.

그림 11-13. DHCPv6 Interface Configuration - Server(DHCPv6 인터페이스 구성 - 서버)



3. 필요에 따라 필드를 수정합니다.

4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

DHCPv6 인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DHCPv6 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

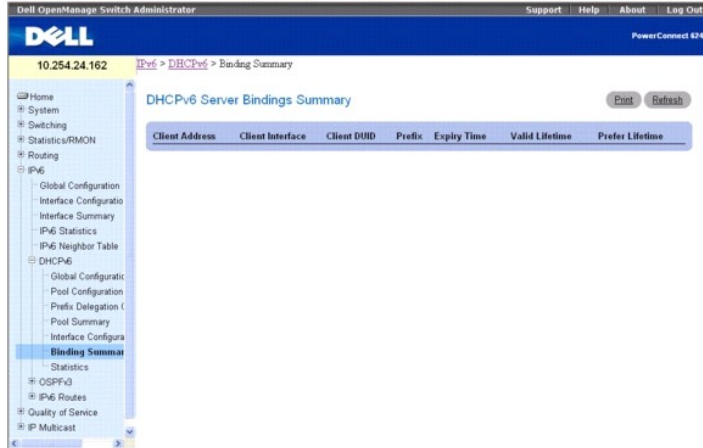
- 1 DHCPv6 명령

DHCPv6 서버 바인딩 요약

Server Bindings Summary(서버 바인딩 요약) 페이지를 사용하여 모든 DHCPv6 서버 바인딩을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6 → DHCPv6 → Bindings Summary(바인딩 요약)**를 클릭합니다.

그림 11-14. Server Bindings Summary(서버 바인딩 요약)



Server Bindings Summary(서버 바인딩 요약) 페이지에는 다음과 같은 필드가 있습니다.

Client Address(클라이언트 주소) - 바인딩에 연결된 클라이언트의 IPv6 주소를 지정합니다.

Client Interface(클라이언트 인터페이스) - 클라이언트 바인딩이 발생한 인터페이스 번호를 지정합니다.

Client DUID(클라이언트 DUID) - 클라이언트의 DHCPv6 고유 식별자를 지정합니다.

Prefix(접두어) - 이 바인딩에 연결되는 접두어 유형을 지정합니다.

Expiry Time(만료 시간) - 바인딩에 연결된 접두어가 만료되는 시간(초)을 지정합니다.

Valid Lifetime(유효 수명) - 바인딩에 연결되는 접두어의 유효 수명 값(초)을 지정합니다.

Prefer Lifetime(기본 수명) - 바인딩에 연결되는 접두어의 기본 설정 수명 값(초)을 지정합니다.

CLI 명령을 사용하여 서버 바인딩 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

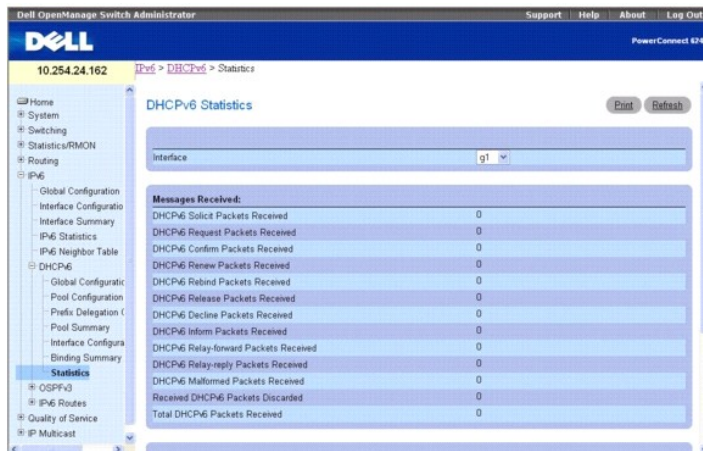
- 1 DHCPv6 명령

DHCPv6 통계

DHCPv6 Statistics(DHCPv6 통계) 페이지를 사용하여 하나 또는 모든 인터페이스의 DHCPv6 통계를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **DHCPv6** → **Statistics(통계)** 를 클릭합니다.

그림 11-15. DHCPv6 Statistics(DHCPv6 통계)



DHCPv6 Statistics(DHCPv6 통계) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다. **All(모두)**를 선택하면 모든 인터페이스의 데이터가 표시됩니다.

수신된 메시지

이 절에서는 수신된 메시지의 모든 인터페이스 레벨 통계 집계를 지정합니다.

DHCPv6 Solicit Packets Received(수신된 DHCPv6 간청 패킷 수) — 간청 수를 지정합니다.

DHCPv6 Request Packets Received(수신된 DHCPv6 요청 패킷 수) — 요청 수를 지정합니다.

DHCPv6 Confirm Packets Received(수신된 DHCPv6 확인 패킷 수) — 확인 수를 지정합니다.

DHCPv6 Renew Packets Received(수신된 DHCPv6 갱신 패킷 수) — 갱신 수를 지정합니다.

DHCPv6 Rebind Packets Received(수신된 DHCPv6 리바인드 패킷 수) — 리바인드 수를 지정합니다.

DHCPv6 Release Packets Received(수신된 DHCPv6 릴리스 패킷 수) — 릴리스 수를 지정합니다.

DHCPv6 Decline Packets Received(수신된 DHCPv6 동의 안 함 패킷 수) — 동의 안 함 수를 지정합니다.

DHCPv6 Inform Packets Received(수신된 DHCPv6 알림 패킷 수) — 알림 수를 지정합니다.

DHCPv6 Relay-forward Packets Received(수신된 DHCPv6 릴레이 전송 패킷 수) — 릴레이 전송 수를 지정합니다.

DHCPv6 Relay-reply Packets Received(수신된 DHCPv6 릴레이 응답 패킷 수) — 릴레이 응답 수를 지정합니다.

DHCPv6 Malformed Packets Received(수신된 DHCPv6 잘못 구성된 패킷 수) — 잘못 구성된 패킷 수를 지정합니다.

Received DHCPv6 Packets Discarded(삭제된 수신 DHCPv6 패킷 수) — 삭제된 패킷 수를 지정합니다.

Total DHCPv6 Packets Received(수신된 전체 DHCPv6 패킷 수) — 수신된 전체 패킷 수를 지정합니다.

전송된 메시지

이 절에서는 전송된 메시지의 모든 인터페이스 레벨 통계 집계를 지정합니다.

DHCPv6 Advertisement Packets Transmitted(전송된 DHCPv6 알림 패킷 수) — 알림 수를 지정합니다.

DHCPv6 Reply Packets Transmitted(전송된 DHCPv6 응답 패킷 수) — 응답 수를 지정합니다.

DHCPv6 Reconfig Packets Transmitted(전송된 DHCPv6 재구성 패킷 수) — 재구성 수를 지정합니다.

DHCPv6 Relay-forward Packets Transmitted(전송된 DHCPv6 릴레이 전송 패킷 수) — 릴레이 전송 수를 지정합니다.

DHCPv6 Relay-reply Packets Transmitted(전송된 DHCPv6 릴레이 응답 패킷 수) — 릴레이 응답 수를 지정합니다.

Total DHCPv6 Packets Sent(전송된 전체 DHCPv6 패킷 수) — 전송된 전체 패킷 수를 지정합니다.

Clear(지우기) — 인터페이스 패킷 카운터를 재설정합니다.

DHCPv6 통계 표시

1. **DHCPv6 Statistics(DHCPv6 통계)** 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

선택된 인터페이스에 대한 DHCPv6 통계가 표시됩니다.

CLI 명령을 사용하여 DHCPv6 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 DHCPv6 명령

OSPFv3

OSPFv3은 IPv6용 OSPF(Open Shortest Path First) 라우팅 프로토콜입니다. 링크 상태 데이터베이스, 인트라/내부 영역 및 AS 외부 라우터와 가상 링크 개념의 OSPFv2와 유사합니다. 다음 사항을 포함하여 많은 측면에서 IPv4의 카운터 포인트와 다릅니다. 피어링은 링크 로컬 주소를 통해 수행되고 프로토콜은 네트워크 중심이 아닌 링크이며 주소 지정 기능이 결과적으로 IPv4 및 IPv6 모두에 사용할 수 있는 리프 LSA로 이동되었습니다. 또한 터널을 통한 작업을 수행할 수 있도록 지정대 지정 링크가 지원됩니다.

OSPF 및 OSPFv3을 동시에 활성화할 수 있습니다. OSPF는 IPv4를 통해 작동하고 OSPFv3은 IPv6을 통해 작동합니다.

OSPFv3 메뉴 페이지에는 OSPFv3 매개변수 및 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 IPv6→ OSPFv3 을 클릭합니다.

이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

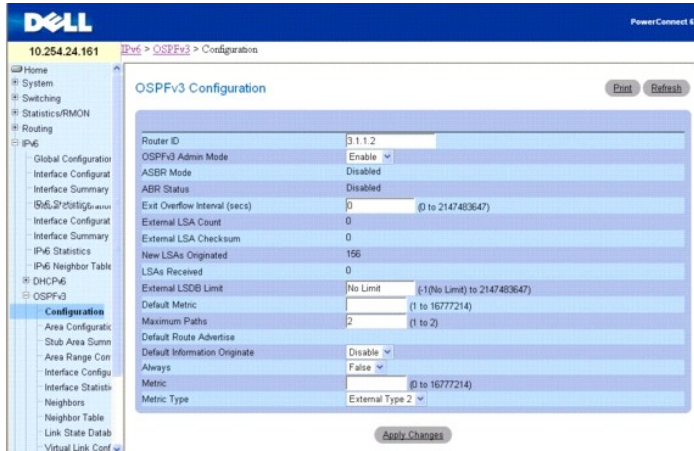
- 1 [OSPFv3 구성](#)
- 1 [OSPFv3 영역 구성](#)
- 1 [OSPFv3 스텝 영역 요약](#)
- 1 [OSPFv3 영역 범위 구성](#)
- 1 [OSPFv3 인터페이스 구성](#)
- 1 [OSPFv3 인터페이스 통계](#)
- 1 [OSPFv3 인접 항목](#)
- 1 [OSPFv3 인접 항목 표](#)
- 1 [OSPFv3 링크 상태 데이터베이스](#)
- 1 [OSPFv3 가상 링크 구성](#)
- 1 [OSPFv3 가상 링크 요약](#)
- 1 [OSPFv3 경로 재배포 구성](#)
- 1 [OSPFv3 경로 재배포 요약](#)

OSPFv3 구성

OSPFv3 Configuration(OSPFv3 구성) 페이지를 사용하여 스위치에 대해 OSPFv3을 활성화하고 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6→ OSPFv3→ Configuration(구성) 을 클릭합니다.

그림 11-16. OSPFv3 Configuration(OSPFv3 구성)



OSPFv3 Configuration(OSPFv3 구성) 페이지에는 다음과 같은 필드가 있습니다.

Router ID(라우터 ID) — 자치 시스템(AS)에서 라우터를 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다. 라우터 ID를 변경하려면 먼저 OSPFv3을 비활성화해야 합니다. 새 라우터 ID를 설정한 후 OSPFv3을 다시 활성화하여 변경사항을 적용해야 합니다. 기본값은 0.0.0.0이지만 이 값은 유효한 라우터 ID가 아니며 **Apply Changes(변경사항 적용)** 단추를 누르기 전에 변경해야 합니다.

OSPFv3 Admin Mode(OSPFv3 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 스위치에 대해 OSPFv3이 활성화됩니다. 기본값은 Enable(활성)입니다. OSPFv3이 활성화되기 전에 라우터 ID를 구성해야 합니다. 이 작업은 IPv6 라우터 OSPF 모드에서 CLI 명령, `router-id`를 발행하여 수행할 수 있습니다.

주: OSPFv3이 라우터에서 초기화되면 라우터가 재설정될 때까지 초기화된 상태로 유지됩니다.

ASBR Mode(ASBR 모드) — ASBR 모드가 활성화되거나 비활성화되었는지 여부를 표시합니다. 활성화된 경우에는 라우터가 자치 시스템의 경계 라우터입니다. 라우터는 다른 프로토콜로부터 알게 된 경로를 재배포하도록 구성된 경우 자동으로 ASBR이 됩니다.

ABR Status(ABR 상태) — 값은 Enable(활성) 또는 Disable(비활성)입니다. 필드는 유효한 구성이 존재하는 경우에만 표시됩니다. 활성화된 경우에는 라우터가 영역 경계 라우터입니다. 비활성화된 경우에는 라우터가 영역 경계 라우터가 아닙니다.

Exit Overflow Interval (secs)(종료 오버플로 간격(초)) — 오버플로 상태가 된 이후 라우터가 오버플로 상태를 벗어나려고 시도하기까지 기다려야 하는 시간(초)을 입력합니다. 이 값을 사용하면 라우터에서 기본값이 아닌 AS-External-LSA를 다시 발생시킬 수 있습니다. 0을 입력할 경우 라우터를 다시 시작해야 오버플로 상태에서 벗어납니다. 범위는 0 ~

2147483647초입니다.

External LSA Count(외부 LSA 수) — 링크 상태 데이터베이스의 외부(LS 유형 5) LSA(Link State Advertisements) 수입니다.

External LSA Checksum(외부 LSA 검사 합계) — 링크 상태 데이터베이스에 포함되어 있는 외부 LSA(Link State Advertisements)의 LS 검사 합계입니다. 이 합계를 사용하면 라우터의 링크 상태 데이터베이스가 변경되었는지 여부를 확인하고 두 라우터의 링크 상태 데이터베이스를 비교할 수 있습니다.

New LSAs Originated(발생한 새 LSA) — 지정된 OSPFv3 영역에서 라우터는 여러 개의 LSA를 발생립니다. 각 라우터는 라우터-LSA를 발생립니다. 라우터가 특정 영역 네트워크에 대해 지정된 라우터인 경우 해당 네트워크에 대한 네트워크-LSA를 발생립니다. 이 값은 이 라우터에서 발생하는 LSA 수를 나타냅니다.

LSAs Received(수신된 LSA 수) — 새 인스턴스화를 위해 결정된 LSA(링크 상태 알람) 수입니다. 자체 생성된 LSA의 최신 인스턴스화는 이 수에 포함되지 않습니다.

External LSDB Limit(외부 LSDB 제한) — 데이터베이스에 저장할 수 있는 최대 AS 외부 LSA 수입니다. -1 값은 저장할 수 있는 수에 대해 제한이 없음을 의미합니다. 유효한 값 범위는 -1 ~ 2147483647입니다.

Default Metric(기본 메트릭) — 재배포된 경로의 메트릭에 대한 기본값을 설정합니다. 이 필드에서는 값이 이미 설정되었거나 기본 메트릭이 표시되고 이전에 구성하지 않은 경우 공란이 표시됩니다. 유효한 값은 1 ~ 16,777,214입니다.

Maximum Paths(최대 경로) — OSPFv3가 지정된 대상에 보고할 수 있는 최대 경로 수를 구성합니다. 유효한 값은 1 ~ 2입니다.

Default Information Originate(기본 정보 발생) — Default Route Advertise(기본 경로 알람)를 활성화하거나 비활성화합니다. Default Information Originate(기본 정보 발생)를 Enable(활성)로 설정한 경우에만 Always(항상), Metric(메트릭) 및 Metric Type(메트릭 유형) 값을 구성할 수 있습니다. Default Information Originate(기본 정보 발생)를 Enable(활성)로 설정하고 Always(항상), Metric(메트릭) 및 Metric Type(메트릭 유형) 값을 이미 설정한 경우 Default Information Originate(기본 정보 발생)를 비활성으로 다시 설정하면 Always(항상), Metric(메트릭) 및 Metric Type(메트릭 유형) 값이 기본값으로 설정됩니다.

Always(항상) — True로 설정한 경우 라우터 알람을 ::/0으로 설정합니다.

Metric(메트릭) — 기본 경로 메트릭을 지정합니다. 유효한 값은 0 ~ 16,777,214입니다.

Metric Type(메트릭 유형) — 기본 경로의 메트릭 유형을 설정합니다. 유효값은 External Type 1(외부 유형 1) 및 External Type 2(외부 유형 2)입니다.

OSPFv3 구성

1. **OSPFv3 Configuration(OSPFv3 구성)** 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

OSPFv3 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPFv3 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. OSPFv3 명령

OSPFv3 영역 구성

OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 사용하여 OSPFv3 영역을 생성하고 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→OSPFv3→Area Configuration(영역 구성)**을 클릭합니다.

그림 11-17. OSPFv3 Area Configuration(OSPFv3 영역 구성)



OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지에는 다음과 같은 필드가 있습니다.

Area ID(영역 ID) — OSPFv3 영역입니다. 영역 ID는 라우터 인터페이스가 연결되는 영역을 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다.

External Routing(외부 라우팅) — AS 외부 LSA가 영역을 플러딩하는지 여부를 포함하여 영역에 대한 라우터의 기능 정의입니다. 스태프 영역인 경우에는 이러한 옵션에 대해 외부 라우팅 기능을 구성할 수 있지만, 스태프 영역이 아닌 경우에는 Import External LSA(외부 LSA 가져오기) 옵션만 사용할 수 있습니다.

SPF Runs(SPF 실행 횟수) — 이 영역의 링크 상태 데이터베이스를 사용하여 내부 영역 경로를 계산한 횟수입니다. 일반적으로 Dijkstra 알고리즘을 사용하여 수행됩니다.

Area Border Router Count(영역 경계 라우터 수) — 이 영역에서 연결 가능한 총 영역 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

Area LSA Count(영역 LSA 수) — AS 외부 LSA를 제외한 이 영역의 링크 상태 데이터베이스에 있는 총 링크 상태 알림 수입니다.

Area LSA Checksum(영역 LSA 검사 합계) — 이 영역의 링크 상태 데이터베이스에 포함된 링크 상태 알림 LS 검사 합의 부호 없는 32비트 합계입니다. 외부(LS 유형 5) 링크 상태 알림은 이 합계에서 제외됩니다. 이 합계를 사용하면 라우터의 링크 상태 데이터베이스가 변경되었는지 여부를 확인하고 두 라우터의 링크 상태 데이터베이스를 비교할 수 있습니다. 이 값은 16진수입니다.

OSPFv3 영역 구성

1. OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

구성이 저장되고 장치가 업데이트됩니다.

Create Stub Area(스태프 영역 만들기) 및 NSSA Create(NSSA 만들기) 단추가 있는 웹 페이지가 다시 나타납니다.

그림 11-18. OSPFv3 Area Configuration - Create Stub Area and NSSA Create(OSPFv3 영역 구성 - 스태프 영역 만들기 및 NSSA 만들기)



OSPFv3 스태프 영역 구성

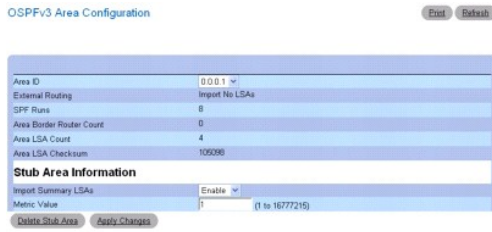
1. OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

Create Stub Area(스태프 영역 만들기) 및 NSSA Create(NSSA 만들기) 단추가 있는 웹 페이지가 다시 나타납니다. [그림 11-18](#)을 참조하십시오.

4. Create Stub Area(스텝 영역 만들기)를 클릭합니다.

Stub Area Information(스텝 영역 정보) 필드가 표시됩니다.

Figure 11-19. OSPFv3 Stub Area Configuration(OSPFv3 스텝 영역 구성)



5. 나머지 필드를 입력합니다.
6. Apply Changes(변경사항 적용)를 클릭합니다.

스텝 영역 정보가 저장되고 장치가 업데이트됩니다.

OSPFv3 NSSA 영역 구성

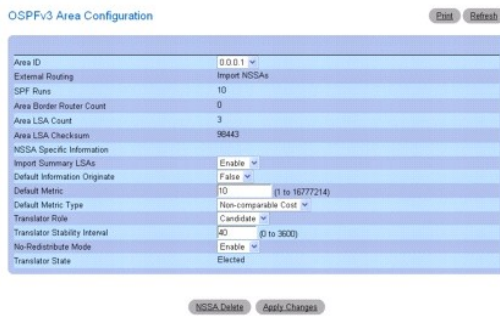
1. OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

Create Stub Area(스텝 영역 만들기) 및 NSSA Create(NSSA 만들기) 단추가 있는 웹 페이지가 다시 나타납니다. [그림 11-18](#)을 참조하십시오.

4. OSPFv3 Area Configuration(OSPFv3 영역 구성) 웹 페이지에서 NSSA Create(NSSA 만들기)를 클릭합니다.

웹 페이지에 NSSA 구성 옵션이 표시됩니다.

Figure 11-20. OSPFv3 Area Configuration - NSSA(OSPFv3 영역 구성 - NSSA)



5. 나머지 필드를 입력합니다.
6. Apply Changes(변경사항 적용)를 클릭합니다.

NSSA 정보가 저장되고 장치가 업데이트됩니다.

OSPFv3 스텝 영역 정보 삭제

1. 구성된 스텝 영역 정보가 있는 OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 엽니다.
2. Delete Stub Area(스텝 영역 삭제)를 클릭합니다.

3. Apply Changes(변경사항 적용)를 클릭합니다.

OSPFv3 NSSA 정보 삭제

1. 구성된 NSSA 정보가 있는 OSPFv3 Area Configuration(OSPFv3 영역 구성) 페이지를 엽니다.
2. NSSA Delete(NSSA 삭제)를 클릭합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

CLI 명령을 사용하여 OSPFv3 영역 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

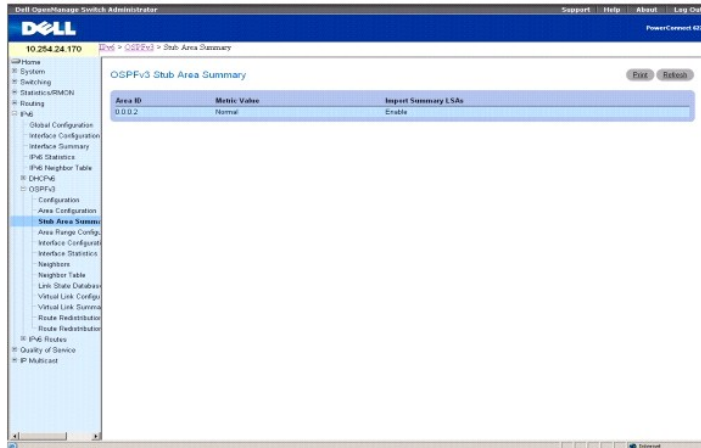
1. OSPFv3 명령

OSPFv3 스텝 영역 요약

OSPFv3 Stub Area Summary(OSPFv3 스텝 영역 요약) 페이지를 사용하여 OSPFv3 스텝 영역 세부 사항을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6→OSPFv3→Stub Area Summary(스텝 영역 요약)를 클릭합니다.

그림 11-21. OSPFv3 Stub Area Summary(OSPFv3 스텝 영역 요약)



OSPFv3 Stub Area Summary(OSPFv3 스텝 영역 요약) 페이지에는 다음과 같은 필드가 있습니다.

Area ID(영역 ID) — 스텝 영역의 영역 ID입니다.

Metric Value(메트릭 값) — 영역에 알려진 기본 경로에 적용된 메트릭 값입니다.

Import Summary LSAs(요약 LSA 가져오기) — 요약 LSA 가져오기가 활성화되었는지 또는 비활성화되었는지 나타냅니다.

CLI 명령을 사용하여 OSPFv3 스텝 영역 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

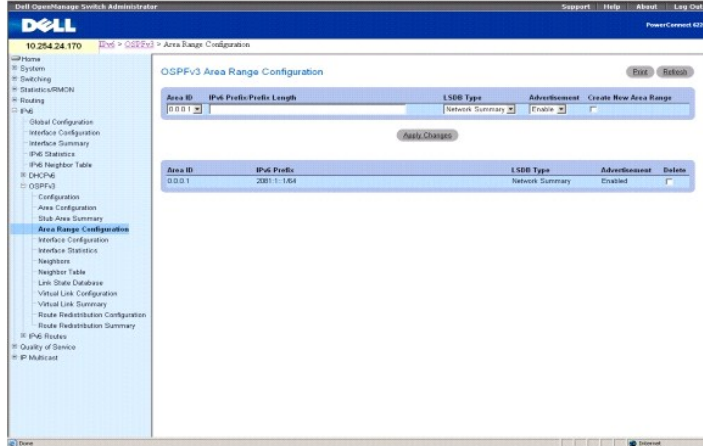
1. OSPFv3 명령

OSPFv3 영역 범위 구성

OSPFv3 Area Range Configuration(OSPFv3 영역 범위 구성) 페이지를 사용하여 OSPFv3 영역 범위를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6→OSPFv3→Area Range Configuration(영역 범위 구성)을 클릭합니다.

Figure 11-22. OSPFv3 Area Range Configuration(OSPFv3 영역 범위 구성)



OSPFv3 Area Range Configuration(OSPFv3 영역 범위 구성) 페이지에는 다음과 같은 필드가 있습니다.

Area ID(영역 ID) — 데이터를 구성할 영역을 선택합니다.

IPv6 Prefix/Prefix Length(IPv6 접두어/접두어 길이) — 선택한 영역의 주소 범위에 대해 IPv6 접두어/접두어 길이를 입력합니다.

LSDB Type(LSDB 유형) — 지정된 영역 및 주소 범위와 연관된 링크 알링 유형을 선택합니다. 기본 유형은 Network Summary(네트워크 요약)입니다.

Advertisement(알림) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. Enable(활성)을 선택하면 네트워크 요약 LSA를 통해 주소 범위가 영역 외부에 알려집니다. 기본값은 Enable(활성)입니다.

Create New Area Range(새 영역 범위 만들기) — 지정된 값을 사용하여 새 OSPFv3 영역 범위를 만들려면 이 확인란을 클릭합니다.

Area ID(영역 ID) — OSPFv3 영역입니다.

IPv6 Prefix(IPv6 접두어) — 영역의 주소 범위에 대한 IPv6 접두어입니다.

LSDB Type(LSDB 유형) — 주소 범위 및 영역에 대한 링크 알링 유형입니다.

Advertisement(알림) — 주소 범위 및 영역에 대한 알림 모드입니다.

Delete(삭제) — 지정된 OSPFv3 영역 범위를 삭제하려면 이 확인란을 클릭합니다.

OSPFv3 영역 범위 구성

1. OSPFv3 Area Range Configuration(OSPFv3 영역 범위 구성) 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

OSPFv3 영역 범위가 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPFv3 영역 범위 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

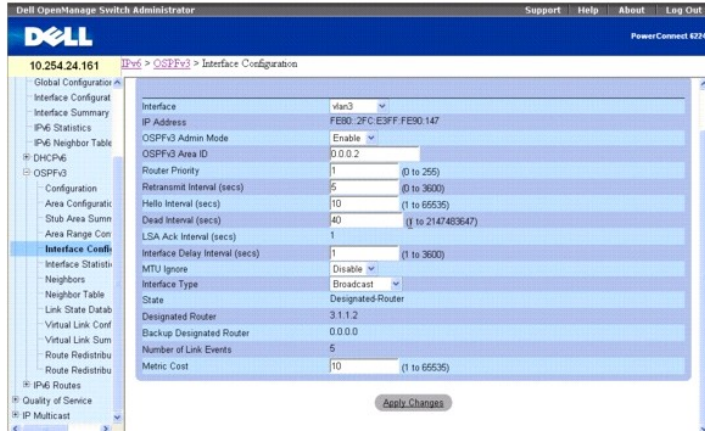
1. OSPFv3 명령

OSPFv3 인터페이스 구성

OSPFv3 Interface Configuration(OSPFv3 인터페이스 구성) 페이지를 사용하여 OSPFv3 인터페이스를 생성하고 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → OSPFv3 → Interface Configuration(인터페이스 구성)을 클릭합니다.

Figure 11-23. OSPFv3 Interface Configuration(OSPFv3 인터페이스 구성)



OSPFv3 Interface Configuration(OSPFv3 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다.

IP Address(IP 주소) — 선택된 인터페이스의 IPv6 주소입니다.

OSPFv3 Admin Mode(OSPFv3 관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택할 수 있습니다. 기본값은 Disable(비활성)입니다. OSPFv3 Admin Mode(OSPFv3 관리 모드)를 활성화하지 않고 OSPFv3 매개변수를 구성할 수 있지만 Admin Mode(관리 모드)를 활성화할 때까지 적용되지 않습니다. 다음 정보는 관리 모드가 활성화된 경우에만 표시됩니다. 상태, 지정된 라우터, 지정된 백업 라우터, 링크 이벤트 수, LSA 승인 간격 및 메트릭 비용. OSPFv3 전체 기능을 사용하려면 인터페이스에 유효한 IPv6 접두어/접두어 길이가 있어야 합니다. 이 작업은 인터페이스 구성 모드에서 `ipv6 address` 명령을 사용하여 CLI를 통해 수행할 수 있습니다.

OSPFv3이 라우터에서 초기화되면 라우터가 재설정될 때까지 초기화된 상태로 유지됩니다.

OSPFv3 Area ID(OSPFv3 영역 ID) — 선택된 라우터 인터페이스가 연결되는 OSPFv3 영역을 고유하게 식별하는, 점으로 된 10진수 형식의 32비트 정수입니다. 존재하지 않는 영역 ID를 할당하면 해당 영역이 기본값으로 생성됩니다.

Router Priority(라우터 우선 순위) — 선택된 인터페이스에 대한 OSPFv3 우선 순위를 입력합니다. 인터페이스의 우선 순위는 0부터 255 사이의 정수로 지정됩니다. 기본값은 1이며 가장 높은 라우터 우선 순위를 나타냅니다. 값이 0인 경우 이 네트워크에서 해당 라우터를 지정된 라우터로 사용할 수 없습니다.

Retransmit Interval (secs)(재전송 간격(초)) — 지정된 인터페이스에 대한 OSPFv3 재전송 간격을 입력합니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)입니다. 이 값은 데이터베이스 설명 및 링크 상태 요청 패킷을 재전송할 때 사용됩니다. 유효한 값의 범위는 0 ~ 3600초(1시간)입니다. 기본값은 5초입니다.

Hello Interval (secs)(Hello 간격(초)) — 지정된 인터페이스에 대한 OSPFv3 Hello 간격(초)을 입력합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 유효한 값의 범위는 1 ~ 65,535이고 기본값은 10초입니다.

Dead Interval (secs)(Dead 간격(초)) — 지정된 인터페이스에 대해 OSPFv3 Dead 간격(초)을 입력합니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 이 값은 Hello 간격의 배수(예: 4)여야 합니다. 유효한 값의 범위는 1 ~ 2,147,483,647이고 기본값은 40입니다.

LSA Ack Interval (secs)(LSA 승인 간격(초)) — LSA 승인 패킷 전송 간격(초)을 표시하며 재전송 간격보다 작아야 합니다.

Interface Delay Interval (secs)(인터페이스 지연 간격(초)) — 지정된 인터페이스에 대한 OSPFv3 운송 지연을 입력합니다. 선택된 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 지정합니다. 유효한 값의 범위는 1 ~ 3600초(1시간)입니다. 기본값은 1초입니다.

MTU Ignore(MTU 무시) — 패킷을 받을 때 OSPFv3 MTU 불일치 감지를 비활성화합니다. 기본값은 Disable(비활성)입니다.

Interface Type(인터페이스 유형) — 브로드캐스트 모드 또는 지정된 지정 모드로 설정할 수 있는 인터페이스 유형을 입력합니다. 기본 인터페이스 유형은 브로드캐스트입니다.

State(상태) — 선택된 라우터 인터페이스의 현재 상태입니다. 상태는 다음 중 하나입니다.

- 1 Down(다운)** — 초기 인터페이스 상태입니다. 이 상태인 경우에는 하위 레벨 프로토콜에서 인터페이스를 사용할 수 없습니다. 또한 인터페이스 매개변수가 해당 초기 값으로 설정됩니다. 모든 인터페이스 타이머가 비활성화되고 인터페이스와 연관된 인접 항목이 없습니다.
- 1 Loopback(루프백)** — 이 상태에서는 라우터의 네트워크 인터페이스가 하드웨어 또는 소프트웨어에서 순환합니다. 따라서 인터페이스를 일반 데이터 트래픽에 사용할 수 없습니다. 그렇더라도, 인터페이스에 ICMP 핑을 보내거나 비트 오류 테스트 등을 수행하여 이 인터페이스의 상태와 관련한 정보를 수집하는 것이 좋습니다. 따라서 IP 패킷의 주소가 루프백 상태의 인터페이스로 지정될 수도 있습니다. 이 과정이 용이하게 진행되도록 라우터 LSA에서 이러한 인터페이스를 대상이 IP 인터페이스 주소인 단일 호스트 경로로 알립니다.
- 1 Waiting(대기)** — 라우터가 수신된 Hello 패킷을 모니터링하여 네트워크에 대한 지정된 (백업) 라우터 ID를 확인하려고 합니다. 라우터를 지정된 백업 라우터 또는 지정된 라우터로 선택하려면 라우터가 대기 상태에 있어야 합니다. 그러면 지정된 (백업) 라우터가 불필요하게 변경되지 않습니다.
- 1 Designated Router(지정된 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 라우터가 됩니다. 인접 항목은 네트워크에 연결된 모든 다른 라우터로 설정됩니다. 또한 라우터가 네트워크 노드에 대한 네트워크 LSA를 발생해야 합니다. 네트워크 LSA에는 네트워크에 연결되는 모든 라우터(지정된 라우터 포함)에 대한 링크가 포함되어 있습니다.
- 1 Backup Designated Router(지정된 백업 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 백업 라우터가 됩니다. 현재의 지정된 라우터가 실패하면 이 라우터가 지정된 라우터로 승격됩니다. 라우터는 인접 항목을 네트워크에 연결된 모든 다른 라우터로 설정합니다. 지정된 백업 라우터는 플러딩 절차 중에는 지정된 라우터와 약간 다른 기능을 수행합니다.
- 1 Other Designated Router(기타 지정된 라우터)** — 다른 라우터를 지정된 라우터 및 지정된 백업 라우터로 선택한 브로드캐스트 또는 NBMA 네트워크에 인터페이스가 연결됩니다. 라우터가 지정된 라우터와 지정된 백업 라우터 모두에 대한 인접 항목을 생성하려고 시도합니다.

상태는 OSPFv3 관리 모드가 활성화된 경우에만 표시됩니다.

Designated Router(지정된 라우터) — 알람을 보내는 라우터의 관점에서 이 네트워크에 대한 지정된 라우터의 ID입니다. 여기서 지정된 라우터는 해당 라우터 ID를 기준으로 식별됩니다. 값이 0.0.0.0이면 지정된 라우터가 없는 것입니다. 이 필드는 OSPFv3 관리 모드가 활성화된 경우에만 표시됩니다.

Backup Designated Router(지정된 백업 라우터) — 알람을 보내는 라우터의 관점에서 이 네트워크에 대한 지정된 백업 라우터의 ID입니다. 여기서 지정된 백업 라우터는 해당 라우터 ID를 기준으로 식별됩니다. 지정된 백업 라우터가 없으면 0.0.0.0으로 설정합니다. 이 필드는 OSPFv3 관리 모드가 활성화된 경우에만 표시됩니다.

Number of Link Events(링크 이벤트 수) — 지정된 OSPFv3 인터페이스가 해당 상태를 변경한 횟수입니다. 이 필드는 OSPFv3 관리 모드가 활성화된 경우에만 표시됩니다.

Metric Cost(메트릭 비용) — 이 인터페이스에 대한 TOS(서비스 종류) 비용 값을 입력합니다. 메트릭 비용 범위는 1 - 65,535입니다. 메트릭 비용은 OSPFv3이 인터페이스 초기화된 경우에만 구성됩니다.

OSPFv3 인터페이스 구성

1. **OSPFv3 Interface Configuration(OSPFv3 인터페이스 구성)** 페이지를 엽니다.
2. OSPFv3을 구성할 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스가 OSPFv3에 대해 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPFv3 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

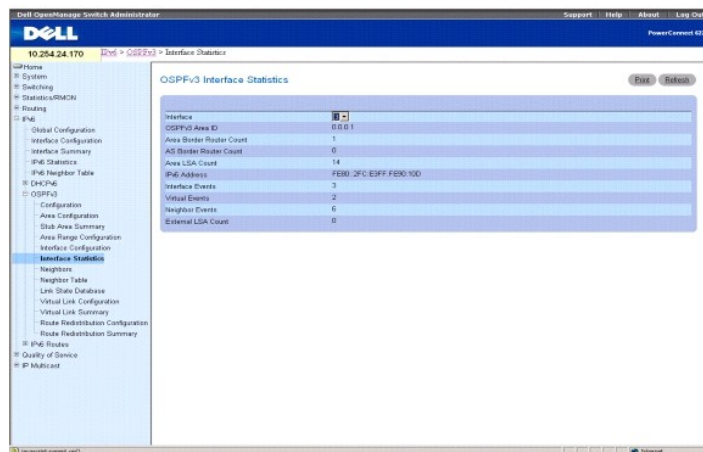
1. OSPFv3 명령

OSPFv3 인터페이스 통계

OSPFv3 Interface Statistics(OSPFv3 인터페이스 통계) 페이지를 사용하여 OSPFv3 인터페이스 통계를 표시합니다. 정보는 OSPF가 활성화된 경우에만 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6** → **OSPFv3** → **Interface Statistics(인터페이스 통계)**를 클릭합니다.

Figure 11-24. OSPFv3 Interface Statistics(OSPFv3 인터페이스 통계)



Interface	OSPFv3 Area ID
GigabitEthernet1	0.0.0.1
Area Border Router Count	1
AS Border Router Count	0
Area LSA Count	14
RPF Address	FE80::2FC:EFF:FE80::10D
Interface Events	3
Virtual Events	2
Neighbor Events	6
External Link Count	0

OSPFv3 Interface Statistics(OSPFv3 인터페이스 통계) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

OSPF Area ID(OSPF 영역 ID) — 선택된 라우터 인터페이스가 속하는 OSPF 영역입니다. OSPF 영역 ID는 인터페이스가 연결되는 영역을 고유하게 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다.

Area Border Router Count(영역 경계 라우터 수) — 이 영역에서 연결 가능한 총 영역 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

AS Border Router Count(AS 경계 라우터 수) — 이 영역에서 연결 가능한 총 차지 시스템 경계 라우터 수입니다. 이 값은 처음에는 0이지만 SPF 통과마다 계산됩니다.

Area LSA Count(영역 LSA 수) — AS 외부 LSA를 제외한 이 영역의 링크 상태 데이터베이스에 있는 총 링크 상태 알림 수입니다.

IPv6 Address(IP 주소) - 인터페이스의 IP 주소입니다.

Interface Events(인터페이스 이벤트 수) — 지정된 OSPF 인터페이스의 상태가 변경되었거나 오류가 발생한 횟수입니다.

Virtual Events(가상 이벤트 수) — 이 가상 링크에서 발생한 상태 변경 또는 오류 수입니다.

Neighbor Events(인접 이벤트 수) — 이 인접 관계의 상태가 변경되었거나 오류가 발생한 횟수입니다.

External LSA Count(외부 LSA 수) — 링크 상태 데이터베이스의 외부(LS 유형 5) 링크 상태 알림 수입니다.

OSPFv3 인터페이스 통계 표시

1. OSPFv3 Interface Statistics(OSPFv3 인터페이스 통계) 페이지를 엽니다.
2. Interface(인터페이스) 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

인터페이스에 대한 통계가 표시됩니다.

CLI 명령을 사용하여 OSPFv3 인터페이스 통계 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

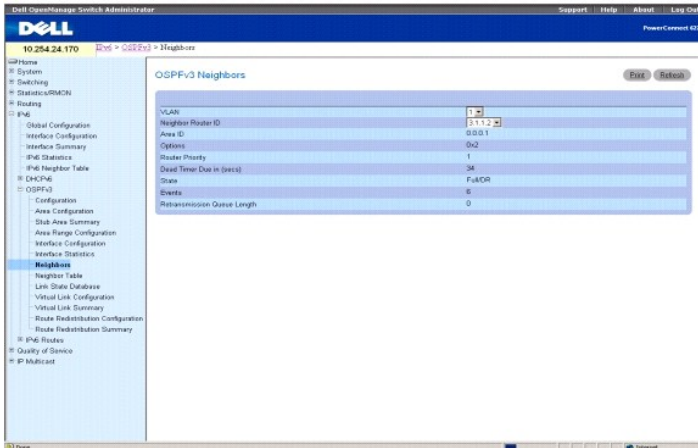
1. OSPFv3 명령

OSPFv3 인접 항목

OSPFv3 Neighbors(OSPFv3 인접 항목) 페이지를 사용하여 선택한 인접 항목 ID의 OSPF 인접 항목 구성을 표시합니다. 특정 인접 항목 ID를 지정하면 해당 인접 항목에 대한 세부 정보가 표시됩니다. 인접 항목 정보는 OSPF를 활성화하고 인터페이스에 인접 항목이 있는 경우에만 표시됩니다. IP 주소는 인접 항목의 IP 주소입니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → OSPFv3 → Neighbors(인접 항목)를 클릭합니다.

Figure 11-25. OSPFv3 Neighbors(OSPFv3 인접 항목)



OSPFv3 Neighbors(OSPFv3 인접 항목) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다.

Neighbor Router ID(인접 항목 라우터 ID) — 데이터를 표시한 인접 항목의 IP 주소를 선택합니다.

Area ID(영역 ID) — 인접 라우터를 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다.

Options(옵션) — 인접 항목이 지원하는 선택적 OSPF 기능입니다. 또한 인접 항목의 선택적 OSPF 기능은 Hello 패킷에도 나열됩니다. 이를 통해 특정 중요 OSPF 기능에 불일치가 있는 경우 수신된 Hello 패킷을 거부할 수 있습니다(예를 들어, 인접 항목 관계를 구성하도록 시작하지 않는 경우).

Router Priority(라우터 우선 순위) — 지정된 인접 항목에 대한 OSPF 우선 순위를 표시합니다. 인접 항목의 우선 순위는 0부터 255 사이의 정수 값으로 지정됩니다. 값이 0이면 라우터를 이 네트워크의 지정된 라우터로 지정할 수 없습니다.

Dead Timer Due in (secs)(Dead 타이머 제한 시간(초)) — Hello 패킷이 도착하지 않는 경우 인접 항목을 Dead 상태로 선언하기 전에 경과되는 시간을 지정합니다.

State(상태) — 인접 항목의 상태는 다음 중 하나입니다.

- 1 **Down(다운)** — 인접 통신의 초기 상태입니다. 인접 항목에서 수신된 최신 정보가 없음을 표시합니다. 빈도는 높지 않지만 NBMA 네트워크에서 Hello 패킷이 다른 상태인 인접 항목으로 전송되는 경우도 있습니다.
- 1 **Attempt(시도)** — 이 상태는 NBMA 네트워크에 연결된 인접 항목에만 유효합니다. 인접 항목으로부터 최근에 수신된 정보는 없지만 인접 항목에 연결하기 위해 보다 효율적인 노력이 필요함을 나타냅니다. 이를 위해 인접 항목에 Hello 간격으로 Hello 패킷을 보냅니다.
- 1 **Init(초기화)** — 이 상태는 인접 항목으로부터 Hello 패킷이 최근에 표시된 적이 있음을 나타냅니다. 아직은 인접 항목과의 양방향 통신이 설정되지 않습니다. 즉, 라우터가 인접 항목의 Hello 패킷에 표시되지 않습니다. 이 상태 이상에 해당하는 모든 인접 항목은 연관된 인터페이스에서 보낸 Hello 패킷에 나열됩니다.
- 1 **2-Way(양방향)** — 이 상태에서는 두 라우터 간에 양방향으로 통신합니다. 양방향 통신은 Hello 프로토콜 작업을 통해 보장됩니다. 이 상태는 시작 인접 관계 설정이 없는 가장 높은 상태입니다. 지정된 (백업) 라우터는 상태가 양방향 이상에 해당하는 인접 항목 집합 중에서 선택됩니다.
- 1 **Exchange Start(교환 시작)** — 인접하는 두 라우터 간의 인접 관계를 생성하는 첫 번째 단계입니다. 이 단계의 목적은 마스터로 사용할 라우터를 결정하고 초기 DD 순번을 결정하는 데 있습니다. 이 상태 이상에서 수행되는 인접 통신을 인접 관계라고 합니다.
- 1 **Exchange(교환)** — 이 상태의 라우터는 인접 항목에 Database Description(데이터베이스 설명) 패킷을 보내 전체 링크 상태를 설명합니다. 이 상태에서는 인접 항목의 최신 LSA를 요청하는 링크 상태 요청 패킷이 전송될 수도 있습니다. 교환 상태 이상에 해당하는 모든 인접 관계는 플러딩 절차에 사용됩니다. 이러한 인접 관계에서는 모든 유형의 OSPF 라우팅 프로토콜 패킷을 완벽하게 전송하고 수신할 수 있습니다.
- 1 **Loading(로드 중)** — 이 상태에서는 교환 상태에서 검색되었지만 아직 수신되지 않은 최신 LSA를 요청하는 링크 상태 요청 패킷이 인접 항목에 전송됩니다.
- 1 **Full(전체)** — 이 상태에서는 인접하는 라우터가 서로 완벽하게 접합합니다. 이러한 인접 상태가 라우터 LSA 및 네트워크 LSA에서 나타납니다.

Events(이벤트 수) — 이 인접 관계의 상태가 변경되었거나 오류가 발생한 횟수입니다.

Retransmission Queue Length(재전송 대기열 길이) — 재전송 대기열의 현재 길이입니다.

OSPFv3 인접 항목 표시

1. OSPFv3 Neighbors(OSPFv3 인접 항목) 페이지를 엽니다.
 2. Interface(인터페이스) 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.
 3. 표시할 Neighbor Router ID(인접 항목 라우터 ID)를 선택합니다.
- 선택된 인터페이스 Neighbor ID(인접 항목 ID)에 대한 통계가 표시됩니다.

CLI 명령을 사용하여 OSPFv3 인접 항목 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

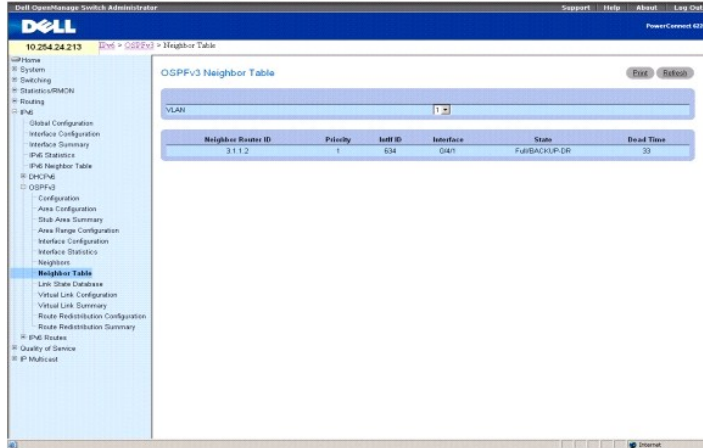
- 1 OSPFv3 명령

OSPFv3 인접 항목 표

OSPFv3 Neighbor Table(OSPFv3 인접 항목 표) 페이지를 사용하여 OSPF 인접 항목 표 목록을 표시합니다. 특정 인접 ID를 지정하면 해당 인접 항목에 대한 자세한 정보가 제공됩니다. 인접 항목 표는 OSPF가 활성화된 경우에만 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → OSPFv3 → Neighbor Table(인접 항목 표)을 클릭합니다.

Figure 11-26. OSPFv3 Neighbor Table(OSPFv3 인접 항목 표)



OSPFv3 Neighbor Table(OSPFv3 인접 항목 표) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다.

Neighbor Router ID(인접 항목 라우터 ID) — 인접 인터페이스를 나타내는, 점으로 된 10진수 형식의 32비트 정수입니다.

Priority(우선 순위) — 지정된 라우터 선택 알고리즘으로 된 이 인접 항목의 우선 순위입니다. 값이 0인 경우 이 네트워크에서 해당 인접 항목을 지정된 라우터로 사용할 수 없습니다.

IntfID — 인접 항목이 이 링크의 해당 Hello 패킷에 알린 인터페이스 ID입니다.

Interface(인터페이스) — 인접 항목 인터페이스 색인을 식별하는 슬롯/포트입니다.

State(상태) — 이 인접 항목과의 관계 상태입니다.

Dead Time(데드 타임) — 마지막 Hello가 인접 항목으로부터 수신한 시간(초)입니다. Init보다 적거나 같은 상태의 인접 항목의 경우 이 값을 0으로 설정합니다.

OSPFv3 인접 항목 표 표시

1. OSPFv3 Neighbor Table(OSPFv3 인접 항목 표) 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

선택한 인터페이스의 OSPF 인접 항목 표가 표시됩니다.

CLI 명령을 사용하여 OSPFv3 인접 항목 표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. OSPFv3 명령

OSPFv3 링크 상태 데이터베이스

OSPFv3 Link State Database(OSPFv3 링크 상태 데이터베이스) 페이지를 사용하여 링크 상태 데이터베이스를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → OSPFv3 → Link State Database(링크 상태 데이터베이스)를 클릭합니다.

그림 11-27. OSPFv3 Link State Database(OSPFv3 링크 상태 데이터베이스)



OSPFv3 Link State Database(OSPFv3 링크 상태 데이터베이스) 페이지에는 다음과 같은 필드가 있습니다.

Adv. Router(Adv. 라우터) — 자치 시스템(AS)에서 라우터를 고유하게 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다. 라우터 ID는 OSPFv3 Configuration(OSPFv3 구성) 페이지에서 설정됩니다.

Area ID(영역 ID) — 라우터 인터페이스 중 하나가 연결되는 OSPF 영역의 ID입니다. 영역 ID는 인터페이스가 연결되는 영역을 고유하게 식별하는, 정으로 된 10진수 형식의 32비트 정수입니다.

LSA Type(LSA 유형) — 링크 상태 알람의 형식과 기능입니다. RFC 2740 섹션 A.4에서 정의된 유형은 다음 중 하나일 수 있습니다.

- 1 Router-LSA
- 1 Network-LSA
- 1 Inter-Area-Prefix-LSA
- 1 Inter-Area-Router-LSA
- 1 AS-External-LSA
- 1 Type-7-LSA
- 1 Link-LSA
- 1 Intra-Area-Prefix-LSA

Link ID(링크 ID) — 링크 상태 ID는 알람에 의해 설명된 라우팅 도메인 부분을 식별합니다. LS ID 값은 알람의 LS 유형에 따라 다릅니다.

Age(보존 기간) — 링크 상태 알람이 처음 발생된 이후에 경과한 시간(초)입니다.

Sequence(순서) — 순서 번호 필드는 부호 있는 32비트 정수입니다. 오래되었거나 중복된 링크 상태 알람을 검색하는 데 사용됩니다. 순서 번호가 클수록 최신 알람입니다.

Checksum(검사 합계) — 검사 합은 알람의 데이터 손실을 검색하는 데 사용됩니다. 데이터 손실은 알람이 불러당되는 동안이나 라우터의 메모리에 유지된 상태에서 발생할 수 있습니다. 이 필드는 LS 보존 기간 필드를 제외한 전체 알람 내용의 검사 합입니다.

Options(옵션) — 링크 상태 알람 헤더의 Options(옵션) 필드는 알람과 관련된 선택적 기능을 나타냅니다. 옵션은 다음과 같습니다.

- 1 V6 — 표시되어 있지 않으면 IPv6 라우팅 계산에서 링크가 제외됩니다.
- 1 E — AS-external-LSA가 불러당되는 방식을 설명합니다.
- 1 MC — 사양에 따른 IP 멀티캐스트 데이터그램의 전달 여부를 설명합니다.
- 1 N — Type-7 LSA의 처리 방식을 설명합니다.
- 1 R — 발신자가 활성 라우터에 있는지 표시합니다. R 옵션은 라우터 비트이며, 표시되어 있지 않으면 알람 노드를 통과하는 경로가 계산되지 않습니다.
- 1 DC — 시스템의 요구 회로 처리 방식을 설명합니다.

Rtr Opt.(라우터 옵션) — 라우터별 옵션을 표시합니다.

CLI 명령을 사용하여 OSPFv3 링크 상태 데이터베이스 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

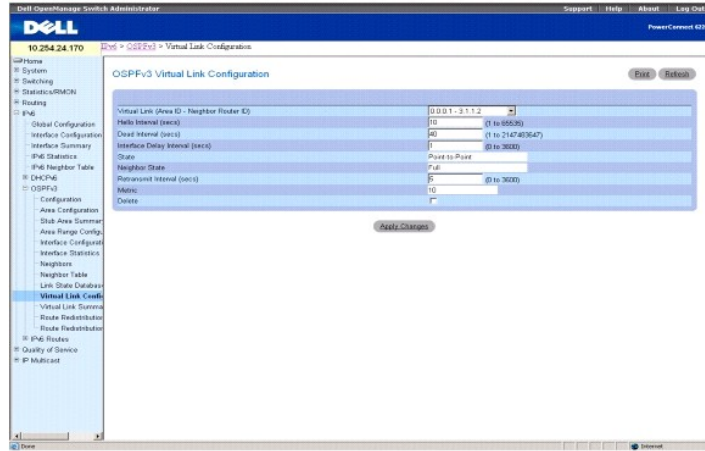
- 1 OSPFv3 명령

OSPFv3 가상 링크 구성

OSPFv3 Virtual Link Configuration(OSPFv3 가상 링크 구성) 페이지를 사용하여 새 가상 링크를 정의하거나 기존 가상 링크를 구성합니다. 이 페이지를 표시하려면 OSPFv3 영역 구성 페이지를 통해 유효한 OSPFv3 영역을 정의해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPV6 → OSPFv3 → Virtual Link Configuration(가상 링크 구성)을 클릭합니다.

그림 11-28. OSPFv3 Virtual Link Configuration(OSPFv3 가상 링크 구성)



OSPFv3 Virtual Link Configuration(OSPFv3 가상 링크 구성) 페이지에는 다음과 같은 필드가 있습니다.

Create New Virtual Link(새 가상 링크 만들기) — 새 가상 링크를 정의하려면 드롭다운 메뉴에서 이 옵션을 선택합니다. 가상 링크 확인 영역이 고정됩니다. 새 화면에 인접 라우터 ID를 입력하라는 메시지가 표시됩니다.

Virtual Link(Area ID - Neighbor Router ID)(가상 링크(영역 ID - 인접 라우터 ID)) — 데이터를 표시 또는 구성할 가상 링크를 선택합니다. 영역 ID와 인접 라우터 ID로 구성됩니다.

Hello Interval (secs)(Hello 간격(초)) — 지정된 인터페이스의 OSPF Hello 간격(초)을 입력합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 유효한 값의 범위는 1 ~ 65,535이고 기본값은 10초입니다.

Dead Interval (secs)(Dead 간격(초)) — 지정된 인터페이스의 OSPF Dead 간격(초)을 입력합니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다. 이 값은 Hello 간격의 배수(예: 4)여야 합니다. 유효한 값의 범위는 1 ~ 2,147,483,647이고 기본값은 40입니다.

Interface Delay Interval (secs)(인터페이스 지연 간격(초)) — 지정된 인터페이스에 대해 OSPF 전송 지연 시간을 입력합니다. 선택된 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 지정합니다. 유효한 값의 범위는 1 ~ 3600초(1시간)입니다. 기본값은 1초입니다.

State(상태) — 선택된 가상 링크의 현재 상태입니다. 상태는 다음 중 하나입니다.

- 1 **Down(다운)** — 초기 인터페이스 상태입니다. 이 상태인 경우에는 하위 레벨 프로토콜에서 인터페이스를 사용할 수 없습니다. 또한 인터페이스 매개변수가 해당 초기 값으로 설정됩니다. 모든 인터페이스 타이머가 비활성화되고 인터페이스와 관련된 인접 항목이 없습니다.
- 1 **Waiting(대기)** — 라우터가 수신된 Hello 패킷을 모니터링하여 지정된 (백업) 라우터 ID를 확인하려고 합니다. 라우터를 지정된 백업 라우터 또는 지정된 라우터로 선택하려면 라우터가 대기 상태에서 벗어나야 합니다. 그러면 지정된 (백업) 라우터가 불필요하게 변경되지 않습니다.
- 1 **Point-to-Point(지정대 지점)** — 인터페이스가 작동 상태이고 가상 링크에 연결되어 있습니다. 이 상태에서 라우터는 인접하는 라우터에 인접 관계를 생성하려고 시도합니다. Hello 패킷이 Hello 간격(초)으로 인접 항목에 전송됩니다.
- 1 **Designated Router(지정된 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 라우터가 됩니다. 인접 항목은 네트워크에 연결된 모든 다른 라우터로 설정됩니다. 또한 라우터가 네트워크 노드에 대한 네트워크 LSA를 발생해야 합니다. 네트워크 LSA에는 네트워크에 연결되는 모든 라우터(지정된 라우터 포함)에 대한 링크가 포함되어 있습니다.
- 1 **Backup Designated Router(지정된 백업 라우터)** — 이 라우터는 연결된 네트워크에서 자체적으로 지정된 백업 라우터가 됩니다. 현재의 지정된 라우터가 실패하면 이 라우터가 지정된 라우터로 승격됩니다. 라우터는 인접 항목을 네트워크에 연결된 모든 다른 라우터로 설정합니다. 지정된 백업 라우터는 플러딩 절차 중에는 지정된 라우터와 약간 다른 기능을 수행합니다.
- 1 **Other Designated Router(기타 지정된 라우터)** — 다른 라우터를 지정된 라우터 및 지정된 백업 라우터로 선택한 브로드캐스트 또는 NBMA 네트워크에 인터페이스가 연결됩니다. 라우터가 지정된 라우터와 지정된 백업 라우터 모두에 대한 인접 항목을 생성하려고 시도합니다.

Neighbor State(인접 상태) — 가상 인접 관계의 상태입니다.

Retransmit Interval(재전송 간격) — 지정된 인터페이스에 대한 OSPF 재전송 간격을 입력합니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)입니다. 이 값은 데이터베이스 설정 및 링크 상태 요청 패킷을 재전송할 때도 사용됩니다. 유효한 값의 범위는 1 ~ 3600초(1시간)입니다. 기본값은 5초입니다.

Metric(메트릭) — 가상 링크에 의해 사용된 메트릭 값입니다.

Delete(삭제) — 라우터 구성에서 지정한 가상 링크를 제거합니다.

새 가상 링크 만들기

1. OSPFv3 Virtual Link Configuration(OSPFv3 가상 링크 구성) 페이지를 엽니다.
2. 새 가상 링크를 정의하려면 드롭다운 메뉴에서 Create New Virtual Link(새 가상 링크 만들기)를 선택합니다.
3. Neighbor Router ID(인접 항목 라우터 ID)를 입력합니다.
4. Create(만들기)를 클릭합니다.

새 링크가 만들어지고 가상 링크 구성 페이지로 돌아갑니다.

가상 링크 구성

1. OSPFv3 Virtual Link Configuration(OSPFv3 가상 링크 구성) 페이지를 엽니다.
2. 구성할 가상 링크를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.
5. 가상 링크가 OSPFv3에 대해 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPFv3 가상 링크 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. OSPFv3 명령

OSPFv3 가상 링크 요약

OSPFv3 Virtual Link Summary(OSPFv3 가상 링크 요약) 페이지를 사용하여 영역 ID 및 인접 항목 라우터 ID별 가상 링크 데이터를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPV6 → OSPFv3 → Virtual Link Summary(가상 링크 요약)를 클릭합니다.

그림 11-29. OSPFv3 Virtual Link Summary(OSPF 가상 링크 요약)

Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Interface Delay Interval (secs)
0.0.0.1	3.1.1.2	10	40	5	1

OSPFv3 Virtual Link Summary(OSPFv3 가상 링크 요약) 페이지에는 다음과 같은 필드가 있습니다.

Area ID(영역 ID) — 배포할 데이터에 대한 가상 링크 식별자의 영역 ID 부분입니다. 영역 ID와 인접 라우터 ID가 결합하여 가상 링크를 정의합니다.

Neighbor Router ID(인접 라우터 ID) — 가상 링크 식별의 인접 항목 부분입니다. 인터페이스가 공통(백본이 아님) 영역을 갖도록 영역 경계 라우터 쌍 안에 가상 링크를 구성할 수 있습니다.

Hello Interval (secs)(Hello 간격(초)) — 가상 링크의 OSPF Hello 간격(초)입니다. Hello 간격 값은 네트워크에 연결된 모든 라우터에 대해 동일해야 합니다.

Dead Interval (secs)(Dead 간격(초)) — 가상 링크의 OSPF Dead 간격(초)입니다. 라우터가 인접 라우터의 Hello 패킷이 표시될 때까지 대기하는 시간을 지정하며, 지정된 시간이 경과하면 해당 라우터가 다운된 것으로 선언합니다. 이 매개변수는 공통 네트워크에 연결된 모든 라우터에 대해 동일해야 하며, Hello 간격의 배수(예: 4)여야 합니다.

Retransmit Interval (secs)(재전송 간격(초)) — 가상 링크의 OSPF 재전송 간격(초)입니다. 이 라우터 인터페이스에 속하는 인접 항목에 대한 링크 상태 알림 간격(초)을 지정합니다. 이 값은 데이터베이스 설명 및 링크 상태 요청 패킷을 재전송할 때도 사용됩니다.

Interface Delay Interval (secs)(인터페이스 지연 간격(초)) — 가상 링크에 대한 OSPF 운송 지연(초)을 입력합니다. 이 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는데 걸리는 예상 시간(초)을 지정합니다.

CLI 명령을 사용하여 OSPFv3 가상 링크 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

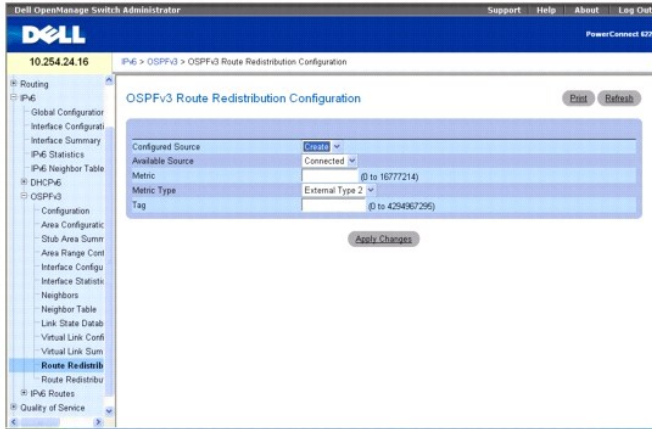
- 1 OSPFv3 명령

OSPFv3 경로 재배포 구성

OSPFv3 Route Redistribution Configuration(OSPFv3 경로 재배포 구성) 페이지를 사용하여 경로 재배포를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6 → OSPFv3 → Route Redistribution Configuration(경로 재배포 구성)**을 클릭합니다.

그림 11-30. OSPFv3 Route Redistribution Configuration(OSPFv3 경로 재배포 구성)



OSPFv3 Route Redistribution Configuration(OSPFv3 경로 재배포 구성) 페이지에는 다음과 같은 필드가 있습니다.

Configured Source(구성된 소스) — 이 드롭다운 메뉴는 동적 선택기이며 OSPF에 의해 재배포용으로 구성된 소스 경로에 의해서만 채워집니다. 선택 상자의 가장 위쪽에 있는 옵션은 Create(만들기)이며 이를 통해 Available Source(사용 가능한 소스) 경로 간에 다른 소스 경로를 구성할 수 있습니다. 유효한 값은 Static(정적), Connected(연결됨) 및 Create(만들기)입니다.

Available Source(사용 가능한 소스) — 이 드롭다운 메뉴는 동적 선택기이며 이전에 OSPF에 의해 재배포용으로 구성되지 않은 소스 경로에 의해서만 채워집니다. 이 메뉴는 Create(만들기) 옵션을 Configured Source(구성된 소스)로 선택한 경우에만 나타납니다. 유효한 값은 Static(정적) 및 Connected(연결됨)입니다.

Metric(메트릭) — 재배포된 경로의 메트릭으로 사용할 메트릭 값을 설정합니다. 소스가 미리 구성되어 있고 수정 가능한 경우에 이 필드에 메트릭이 표시됩니다. 유효한 값은 0 ~ 16,777,214입니다.

Metric Type(메트릭 유형) — 재배포된 경로의 OSPF 메트릭 유형을 설정합니다.

Tag(태그) — 재배포된 경로의 태그 필드를 설정합니다. 이 필드는 소스가 미리 구성된 경우 태그를 표시하며 그렇지 않은 경우 0이 표시됩니다. 유효한 값은 0 ~ 4294967295입니다.

OSPFv3 경로 재배포 구성

1. OSPFv3 Route Redistribution Configuration(OSPFv3 경로 재배포 구성) 페이지를 엽니다.
2. 새 구성된 소스를 설정하려면 **Create(만들기)**를 지정하고 기존 구성된 소스를 수정하려면 **Connected(연결됨)** 또는 **Static(정적)**을 지정합니다.

Figure 11-31. OSPFv3 Route Redistribution Configuration - Configured Source(OSPFv3 경로 재배포 구성 - 구성된 소스)



3. 필요에 따라 나머지 필드를 설정 또는 수정합니다.

4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

선택한 경로 재배포가 OSPFv3에 대해 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 OSPFv3 경로 재배포 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

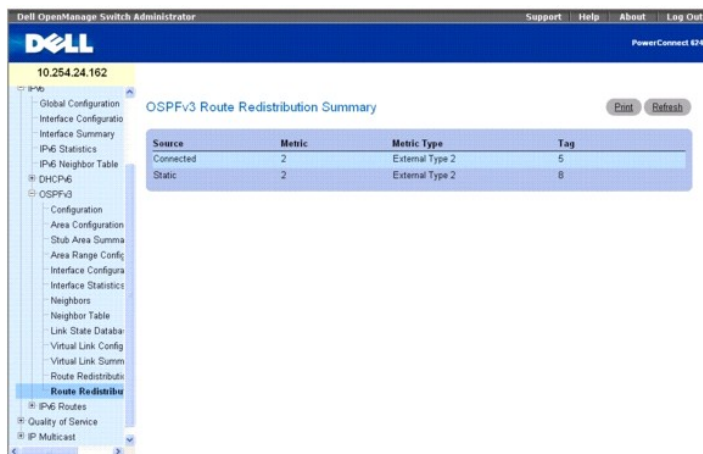
- 1 OSPFv3 명령

OSPFv3 경로 재배포 요약

OSPFv3 Route Redistribution Summary(OSPFv3 경로 재배포 요약) 페이지를 사용하여 소스별 경로 재배포 설정을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6→OSPFv3→Route Redistribution Summary(경로 재배포 요약)를 클릭합니다.

Figure 11-32. OSPFv3 Route Redistribution Summary(OSPFv3 경로 재배포 요약)



OSPFv3 Route Redistribution Summary(OSPFv3 경로 재배포 요약) 페이지에는 다음과 같은 필드가 있습니다.

Source(소스) — OSPF가 재배포할 소스 경로입니다.

Metric(메트릭) — 지정된 소스 경로에 대해 재배포된 경로의 메트릭입니다. 구성되지 않은 경우 Unconfigured(구성 안 됨)를 표시합니다.

Metric Type(메트릭 유형) — 재배포된 경로의 OSPF 메트릭 유형입니다.

Tag(태그) — 재배포된 경로의 태그 필드입니다. 이 필드는 소스가 미리 구성된 경우 태그를 표시하며 그렇지 않은 경우 0이 표시됩니다.

CLI 명령을 사용하여 OSPFv3 경로 재배포 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. OSPFv3 명령

IPv6 경로

IPv6 Routes(IPv6 경로) 메뉴 페이지에는 IPv6 경로 매개변수 및 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→IPv6 Routes(IPv6 경로)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

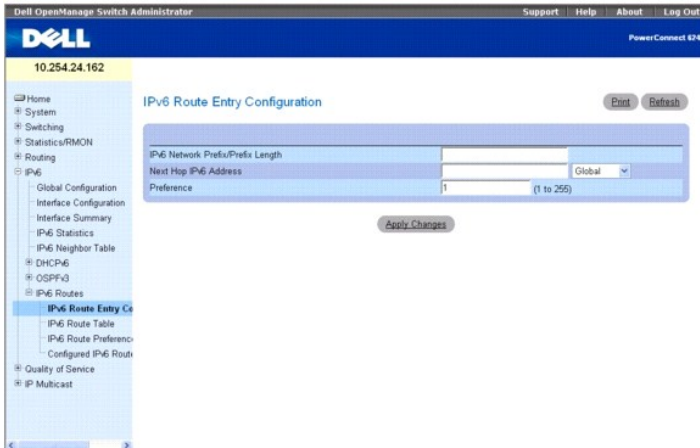
1. [IPv6 경로 항목 구성](#)
1. [IPv6 경로표](#)
1. [IPv6 경로 기본 설정](#)
1. [구성된 IPv6 경로](#)

IPv6 경로 항목 구성

IPv6 Route Entry Configuration(IPv6 경로 항목 구성) 페이지를 사용하여 IPv6 경로에 대한 정보를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IPv6→IPv6 Routes(IPv6 경로)→IPv6 Route Entry Configuration(IPv6 경로 항목 구성)**을 클릭합니다.

그림 11-33. IPv6 Route Entry Configuration(IPv6 경로 항목 구성)



IPv6 Route Entry Configuration(IPv6 경로 항목 구성) 페이지에는 다음과 같은 필드가 있습니다.

IPv6 Network Prefix/PrefixLength(IPv6 네트워크 접두어/접두어 길이) — 유효한 IPv6 네트워크 주소 및 접두어를 입력합니다.

Next Hop IPv6 Address(다음 홉 IPv6 주소) — IPv6 다음 홉 주소를 입력합니다. 지정된 다음 홉 IPv6 주소가 링크 로컬 IPv6 주소인 경우 링크 로컬 IPv6 다음 홉 주소에 대한 인터페이스를 지정합니다. 이 주소를 적용하려면 드롭다운 메뉴에서 Global(전역) 또는 Link-local(링크 로컬)을 선택합니다.

Preference(기본 설정) — 제공된 경로에 대해 기본 설정 값을 입력합니다. 유효한 값은 1 - 255이고 기본값은 1입니다.

IPv6 경로 항목 구성

1. **IPv6 Route Entry Configuration(IPv6 경로 항목 구성)** 페이지를 엽니다.
2. 필요에 따라 필드를 수정합니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

경로 항목이 IPv6에 대해 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 경로 항목 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

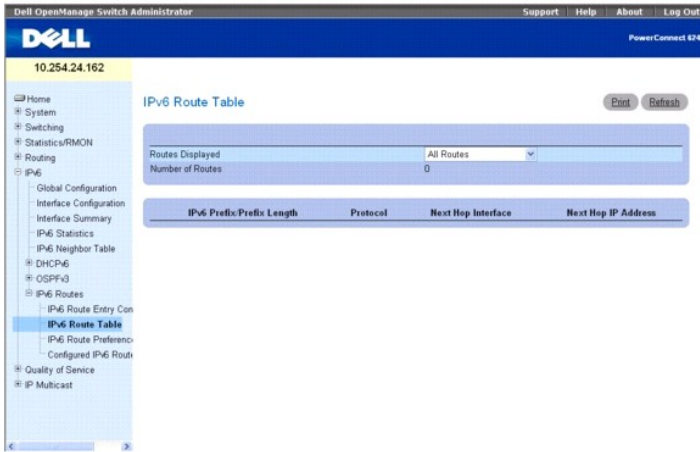
- 1 IPv6 라우팅 명령

IPv6 경로표

IPv6 Route Table(IPv6 경로표) 페이지를 사용하여 모든 활성 IPv6 경로 및 설정을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → IPv6 Routes(IPv6 경로) → IPv6 Route Table(IPv6 경로표)을 클릭합니다.

그림 11-34. IPv6 Route Table(IPv6 경로표)



IPv6 Route Table(IPv6 경로표) 페이지에는 다음과 같은 필드가 있습니다.

Routes Displayed(표시된 경로) — 드롭다운 메뉴에서 Configured Routes(구성된 경로), Best Routes(최적 경로) 또는 All Routes(모든 경로)를 보려면 선택합니다.

Number of Routes(경로 수) — 선택한 경로 유형에 대해 경로표에 전체 활성 경로/최적 경로 수를 표시합니다.

IPv6 Prefix/Prefix Length(IPv6 접두어/접두어 길이) — 활성 경로에 대해 네트워크 접두어 및 접두어 길이를 표시합니다.

Protocol(프로토콜) — 활성 경로에 대해 프로토콜 유형을 표시합니다.

Next Hop Interface(다음 홉 인터페이스) — 경로가 활성 상대인 인터페이스를 표시합니다.

Next Hop IP Address(다음 홉 IP 주소) — 활성 경로에 대해 다음 홉 IPv6 주소를 표시합니다.

IPv6 경로표 표시

1. IPv6 Route Table(IPv6 경로표) 페이지를 엽니다.
2. Routes Displayed(표시된 경로) 필드에서 표시할 경로 유형을 선택합니다.

선택한 경로가 표시됩니다.

CLI 명령을 사용하여 IPv6 경로표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

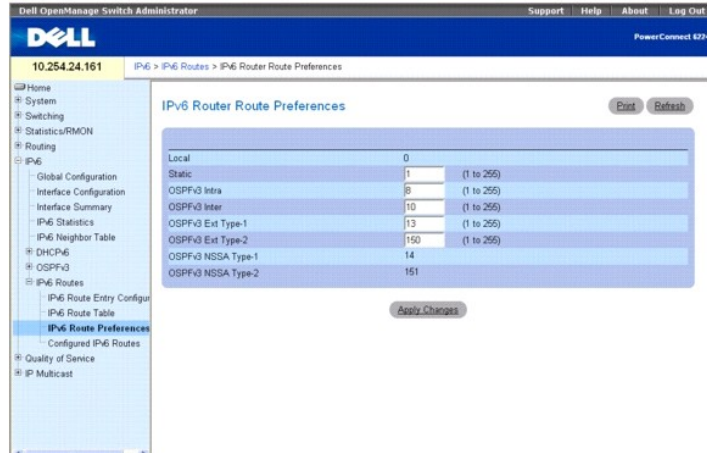
- 1 IPv6 라우팅 명령

IPv6 경로 기본 설정

IPv6 Route Preferences(IPv6 경로 기본 설정) 페이지를 사용하여 각 프로토콜에 대한 기본 설정을 구성합니다. 이러한 값은 1 - 255 범위의 임의의 값이며 경로 메트릭에 대해 독립적입니다. 대부분의 라우팅 프로토콜은 경로 메트릭을 사용하여 다른 프로토콜에 관계 없이 프로토콜에 알려진 최단 경로를 결정합니다. 기본 설정 값이 가장 낮은 경로를 선택하여 대상에 대한 최단 경로를 선택합니다. 대상에 대한 경로가 여러 개 있는 경우 기본 설정 값을 사용하여 기본 경로를 결정합니다. 기본 설정 값이 동일한 경로가 있는 경우 최단 경로 메트릭을 가진 경로가 선택됩니다. 메트릭 불일치 문제를 방지하려면 각 프로토콜에 대해 서로 다른 기본 설정값을 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → IPv6 Routes(IPv6 경로) → IPv6 Route Preferences(IPv6 경로 기본 설정)를 클릭합니다.

Figure 11-35. IPv6 Route Preferences(IPv6 경로 기본 설정)



IPv6 Route Preferences(IPv6 경로 기본 설정) 페이지에는 아래와 같은 필드가 있습니다. 각각의 경우에서 최하위 값은 최상위 기본 설정을 표시합니다.

Local(로컬) — 로컬 기본 설정을 표시하며 구성할 수 없습니다. 값은 0이며 최상위 기본 설정입니다.

Static(정적) — 라우터의 정적 경로 기본 설정값입니다. 기본값은 1이고 범위는 1 ~ 255입니다.

OSPFv3 Intra(OSPFv3 인트라) — 라우터의 OSPFv3 인트라 경로 기본 설정 값입니다. 기본값은 8이고 범위는 1 ~ 255입니다. OSPFv3 사양에서는 OSPFv3을 통해 전달되는 경로에 대한 기본 설정을 intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPFv3 Inter(OSPFv3 내부) — 라우터의 OSPFv3 내부 경로 기본 설정 값입니다. 기본값은 10이고 범위는 1 ~ 255입니다. OSPFv3 사양에서는 OSPFv3을 통해 전달되는 경로에 대한 기본 설정을 intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPFv3 Type-1 — 라우터의 OSPFv3 Type-1 경로 기본 설정 값입니다. 기본값은 13이고 범위는 1 ~ 255입니다. OSPFv3 사양에서는 OSPFv3을 통해 전달되는 경로에 대한 기본 설정을 intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPFv3 Type-2 — 라우터의 OSPFv3 Type-2 경로 기본 설정 값입니다. 기본값은 150이고 범위는 1 ~ 255입니다. OSPFv3 사양에서는 OSPFv3을 통해 전달되는 경로에 대한 기본 설정을 intra(인트라) < inter(내부) < type-1 < type-2와 같은 순서로 지정해야 합니다.

OSPFv3 NSSA Type-1 — 라우터의 OSPFv3 NSSA Type-2 경로 기본 설정 값입니다.

OSPFv3 NSSA Type-2 — 라우터의 OSPFv3 NSSA Type-2 경로 기본 설정 값입니다.

IPv6 경로 기본 설정 구성

1. IPv6 Route Preferences(IPv6 경로 기본 설정) 페이지를 엽니다.
2. 각 프로토콜에 대한 기본 설정을 구성합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

경로 기본 설정이 IPv6에 대해 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IPv6 경로 기본 설정 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

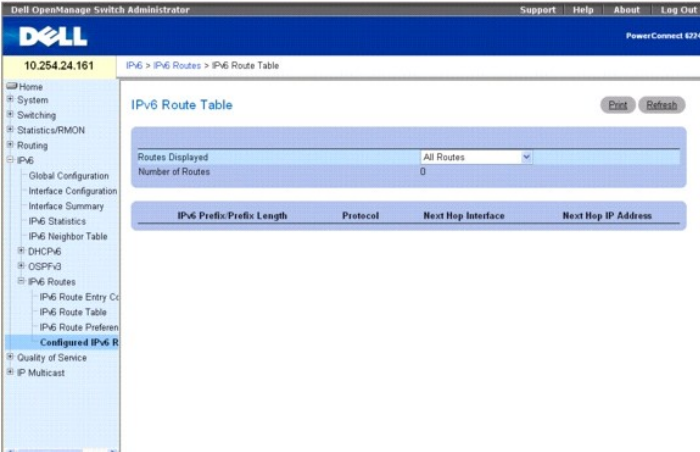
- 1 IPv6Routing 명령

구성된 IPv6 경로

Configured IPv6 Routes(구성된 IPv6 경로) 페이지를 사용하여 선택한 IPv6 경로를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IPv6 → IPv6 Routes(IPv6 경로) → Configured IPv6 Routes(구성된 IPv6 경로)를 클릭합니다.

그림 11-36. Configured IPv6 Routes(구성된 IPv6 경로)



Configured IPv6 Routes(구성된 IPv6 경로) 페이지에는 다음과 같은 필드가 있습니다.

Routes Displayed(표시된 경로) — Configured Routes(구성된 경로), Best Routes(최적 경로) 또는 All Routes(모든 경로)를 보려면 선택합니다.

Configured Routes(구성된 경로) 옵션이 선택되어 있으면 다음 필드가 나타납니다.

IPv6 Prefix/Prefix Length(IPv6 접두어/접두어 길이) — 구성된 경로에 대해 네트워크 접두어 및 접두어 길이를 표시합니다.

Next Hop IP(다음 홉 IP) — 구성된 경로에 대해 다음 홉 IPv6 주소를 표시합니다.

Next Hop Interface(다음 홉 인터페이스) — 구성된 경로에 대해 다음 홉 인터페이스를 표시합니다.

Preference(기본 설정) — 구성된 경로에 대해 경로 기본 설정을 표시합니다.

Delete(삭제) — 이 상자 및 Refresh(재생) 단추를 클릭하여 표시된 경로를 삭제합니다.

Best Routes(최적의 경로) 또는 All Routes(모든 경로) 옵션이 선택되어 있으면 다음 필드가 나타납니다.

Number of Routes(경로 수) — Best Routes(최적의 경로) 또는 All Routes(모든 경로)의 수를 표시합니다.

IPv6 Prefix/Prefix Length(IPv6 접두어/접두어 길이) — 구성된 경로에 대해 네트워크 접두어 및 접두어 길이를 표시합니다.

Protocol(프로토콜) — 구성된 경로에 사용 중인 프로토콜을 표시합니다.

Next Hop Interface(다음 홉 인터페이스) — 구성된 경로에 대해 다음 홉 인터페이스를 표시합니다.

Next Hop IP Address(다음 홉 IP 주소) — 구성된 경로에 대해 다음 홉 IPv6 주소를 표시합니다.

IPv6 경로 표시

1. Configured IPv6 Routes(구성된 IPv6 경로) 페이지를 엽니다.
2. Routes Displayed(표시된 경로) 드롭다운 메뉴에서 표시할 경로를 선택합니다.

선택한 경로 및 구성이 표시됩니다.

CLI 명령을 사용하여 IPv6 경로 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 IPv6 라우팅 명령

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

서비스 품질(QoS)구성

Dell™ PowerConnect™ M6220 사용 설명서

- [서비스 품질\(QoS\) 개요](#)
- [구분된 서비스 구성](#)
- [서비스 등급](#)

이 절에서는 서비스 품질(QoS)의 개요를 제공하고 Quality of Service(서비스 품질) 메뉴 페이지에서 사용할 수 있는 QoS 기능인 구분된 서비스 및 서비스 등급에 대해 설명합니다.

서비스 품질(QoS) 개요

일반적인 스위치에서 각 물리적 포트는 연결된 네트워크에서 패킷을 전송하기 위한 하나 이상의 대기열로 구성됩니다. 포트당 여러 개의 대기열이 제공되는 경우도 있으며, 이 경우 사용자 정의 기준에 따라 특정 패킷에 우선권이 주어집니다. 패킷이 포트에서 전송 대기 상태일 때 대기열이 구성된 방법과 포트의 다른 대기열에 있는 트래픽의 양에 따라 서비스되는 속도가 달라집니다. 지연이 필요한 경우 스케줄러에서 전송할 대기열을 승인할 때까지 패킷은 대기열에 보관됩니다. 대기열이 꼭 차서 더 이상 전송 패킷을 보관할 장소가 없게 되면 스위치가 패킷을 삭제합니다.

QoS를 사용하면 엄격한 시간 요구사항이 적용되는 패킷과 지연에 민감하지 않은 패킷을 구별하여 일관되고 예측 가능한 데이터를 제공할 수 있습니다. 엄격한 시간 요구사항이 적용되는 패킷은 QoS 가능 네트워크에서 "특별하게 처리"됩니다. 따라서 네트워크의 모든 요소는 QoS 사용 가능해야 합니다. QoS를 사용할 수 없는 노드가 하나라도 있을 경우 네트워크 경로에 결함이 발생하여 전체 패킷 흐름 성능이 손상됩니다.

Quality of Service(서비스 품질) 메뉴 페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)**를 클릭합니다. 사용 가능한 두 가지 유형의 QoS가 이 메뉴 페이지에 링크로 제공됩니다. 링크는 다음과 같습니다.

- 1 [구분된 서비스 구성](#)
- 1 [서비스 등급](#)

구분된 서비스 구성

DiffServ 개요

QoS 기능은 트래픽을 스트림으로 분류하고 정의된 출발 동작에 따라 특정 QoS를 처리할 수 있는 구분된 서비스(DiffServ)를 지원합니다.

표준 IP 기반 네트워크는 "Best effort" 데이터 전달 서비스를 제공하도록 설계되었습니다. "Best effort" 서비스란 데이터가 전달된다는 보장은 없지만 네트워크에서 데이터를 시기적절하게 전달하려고 노력한다는 의미입니다. 전체 중에는 패킷이 지연되거나 산발적으로 전송되거나 삭제될 수도 있습니다. 전자 우편, 파일 전송과 같은 일반적인 인터넷 응용프로그램의 경우 서비스 성능이 약간 저하되는 것은 별 문제가 되지 않으며 대부분의 경우 이러한 성능 저하를 인식할 수 없습니다. 반대로 음성 또는 멀티미디어와 같이 엄격한 시간 요구사항을 가진 응용프로그램에는 서비스 성능 저하가 부정적인 영향을 미칩니다.

DiffServ 정의

QoS용 DiffServ를 사용하려면 먼저 **Differentiated Services(구분된 서비스)** 메뉴 페이지에서 액세스 가능한 웹 페이지를 사용하여 다음 범주와 기준을 정의해야 합니다.

1. 등급: 등급을 만들고 등급 기준을 정의합니다.
2. 정책: 정책을 만들고 등급을 정책에 연결한 다음 정책 문을 정의합니다.
3. 서비스: 정책을 인바운드 인터페이스에 추가합니다.

패킷은 정의된 기준에 따라 분류 및 처리됩니다. 분류 기준은 등급별로 정의됩니다. 처리는 정책 속성별로 정의됩니다. 정책 속성은 등급 인스턴스별로 정의될 수 있으며 일치하는 항목이 있을 때 적용되는 속성입니다. 정책은 여러 등급을 포함할 수 있습니다. 정책이 활성 상태일 때 수행되는 조치는 패킷과 일치하는 등급에 따라 다릅니다.

패킷 처리는 패킷에 대한 등급 일치 기준을 검사하여 시작됩니다. 정책 내에서 등급 일치 항목이 있을 때 해당 정책이 패킷에 적용됩니다.

Differentiated Services(구분된 서비스) 메뉴 페이지에는 다양한 Diffserv 구성 및 디스플레이 기능에 대한 링크가 있습니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)**→ **Differentiated Services(구분된 서비스)**를 클릭합니다. Differentiated Services(구분된 서비스) 메뉴 페이지에는 다음과 같은 기능에 대한 링크가 포함되어 있습니다.

- 1 [Diffserv 구성](#)
- 1 [등급 구성](#)
- 1 [등급 기준](#)
- 1 [정책 구성](#)

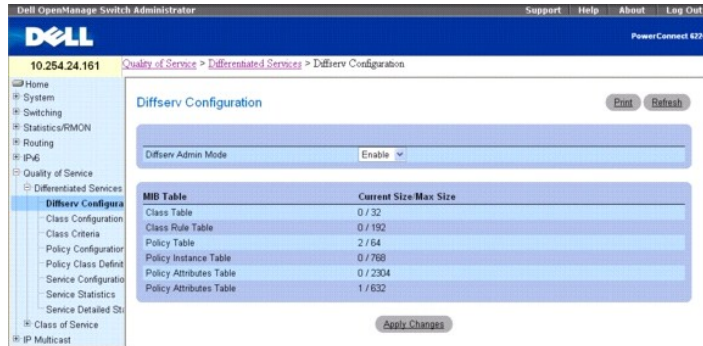
- 1 [정책 등급 정의](#)
- 1 [서비스 구성](#)
- 1 [자세한 서비스 통계](#)

Diffserv 구성

Diffserv Configuration(Diffserv 구성) 페이지를 사용하여 DiffServ General Status Group(Diffserv 일반 상태 그룹) 정보를 표시합니다. 이 정보에는 현재 관리 모드 설정을 비롯하여 각 기본 DiffServ 개인 MIB 표에 있는 현재 행 수 및 최대 행 수가 포함되어 있습니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질) → Differentiated Services(구분된 서비스) → Diffserv Configuration(Diffserv 구성)**을 클릭합니다.

그림 12-1. Diffserv Configuration(Diffserv 구성)



Diffserv Configuration(Diffserv 구성) 페이지에는 다음과 같은 필드가 있습니다.

Diffserv Admin Mode(Diffserv 관리 모드) — 관리 모드를 설정 및 해제합니다. 이 필드가 비활성화된 상태에서는 DiffServ 구성이 유지되고 변경 가능하지만 활성화되지 않습니다. 이 필드를 활성화하면 구분된 서비스가 활성화됩니다.

MIB 표

Class Table(등급 표) — 등급 표의 현재 행 수와 최대 행 수를 표시합니다.

Class Rule Table(등급 규칙 표) — 등급 규칙 표의 현재 행 수와 최대 행 수를 표시합니다.

Policy Table(정책 표) — 정책 표의 현재 행 수와 최대 행 수를 표시합니다.

Policy Instance Table(정책 인스턴스 표) — 정책 인스턴스 표의 현재 행 수와 최대 행 수를 표시합니다.

Policy Attributes Table(정책 속성 표) — 정책 속성 표의 현재 행 수와 최대 행 수를 표시합니다.

Service Table(서비스 표) — 서비스 표의 현재 행 수와 최대 행 수를 표시합니다.

Diffserv 관리 모드 변경

1. **Diffserv Configuration(Diffserv 구성)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 **Enable(활성화)** 또는 **Disable(비활성화)**를 선택하여 **Diffserv Admin Mode(Diffserv 관리 모드)**를 켜거나 끕니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

Diffserv 관리 모드가 변경되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 MIB 표 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

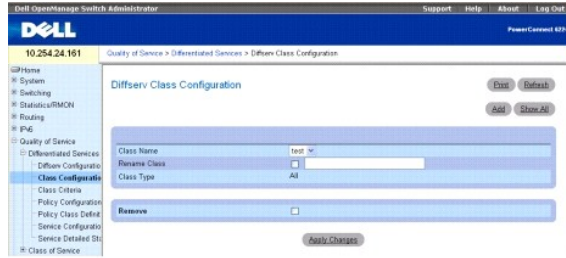
- 1 QoS 명령

등급 구성

Diffserv Class Configuration(Diffserv 등급 구성) 페이지를 사용하여 새 Diffserv 등급 이름을 추가하거나 기존 등급의 이름을 변경 또는 삭제합니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Differentiated Services(구분된 서비스)** → **Class Configuration(등급 구성)** 을 클릭합니다.

그림 12-2. Diffserv Class Configuration(Diffserv 등급 구성)



Diffserv Class Configuration(Diffserv 등급 구성) 페이지에는 다음과 같은 필드가 있습니다.

Class Name(등급 이름) — 이름을 변경하거나 삭제할 등급 이름을 선택합니다. 새 등급 이름을 설정하려면 **Add(추가)** 를 클릭합니다.

Rename Class(등급 이름 변경) — 확인란을 선택한 후 새 이름을 입력하여 표시되는 등급의 이름을 변경합니다.

Class Type(등급 유형) — 모든 등급 유형을 나열합니다. 현재 하드웨어는 **Class Type(등급 유형)** 값 **All(모두)** 만 지원합니다.

All(모두) — 등급에 대해 정의된 다양한 일치 기준을 모두 충족해야 패킷이 일치합니다. All(모두)은 모든 일치 기준의 논리 AND를 나타냅니다.

Remove(제거) — 확인란을 선택하고 **Apply Changes(변경사항 적용)** 를 클릭하면 표시된 등급 이름이 삭제됩니다.

등급 구성 이름 변경

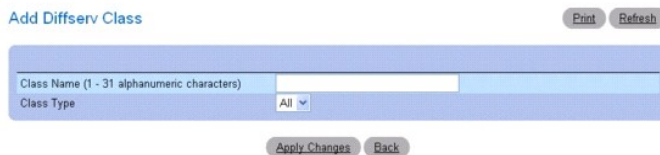
1. **Class Configuration(등급 구성)** 페이지를 엽니다.
2. **Class Name(등급 이름)** 드롭다운 메뉴에서 변경할 등급 이름을 선택합니다.
3. **Rename Class(등급 이름 변경)** 상자를 클릭하고 옆에 있는 필드에 새 이름을 입력합니다.
4. **Apply Changes(변경사항 적용)** 를 클릭합니다.

등급 구성 이름이 변경되고 장치가 업데이트됩니다.

Diffserv 등급 구성 추가

1. **Class Configuration(등급 구성)** 페이지를 엽니다.
2. **Add(추가)** 를 클릭합니다.
Add Diffserv Class(Diffserv 등급 추가) 페이지가 표시됩니다.

그림 12-3. Add Diffserv Class(Diffserv 등급 추가)



3. **Class Name(등급 이름)** 필드에 새 이름을 입력합니다.
4. **Apply Changes(변경사항 적용)** 를 클릭합니다.
Class Name(등급 이름) 이 추가되고 장치가 업데이트됩니다.

등급 구성 제거

1. **Class Configuration(등급 구성)** 페이지를 엽니다.
2. **Class Name(등급 이름)** 드롭다운 메뉴에서 삭제할 등급 이름을 선택합니다.
3. **Remove(제거)** 확인란을 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

관련 등급 구성이 제거되고 장치가 업데이트됩니다.

등급 구성 표시

1. **Class Configuration(등급 구성)** 페이지를 엽니다.
 2. **Show All(모두 표시)**를 클릭합니다.
- 모든 등급 구성이 **Diffserv Class Summary(Diffserv 등급 요약)** 페이지에 표시됩니다.

그림 12-4. Diffserv Class Summary(Diffserv 등급 요약)

	Class Name	Class Type	Reference Class
1	Class B	All	Class A
2	Class A	All	Class A
3	Class C	All	Class B

CLI 명령을 사용하여 등급 구성 추가

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

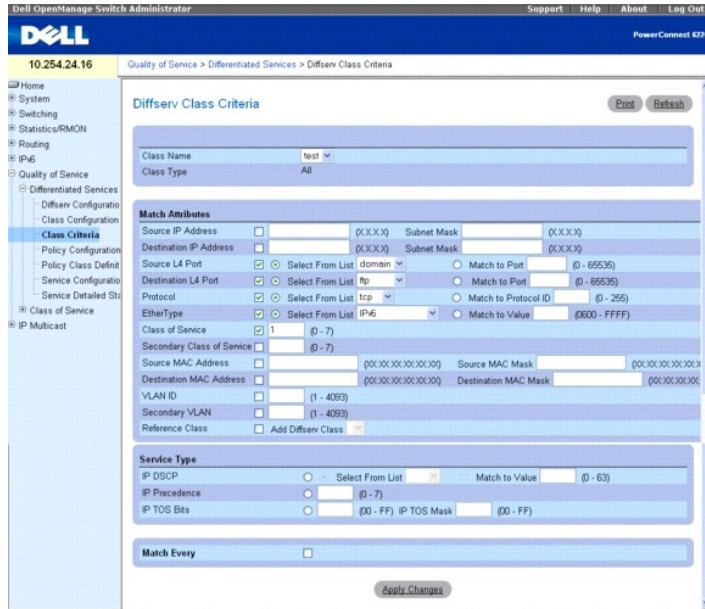
1. QoS 명령

등급 기준

DiffServ Class Criteria(Diffserv 등급 기준) 페이지를 사용하여 DiffServ 등급에 연결할 기준을 정의합니다. 패킷이 수신되면 이러한 DiffServ 등급을 사용하여 패킷의 우선 순위가 지정됩니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Differentiated Services(구분된 서비스)** → **Class Criteria(등급 기준)**를 클릭합니다.

그림 12-5. Diffserv Class Criteria(Diffserv 등급 기준)



Diffserv Class Criteria(Diffserv 등급 기준) 페이지에는 다음과 같은 필드가 있습니다.

Class Name(등급 이름) — 기준을 지정할 등급 이름을 선택합니다.

Class Type(등급 유형) — 등급 유형을 표시합니다. 구성 가능한 클래스 유형 중 지원되는 유형은 **All(모두)**입니다.

일치 특성

다음 필드를 사용하여 패킷을 등급에 일치시킵니다. 등급 기준으로 사용할 각 필드에 대한 확인란을 클릭한 후 관련 필드에 데이터를 입력합니다. 등급에 일치하는 기준이 여러 개 있을 수 있습니다. 논리는 이 기준에 대해 Boolean "논리 AND"입니다.

Source IP Address(소스 IP 주소) — 패킷의 소스 포트 IP 주소가 여기에 나열된 주소와 일치해야 합니다.

Subnet Mask(서브네트 마스크) — 소스 IP 주소의 서브네트 마스크입니다. **Source IP Address(소스 IP 주소)**를 선택한 경우 이 필드는 필수 항목입니다.

Destination IP Address(대상 IP 주소) — 패킷의 대상 포트 IP 주소가 여기에 나열된 주소와 일치해야 합니다.

Subnet Mask(서브네트 마스크) — 대상 IP 주소의 서브네트 마스크입니다. **Source IP Address(소스 IP 주소)**를 선택한 경우 이 필드는 필수 항목입니다.

Source L4 Port(소스 L4 포트) — 패킷의 TCP/UDP 소스 포트가 여기에 나열된 포트와 일치해야 합니다. 다음 옵션 중 하나를 선택하십시오.

Select From List(목록에서 선택) — 패킷을 일치시킬 잘 알려진 소스 포트 목록에서 선택하려면 클릭합니다.

Match to Port(포트 일치) — 패킷을 일치시킬 사용자 정의 포트 ID를 추가하려면 클릭합니다.

Destination L4 Port(대상 L4 포트) — 패킷의 TCP/UDP 대상 포트가 여기에 나열된 포트와 일치해야 합니다. 다음 중 하나를 선택하십시오.

Select From List(목록에서 선택) — 패킷을 일치시킬 잘 알려진 대상 포트 목록에서 선택합니다.

Match to Port(포트 일치) — 패킷을 일치시킬 사용자 정의 포트 ID를 추가하려면 클릭합니다.

Protocol(프로토콜) — 패킷의 프로토콜이 여기에 나열된 프로토콜과 일치해야 합니다. 다음 중 하나를 선택하십시오.

Select from List(목록에서 선택) — 프로토콜 드롭다운 목록에서 선택합니다.

Match to Protocol ID(프로토콜 ID 일치) — 패킷을 일치시킬 프로토콜 ID를 입력합니다.

EtherType — 프레임의 EtherType이 여기에 나열된 EtherType과 일치해야 합니다. 다음 중 하나를 선택하십시오.

Select from List(목록에서 선택) — Ethertypes 드롭다운 목록에서 선택합니다.

Match to Port(포트 일치) — 패킷을 일치시킬 EtherType ID를 입력합니다.

Class of Service (CoS)(서비스 등급(CoS)) — 수신 패킷을 여기에 입력된 CoS에 일치시키려면 패킷의 CoS가 필요합니다.

Source MAC Address(소스 MAC 주소) — 수신 패킷을 여기에 입력된 주소에 일치시키려면 소스 MAC 주소가 필요합니다.

Source MAC Mask(소스 MAC 마스크) — 소스 MAC 주소 와일드카드 마스크를 지정합니다. 와일드카드 마스크에 따라 사용되는 비트와 무시되는 비트가 결정됩니다. 와일드카드 마스크가 255.255.255.255이면 중요한 비트가 없는 것입니다. 와일드카드가 0.0.0.0이면 모든 비트가 중요합니다. **Source MAC Address(소스 MAC 주소)**를 선택한 경우 이 필드는

필수 항목입니다.

Destination MAC Address(대상 MAC 주소) — 수신 패킷을 여기에 입력된 주소에 일치시키려면 대상 MAC 주소가 필요합니다.

Destination MAC Mask(대상 MAC 마스크) — 대상 MAC 주소 와일드카드 마스크를 지정합니다. 와일드카드 마스크에 따라 사용되는 비트와 무시되는 비트가 결정됩니다. 와일드카드 마스크가 255.255.255.255이면 중요한 비트가 없는 것입니다. 와일드카드가 0.0.0.0이면 모든 비트가 중요합니다. **Destination MAC Address(대상 MAC 주소)**를 선택한 경우가 필드는 필수 항목입니다.

VLAN ID — 수신 패킷을 여기에 입력된 VLAN ID에 일치시키려면 패킷의 VLAN ID가 필요합니다.

Secondary VLAN ID(보조 VLAN ID) — 수신 패킷을 여기에 입력된 VLAN ID에 일치시키려면 패킷의 보조 VLAN ID가 필요합니다.

Reference Class(참조 등급) — 기존에 대한 참조를 시작할 등급을 선택합니다. **Add Diffserv Class(Diffserv 등급 추가)** 확인란을 선택한 다음 관련 드롭다운 메뉴에서 이전에 구성된 Diffserv 등급을 선택합니다.

서비스 유형 기준

등급 기준에 대한 일치 패킷에서 사용할 다음 세 일치 필드 중 하나를 선택하려면 클릭합니다.

IP DSCP — 선택한 경우 패킷의 DSCP를 등급 기준의 DSCP에 일치시킵니다. 드롭다운 메뉴에서 DSCP 유형을 선택하거나 일치시킬 DSCP 값을 입력합니다.

IP Precedence(IP 우선 순위) — 선택하여 값을 입력한 경우 패킷의 IP 우선 순위 값을 등급의 IP 우선 순위 값과 일치시킵니다.

IP TOS Bits(IP TOS 비트) — 선택하여 값을 입력한 경우 IP 헤더에 있는 패킷의 서비스 유형 비트를 등급 기준의 서비스 유형과 일치시킵니다.

Match Every(모두 일치) — **Match Every(모두 일치)**를 선택한 경우 패킷이 모든 기준에 일치해야 합니다.

등급 기준 정의

1. **DiffServ Class Criteria(Diffserv 등급 기준)** 페이지를 엽니다.
2. 드롭다운 메뉴에서 일치 속성을 입력할 **Class Name(등급 이름)**을 선택합니다.
3. 이 등급에 대해 일치시킬 속성을 선택하고 해당 기준을 지정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

기준이 이 등급에 추가되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 등급 기준 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

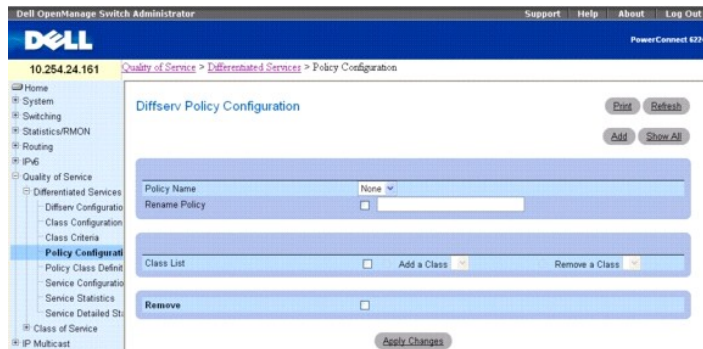
1. QoS 명령

정책 구성

DiffServ Policy Configuration(Diffserv 정책 구성) 페이지를 사용하여 등급 모음을 하나 이상의 정책 문에 연결합니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Differentiated Services(구분된 서비스)** → **Policy Configuration(정책 구성)**을 클릭합니다.

그림 12-6. DiffServ Policy Configuration(Diffserv 정책 구성)



Diffserv Policy Configuration(Diffserv 정책 구성) 페이지에는 다음과 같은 필드가 있습니다.

Policy Name(정책 이름) — 등급에 연결할 정책 이름을 선택합니다.

Rename Policy(정책 이름 변경) — 확인란을 선택하고 새 이름을 입력한 다음 **Apply Changes(변경사항 적용)**를 클릭하여 정책 이름을 변경합니다.

Class List(등급 목록) — 정책에 대한 등급 연결을 구성합니다.

Add a Class(등급 추가) — 드롭다운 메뉴에서 선택한 등급을 정책에 연결합니다.

Remove a Class(등급 제거) — 선택된 등급을 정책에서 제거합니다.

Remove(제거) — 선택된 정책 이름을 장치에서 삭제합니다.

등급과 정책 연결 또는 연결 제거

1. **Diffserv Policy Configuration(Diffserv 정책 구성)** 페이지를 엽니다.
2. 등급에 연결할 **Policy Name(정책 이름)**을 선택합니다.
3. **Class List(등급 목록)** 필드에서 확인란을 선택한 다음 **Add a Class(등급 추가)** 또는 **Remove a Class(등급 삭제)** 라디오 단추를 클릭하고 관련 드롭다운 메뉴에서 **class(등급)**를 선택합니다.
Add a Class(등급 추가)를 사용하여 이 정책과 등급을 연결합니다. **Remove a Class(등급 삭제)**를 사용하여 이 정책에서 등급을 삭제합니다.
4. 해당 드롭다운 메뉴에서 적용할 등급을 선택합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.
수정된 정책이 저장되고 장치가 업데이트됩니다.

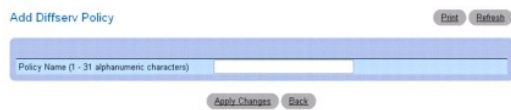
정책 이름 변경

1. **Diffserv Policy Configuration(Diffserv 정책 구성)** 페이지를 엽니다.
2. 이름을 변경할 **Policy Name(정책 이름)**을 선택합니다.
3. **Rename Policy(정책 이름 변경)**를 선택하고 옆에 있는 필드에 새 이름을 입력하여 정책의 이름을 변경합니다.
수정된 정책 이름이 저장되고 장치가 업데이트됩니다.

새 정책 이름 추가

1. **Diffserv Policy Configuration(Diffserv 정책 구성)** 페이지를 엽니다.
2. **Add(추가)**를 클릭합니다.
Add Diffserv Policy(Diffserv 정책 추가) 페이지가 표시됩니다.

그림 12-7. Add Diffserv Policy(Diffserv 정책 추가)



3. 새 **Policy Name(정책 이름)**을 입력합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.
새 정책이 저장되고 장치가 업데이트됩니다.

정책 요약 표시

1. Policy Configuration(정책 구성) 페이지를 엽니다.
2. Show All(모두 표시)을 클릭합니다.

Diffserv Policy Summary(Diffserv 정책 요약) 페이지에 모든 정책 이름, 해당 정책 유형 및 구성원 등급이 표시됩니다.

그림 12-8. Diffserv Policy Summary(Diffserv 정책 요약)

Policy Name	Member Classes
1	1 2
2	1 2

정책 구성 제거

1. Diffserv Policy Configuration(Diffserv 정책 구성) 페이지를 엽니다.
2. Policy Name(정책 이름) 드롭다운 메뉴에서 삭제할 정책 이름을 선택합니다.
3. Remove(제거) 확인란을 선택합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.

관련 정책 구성이 제거되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 정책 구성 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. QoS 명령

정책 등급 정의

DiffServ Policy Class Definition(Diffserv 정책 등급 정의) 페이지를 사용하여 등급을 정책에 연결하고 해당 정책 등급 인스턴스에 대한 속성을 정의합니다.

페이지를 표시하려면 디렉터리 화면에서 Quality of Service(서비스 품질) → Differentiated Services(구분된 서비스) → Policy Class Definition(정책 등급 정의)을 클릭합니다.

그림 12-9. Diffserv Policy Class Definition(Diffserv 정책 등급 정의)

DiffServ Policy Class Definition

Policy Name: East
Member Classes: 1

Drop Packets:

Assign Queue: 5 (0-5) Configured: None

Traffic Conditioning: Configured: None

Redirect Interface: Unit 1, Port 1, LAG ch1

Flow Based Mirroring: Unit 1, Port 1, LAG ch1

Apply Changes

DiffServ Policy Class Definition(Diffserv 정책 등급 정의) 페이지에는 다음과 같은 필드가 있습니다.

Policy Name(정책 이름) — 드롭다운 메뉴에서 구성원 등급에 연결할 정책을 선택합니다.

Member Classes(구성원 등급) — 드롭다운 메뉴에서 이 정책 이름에 연결할 구성원 등급을 선택합니다.

Drop Packets(패킷 삭제) — 이 정책 등급에 대해 패킷을 삭제하려면 이 필드를 선택합니다.

Assign Queue(대기열 할당) — 이 정책 등급의 패킷을 대기열에 할당합니다. 유효한 범위는 0 ~ 6입니다.

Traffic Conditioning(트래픽 조건) — 확인란을 선택하고 드롭다운 메뉴에서 조건을 선택한 경우 트래픽 조건 유형을 지정합니다. 이 필드는 이 정책 등급과 일치하는 트래픽을 처리하는 방법에 영향을 줍니다. **None(없음)**, **Marking(표시)** 및 **Policing(정책 지정)** 중에서 선택합니다. **Marking(표시)** 또는 **Policing(정책 지정)**을 선택하면 화면이 변경되어 관련 필드가 표시됩니다.

1. **None(없음)**: 패킷을 처리하는 동안 트래픽 조건을 발생하지 않도록 지정합니다. 기본 설정입니다.
1. **Marking(표시)**: 패킷에서 IP DSCP, IP Precedence(IP 우선 순위), Class of Service(서비스 등급) 필드 중 하나를 표시할 수 있습니다. **Marking(표시)**을 선택할 때 표시되는 필드에 대한 자세한 내용은 "[패킷 표시 트래픽 조건](#)"을 참조하십시오.
1. **Policing(정책 지정)**: 정책 지정이 수행되는 방법을 구성하고 일치 패킷과 비일치 패킷의 처리 방법을 구성할 수 있습니다. **Policing(정책 지정)**을 선택할 때 표시되는 필드에 대한 자세한 내용은 "[정책 지정 트래픽 조건](#)"을 참조하십시오.

Redirect Interface(인터페이스 재지정) — Redirect Interface(인터페이스 재지정)가 이 정책 등급에 적용되는지 표시하고 인터페이스 또는 LAG를 지정합니다.

Flow Based Mirroring(흐름 기반 미러링) — Flow Based Mirroring(흐름 기반 미러링)이 이 정책 등급에 적용되는지 표시하고 인터페이스 또는 사용된 LAG를 지정합니다..

정책 등급 인스턴스 정의

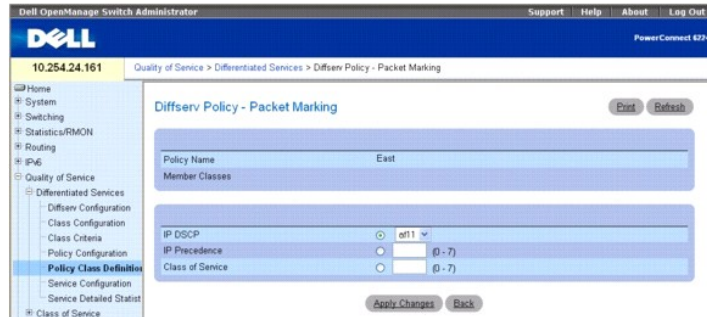
1. Diffserv Policy Class Definition(Diffserv 정책 등급 정의) 페이지를 엽니다.
2. 연결할 정책 및 구성원 등급을 선택합니다.
3. 페이지의 나머지 필드를 사용하여 이 정책 등급 인스턴스에 적용할 속성을 지정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

정책 등급이 정의되고 장치가 업데이트됩니다.

패킷 표시 트래픽 조건

Marking(표시)을 **Traffic Condition(트래픽 조건)**으로 선택하면 다음과 같은 Packet Marking(패킷 표시) 페이지가 표시됩니다.

그림 12-10. Policy Class Definition - Packet Marking(정책 등급 정의 - 패킷 표시)



Diffserv Policy - Packet Marking(Diffserv 정책 - 패킷 표시) 페이지에는 다음과 같은 필드가 있습니다.

Policy Name(정책 이름) — 구성원 등급과 연결된 정책을 표시합니다.

Member Classes(구성원 등급) — 이 정책 이름과 연결된 구성원 등급을 표시합니다.

패킷에 다음 필드 중 하나를 표시할 수 있습니다.

IP DSCP — 표시할 IP DSCP를 선택합니다. 드롭다운 메뉴에서 선택하거나 User Value(사용자 값) 필드에 직접 입력합니다.

IP Precedence(IP 우선 순위) 표시할 지정된 IP Precedence(IP 우선 순위) 대기열 번호를 선택합니다.

Class of Service(서비스 등급) — 표시할 서비스 등급 대기열 번호를 선택합니다.

정책 등급 인스턴스에 대한 패킷 표시 구성

1. Diffserv Policy Class Definition(Diffserv 정책 등급 정의) 페이지의 **Traffic Conditioning(트래픽 조건)** 드롭다운 메뉴에서 **Marking(표시)**를 선택합니다.
Packet Marking(패킷 표시) 페이지가 [그림 12-10](#)과 같이 표시됩니다.

2. IP DSCP, IP Precedence(IP 우선 순위) 또는 Class of Service(서비스 등급)를 선택하여 이 정책 등급에 대해 표시합니다.

3. 이 필드에 대한 값을 선택하거나 입력합니다.

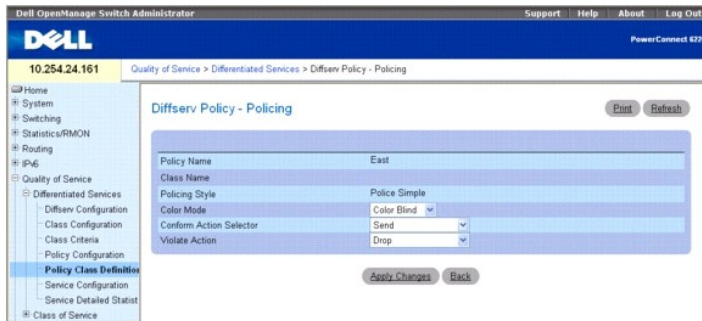
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

정책 등급이 정의되고 장치가 업데이트됩니다.

정책 지정 트래픽 조건

Policing(정책 지정)을 Traffic Condition(트래픽 조건)으로 선택하면 다음과 같은 Diffserv Policy - Policing(Diffserv 정책 - 정책 지정) 페이지가 표시됩니다.

그림 12-11. Policy Class Definition - Policing(정책 등급 정의 - 정책 지정)



Diffserv Policy - Policing(Diffserv 정책 - 정책 지정) 페이지에는 다음과 같은 필드가 있습니다.

Policy Name(정책 이름) — 정책 지정을 구성할 정책을 표시합니다.

Class Name(등급 이름) — 이 정책 이름과 연결된 구성원 등급을 표시합니다.

Policing Style(정책 지정 유형) — 사용 중인 정책 지정 유형을 표시합니다.

Color Mode(색상 모드) — 사용되는 색상 정책 유형을 선택합니다. 드롭다운 메뉴에서 Color Blind(색상 무시) 또는 Color Aware(색상 인식)를 선택합니다.

Conform Action Selector(준수 조치 선택기) — 일치(정책 비율 이하) 패킷을 처리하는 방법을 선택합니다. 옵션은 Send(보내기), Drop(삭제), Mark CoS(CoS 표시), Mark IP DSCP(IP DSCP 표시), Mark IP Precedence(IP 우선 순위 표시) 등입니다.

Violate Action(위반 조치) — 불일치(정책 비율 이상) 패킷을 처리하는 방법을 선택합니다. 옵션은 Send(보내기), Drop(삭제), Mark CoS(CoS 표시), Mark IP DSCP(IP DSCP 표시), Mark IP Precedence(IP 우선 순위 표시) 등입니다.

정책 등급 인스턴스에 대한 정책 구성

1. Diffserv Policy Class Definition(Diffserv 정책 등급 정의) 페이지의 Traffic Conditioning(트래픽 조건) 드롭다운 메뉴에서 Policing(정책 지정)을 선택합니다.

Diffserv Policy - Policing(Diffserv 정책 - 정책 지정) 페이지가 [그림 12-11](#)과 같이 표시됩니다.

2. 하나 이상의 정책 지정 기준을 선택하여 이 정책 등급에 대해 사용하려면 선택합니다.

3. 선택된 각 필드에 대한 값을 선택하거나 입력합니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

다음 Policy Rate Configuration(정책 비율 구성) 페이지가 표시됩니다.

그림 12-12. Policy Rate Configuration(정책 비율 구성)



5. Committed Rate(저장된 비율) 및/또는 Committed Burst Size(저장된 버스트 크기)에 대해 원하는 기준 값을 입력합니다.

6. **Apply Changes(변경사항 적용)**

를 클릭합니다.

저장된 정책 등급 인스턴스에 대해 정책 지정이 구성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 정책 등급 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

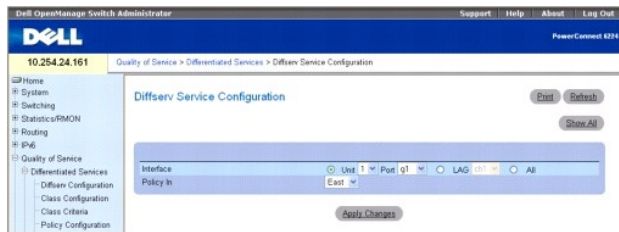
1. QoS 명령

서비스 구성

Diffserv Service Configuration(Diffserv 서비스 구성) 페이지를 사용하여 포트에 대한 정책을 활성화합니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Differentiated Services(구분된 서비스)** → **Service Configuration(서비스 구성)**을 클릭합니다.

그림 12-13. Diffserv Service Configuration(Diffserv 서비스 구성)



Diffserv Service Configuration(Diffserv 서비스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 적용할 인터페이스(Unit/Port(장치/포트), LAG 또는 All(모두))를 선택합니다.

Policy In(정책 위치) — 드롭다운 메뉴에서 포트에 연결할 정책을 선택합니다.

포트에 대한 정책 활성화

1. **Diffserv Service Configuration(Diffserv 서비스 구성)** 페이지를 엽니다.

2. 드롭다운 메뉴에서 인터페이스를 선택합니다.

3. 드롭다운 메뉴에서 정책을 선택합니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

정책이 인터페이스에서 활성화되고 장치가 업데이트됩니다.

Diffserv 서비스 요약 표시

1. **Diffserv Service Configuration(Diffserv 서비스 구성)** 페이지를 엽니다.

2. Show All(모두 표시)을 클릭합니다.

Diffserv Service Summary(Diffserv 서비스 요약) 페이지가 표시됩니다.

그림 12-14. Diffserv Service Summary(Diffserv 서비스 요약)

Interface	Direction	Operation Status	Policy Name
1/g1	In	Down	East

CLI 명령을 사용하여 포트에 정책 할당

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

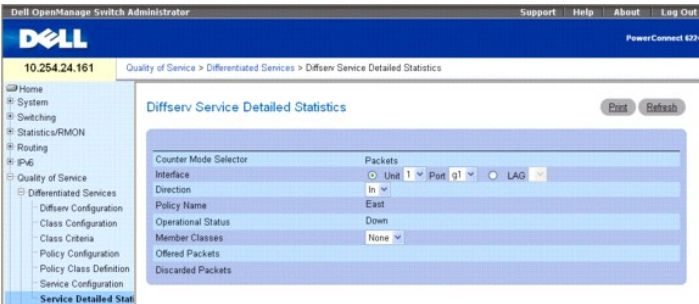
1. QoS 명령

자세한 서비스 통계

Diffserv Service Detailed Statistics(자세한 Diffserv 서비스 통계) 페이지를 사용하여 특정 포트 및 등급에 대한 패킷 세부 사항을 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 Quality of Service(서비스 품질)→ Differentiated Services(구분된 서비스)→ Service Detailed Statistics(자세한 서비스 통계)를 클릭합니다.

그림 12-15. Diffserv Service Detailed Statistics(자세한 Diffserv 서비스 통계)



Diffserv Service Detailed Statistics(자세한 Diffserv 서비스 통계) 페이지에는 다음과 같은 필드가 있습니다.

Counter Mode Selector(카운터 모드 선택기) — 표시할 통계 유형입니다. 패킷만 사용할 수 있습니다.

Interface(인터페이스) — 서비스 통계를 표시할 Unit(장치) 및 Port(포트) 또는 LAG를 선택합니다.

Direction(방향) — 서비스 통계를 표시할 패킷의 방향을 선택합니다.

Policy Name(정책 이름) — 선택한 인터페이스에 연결된 정책을 표시합니다.

Operational Status(작업 상태) — 이 인터페이스에 대한 정책이 활성 상태인지 여부를 표시합니다.

Member Classes(구성원 등급) — 옥텟 통계를 표시할 구성원 등급을 선택합니다.

Offered Packets(제공된 패킷) — 정책과 일치하는 패킷 수를 표시합니다.

Discarded Packets(삭제된 패킷) — 정책에 따라 삭제되는 패킷 수를 표시합니다.

서비스 통계 표시

1. Diffserv Service Detailed Statistics(자세한 Diffserv 서비스 통계) 페이지를 엽니다.
2. 필요에 따라 필드를 입력합니다.

지정된 인터페이스, 방향 및 등급에 대해 패킷 통계를 표시합니다.

CLI 명령을 사용하여 서비스 통계 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 QoS 명령

서비스 등급

서비스 등급(CoS) 대기열 기능을 사용하면 스위치 대기열의 특정 부분을 직접 구성할 수 있습니다. 복잡한 DiffServ가 필요하지 않은 경우 네트워크 트래픽 유형별로 원하는 QoS 동작을 제공합니다. 인터페이스에 도착하는 패킷의 우선 순위를 사용하여 할당표를 통해 해당 아웃바운드 CoS 대기열로 패킷을 이동할 수 있습니다. 보장되는 최소 대역폭, 전송 속도 구성 등과 같이 대기열 할당에 영향을 미치는 CoS 대기열 특성은 대기열 또는 포트 레벨에서 사용자 구성 가능합니다.

포트당 7개의 대기열이 지원됩니다. 하드웨어는 8개의 대기열을 지원하지만 대기열 하나는 스택 서비스시스템에서 내부용으로 사용하도록 항상 예약되어 있습니다.

페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Class of Service(서비스 등급)**를 클릭합니다. **Class of Service(서비스 등급)** 메뉴 페이지에는 다음과 같은 기능에 대한 링크가 포함되어 있습니다.

- 1 [할당표 구성](#)
- 1 [인터페이스 구성](#)
- 1 [인터페이스 대기열 구성](#)

할당표 구성

패킷 필드 중 하나를 신뢰하거나(802.1p, IP Precedence(IP 우선 순위), IP DSCP) 패킷의 우선 순위 지정을 신뢰하지 않도록(신뢰되지 않는 모드) 스위치의 각 포트를 구성할 수 있습니다. 포트는 신뢰 모드로 설정된 경우 사용 중인 신뢰할 수 있는 필드에 적합한 할당표를 사용합니다. 이 할당표는 해당 전송 포트에서 패킷을 전달할 CoS 대기열을 나타냅니다. 신뢰할 수 있는 필드는 할당표의 패킷 내에 있어야 하므로 패킷 내에 없는 경우에 수행되는 기본 조치가 있습니다. 이러한 조치의 예로는 현재 802.1p 할당표에서 트래픽 등급에 할당된 기존 포트 기본 우선 순위에 따라 수신 포트에 대해 구성된 특정 CoS 레벨로 패킷을 직접 전달하는 방법을 들 수 있습니다.

포트가 신뢰되지 않는 모드로 구성되어 있는 경우에는 수신 패킷 우선 순위 지정을 신뢰하지 않고 포트 기본 우선 순위 값을 대신 사용합니다. 신뢰되지 않는 포트를 수신할 때 도착하는 모든 패킷은 수신 포트에 대해 구성된 기본 우선 순위에 따라 해당 전송 포트의 특정 CoS 대기열에 전달됩니다. IP 패킷이 아닌 패킷이 IP DSCP 값을 신뢰하도록 구성된 포트에 도착할 때 처리된 신뢰할 수 있는 포트 할당을 사용할 수 없는 경우에도 이 프로세스가 사용됩니다.

Mapping Table Configuration(할당표 구성) 페이지를 사용하여 서비스 등급을 패킷에 할당하는 방법을 정의합니다.

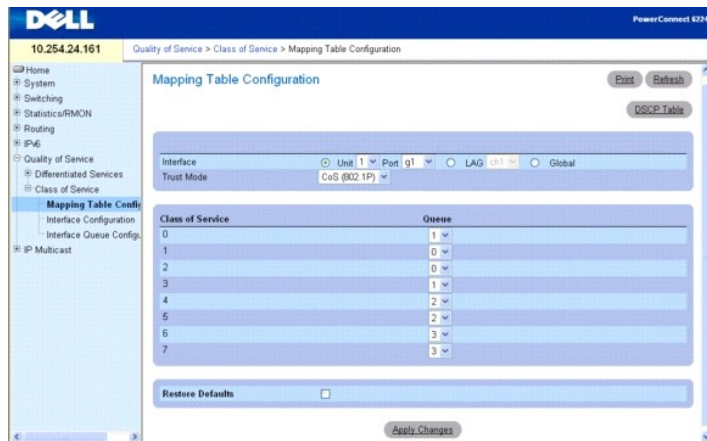
페이지를 표시하려면 디렉터리 화면에서 **Quality of Service(서비스 품질)** → **Class of Service(서비스 등급)** → **Mapping Table Configuration(할당표 구성)**을 클릭합니다.

Mapping Table Configuration(할당표 구성) 페이지에서 선택한 Trust Mode(신뢰 모드)에 따라 페이지가 표시되는 방법과 해당 페이지에서 액세스할 수 있는 필드가 결정됩니다. 여기서는 다음과 같은 3가지 신뢰 모드를 사용할 수 있습니다.

- 1 Untrusted(None)(신뢰되지 않음(사용 안함))
- 1 CoS(802.1P)
- 1 IP DSCP

CoS(802.1P)가 기본 모드이므로 **Class of Service(서비스 등급)** 메뉴 페이지에서 **Mapping Table Configuration(할당표 구성)**을 선택하면 이 페이지가 표시됩니다.

그림 12-16. Mapping Table Configuration – CoS (802.1P)(할당표 구성 - CoS(802.1P))



CoS (802.1P) 신뢰 모드

CoS (802.1P) Mapping Table Configuration(할당표 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 서비스 구성 등급이 적용되는 인터페이스를 선택합니다. 장치 및 포트 또는 LAG를 선택하거나 Global(전역)을 선택하여 모든 인터페이스에 구성 등급을 적용합니다.

Trust Mode(신뢰 모드) — 적용할 신뢰 모드를 선택합니다. CoS (802.1P)가 기본값입니다.

Class of Service(서비스 등급) — 각 서비스 등급을 별도의 행에 나열하므로 서비스 등급마다 별도의 대기열을 할당할 수 있습니다.

Queue(대기열) — 드롭다운 메뉴에서 각 Class of Service(서비스 등급)에 대한 대기열을 선택합니다. 처음에는 기본 대기열이 표시됩니다.

Restore Defaults(기본값 복원) — 확인란을 선택하고 Apply Changes(변경사항 적용)를 클릭하면 기본 대기열 값이 복원됩니다.

CoS (802.1P) 신뢰 모드 구성

1. Mapping Table Configuration(할당표 구성) 페이지를 엽니다.
2. 적용할 장치 및 포트 또는 LAG를 선택하거나 Global(전역)을 선택하여 모든 인터페이스에 설정을 적용합니다.
3. Trust Mode(신뢰 모드)를 선택합니다.
4. 각 Class of Service(서비스 등급)에 연결할 Queue(대기열)를 선택합니다.
5. Apply Changes(변경사항 적용)를 클릭합니다.

변경사항이 선택된 인터페이스에 적용되고 장치가 업데이트됩니다.

대기열 기본값 복원

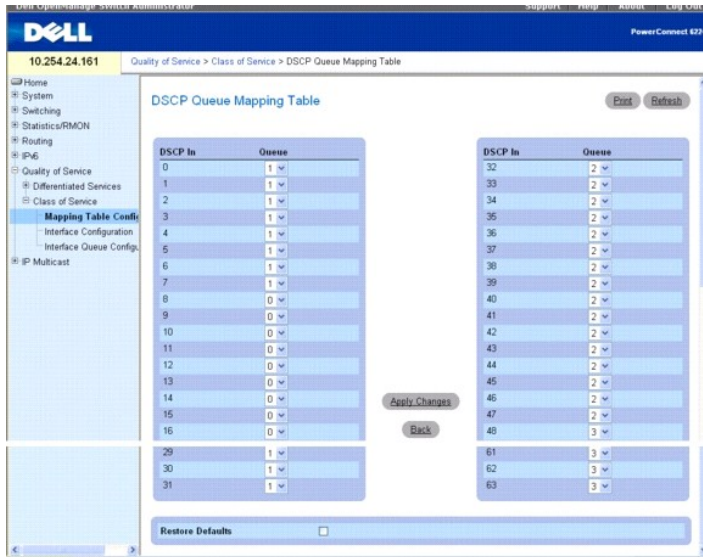
1. Mapping Table Configuration(할당표 구성) 페이지를 엽니다.
2. Restore Defaults(기본값 복원) 확인란을 클릭합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

대기열이 각 서비스 등급에 대한 기본값으로 돌아가고 장치가 업데이트됩니다.

IP DSCP 표 구성

DSCP Queue Mapping Table(DSCP 대기열 할당표)을 액세스하려면 디렉터리 화면에서 Quality of Service(서비스 품질)→Class of Service(서비스 등급)→Mapping Table Configuration(할당표 구성)을 클릭한 다음 DSCP 표 링크를 클릭합니다.

그림 12-17. DSCP Queue Mapping Table(DSCP 대기열 할당표)



DSCP Queue Mapping Table(DSCP 대기열 할당표) 페이지에는 다음과 같은 필드가 있습니다.

DSCP In — 기본으로 선택한 다음 사용할 패킷 내 DiffServ Code Point(DiffServ 코드 지정)를 입력하려면 선택합니다. 이 필드에 따라 패킷이 전송되는 대기열이 결정됩니다.

Queue ID(대기열 ID) — 패킷이 전송되는 대기열을 선택합니다.

대기열 기본값 복원

1. DSCP Queue Mapping Table(DSCP 대기열 할당표) 페이지를 엽니다.
2. Restore Defaults(기본값 복원) 확인란을 클릭합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

대기열 값이 기본값으로 복원되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 할당표 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

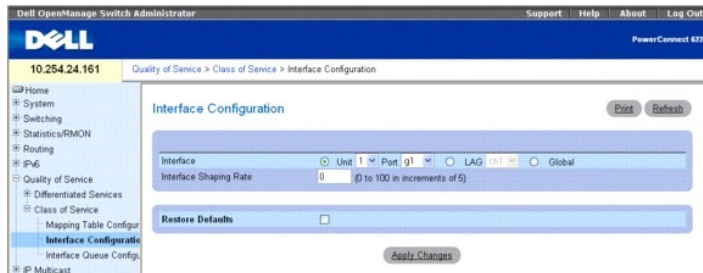
1. QoS 명령

인터페이스 구성

Interface Configuration(인터페이스 구성) 페이지를 사용하여 CoS 구성을 위한 포트를 개별적으로 지정하고 인터페이스 형성 비율을 선택된 포트에 적용합니다.

Interface Configuration(인터페이스 구성) 페이지를 표시하려면 디렉터리 화면에서 Quality of Service(서비스 품질) → Class of Service(서비스 등급) → Interface Configuration(인터페이스 구성)을 클릭합니다.

그림 12-18. Interface Configuration(인터페이스 구성)



Interface Configuration(인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — Interface Shaping Rate(인터페이스 형성 비율)를 적용할 인터페이스를 선택합니다.

Interface Shaping Rate(인터페이스 형성 비율) — 포트에서 내보낼 수 있는 트래픽의 양에 대한 최대값을 설정합니다. 지정된 값은 최대 교성 대역폭의 비율(%)을 나타냅니다. 유효한 값은 0-100이며 5씩 증분됩니다.

Restore Defaults(기본값 복원) — 확인란을 선택하면 선택된 인터페이스에 대한 기본 인터페이스 형성 비율이 복원됩니다.

인터페이스 구성 정의

1. Interface Configuration(인터페이스 구성) 페이지를 엽니다.
2. 적용할 장치 및 포트 또는 LAG를 선택하거나 Global(전역)을 선택하여 모든 인터페이스에 설정을 적용합니다.
3. 이 포트에 적용할 Interface Shaping Rate(인터페이스 형성 비율)를 입력합니다.
4. Apply Changes(변경사항 적용)를 클릭합니다.
새 Interface Shaping Rate(인터페이스 형성 비율)가 선택한 인터페이스에 적용되고 장치가 업데이트됩니다.

기본 형성 비율 복원

1. Interface Configuration(인터페이스 구성) 페이지를 엽니다.
2. Restore Defaults(기본값 복원) 확인란을 클릭합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.
모든 포트가 기본 형성 비율로 복원되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 인터페이스 구성 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. QoS 명령

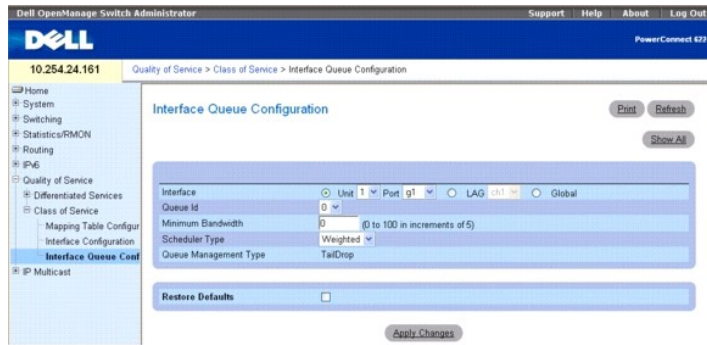
인터페이스 대기열 구성

Interface Queue Configuration(인터페이스 대기열 구성) 페이지에서 스위치 송신 대기열을 구성하여 특정 대기열에서 수행하는 작업을 정의합니다. 사용자 구성 가능한 매개변수는 대기열에 사용되는 대역폭의 양, 정제 시의 대기열 수준, 포트에 있는 모든 대기열로부터의 패킷 전송 일정 등을 제어합니다. 각 포트에는 자체 CoS 대기열 관련 구성이 있습니다.

각 CoS 대기열 매개변수를 전역적 또는 포트 단위로 구성하여 구성 프로세스를 간소화할 수 있습니다. 전역 구성 변경은 시스템에 있는 모든 포트에 자동으로 적용됩니다.

Interface Queue Configuration(인터페이스 대기열 구성) 페이지를 표시하려면 디렉터리 화면에서 Quality of Service(서비스 품질)→Class of Service(서비스 등급)→Interface Queue Configuration(인터페이스 대기열 구성)을 클릭합니다.

그림 12-19. Interface Queue Configuration(인터페이스 대기열 구성)



Interface Queue Configuration(인터페이스 대기열 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 구성 중인 **Interface(인터페이스)**(Unit/Port(장치/포트), LAG 또는 Global(전역))를 지정합니다.

Queue ID(대기열 ID) — 드롭다운 메뉴에서 구성할 대기열을 선택합니다.

Minimum Bandwidth(최소 대역폭) — 포트에 대한 최소 교섭 대역폭 비율(%)을 선택합니다. 0부터 100 사이의 비율(%)을 5씩 증분하여 지정합니다.

Scheduler Type(스케줄러 유형) — 드롭다운 메뉴에서 대기열 처리 유형을 선택합니다. 옵션은 **Weighted(가중)** 및 **Strict(엄격)**입니다. 대기열 단위로 정의하면 트래픽 유형별로 원하는 서비스 특성을 생성할 수 있습니다.

Weighted(가중) — 엄격 라운드 로빈은 각 대기열에 가중치를 연결합니다. 기본 설정입니다.

Strict(엄격) — 엄격 우선 순위는 대기열에서 우선 순위가 가장 높은 트래픽을 먼저 처리합니다.

Queue Management Type(대기열 관리 유형) — 모든 패킷에 대해 사용되는 패킷 관리 유형(Taildrop)을 표시합니다. 정체가 발생할 때까지는 대기열의 모든 패킷이 안전합니다. 이 지정에서 대기열에 들어오는 추가 패킷은 삭제됩니다.

인터페이스 대기열 구성

1. **Interface Queue Configuration(인터페이스 대기열 구성)** 페이지를 엽니다.
2. **Interface Unit(인터페이스 장치)** 및 **Port(포트)** 드롭다운 메뉴에서 적용할 포트를 선택합니다.
3. 나머지 필드를 사용하여 이 포트에 대한 설정과 대기열을 구성합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.

대기열이 구성되고 장치가 업데이트됩니다.

인터페이스 대기열 설정 표시

1. **Interface Queue Configuration(인터페이스 대기열 구성)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.
Interface Queue Status(인터페이스 대기열 상태) 페이지가 표시됩니다.
3. **Unit / Port(장치 / 포트)**, **LAG** 또는 **Global(전역)**을 선택합니다.

그림 12-20. Interface Queue Status(인터페이스 대기열 상태)

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop

CLI 명령을 사용하여 인터페이스 대기열 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. QoS 명령

[목차 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

IP 멀티캐스트 구성

Dell™ PowerConnect™ M6220 사용 설명서

- [DVMRP](#)
- [IGMP](#)
- [멀티캐스트](#)
- [PIM-DM](#)
- [PIM-SM](#)

멀티캐스트 프로토콜은 멀티캐스트 패킷을 하나의 소스에서 여러 수신기로 전달하는 데 사용됩니다. 또한, 대역폭 사용을 향상시키고, 호스트 및 라우터 처리를 단축하므로 음성/오디오 회의, 화이트보드 도구 및 주식 시세표 등과 같은 응용프로그램에 이상적입니다.

멀티캐스트 응용프로그램은 패킷 복사본 하나를 단일 수신기(유니캐스트 주소)가 아니라 수신기 그룹(멀티캐스트 그룹 주소)으로 보냅니다. 멀티캐스트는 패킷을 수신해야 하는 네트워크 및 호스트에만 패킷을 전달하는 데 네트워크를 사용합니다.

멀티캐스트 가능/활성화 라우터는 MRIB(Multicast Routing Information Base)의 경로를 기반으로 멀티캐스트 패킷을 전달합니다. 이러한 경로는 라우터에서 실행 중인 멀티캐스트 프로토콜이 멀티캐스트 배포 트리를 구축하는 중에 MRIB에서 만들어집니다. 각 IP 멀티캐스트 라우팅 프로토콜은 서로 다른 기술을 사용하여 이러한 멀티캐스트 배포 트리를 작성합니다.

멀티캐스팅을 지원하지 않는 네트워크 부분(멀티캐스트를 사용할 수 없는 라우터)을 통해 멀티캐스트 트래픽을 연결할 경우 멀티캐스트 패킷은 IP 데이터그램에 캡슐화되어 유니캐스트 패킷으로 전송됩니다. 터널의 원격 끝에 있는 멀티캐스트 라우터는 패킷을 수신할 경우 IP 캡슐화를 해제한 다음 IP 멀티캐스트 패킷으로 패킷을 전달합니다. IP의 이 멀티캐스트 패킷 캡슐화 과정을 터널링이라고 합니다.

IP Multicast(IP 멀티캐스트) 메뉴 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)**를 클릭합니다. **IP Multicast(IP 멀티캐스트)** 메뉴 페이지에는 다음과 같은 절차에 대한 링크가 포함되어 있습니다.

- 1 [DVMRP](#)
- 1 [IGMP](#)
- 1 [멀티캐스트](#)
- 1 [PIM-DM](#)
- 1 [PIM-SM](#)

DVMRP

DVMRP는 탐침 패킷을 모든 DVMRP 활성화 라우터와 교환하며, 양방향 인접 관계를 설정하고 인접 표를 구축합니다. 또한 보고서 패킷을 교환하고 유니캐스트 토폴로지 표를 만든 다음 해당 표를 사용하여 멀티캐스트 라우팅 표를 구축합니다. 이 표는 멀티캐스트 패킷을 경로 지정하는 데 사용됩니다. 모든 DVMRP 라우터가 동일한 유니캐스트 라우팅 프로토콜을 사용하기 때문에 라우팅 루프가 발생하지 않습니다.

DVMRP 메뉴 페이지에는 DVMRP 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→DVMRP**를 클릭합니다.

이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

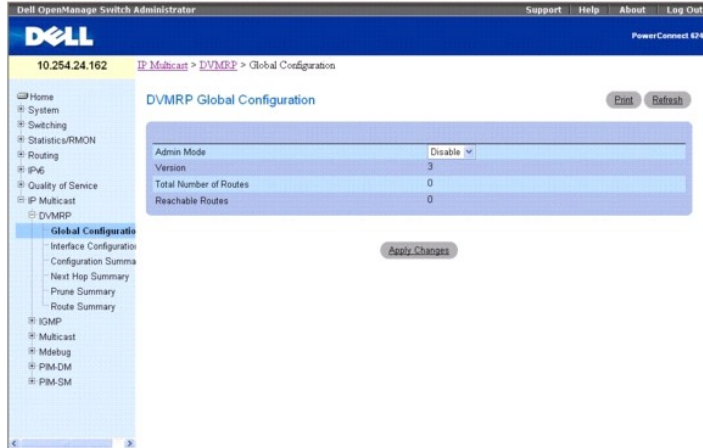
- 1 [DVMRP 전역 구성](#)
- 1 [DVMRP 인터페이스 구성](#)
- 1 [DVMRP 구성 요약](#)
- 1 [다음 홈 요약](#)
- 1 [정리 요약](#)
- 1 [경로 요약](#)

DVMRP 전역 구성

DVMRP Global Configuration(DVMRP 전역 구성) 페이지를 사용하여 전역 DVMRP 설정을 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→DVMRP→Global Configuration(전역 구성)**을 클릭합니다.

그림 13-1. DVMRP Global Configuration(DVMRP 전역 구성)



DVMRP Global Configuration(DVMRP 전역 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Admin Mode(관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택합니다. 그러면 DVMRP의 관리 상태가 활성 또는 비활성으로 설정됩니다. 기본값은 Disable(비활성)입니다.

Version(버전) — DVMRP 버전 문자열의 현재 값입니다.

Total Number of Routes(총 경로 수) — DVMRP 라우팅 표에 있는 경로 수입니다.

Reachable Routes(연결 가능한 경로) — DVMRP 라우팅 표에서 유효한 메트릭을 가진 경로 수입니다.

DVMRP 관리 모드 설정

1. DVMRP Global Configuration(DVMRP 전역 구성) 페이지를 엽니다.
2. **Admin Mode(관리 모드)**를 Enable(활성) 또는 Disable(비활성)로 설정하여 DVMRP를 켜거나 끕니다.
3. **Apply Changes(변경사항 적용)**를 클릭하십시오.

DVMRP 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DVMRP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

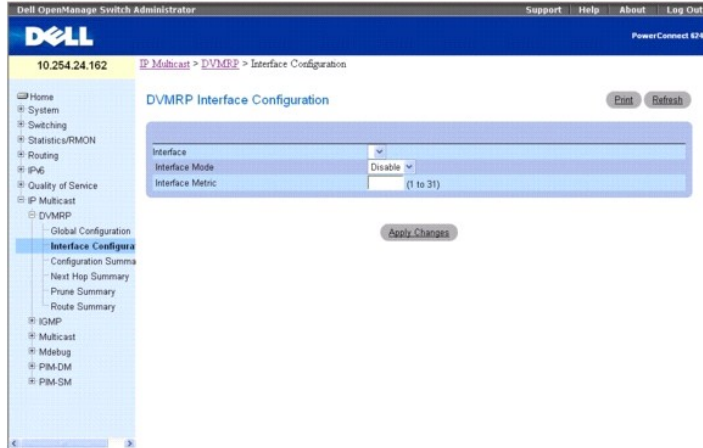
1. DVMRP 명령

DVMRP 인터페이스 구성

DVMRP Interface Configuration(DVMRP 인터페이스 구성) 페이지를 사용하여 DVMRP 인터페이스를 구성합니다. DVMRP 인터페이스를 구성하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다. 그렇지 않으면 사용할 수 있는 라우터 인터페이스가 없다는 메시지가 표시되고 구성 화면이 표시되지 않습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → DVMRP → Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 13-2. DVMRP Interface Configuration(DVMRP 인터페이스 구성)



DVMRP Interface Configuration(DVMRP 인터페이스 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 구성할 인터페이스를 선택합니다. DVMRP 인터페이스를 구성하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다.

Interface Mode(인터페이스 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 선택된 DVMRP 라우팅 인터페이스의 관리 모드를 설정합니다.

Interface Metric(인터페이스 메트릭) — 선택한 인터페이스에 대한 DVMRP 메트릭을 입력합니다. 이 값은 DVMRP 메시지에 이 네트워크를 연결하는 비용으로 전송됩니다. 유효한 값은 1 ~ 31입니다.

DVMRP 인터페이스 구성

1. **DVMRP Interface Configuration(DVMRP 인터페이스 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에서 구성할 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 DVMRP 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

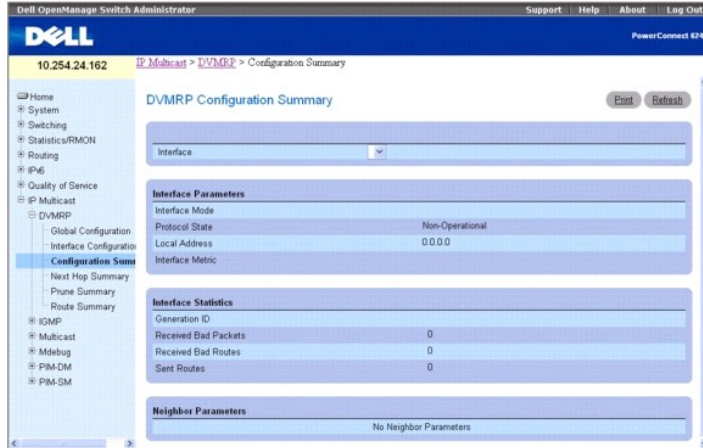
1. DVMRP 명령

DVMRP 구성 요약

DVMRP Configuration Summary(DVMRP 구성 요약) 페이지를 사용하여 선택된 인터페이스에 대한 DVMRP 구성 및 데이터를 표시하거나 인쇄합니다. DVMRP 인터페이스에 대한 데이터를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다. 그렇지 않으면 사용할 수 있는 라우터 인터페이스가 없다는 메시지가 표시되고 구성 요약 화면이 표시되지 않습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → DVMRP → Configuration Summary(구성 요약)**를 클릭합니다.

그림 13-3. DVMRP Configuration Summary(DVMRP 구성 요약)



DVMRP Configuration Summary(DVMRP 구성 요약) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다. DVMRP 인터페이스에 대한 데이터를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다.

인터페이스 매개변수

Interface Mode(인터페이스 모드) — 선택된 DVMRP 라우팅 인터페이스의 관리 모드(Enable(활성) 또는 Disable(비활성))를 표시합니다.

Protocol State(프로토콜 상태) — 선택된 인터페이스에서 DVMRP 프로토콜의 작동 상태(Operational(작동) 또는 Non-operational(비작동))를 표시합니다.

Local Address(로컬 주소) — 선택된 인터페이스에서 보낸 패킷에서 소스 주소로 사용되는 IP 주소를 표시합니다.

Interface Metric(인터페이스 메트릭) — 선택된 인터페이스에 대한 거리 백터를 계산하는 데 사용되는 메트릭을 표시합니다.

인터페이스 통계

Generation ID(생성 ID) — 선택된 인터페이스에 대해 라우터에서 사용되는 DVMRP 생성 ID를 표시합니다. 이 값은 인터페이스가 시작/다시 시작되어 정리 메시지에 저장될 때마다 다시 설정됩니다. 생성 ID가 변경되면 인접 라우터에 이 라우터에 대한 이전 정보를 삭제하도록 알려줍니다.

Received Bad Packets(수신된 불량 패킷 수) — 선택된 인터페이스에서 수신된 잘못된 패킷 수를 나타냅니다.

Received Bad Routes(수신된 불량 경로 수) — 선택된 인터페이스에서 수신된 잘못된 경로 수를 나타냅니다.

Sent Routes(보낸 경로 수) — 선택된 인터페이스에서 보낸 경로 수를 나타냅니다.

인접 매개변수

Neighbor IP(인접 IP) — 정보가 표시되는 인접 IP 주소입니다.

State(상태) — 선택된 인터페이스에서 지정된 인접 라우터의 상태(활성 또는 다운)를 나타냅니다.

Neighbor Uptime(인접 항목 가동 시간) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 가동 시간을 나타냅니다. 인접 항목이 확인된 이후에 경과한 시간입니다.

Neighbor Expiry Time(인접 항목 만료 시간) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 만료 시간을 나타냅니다. 이 인접 항목이 만료될 때까지 남아 있는 시간이며, 인접 라우터의 상태가 다운인 경우에는 적용되지 않습니다.

Generation ID(생성 ID) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 생성 ID를 나타냅니다.

Major Version(최대 버전) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 최대 버전을 나타냅니다.

Minor Version(최소 버전) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 최소 버전을 나타냅니다.

Capabilities(기능) — 선택된 인터페이스에서 지정된 인접 항목의 DVMRP 기능을 나타냅니다.

Received Routes(수신된 경로 수) — 선택된 인터페이스에서 지정된 인접 항목의 수신된 경로 수를 나타냅니다.

Received Bad Packets(수신된 불량 패킷 수) — 선택된 인터페이스에서 지정된 인접 항목의 수신된 잘못된 패킷 수를 나타냅니다.

Received Bad Routes(수신된 불량 경로 수) — 선택된 인터페이스에서 지정된 인접 항목의 수신된 잘못된 경로 수를 나타냅니다.

CLI 명령을 사용하여 DVMRP 구성 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 DVMRP 명령

다음 홉 요약

Next Hop Summary(다음 홉 요약) 페이지를 사용하여 Source IP(소스 IP)별로 다음 홉 요약을 표시하거나 인쇄합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IP Multicast(IP 멀티캐스트) → DVMRP → Next Hop Summary(다음 홉 요약)를 클릭합니다.

그림 13-4. Next Hop Summary(다음 홉 요약)

Source IP	Source Mask	Next Hop Interface	Type
3.1.1.0	255.255.255.0	vlan3	Leaf

Next Hop Summary(다음 홉 요약) 페이지에는 다음 필드가 표시됩니다.

Source IP(소스 IP) — 이 표 항목에 대한 소스 네트워크를 식별하기 위해 소스 마스크와 함께 사용되는 IP 주소를 표시합니다.

Source Mask(소스 마스크) — 소스 IP 주소와 함께 사용되는 네트워크 마스크를 표시합니다.

Next Hop Interface(다음 홉 인터페이스) — 이 다음 홉에 대한 송신 인터페이스를 표시합니다.

Type(유형) — 다음 홉 유형을 표시합니다. 리프는 송신 인터페이스에 다운스트림 종속 인접 항목이 없는 것을 의미합니다. 그렇지 않은 경우에는 유형은 Branch(분기)입니다.

CLI 명령을 사용하여 다음 홉 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

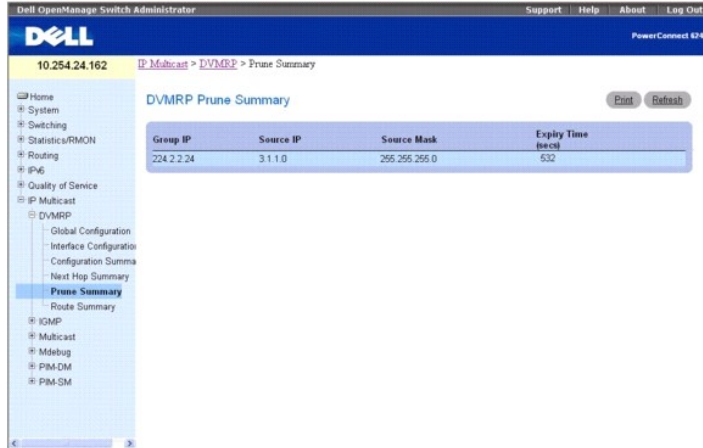
1. DVMRP 명령

정리 요약

Prune Summary(정리 요약) 페이지를 사용하여 Group IP(그룹 IP)별로 정리 요약을 표시하거나 인쇄합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IP Multicast(IP 멀티캐스트) → DVMRP → Prune Summary(정리 요약)를 클릭합니다.

그림 13-5. Prune Summary(정리 요약)



Prune Summary(정리 요약) 페이지에는 다음 필드가 표시됩니다.

Group IP(그룹 IP) - 정리된 그룹 주소입니다.

Source IP(소스 IP) - 정리된 소스 또는 소스 네트워크의 주소입니다.

Source Mask(소스 마스크) - 정리된 소스 또는 소스 네트워크를 식별하기 위해 소스 IP 주소와 결합할 서브네트 마스크입니다.

Expiry Time (secs)(만료 시간(초)) - 업스트림 인접 항목에서 이 정리가 만료될 때까지 남아 있는 시간입니다. 다운스트림 인접 항목으로부터 정리 메시지가 수신되지 않으면 기본 정리 수명 타이머 값으로 설정되고, 그렇지 않으면 수신된 가장 작은 값 또는 기본 타이머 중 작은 값으로 설정됩니다.

CLI 명령을 사용하여 정리 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

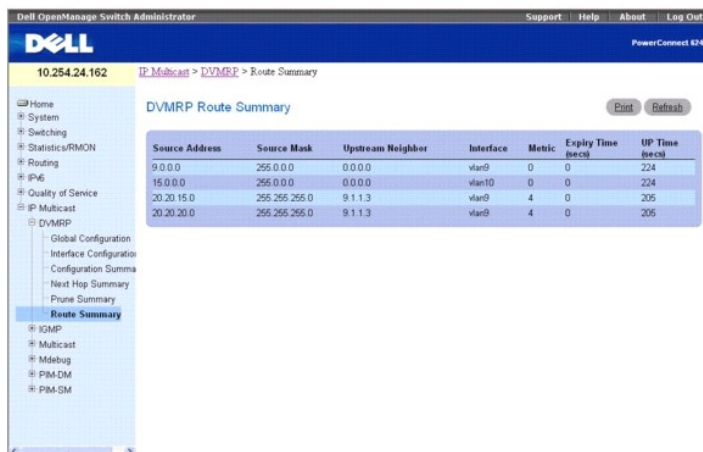
- 1 DVMRP 명령

경로 요약

Route Summary(경로 요약) 페이지를 사용하여 DVMRP 경로 요약을 표시하거나 인쇄합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)** → **DVMRP** → **Route Summary(경로 요약)**를 클릭합니다.

그림 13-6. Route Summary(경로 요약)



Route Summary(경로 요약) 페이지에는 다음 필드가 표시됩니다.

Source Address(소스 주소) - 이 항목의 소스를 식별하기 위해 소스 마스크와 결합된 네트워크 주소입니다.

Source Mask(소스 마스크) - 이 항목의 소스를 식별하기 위해 소스 주소와 결합될 서브네트 마스크입니다.

Upstream Neighbor(업스트림 인접) — 이러한 소스에서 보낸 IP 데이터그램을 수신하는 업스트림 인접 항목(예: RPF 인접)의 주소입니다.

Interface(인터페이스) — 이러한 소스에서 보낸 IP 데이터그램을 수신하는 인터페이스입니다. 값이 0이면 일반적으로 경로가 다음 홉 인터페이스가 존재하지 않는 결함이라는 의미입니다.

Metric(메트릭) — 소스 서브네트까지의 홉 거리입니다.

Expiry Time(만료 시간) — 이 항목이 만료될 때까지 남아 있는 최소 시간입니다.

Up Time(가동 시간) — 이 항목으로 표시되는 경로가 라우터에 의해 탐지된 이후에 경과한 시간입니다.

CLI 명령을 사용하여 DVMRP 경로 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 DVMRP 명령

IGMP

IGMP(Internet Group Management Protocol)는 IPv4 시스템(호스트 및 라우터)이 IP 멀티캐스트 그룹 멤버십을 인접한 멀티캐스트 라우터에 보고하는 데 사용됩니다. 6200 시리즈는 IGMP 프로토콜의 멀티캐스트 라우터 역할을 수행합니다. 즉, 활성 멀티캐스트 라우팅에 필요한 멤버십 정보를 수집합니다. 6200 시리즈에서 현재 지원되는 멀티캐스트 라우팅 프로토콜은 DVMRP, PIM-DM 및 PIM-SM입니다.

6200 시리즈는 IGMP 버전 3을 지원합니다. 버전 3은 소스 필터링을 추가로 지원합니다. 이 기능을 사용하면 특정 소스 주소에서 보낸 수신 패킷에 대해서만 보고(SSM[Source-Specific Multicast]에 필요)하거나, 특정 소스 주소를 제외한 모든 주소에서 특정 멀티캐스트 주소로 보낸 수신 패킷에 대해서만 보고할 수 있습니다. 버전 3은 버전 1 및 2와 상호 작용하도록 설계되었습니다.

IGMP 메뉴 페이지에는 IGMP 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → IGMP**를 클릭합니다.

이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

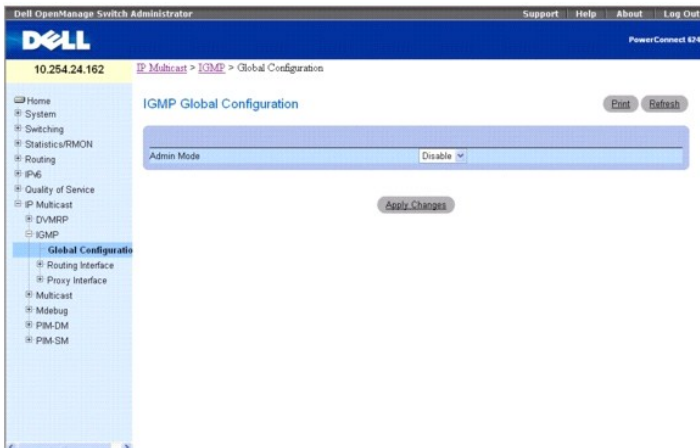
- 1 [IGMP 전역 구성](#)
- 1 [라우팅 인터페이스](#)
- 1 [프록시 인터페이스](#)

IGMP 전역 구성

IGMP Global Configuration(IGMP 전역 구성) 페이지를 사용하여 시스템의 IGMP를 활성화 또는 비활성으로 설정합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → IGMP → Global Configuration(전역 구성)**을 클릭합니다.

그림 13-7. IGMP Global Configuration(IGMP 전역 구성)



IGMP Global Configuration(IGMP 전역 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Admin Mode(관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 라우터의 IGMP 관리 상태를 활성화 또는 비활성으로 설정합니다. 기본값은 Disable(비활성)입니다.

IGMP 모드 설정

1. IGMP Global Configuration(IGMP 전역 구성) 페이지를 엽니다.
2. Admin Mode(관리 모드)를 Enable(활성) 또는 Disable(비활성)로 설정하여 IGMP를 켜거나 끕니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

새 IGMP 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IGMP 모드 설정

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. IGMP 명령

라우팅 인터페이스

Routing Interface(라우팅 인터페이스) 메뉴 페이지에는 IGMP 라우팅 매개변수와 데이터를 구성 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 IP Multicast(IP 멀티캐스트)→IGMP→Routing Interface(라우팅 인터페이스)를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

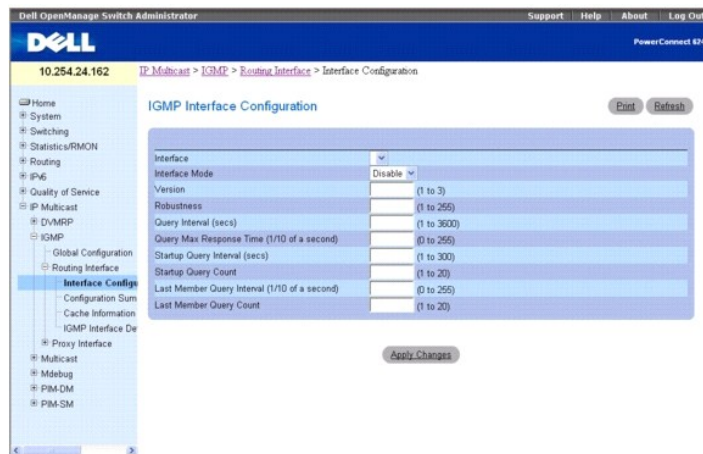
1. [IGMP 인터페이스 구성](#)
1. [IGMP 구성 요약](#)
1. [IGMP 캐쉬 정보](#)
1. [IGMP 인터페이스 세부 멤버십 정보](#)

IGMP 인터페이스 구성

IGMP Interface Configuration(IGMP 인터페이스 구성) 페이지를 사용하여 라우터 인터페이스 매개변수를 구성 및/또는 표시합니다. 이 페이지를 액세스하여 IP 멀티캐스트 IGMP를 구성하려면 먼저 하나 이상의 유효한 라우팅 인터페이스를 구성해야 합니다.

페이지를 표시하려면 디렉터리 화면에서 IP Multicast(IP 멀티캐스트)→IGMP→Routing Interface(라우팅 인터페이스)→Interface Configuration(인터페이스 구성)을 클릭합니다.

그림 13-8. IGMP Interface Configuration(IGMP 인터페이스 구성)



IGMP Interface Configuration(IGMP 인터페이스 구성) 페이지에는 다음과 같은 필드가 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 표시 또는 구성할 인터페이스를 선택합니다.

Interface Mode(인터페이스 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 선택된 인터페이스의 IGMP 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다.

Version(버전) — 선택된 인터페이스에서 구성할 IGMP 버전을 입력합니다. 유효한 값은 1 ~ 3이고, 기본값은 3입니다. 이 필드는 IGMP 인터페이스 모드를 활성화한 경우에만 구성할 수 있습니다.

Robustness(견고성) — 견고성 값을 입력합니다. 이 변수는 서브네트의 예상 패킷 손실에 맞게 조정될 수 있습니다. 서브네트가 손상될 것 같으면 이 매개변수에 대해 더 높은 값을 입력합니다. IGMP는 패킷 손실에 견고합니다(견고성 변수-1). 유효한 값은 1 ~ 255이고 기본값은 2입니다.

Query Interval(secs)(쿼리 간격(초)) — 이 인터페이스에서 IGMP 호스트 쿼리 패킷을 전송하는 빈도(초)를 입력합니다. 유효한 값은 1 ~ 3600이고 기본값은 125입니다.

Query Max Response Time(1/10 of a second)(쿼리 최대 응답 시간(1/10초)) — 이 인터페이스의 IGMPv2 쿼리에서 알릴 최대 쿼리 응답 시간(1/10초)을 입력합니다. 기본값은 100이고, 유효한 값은 0 ~ 255입니다.

Startup Query Interval (secs)(시작 쿼리 간격(초)) — 선택된 인터페이스에서 시작 쿼리 전송 사이의 간격(초)을 입력합니다. 유효한 값은 1 ~ 300이고 기본값은 31입니다.

Startup Query Count(시작 쿼리 수) — 시작할 때 전송할 쿼리 수를 입력합니다. 유효한 값은 1 ~ 200이고 기본값은 2입니다.

Last Member Query Interval (1/10 of a second)(마지막 구성원 쿼리 간격(1/10초)) — 마지막 구성원 쿼리 간격(1/10초)을 입력합니다. 이 시간은 그룹 탈퇴 메시지에 대한 응답으로 전송되는 그룹별 쿼리에 상임할 최대 응답 시간이며, 그룹별 쿼리 메시지 간격입니다. 유효한 값은 0 ~ 255이고, 기본값은 10입니다. 이 값은 IGMP 버전 1에는 사용되지 않습니다.

Last Member Query Count(마지막 구성원 쿼리 수) — 그룹 탈퇴 보고서를 수신할 때 전송할 쿼리 수를 입력합니다. 유효한 값은 1 ~ 200이고 기본값은 2입니다.

IGMP 라우팅 인터페이스 구성

1. **IGMP Interface Configuration(IGMP 인터페이스 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에서 구성할 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IGMP 라우팅 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. IGMP 명령

IGMP 구성 요약

IGMP Configuration Summary(IGMP 구성 요약) 페이지를 사용하여 IGMP 라우팅 매개변수 및 데이터를 표시합니다. 이 페이지를 사용하려면 IGMP 라우터 인터페이스를 하나 이상 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → IGMP → Routing Interface(라우팅 인터페이스) → Configuration Summary(구성 요약)**를 클릭합니다.

그림 13-9. IGMP Configuration Summary(IGMP 구성 요약)



IGMP Configuration Summary(IGMP 구성 요약) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

인터페이스 매개변수

Interface Mode(인터페이스 모드) — 선택된 인터페이스의 IGMP 관리 상태입니다.

IP Address(IP 주소) — 선택한 인터페이스의 IP 주소입니다.

Subnet Mask(서브넷 마스크) — 선택된 인터페이스의 IP 주소에 대한 서브넷 마스크입니다.

Protocol State(프로토콜 상태) — 선택된 인터페이스의 IGMP 작동 상태입니다.

Version(버전) — 선택된 인터페이스에 구성되어 있는 IGMP 버전입니다.

Query Interval(secs)(쿼리 간격(초)) — 선택된 인터페이스에서 IGMP 호스트 쿼리 패킷을 전송하는 빈도입니다.

Query Max Response Time (1/10 of a second)(쿼리 최대 응답 시간(1/10초)) — 선택된 인터페이스에서 전송된 IGMPv2 쿼리에서 알릴 최대 쿼리 응답 시간입니다.

Robustness(견고성) — 선택된 인터페이스에 대한 견고성 매개변수입니다. 이 변수는 서브넷의 예상 패킷 손실에 맞게 조정될 수 있습니다. 서브넷이 손상될 것 같으면 견고성 변수를 증가할 수 있습니다. IGMP는 패킷 손실에 견고합니다(견고성 변수-1).

Startup Query Interval (secs)(시작 쿼리 간격(초)) — 선택된 인터페이스에서 시작 쿼리가 전송되는 간격입니다.

Startup Query Count(시작 쿼리 수) — 시작할 때 전송할 쿼리 수입니다.

Last Member Query Interval (1/10 of a second)(마지막 구성원 쿼리 간격(1/10초)) — 마지막 구성원 쿼리 간격은 그룹 탈퇴 메시지에 대한 응답으로 전송되는 그룹별 쿼리에 상임할 최대 응답 시간이며, 그룹별 쿼리 메시지 간격입니다. 이 값을 조정하여 네트워크의 탈퇴 대기 시간을 수정할 수 있습니다. 값을 줄이면 그룹의 마지막 구성원 손실을 감지하는 데 걸리는 시간이 단축됩니다. 이 값은 IGMP 버전 1에는 사용되지 않습니다.

Last Member Query Count(마지막 구성원 쿼리 수) — 그룹 탈퇴 보고서를 수신할 때 전송할 쿼리 수입니다.

인터페이스 통계

Querier(쿼리기) — IP 서브넷에서 선택된 인터페이스가 연결되는 IGMP 쿼리의 주소입니다.

Querier Status(쿼리기 상태) — 선택된 인터페이스가 쿼리기 모드 상태인지 여부를 나타냅니다.

Querier Up Time (secs)(쿼리기 가동 시간(초)) — IGMP 인터페이스 쿼리기가 마지막으로 변경된 이후에 경과된 시간(초)입니다.

Querier Expiry Time (secs)(쿼리기 만료 시간(초)) — 다른 쿼리기 제공 타이머가 만료되기 이전에 남아 있는 시간(초)입니다. 로컬 시스템이 쿼리기인 경우에는 이 값이 0입니다.

Wrong Version Queries(잘못된 버전 쿼리 수) — 항목의 수명 동안 인터페이스에 대해 구성된 IGMP 버전과 일치하지 않는 IGMP 버전을 가진 선택된 인터페이스에서 수신한 쿼리 수입니다. IGMP에서는 LAN의 모든 라우터가 동일한 IGMP 버전을 실행하도록 구성해야 합니다. 따라서, 잘못된 버전 번호를 가진 쿼리가 수신되면 구성 오류가 표시됩니다.

Number of Joins(연결 횟수) — 선택된 인터페이스에서 그룹 멤버십이 추가된 횟수입니다. 즉, 이 인터페이스에 대한 항목이 캐시 표에 추가된 횟수입니다. 이 값은 인터페이스에서의 IGMP 활동량을 나타냅니다.

Number of Groups(그룹 수) — 캐시 표에 있는 선택된 인터페이스에 대한 현재 항목 수입니다.

CLI 명령을 사용하여 IGMP 라우팅 구성 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

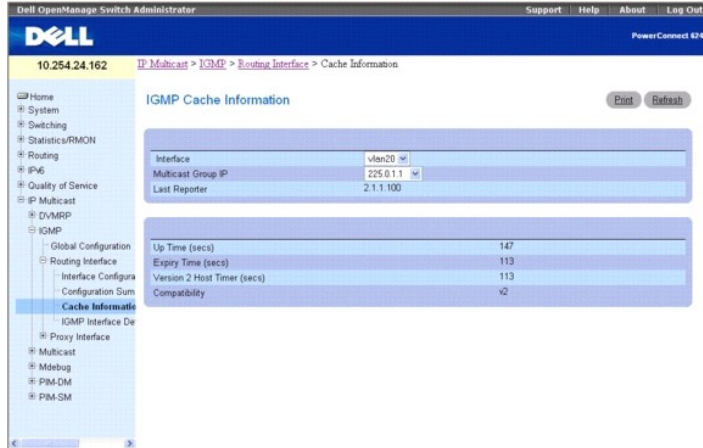
- 1 IGMP 명령

IGMP 캐시 정보

IGMP Cache Information(IGMP 캐시 정보) 페이지를 사용하여 IP 멀티캐스트 그룹 주소에 대한 캐시 매개변수 및 데이터를 표시합니다. 이 페이지를 사용하려면 IGMP 라우터 인터페이스를 하나 이상 구성해야 합니다. 선택된 인터페이스에서 그룹 멤버십 보고서를 수신한 경우에만 여기에 데이터가 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → IGMP → Routing Interface(라우팅 인터페이스) → Cache Information(캐시 정보)**을 클릭합니다.

그림 13-10. IGMP Cache Information(IGMP 캐시 정보)



IGMP Cache Information(IGMP 캐시 정보) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

Multicast Group IP(멀티캐스트 그룹 IP) — 데이터를 표시할 IP 멀티캐스트 그룹 주소를 선택합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우 이 선택을 수행할 수 없으며 이 페이지에서 아무 데이터도 표시되지 않습니다.

Last Reporter(마지막 보고자) — 선택된 인터페이스의 IP 멀티캐스트 그룹 주소에 대해 수신된 마지막 멤버십 보고서의 소스 IP 주소입니다.

Up Time(가동 시간) — 이 항목이 만들어진 이후에 경과한 시간입니다.

Expiry Time(만료 시간) — 이 항목이 만료될 때까지 남아 있는 최소 시간입니다.

Version 1 Host Timer(버전 1 호스트 타이머) — 이 인터페이스에 연결된 IP 서브네트에 IGMP 버전 2 구성원이 더 이상 없는 것으로 로컬 라우터에서 간주될 때까지 남아 있는 시간입니다. IGMPv1 멤버십 보고서가 수신되면 이 타이머가 그룹 멤버십 타이머로 다시 설정됩니다. 이 타이머가 0이 아니지만, 로컬 라우터는 선택된 인터페이스에서 수신되는 이 그룹에 대한 IGMPv2 알림 메시지를 무시합니다. 이 필드는 인터페이스가 IGMP 버전 1에 대해 구성된 경우에만 표시됩니다.

Version 2 Host Timer(버전 2 호스트 타이머) — 이 인터페이스에 연결된 IP 서브네트에 IGMP 버전 2 구성원이 더 이상 없는 것으로 로컬 라우터에서 간주될 때까지 남아 있는 시간입니다. IGMPv2 멤버십 보고서가 수신되면 이 타이머가 그룹 멤버십 타이머로 다시 설정됩니다. 이 타이머가 0이 아니지만, 로컬 라우터는 선택된 인터페이스에서 수신되는 이 그룹에 대한 IGMPv1 및 IGMPv3 알림 메시지를 무시합니다. 이 필드는 인터페이스가 IGMP 버전 2에 대해 구성된 경우에만 표시됩니다.

Compatibility(호환성) — 이 매개변수는 지정된 인터페이스에서 이 그룹에 대한 그룹 호환성 모드(v1, v2 및 v3)를 표시합니다.

Filter Mode(필터 모드) — 이 인터페이스에서 지정된 그룹에 대한 소스 필터 모드(포함/제외/해당 없음)입니다. 해당 없음 모드가 활성화되면 필드가 비어 있습니다.

CLI 명령을 사용하여 캐시 정보 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

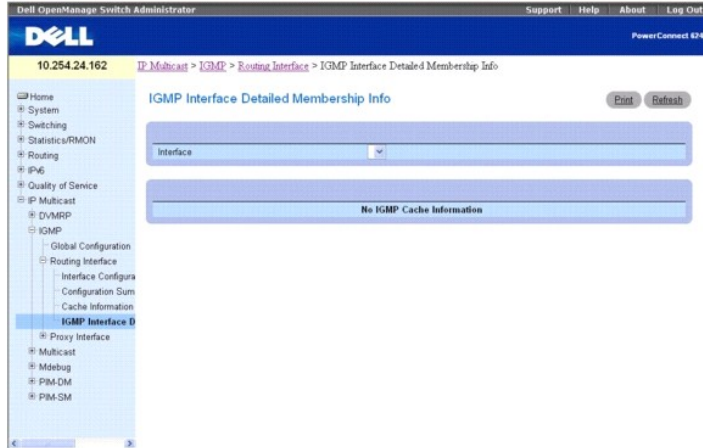
- 1 IGMP 명령

IGMP 인터페이스 세부 멤버십 정보

IGMP Interface Detailed Membership Info(IGMP 인터페이스 세부 멤버십 정보) 페이지를 사용하여 인터페이스에 대한 세부 멤버십 정보를 표시합니다. 이 페이지를 사용하면 IGMP 라우터 인터페이스를 하나 이상 구성해야 합니다. 선택된 인터페이스에서 그룹 멤버십 보고서를 수신한 경우에만 여기에 데이터가 표시됩니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→IGMP→Routing Interface(라우팅 인터페이스)→Interface Membership Info Detailed(인터페이스 멤버십 세부 정보)**를 클릭합니다.

그림 13-11. IGMP Interface Detailed Membership Info(IGMP 인터페이스 멤버십 세부 정보)



IGMP Interface Detailed Membership Info(IGMP 인터페이스 세부 멤버십 정보) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

Multicast Group IP(멀티캐스트 그룹 IP) — 데이터를 표시할 IP 멀티캐스트 그룹 주소를 선택합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우 이 선택을 수행할 수 없으며 나머지 아무 필드도 표시되지 않습니다.

Interface(인터페이스) — 멀티캐스트 패킷이 전달되는 인터페이스입니다.

Group Compatibility Mode(그룹 호환성 모드) — 지정된 인터페이스에서 이 그룹에 대한 그룹 호환성 모드(v1, v2 및 v3)입니다.

Source Filter Mode(소스 필터 모드) — 이 인터페이스에서 지정된 그룹에 대한 소스 필터 모드(포함/제외/해당 없음)입니다.

Source Hosts(소스 호스트) — 이 멀티캐스트 주소의 구성원인 소스 주소입니다.

Expiry Time(만료 시간) — 이 멀티캐스트 그룹의 구성원인 각 소스 주소에 대한 만료 시간 간격입니다. 지정된 소스 항목이 만료되는 시간 간격입니다.

IGMP 인터페이스 세부 멤버십 표시

1. IGMP Interface Detailed Membership Info(IGMP 인터페이스 세부 멤버십 정보) 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.
3. 원하는 **Multicast Group IP(멀티캐스트 그룹 IP)**를 선택합니다.

이 인터페이스 및 멀티캐스트 그룹 IP에 대한 세부 멤버십 정보가 표시됩니다.

CLI 명령을 사용하여 IGMP 인터페이스 세부 멤버십 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. IGMP 명령

프록시 인터페이스

IGMP 프록시의 목적은 멀티캐스트 라우터를 활성화하여 멀티캐스트 그룹 멤버십 정보를 수집하고 그룹 멤버십 정보를 기반으로 멀티캐스트 패킷을 전달할 수 있게 하는 것입니다. IGMP 프록시는 패킷 경로 루프 수정을 위한 기능(예: 스페닝 트리)을 지원하지 않기 때문에 멀티캐스트 라우팅 프로토콜(예: DVMRP, PIM-DM 및 PIM-SM)이 필요하지 않고 트리 모양 토폴로지가 있는 특정 토폴로지에서만 작동할 수 있습니다.

Proxy Interface(프록시 인터페이스) 메뉴 페이지에는 프록시 인터페이스 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 메뉴를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→IGMP→Proxy Interface(프록시 인터페이스)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

1. [IGMP 프록시 인터페이스 구성](#)
1. [IGMP 프록시 구성 요약](#)
1. [IGMP 프록시 인터페이스 멤버십 정보](#)
1. [IGMP 프록시 인터페이스 세부 멤버십 정보](#)

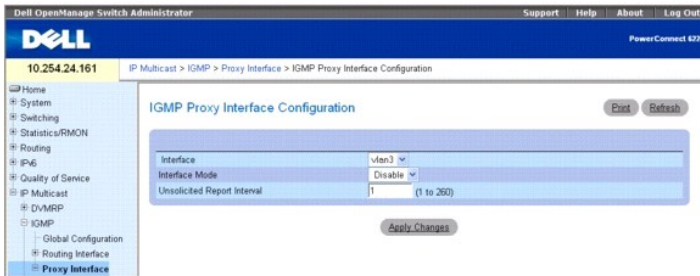
IGMP 프록시 인터페이스 구성

IGMP 프록시는 IGMP 라우터(IPv4 시스템)에 의해 사용되어 시스템이 표준 IGMP 라우터 인터페이스를 통해 검색된 호스트를 대신하여 IGMP 호스트 메시지를 표시하게 합니다. 따라서, 이 기능은 라우터 인터페이스에 있는 모든 호스트에 대한 프록시 역할을 합니다.

IGMP Proxy Interface Configuration(IGMP 프록시 인터페이스 구성) 페이지를 사용하여 인터페이스에 대한 IGMP 프록시를 구성합니다. IGMP 프록시 인터페이스에 대한 데이터를 구성하거나 표시하려면 먼저 IGMP 라우팅 인터페이스가 아닌 하나 이상의 라우터 인터페이스를 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→IGMP→Proxy Interface(프록시 인터페이스)→Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 13-12. IGMP Proxy Interface Configuration(IGMP 프록시 인터페이스 구성)



IGMP Proxy Interface Configuration(IGMP 프록시 인터페이스 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 데이터를 표시 또는 구성할 포트를 선택합니다. IGMP 프록시 인터페이스에 대한 데이터를 구성하거나 표시하려면 먼저 IGMP 라우팅 인터페이스가 아닌 하나 이상의 라우터 인터페이스를 구성해야 합니다. 이 필드는 인터페이스 모드가 비활성화된 경우에만 구성할 수 있습니다.

Interface Mode(인터페이스 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 선택된 인터페이스의 IGMP 프록시 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다. IGMP 프록시 인터페이스 모드를 활성화하려면 라우팅, IGMP 및 멀티캐스트 전역 관리 모드를 활성화해야 합니다.

Unsolicited Report Interval(임의 보고서 간격) — 임의의 시간 간격 값(초)을 입력합니다. Unsolicited Report Interval(임의 보고서 간격)은 그룹에서 멤버십에 대한 호스트의 초기 보고서 반복 간격입니다. 유효한 값은 1 ~ 260이고 기본값은 1입니다.

IGMP 프록시 인터페이스 구성

1. **IGMP Proxy Interface Configuration(IGMP 프록시 인터페이스 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

프록시 인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 IGMP 프록시 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

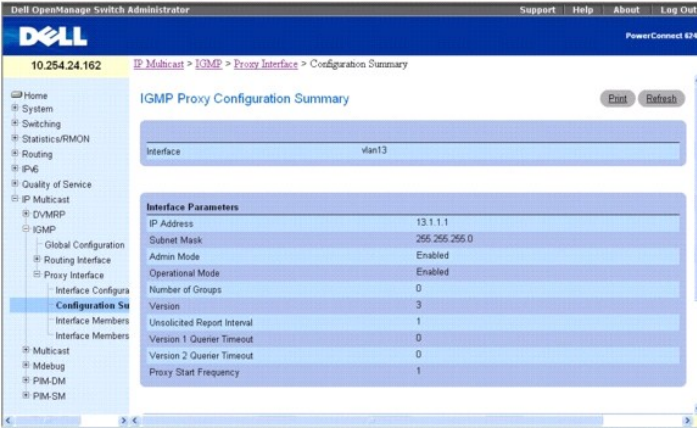
1. IGMP 프록시 명령

IGMP 프록시 구성 요약

IGMP Proxy Configuration Summary(IGMP 프록시 구성 요약) 페이지를 사용하여 인터페이스별 프록시 인터페이스 구성을 표시합니다. 이 페이지에 데이터를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→IGMP→Proxy Interface(프록시 인터페이스)→Configuration Summary(구성 요약)**를 클릭합니다.

그림 13-13. IGMP Proxy Configuration Summary(IGMP 프록시 구성 요약)



IGMP Proxy Configuration Summary(IGMP 프록시 구성 요약) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — IGMP 프록시가 활성화된 인터페이스를 표시합니다. IGMP 프록시 인터페이스는 하나만 존재할 수 있습니다.

IP Address(IP 주소) — IGMP 프록시 인터페이스의 IP 주소입니다.

Subnet Mask(서브네트 마스크) — IGMP 프록시 인터페이스의 IP 주소에 대한 서브네트 마스크입니다.

Admin Mode(관리 모드) — 선택된 인터페이스의 IGMP 프록시 관리 상태입니다.

Operational Mode(작동 모드) — IGMP 프록시 인터페이스의 작동 상태입니다.

Number of Groups(그룹 수) — 캐시 표에 있는 IGMP 프록시 인터페이스에 대한 현재 멀티캐스트 그룹 항목 수입니다.

Version(버전) — IGMP 프록시 인터페이스에 구성되어 있는 IGMP 버전입니다.

Unsolicited Report Interval(임의 보고서 간격) — Unsolicited Report Interval(임의 보고서 간격)은 그룹에서 멤버십에 대한 호스트의 초기 보고서 반복 간격입니다. 기본값: 1 second.

Version 1 Querier Timeout(버전 1 쿼리기 타임아웃) — 오래된 IGMP 버전 2 쿼리기 타임아웃 값(초)입니다. Older Version Querier Interval(이전 버전 쿼리기 간격)은 이전 버전 쿼리가 수신될 때 호스트를 IGMPv3 모드로 다시 전환하기 위한 타임아웃입니다. 이전 버전 쿼리가 수신되면 호스트는 Older Version Querier Present Timer(이전 버전 쿼리기 제공 타이머)를 Older Version Querier Interval(이전 버전 쿼리기 간격)로 설정합니다.

Version 2 Querier Timeout(버전 2 쿼리기 타임아웃) — 오래된 IGMP 버전 2 쿼리기 타임아웃 값(초)입니다.

Proxy Start Frequency(프록시 시작 빈도) — 프록시가 실행된 횟수입니다.

Proxy Interface Statistics(프록시 인터페이스 통계) — 수신된 쿼리, 수신/전송된 보고서, 수신/전송된 탈퇴

CLI 명령을 사용하여 IGMP 프록시 인터페이스 구성 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

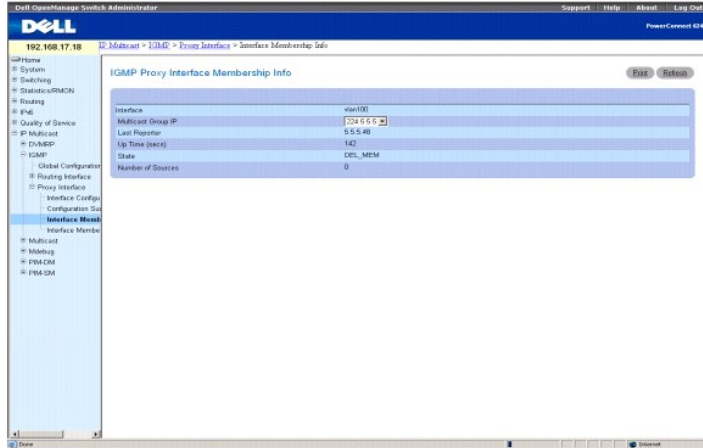
- 1 IGMP 프록시 명령

IGMP 프록시 인터페이스 멤버십 정보

IGMP Proxy Interface Membership Info(IGMP 프록시 인터페이스 멤버십 정보) 페이지를 사용하여 특정 IP 멀티캐스트 그룹 주소에 대한 인터페이스 멤버십 데이터를 표시합니다. 인터페이스 멤버십 정보를 표시하려면 먼저 IGMP 라우팅 인터페이스가 아닌 하나 이상의 라우터 인터페이스를 구성해야 합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우에는 이 페이지에 아무 데이터도 표시되지 않습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)** → **IGMP** → **Proxy Interface(프록시 인터페이스)** → **Interface Membership Info(인터페이스 멤버십 정보)**를 클릭합니다.

그림 13-14. IGMP Proxy Interface Membership Info(IGMP 프록시 인터페이스 멤버십 정보)



IGMP Proxy Interface Membership Info(IGMP 프록시 인터페이스 멤버십 정보) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — IGMP 프록시가 활성화된 인터페이스를 표시합니다.

Multicast Group IP(멀티캐스트 그룹 IP) — 데이터를 표시할 IP 멀티캐스트 그룹 주소를 선택합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우 이 선택을 수행할 수 없으며 다음과 같은 아무 데이터도 표시되지 않습니다.

Last Reporter(마지막 보고자) — IGMP 프록시 인터페이스에서 IP 멀티캐스트 그룹 주소에 대해 수신된 마지막 멤버십 보고서의 소스 IP 주소입니다.

Up Time (secs)(가동 시간(초)) — 이 항목이 만들어진 이후에 경과한 시간입니다.

State(상태) — 호스트 항목의 상태입니다. 호스트의 상태는 다음 중 하나입니다. 비구성원 상태 - 인터페이스의 그룹에 속하지 않습니다. 지연 구성원 상태 - 호스트가 인터페이스의 그룹에 속하고 보고서 타이머가 실행 중입니다. 보고서 타이머는 보고서를 전송하는 데 사용됩니다. 유휴 구성원 상태 - 호스트가 인터페이스의 그룹에 속하고 보고서 타이머가 실행되고 있지 않습니다.

Number of Sources(소스 수) — 선택된 멀티캐스트 그룹에 있는 소스 호스트 수입니다.

CLI 명령을 사용하여 IGMP 프록시 인터페이스 멤버십 정보 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

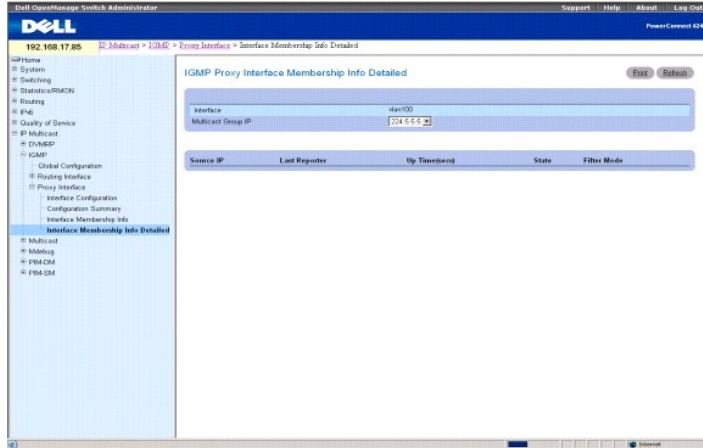
- 1 IGMP 프록시 명령

IGMP 프록시 인터페이스 세부 멤버십 정보

IGMP Proxy Interface Membership Info Detailed(IGMP 프록시 인터페이스 멤버십 세부 정보) 페이지를 사용하여 세부 인터페이스 멤버십 데이터를 표시합니다. 세부 인터페이스 멤버십 정보를 표시하려면 먼저 IGMP 라우팅 인터페이스가 아닌 하나 이상의 라우터 인터페이스를 구성해야 합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우에는 데이터를 표시할 수 없습니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)** → **IGMP** → **Proxy Interface(프록시 인터페이스)** → **Interface Membership Info Detailed(인터페이스 멤버십 세부 정보)**를 클릭합니다.

그림 13-15. IGMP Proxy Interface Membership Info Detailed(IGMP 프록시 인터페이스 멤버십 세부 정보)



IGMP Proxy Interface Membership Info Detailed(IGMP 프록시 인터페이스 멤버십 세부 정보) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

Multicast Group IP(멀티캐스트 그룹 IP) — 데이터를 표시할 IP 멀티캐스트 그룹 주소를 선택합니다. 선택된 인터페이스에서 수신된 그룹 멤버십 보고서가 없는 경우 이 선택을 수행할 수 없으며 구성이 불가능한 아무 데이터도 표시되지 않습니다.

Source IP(소스 IP) — 이 매개변수는 이 멀티캐스트 주소의 구성원인 소스 주소를 표시합니다.

Last Reporter(마지막 보고자) — 선택된 인터페이스의 IP 멀티캐스트 그룹 주소에 대해 수신된 마지막 멤버십 보고서의 소스 IP 주소입니다.

Up Time (secs)(가동 시간(초)) — 항목이 캐쉬 표에 만들어진 이후의 가동 시간을 표시합니다.

State(상태) — 호스트 항목의 상태입니다. 호스트의 상태는 다음 중 하나입니다.

Non-member State(비구성원 상태) — 인터페이스의 그룹에 속하지 않습니다.

Delaying Member State(지연 구성원 상태) — 호스트가 인터페이스의 그룹에 속하고 보고서 타이머가 실행 중입니다. 보고서 타이머는 보고서를 전송하는 데 사용됩니다.

Idle Member State(유휴 구성원 상태) — 호스트가 인터페이스의 그룹에 속하고 보고서 타이머가 실행 중이 아닙니다.

Filter Mode(필터 모드) — IGMP 프록시 인터페이스에서 지정된 그룹에 대한 그룹 필터 모드(포함/제외/없음)입니다.

IGMP 프록시 인터페이스 멤버십 세부 정보 표시

1. IGMP Proxy Interface Membership Info Detailed(IGMP 프록시 인터페이스 멤버십 세부 정보) 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.
3. 원하는 **Multicast Group IP(멀티캐스트 그룹 IP)**를 선택합니다.
이 인터페이스 및 멀티캐스트 그룹 IP에 대한 세부 멤버십 데이터가 표시됩니다.

CLI 명령을 사용하여 세부 인터페이스 멤버십 세부 정보 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. IGMP 프록시 명령

멀티캐스트

Multicast(멀티캐스트) 메뉴 페이지에는 **Multicast(멀티캐스트)** 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→Multicast(멀티캐스트)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

1. [멀티캐스트 전역 구성](#)
1. [멀티캐스트 인터페이스 구성](#)
1. [멀티캐스트 Mroute 요약](#)

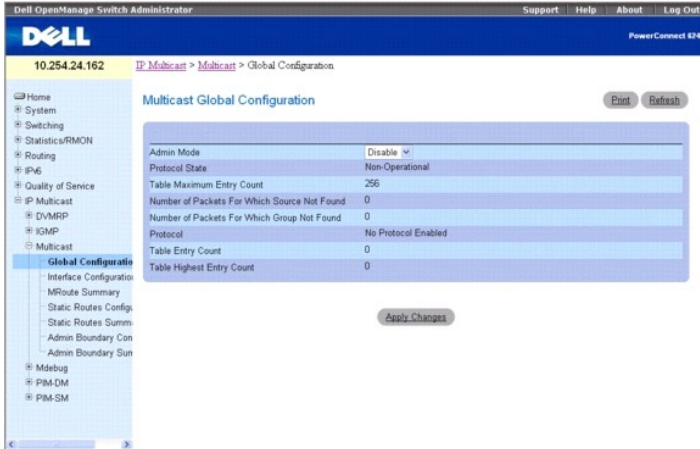
- 1 [멀티캐스트 정적 경로 구성](#)
- 1 [멀티캐스트 정적 경로 요약](#)
- 1 [멀티캐스트 관리 경계 구성](#)
- 1 [멀티캐스트 관리 경계 요약](#)

멀티캐스트 전역 구성

Multicast Global Configuration(멀티캐스트 전역 구성) 페이지를 사용하여 라우터의 멀티캐스트 전달 관리 상태를 구성하고 전역 멀티캐스트 매개변수를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 IP Multicast(IP 멀티캐스트) → Multicast(멀티캐스트) → Global Configuration(전역 구성)을 클릭합니다.

그림 13-16. Multicast Global Configuration(멀티캐스트 전역 구성)



Multicast Global Configuration(멀티캐스트 전역 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Admin Mode(관리 모드) — Enable(활성) 또는 Disable(비활성)을 선택하여 라우터의 멀티캐스트 전달 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다.

Protocol State(프로토콜 상태) — 멀티캐스트 전달 모듈의 작동 상태입니다.

Table Maximum Entry Count(표 최대 항목 수) — IP 멀티캐스트 라우팅 표의 최대 항목 수입니다.

Number Of Packets For Which Source Not Found(소스 없는 패킷 수) — 라우팅되지만 RPF 검사에 실패한 멀티캐스트 패킷 수입니다.

Number Of Packets For Which Group Not Found(그룹 없는 패킷 수) — 라우팅되지만 멀티캐스트 경로가 없는 멀티캐스트 패킷 수입니다.

Protocol(프로토콜) — 라우터에 현재 활성화되어 있는 멀티캐스트 라우팅 프로토콜입니다(있는 경우).

Table Entry Count(표 항목 수) — 멀티캐스트 경로 표에 현재 있는 멀티캐스트 경로 항목 수입니다.

Table Highest Entry Count(표 최대 항목 수) — 멀티캐스트 경로 표에 있는 최대 멀티캐스트 경로 항목 수입니다.

멀티캐스트 전달 관리 모드 구성

1. Multicast Global Configuration(멀티캐스트 전역 구성) 페이지를 엽니다.
2. Admin Mode(관리 모드)로 Enable(활성화) 또는 Disable(비활성화)을 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

멀티캐스트 전역 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 멀티캐스트 전달 매개변수 구성/표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

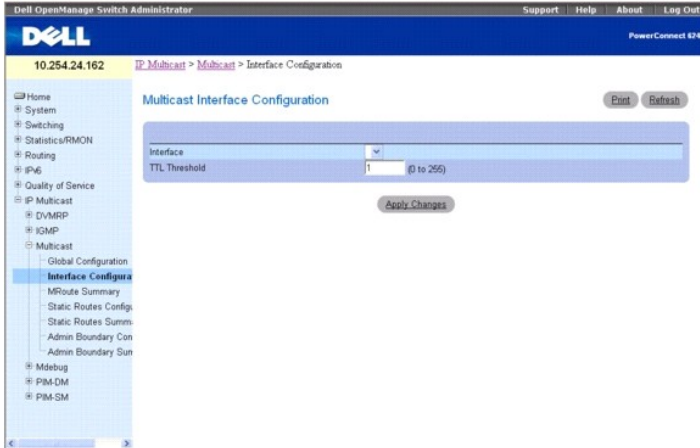
- 1 멀티캐스트 명령

멀티캐스트 인터페이스 구성

Multicast Interface Configuration(멀티캐스트 인터페이스 구성) 페이지를 사용하여 멀티캐스트 인터페이스에 대한 TTL 임계값을 구성합니다. 이 페이지에 필드를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → Multicast(멀티캐스트) → Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 13-17. Multicast Interface Configuration(멀티캐스트 인터페이스 구성)



Multicast Interface Configuration(멀티캐스트 인터페이스 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 구성할 라우팅 인터페이스를 선택합니다.

TTL Threshold(TTL 임계값) — 값이 그 이하로 떨어질 경우 선택된 인터페이스에서 멀티캐스트 데이터 패킷이 전달되지 않는 TTL 임계값을 입력합니다. 0과 255 사이의 숫자를 입력합니다. 0을 입력할 경우 선택된 인터페이스에 대한 모든 멀티캐스트 패킷이 전달됩니다. 이 필드를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다.

멀티캐스트 인터페이스 구성

1. **Multicast Interface Configuration(멀티캐스트 인터페이스 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 드롭다운 메뉴에서 구성할 인터페이스를 선택합니다.
3. 원하는 **TTL 임계값**을 입력합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

멀티캐스트 인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 멀티캐스트 인터페이스 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

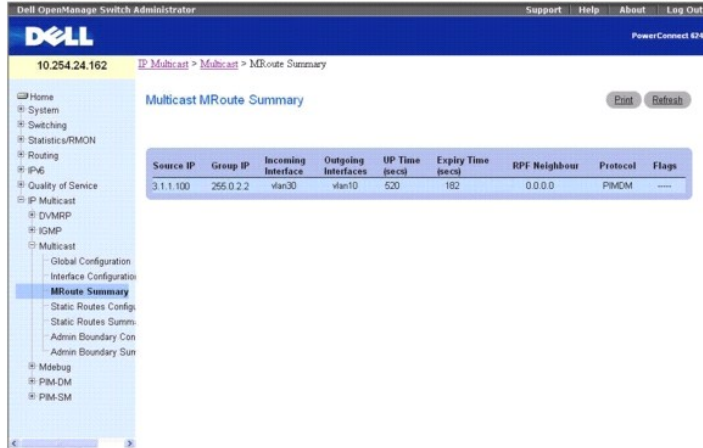
1. 멀티캐스트 명령

멀티캐스트 Mroute 요약

Multicast Mroute Summary(멀티캐스트 Mroute 요약) 페이지를 사용하여 MRoute 데이터를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → Multicast(멀티캐스트) → MRoute Summary(MRoute 요약)**를 클릭합니다.

그림 13-18. Multicast Mroute Summary(멀티캐스트 MRoute 요약)



Multicast Mroute Summary(멀티캐스트 MRoute 요약) 페이지에는 다음 필드가 표시됩니다.

Source IP(소스 IP) — 그룹 IP와 결합되어 Mroute 표 항목을 식별하는 멀티캐스트 패킷 소스의 IP 주소입니다.

Group IP(그룹 IP) — 대상 그룹 IP 주소입니다.

Incoming Interface(수신 인터페이스) — 이 소스/그룹에 대한 멀티캐스트 패킷이 도착하는 수신 인터페이스입니다.

Outgoing Interfaces(전송 인터페이스) — 이 소스/그룹에 대한 멀티캐스트 패킷이 전달되는 전송 인터페이스 목록입니다.

Up Time (secs)(가동 시간(초)) — 항목이 만들어진 이후에 경과한 시간(초)입니다.

Expiry Time (secs)(만료 시간(초)) — 이 항목이 만료되고 표에서 제거될 때까지 남은 시간(초)입니다.

RPF Neighbor(RPF 인접 항목) — 역경로 전달 인접 항목의 IP 주소입니다.

Protocol(프로토콜) — 이 항목을 만든 멀티캐스트 라우팅 프로토콜입니다. 다음을 사용할 수 있습니다.

- 1 PIM-DM
- 1 PIM-SM
- 1 DVMRP

Flags(플래그) — 실행 중인 멀티캐스트 라우팅 프로토콜이 PIM-SM인 경우에만 이 필드에 표시되는 값이 유효합니다. 가능한 값은 RPT 또는 SPT입니다. 다른 프로토콜의 경우 "-----"이 표시됩니다.

CLI 명령을 사용하여 MRoute 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

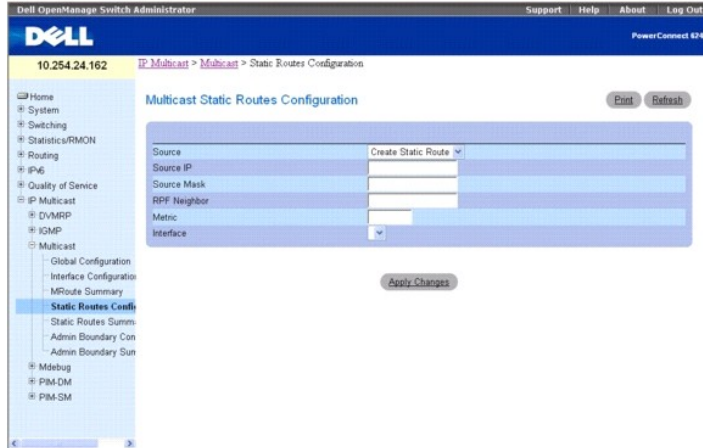
- 1 멀티캐스트 명령

멀티캐스트 정적 경로 구성

Multicast Static Routes Configuration(멀티캐스트 정적 경로 구성) 페이지를 사용하여 Mroute 표에서 새 정적 항목을 구성하거나 기존 항목을 수정합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)** → **Multicast(멀티캐스트)** → **Static Routes Configuration(정적 경로 구성)**를 클릭합니다.

그림 13-19. Multicast Static Routes Configuration(멀티캐스트 정적 경로 구성)



Multicast Static Routes Configuration(멀티캐스트 정적 경로 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Source(소스) — Create Static Route(정적 경로 만들기)를 선택하여 Mroute 표에서 새 정적 항목을 구성하거나, 드롭다운 메뉴에서 기존 항목 중 하나를 선택합니다.

Source IP(소스 IP) — 만드는 항목에 대한 멀티캐스트 패킷 소스를 식별하는 IP 주소를 입력합니다.

Source Mask(소스 마스크) — 소스 IP 주소에 적용할 서브네트 마스크를 입력합니다.

RPF Neighbor(RPF 인접 항목) — 소스 경로에 인접 라우터의 IP 주소를 입력합니다.

Metric(메트릭) — 멀티캐스트 소스 경로의 링크 상태 비용을 입력합니다. 범위는 0-255이고, 기본값은 1입니다. 정적 경로를 선택하고 이 필드를 편집하여 구성된 경로에 대한 메트릭을 변경할 수 있습니다.

Interface(인터페이스) — 드롭다운 메뉴에서 인터페이스 번호를 선택합니다. 지정된 소스 IP 주소에 대한 인접 라우터에 연결되는 인터페이스입니다.

정적 경로 구성

1. **Static Routes(정적 경로)** 페이지를 엽니다.
2. **Source(소스)** 필드에서 **Create Static Route(정적 경로 만들기)**를 선택하여 새 정적 항목을 구성하거나 기존 항목 중 하나를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

새 정적 경로 또는 수정된 정적 경로가 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 정적 경로 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

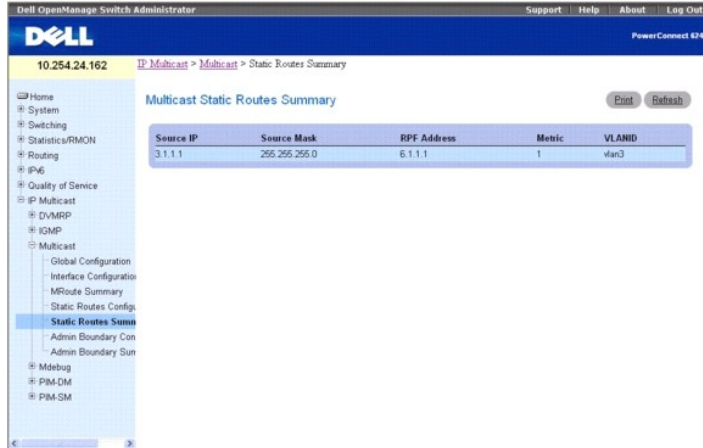
1. 멀티캐스트 명령

멀티캐스트 정적 경로 요약

Multicast Static Routes Summary(멀티캐스트 정적 경로 요약) 페이지를 사용하여 정적 경로와 해당 구성을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)**→**Multicast(멀티캐스트)**→**Static Routes Summary(정적 경로 요약)**를 클릭합니다.

그림 13-20. Multicast Static Routes Summary(멀티캐스트 정적 경로 요약)



Multicast Static Routes Summary(멀티캐스트 정적 경로 요약) 페이지에는 다음 필드가 표시됩니다.

Source IP(소스 IP) — 이 경로에 대한 멀티캐스트 패킷 소스를 식별하는 IP 주소입니다.

Source Mask(소스 마스크) — 소스 IP 주소에 적용되는 서브넷 마스크입니다.

RPF Address(RPF 주소) — RPF 인접 항목의 IP 주소입니다.

Metric(메트릭) — 멀티캐스트 소스 경로의 링크 상태 비용입니다. 범위는 0-255입니다.

VLANID — 지정된 소스 IP 주소에 대한 RPF로 사용되는 수신 VLAN의 번호입니다.

CLI 명령을 사용하여 정적 경로 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

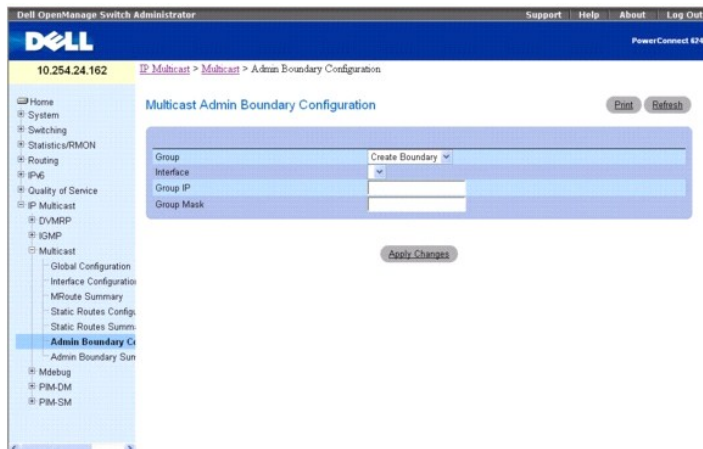
1. 멀티캐스트 명령

멀티캐스트 관리 경계 구성

관리 경계 범위 정의를 사용하면 지정된 라우팅 인터페이스에서 지정된 멀티캐스트 주소 범위에 대한 멀티캐스트 트래픽 수신/전송을 중지할 수 있습니다. **Multicast Admin Boundary Configuration(멀티캐스트 관리 경계 구성)** 페이지를 사용하여 새 관리 경계 범위 또는 기존 관리 경계 범위를 구성합니다. 이 페이지를 표시하려면 유효한 라우팅 인터페이스 및 멀티캐스트를 구성해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)** → **Multicast(멀티캐스트)** → **Admin Boundary Configuration(관리 경계 구성)**을 클릭합니다.

그림 13-21. Multicast Admin Boundary Configuration(멀티캐스트 관리 경계 구성)



Multicast Admin Boundary Configuration(멀티캐스트 관리 경계 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Group(그룹) — 드롭다운 메뉴에서 **Create Boundary(경계 만들기)**를 선택하여 새 관리 범위 경계를 만들거나, 기존 경계 사양 중 하나를 선택하여 해당 구성을 표시하거나 업데이트합니다.

Interface(인터페이스) — 관리 경계 범위를 구성할 라우터 인터페이스를 선택합니다.

Group IP(그룹 IP) — 제외할 주소 범위의 시작 부분에 해당하는 멀티캐스트 그룹 주소를 입력합니다. 주소는 범위가 239.0.0.0 ~ 239.255.255.255이어야 합니다.

Group Mask(그룹 마스크) — 멀티캐스트 그룹 주소에 적용할 마스크를 입력합니다. 마스크와 그룹 IP를 조합하여 선택된 인터페이스에 대해 관리되는 주소 범위를 지정합니다.

관리 경계 구성

1. **Multicast Admin Boundary Configuration(멀티캐스트 관리 경계 구성)** 페이지를 엽니다.
2. **Group IP(그룹 IP)** 필드에서 **Create Boundary(경계 만들기)**를 선택하여 새 관리 범위 경계를 구성하거나 기존 항목 중 하나를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

새 관리 범위 경계 또는 수정된 관리 범위 경계가 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 관리 경계 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. 멀티캐스트 명령

멀티캐스트 관리 경계 요약

Multicast Admin Boundary Summary(멀티캐스트 관리 경계 요약) 페이지를 사용하여 기존 관리 경계 범위를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → Multicast(멀티캐스트) → Admin Boundary Summary(관리 경계 요약)**를 클릭합니다.

그림 13-22. Multicast Admin Boundary Summary(멀티캐스트 관리 경계 요약)

Interface	Group IP	Group Mask
vlan0	239.10.10.0	255.255.255.0
vlan200	239.10.200.0	255.255.255.0

Multicast Admin Boundary Summary(멀티캐스트 관리 경계 요약) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — 관리되는 주소 범위가 적용되는 라우터 인터페이스입니다.

Group IP(그룹 IP) — 제외할 주소 범위의 시작 부분에 해당하는 멀티캐스트 그룹 주소입니다.

Group Mask(그룹 마스크) — 멀티캐스트 그룹 주소에 적용되는 마스크입니다. 마스크와 그룹 IP를 조합하여 선택된 인터페이스에 대해 관리되는 주소 범위를 지정합니다.

CLI 명령을 사용하여 멀티캐스트 관리 경계 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. 멀티캐스트 명령

PIM-DM

PIM-DM 프로토콜은 간단한 프로토콜 독립 멀티캐스트 라우팅 프로토콜입니다. 이 프로토콜은 기존 유니캐스트 라우팅 표와 연결/정리/결합 메커니즘을 사용하여 트리를 구축합니다. PIM-DM은 RPF를 활용하는 소스 기반 최단 경로 배포 트리를 생성합니다. PIM-SM의 경우와 마찬가지로 공유 배포 트리를 구축할 때는 PIM-DM을 사용할 수 없습니다. PIM-DM에서는 발신기가 데이터 보내기를 시작하면 모든 다운스트림 라우터와 호스트가 멀티캐스트 데이터그램을 수신하려는 것으로 가정합니다. PIM-DM은 처음에는 멀티캐스트 트래픽을 전체 네트워크로 플러딩합니다. 다운스트림 인접 항목이 없는 라우터가 그 중 원하지 않는 트래픽을 다시 정리합니다. PRUNE(정리) 메시지 외에도 PIM-DM은 결합 및 설정 메시지를 활용합니다. 결합 메시지는 새 호스트가 그룹을 연결하려고 할 때마다 사용됩니다. 설정 메시지는 동일한 다중 액세스 네트워크에서 중복 흐름을 중단하는 데 사용됩니다.

PIM-DM 버전에는 두 가지가 있습니다. 버전 2는 IGMP 메시지를 사용하지 않고, IP 패킷에 캡슐화되는 메시지를 사용하여 프로토콜 번호는 103입니다. 버전 2에서는 Hello 메시지가 캐리 메시지 대신에 사용됩니다.

PIM-DM은 다음에 적합합니다.

- 1 수신기가 집약적으로 배포된 경우
- 1 발신기는 소수이고 수신기는 다수인 경우(찾은 플러딩이 원인)
- 1 멀티캐스트 트래픽이 많은 경우
- 1 트래픽이 일정한 스트림인 경우

PIM-DM 메뉴 페이지에는 PIM-DM 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → PIM-DM**을 클릭합니다.

이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

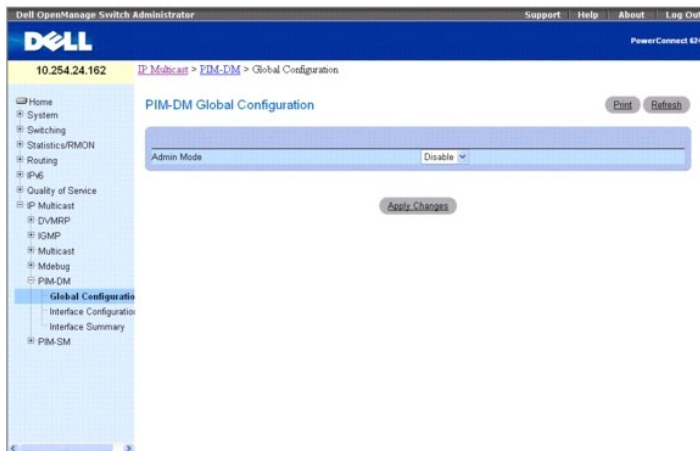
- 1 [PIM-DM 전역 구성](#)
- 1 [PIM-DM 인터페이스 구성](#)
- 1 [PIM-DM 인터페이스 요약](#)

PIM-DM 전역 구성

PIM-DM Global Configuration(PIM-DM 전역 구성) 페이지를 사용하여 이 시스템의 PIM-DM 관리 상태를 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트) → PIM-DM → Global Configuration(전역 구성)**을 클릭합니다.

그림 13-23. PIM-DM Global Configuration(PIM-DM 전역 구성)



PIM-DM Global Configuration(PIM-DM 전역 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Admin Mode(관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 시스템의 PIM-DM 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다.

PIM-DM 구성

- 1 PIM-DM Global Configuration(PIM-DM 전역 구성) 페이지를 엽니다.
- 2 **Admin Mode(관리 모드)**를 Enable(활성) 또는 Disable(비활성)로 설정하여 PIM-DM을 켜거나 끕니다.
- 3 **Apply Changes(변경사항 적용)**를 클릭하십시오.

PIM-DM 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 PIM-DM 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

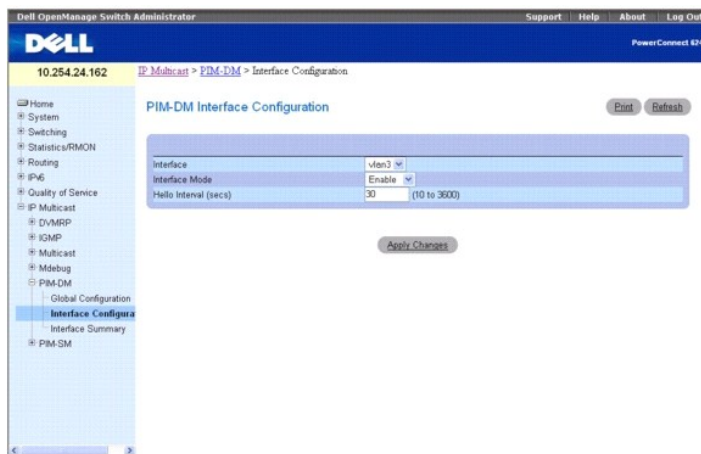
- 1 PIM-DM 명령

PIM-DM 인터페이스 구성

PIM-DM Interface Configuration(PIM-DM 인터페이스 구성) 페이지에서 PIM-DM을 사용하여 특정 인터페이스를 구성합니다. 이 인터페이스 구성 페이지를 표시하려면 **PIM-DM Global Configuration(PIM-DM 전역 구성)** 페이지에서 PIM-DM을 활성화해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→PIM-DM→Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 13-24. PIM-DM Interface Configuration(PIM-DM 인터페이스 구성)



PIM-DM Interface Configuration(PIM-DM 인터페이스 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다. PIM-DM 인터페이스를 구성 또는 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

Interface Mode(인터페이스 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 선택된 인터페이스의 PIM-DM 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다.

Hello Interval (secs)(Hello 간격(초)) — 선택된 인터페이스에서 전송되는 PIM hello 메시지 간의 간격(초)을 입력합니다. 기본값은 30이고, 유효한 값은 10 ~ 3600입니다.

인터페이스에 대한 PIM-DM 구성

1. **PIM-DM Interface Configuration(PIM-DM 인터페이스 구성)** 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에서 구성할 인터페이스를 선택합니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 인터페이스에 대한 PIM-DM 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 PIM-DM 명령

PIM-DM 인터페이스 요약

PIM-DM Interface Summary(PIM-DM 인터페이스 요약) 페이지를 사용하여 PIM-DM 인터페이스와 해당 설정을 표시합니다. 이 페이지를 표시하려면 이 라우터에서 하나 이상의 인터페이스를 PIM-DM으로 설정해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP 멀티캐스트)→PIM-DM→Interface Summary(인터페이스 요약)**를 클릭합니다.

그림 13-25. PIM-DM Interface Summary(PIM-DM 인터페이스 요약)



PIM-DM Interface Summary(PIM-DM 인터페이스 요약) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다. PIM-DM 인터페이스에 대한 데이터를 표시하려면 먼저 하나 이상의 라우터 인터페이스를 구성해야 합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

인터페이스 매개변수

Interface Mode(인터페이스 모드) — 선택된 인터페이스의 PIM-DM 관리 상태를 표시합니다. 기본값은 Disable(비활성)입니다.

Protocol State(프로토콜 상태) — 이 인터페이스에서의 PIM-DM 프로토콜의 작동 상태입니다.

Hello Interval(secs)(Hello 간격(초)) — 선택된 인터페이스에서 PIM hello 메시지가 전송되는 빈도입니다.

IP Address(IP 주소) — 선택된 인터페이스의 IP 주소입니다.

인터페이스 통계

Neighbor Count(인접 항목 수) — 선택된 인터페이스의 PIM 인접 항목 수입니다.

Designated Router(지정된 라우터) — 선택된 PIM 인터페이스에서 지정된 라우터입니다. 지정된 라우터의 경우 0.0.0.0입니다.

Interface Neighbors(인터페이스 인접 항목)

Neighbor IP(인접 IP) — 이 항목에 정보가 있는 PIM 인접 항목의 IP 주소입니다.

Up Time(가동 시간)(hh:mm:ss) — 이 PIM 인접 항목(마지막)이 로컬 라우터의 인접 항목이 된 이후에 경과한 시간입니다.

Expiry Time(만료 시간)(hh:mm:ss) — 이 PIM 인접 항목이 만료되기 이전에 남아 있는 최소 시간입니다.

CLI 명령을 사용하여 PIM-DM 인터페이스 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 PIM-DM 명령

PIM-SM

PIM-SM을 사용하면 멀티캐스트 트래픽을 멀티캐스트 그룹으로 효과적으로 라우팅하여 WAN을 확장할 수 있지만 대역폭이 제한됩니다. PIM-SM에서는 기본적으로 공유 트리를 사용하고 효율성을 위해 소스 기반 트리를 구현합니다. 이 데이터 링크같은 트리 간을 전환하는 데 사용됩니다. PIM-SM에서는 호스트에서 특별히 요청하지 않는 한 멀티캐스트 트래픽을 원하는 호스트가 없는 것으로 가정합니다. PIM-SM에서는 소스 트래픽이 수신기에 할래이되는 정의된 집합 지점(RP)에 집중된 공유 배포 트리를 만듭니다. 발신기가 먼저 멀티캐스트 데이터를 RP로 보내면 RP에서는 공유 트리를 따라 해당 데이터를 수신기로 전송합니다. RP에 집중된 공유 트리는 최단/최적 경로를 제공할 필요가 없습니다. 그런 경우 PIM-SM을 사용하여 보다 효율적인 소스별 트리로 전환할 수 있습니다.

PIM-SM 메뉴 페이지에는 PIM-SM 매개변수와 데이터를 정의 및 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **IP Multicast(IP**

멀티캐스트) → PIM-SM을 클릭합니다.

이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

- 1 [PIM-SM 전역 구성](#)
- 1 [PIM-SM 전역 상태](#)
- 1 [PIM-SM 인터페이스 구성](#)
- 1 [PIM-SM 인터페이스 요약](#)
- 1 [구성 요소 요약](#)
- 1 [RP 설정 요약](#)
- 1 [후보 RP 요약](#)
- 1 [정적 RP 구성](#)

PIM-SM 전역 구성

PIM-SM Global Configuration(PIM-SM 전역 구성) 페이지를 사용하여 이 시스템에 대한 전역 PIM-SM 설정을 구성합니다.

이 페이지를 표시하려면 디렉터리 화면에서 Multicast(멀티캐스트) → PIM-SM → Global Configuration(전역 구성)을 클릭합니다.

그림 13-26. PIM-SM Global Configuration(PIM-SM 전역 구성)



PIM-SM Global Configuration(PIM-SM 전역 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Admin Mode(관리 모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 시스템의 PIM-SM 관리 상태를 설정합니다. PIM-SM을 활성화하려면 먼저 IGMP를 활성화해야 합니다. 기본값은 Disable(비활성)입니다.

Join/Prune Interval (secs)(연결/정리 간격(초)) — PIM-SM Join/Prune(PIM-SM 연결/정리) 메시지의 전송 간격을 입력합니다. 유효한 값은 10 ~ 3600초입니다. 기본값은 60입니다.

Data Threshold Rate (Kbps)(데이터 임계값(Kbps)) — 마지막 홉 라우터가 소스별 최단 경로 트리로 전환되는 최소 소스 데이터 속도(Kbits/초)를 입력합니다. 유효한 값은 0 ~ 2000KB/초이고 기본값은 50입니다.

Register Threshold Rate (Kbps)(등록 임계값(Kbps)) — 집합 지정 라우터가 소스별 최단 경로 트리로 전환되는 최소 소스 데이터 속도(Kbits/초)를 입력합니다. 유효한 값은 0 ~ 2000KB/초이고 기본값은 50입니다.

PIM-SM 구성

1. PIM-SM Global Configuration(PIM-SM 전역 구성) 페이지를 엽니다.
2. Admin Mode(관리 모드)를 Enable(활성) 또는 Disable(비활성)로 설정하여 PIM-SM을 켜거나 끕니다.
3. 필요에 따라 나머지 필드를 수정합니다.
4. Apply Changes(변경사항 적용)를 클릭하십시오.

인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 PIM-SM 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

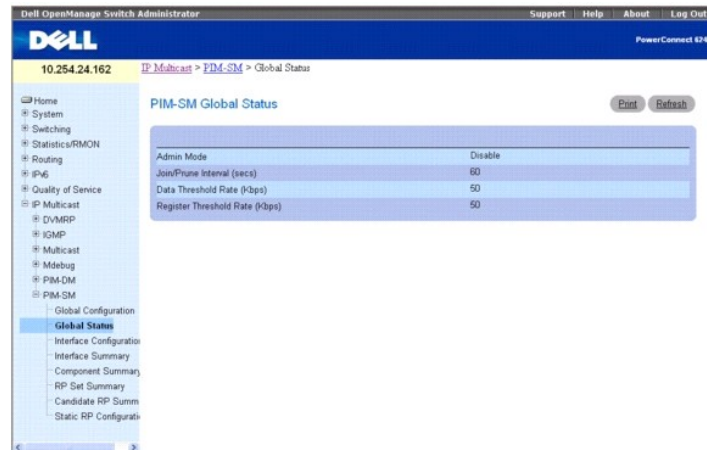
- 1 PIM-SM 명령

PIM-SM 전역 상태

PIM-SM Global Status(PIM-SM 전역 상태) 페이지를 사용하여 PIM-SM Global Configuration(PIM-SM 전역 구성) 페이지에 선택된 전역 설정을 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→PIM-SM→Global Status(전역 상태)**를 클릭합니다.

그림 13-27. PIM-SM Global Status(PIM-SM 전역 상태)



PIM-SM Global Status(PIM-SM 전역 상태) 페이지에는 다음 필드가 표시됩니다.

Admin Mode(관리 모드) — 라우터의 PIM-SM 관리 상태; Enable(활성) 또는 Disable(비활성).

Join/Prune Interval (secs)(연결/정리 간격(초)) — PIM-SM 연결/정리 메시지의 전송 간격입니다.

Data Threshold Rate (Kbps)(데이터 임계값(Kbps)) — 마지막 홉 라우터가 소스별 최단 경로 트리로 전환되는 최소 소스 데이터 속도(Kbits/초)입니다.

Register Threshold Rate (Kbps)(등록 임계값(Kbps)) — 집합 지점 라우터가 소스별 최단 경로 트리로 전환되는 최소 소스 데이터 속도(Kbits/초)입니다.

CLI 명령을 사용하여 PIM-SM 전역 상태 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

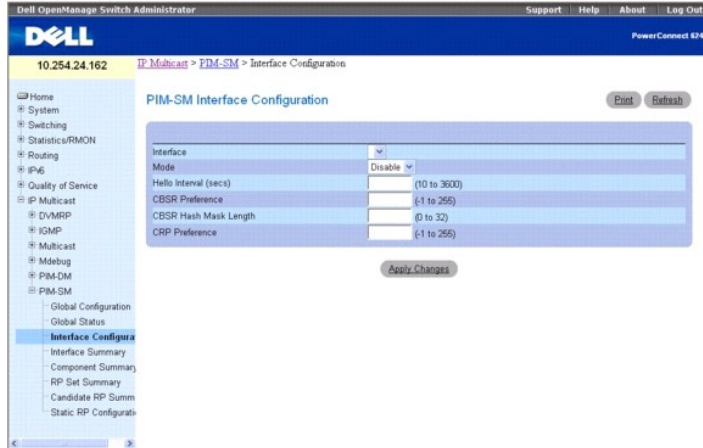
- 1 PIM-SM 명령

PIM-SM 인터페이스 구성

PIM-SM Interface Configuration(PIM-SM 인터페이스 구성) 페이지를 사용하여 인터페이스에 대한 PIM-SM을 구성합니다. 이 인터페이스 구성 페이지를 표시하려면 **PIM-SM Global Configuration(PIM-SM 전역 구성)** 페이지에서 PIM-SM을 활성화해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→PIM-SM→Interface Configuration(인터페이스 구성)**을 클릭합니다.

그림 13-28. PIM-SM Interface Configuration(PIM-SM 인터페이스 구성)



PIM-SM Interface Configuration(PIM-SM 인터페이스 구성) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 데이터를 표시 또는 구성할 인터페이스를 선택합니다. 데이터를 표시 또는 구성하려면 하나 이상의 라우팅 인터페이스가 있어야 합니다.

Mode(모드) — 드롭다운 메뉴에서 Enable(활성) 또는 Disable(비활성)을 선택하여 이 인터페이스의 PIM-SM 관리 상태를 설정합니다. 기본값은 Disable(비활성)입니다.

Hello Interval (secs)(Hello 간격(초)) — 이 인터페이스에서 PIM Hello 메시지가 전송되는 간격(초)을 입력합니다. 유효한 값은 10 ~ 3600초입니다. 기본값은 30입니다.

CBSR Preference(CBSR 기본 설정) — 로컬 인터페이스에 대한 기본 설정 값을 후보 부트스트랩 라우터로 입력합니다. 값 -1은 로컬 인터페이스가 후보 BSR 인터페이스가 아님을 나타내는 데 사용됩니다. 유효한 값은 -1 ~ 255이고 기본값은 0입니다.

CBSR Hash Mask Length(CBSR 해시 마스크 길이) — 이 인터페이스가 부트스트랩 라우터로 선택된 경우 부트스트랩 메시지에서 알릴 CBSR 해시 마스크 길이를 입력합니다. 이 해시 마스크 길이는 해시 알고리즘에서 특정 그룹에 대한 RP를 선택하는 데 사용됩니다. 유효한 값은 0 ~ 32이고 기본값은 30입니다.

CRP Preference(CRP 기본 설정) — 로컬 인터페이스에 대한 기본 설정 값을 후보 부트스트랩 라우터로 입력합니다. 값 -1은 로컬 인터페이스가 후보 BSR 인터페이스가 아님을 나타내는 데 사용됩니다. 유효한 값은 -1 ~ 255이고 기본값은 0입니다.

인터페이스에 대한 PIM-SM 구성

1. PIM-SM Interface Configuration(PIM-SM 인터페이스 구성) 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에서 구성할 인터페이스를 선택합니다.
3. **Mode(모드)** 필드에서 **Enable(활성)**을 선택합니다.
4. 필요에 따라 나머지 필드를 수정합니다.
5. **Apply Changes(변경사항 적용)**를 클릭하십시오.

인터페이스 구성이 저장되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 인터페이스에 대한 PIM-SM 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

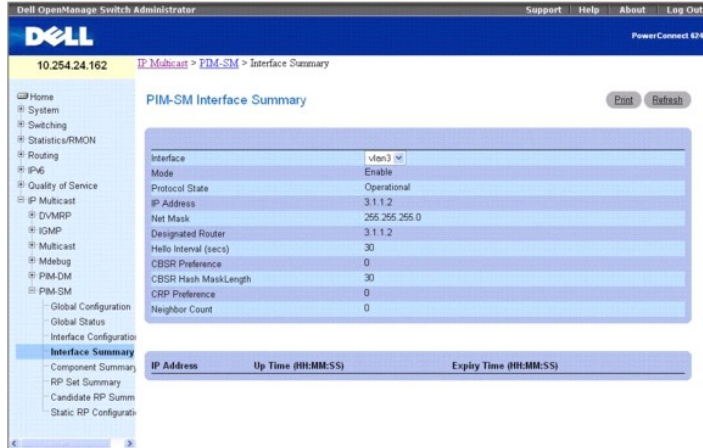
- 1 PIM-SM 명령

PIM-SM 인터페이스 요약

PIM-SM Interface Summary(PIM-SM 인터페이스 요약) 페이지를 사용하여 PIM-SM 인터페이스와 해당 설정을 표시합니다. 이 페이지를 표시하려면 이 라우터에서 하나 이상의 인터페이스를 PIM-SM으로 설정해야 합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트) → PIM-SM → Interface Summary(인터페이스 요약)**를 클릭합니다.

그림 13-29. PIM-SM Interface Summary(PIM-SM 인터페이스 요약)



PIM-SM Interface Summary(PIM-SM 인터페이스 요약) 페이지에는 다음 필드가 표시됩니다.

Interface(인터페이스) — 데이터를 표시할 인터페이스를 선택합니다.

Mode(모드) — 라우터의 PIM-SM 관리 상태: Enable(활성) 또는 Disable(비활성).

Protocol State(프로토콜 상태) — 선택된 인터페이스에서 PIM-SM 프로토콜의 작동 상태(Operational(작동) 또는 Non-operational(비작동))를 나타냅니다.

IP Address(IP 주소) — 선택된 PIM 인터페이스의 IP 주소입니다.

Net Mask(넷 마스크) — 선택된 인터페이스의 IP 주소에 대한 네트워크 마스크입니다.

Designated Router(지정된 라우터) — 선택된 PIM 인터페이스에서 지정된 라우터입니다. 지정된 인터페이스의 경우 이 개체 값이 0.0.0.0입니다.

Hello Interval(secs)(Hello 간격(초)) — 선택된 인터페이스에서 PIM Hello 메시지가 전송되는 빈도입니다.

CBSR Preference(CBSR 기본 설정) — 로컬 인터페이스에 대한 기본 설정 값을 후보 부트스트랩 라우터로 나타냅니다. 값 -1은 로컬 인터페이스가 후보 BSR 인터페이스가 아님을 나타내는 데 사용됩니다.

CBSR Hash Mask Length(CBSR 해시 마스크 길이) — 이 인터페이스가 부트스트랩 라우터로 선택된 경우에 부트스트랩 메시지에서 알릴 CBSR 해시 마스크 길이입니다. 이 해시 마스크 길이는 해시 알고리즘에서 특정 그룹에 대한 RP를 선택하는 데 사용됩니다.

CRP Preference(CRP 기본 설정) — 로컬 인터페이스에 대한 기본 설정 값을 후보 부트스트랩 라우터로 나타냅니다. 값 -1은 로컬 인터페이스가 후보 BSR 인터페이스가 아님을 나타내는 데 사용됩니다.

Neighbor Count(인접 항목 수) — 선택된 인터페이스의 PIM 인접 항목 수입니다.

IP Address(IP 주소) — 이 항목에 대한 PIM 인접 항목의 IP 주소입니다.

Up Time(가동 시간)(hh:mm:ss) — 이 PIM 인접 항목(마지막)이 로컬 라우터의 인접 항목이 된 이후에 경과한 시간입니다.

Expiry Time(만료 시간)(hh:mm:ss) — 이 PIM 인접 항목이 만료되기 이전에 남아 있는 최소 시간입니다.

PIM-SM 인터페이스 요약 표시

1. PIM-SM Interface Summary(PIM-SM 인터페이스 요약) 페이지를 엽니다.

2. **Interface(인터페이스)** 드롭다운 메뉴에서 표시할 인터페이스를 선택합니다.

이 인터페이스에 대한 PIM-SM 구성 데이터가 표시됩니다.

CLI 명령을 사용하여 PIM-SM 인터페이스 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

1. PIM-SM 명령

구성 요소 요약

Component Summary(구성 요소 요약) 페이지를 사용하여 PIM-SM 구성 요소 데이터를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→ PIM-SM→ Component Summary(구성 요소 요약)**를 클릭합니다.

그림 13-30. Component Summary(구성 요소 요약)



Component Summary(구성 요소 요약) 페이지에는 다음 필드가 표시됩니다.

Component Index(구성 요소 색인) — 구성 요소 색인을 식별하는 고유한 번호입니다.

Component BSR Address(구성 요소 BSR 주소) — 로컬 PIM 영역에 대한 BSR(Bootstrap Router)의 IP 주소입니다.

Component BSR Expiry Time(구성 요소 BSR 만료 시간) (hh:mm:ss) — 로컬 도메인에서 부트스트랩 라우터가 선연되기 이전에 남아 있는 최소 시간입니다.

Component CRP Hold Time(구성 요소 CPR 지속 시간) (hh:mm:ss) — 로컬 도메인의 후보 집합 지점인 구성 요소의 지속 시간입니다.

CLI 명령을 사용하여 PIM-SM 구성 요소 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

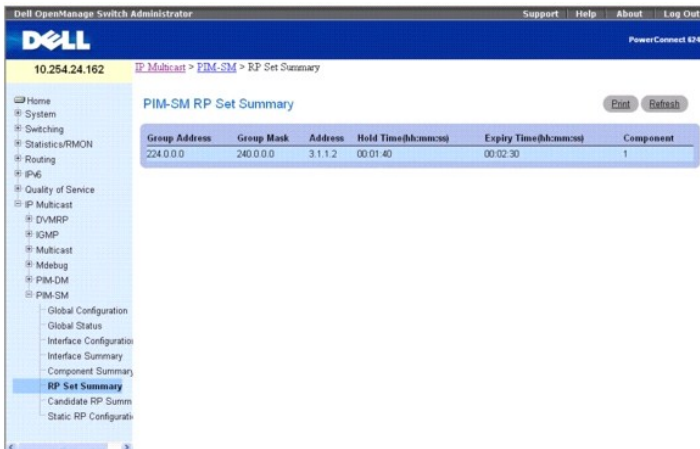
- 1 PIM-SM 명령

RP 설정 요약

PIM-SM RP Set Summary(PIM-SM RP 설정 요약) 페이지를 사용하여 PIM-SM 라우터에 대한 정적 RP 정보를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→ PIM-SM→ RP Set Summary(RP 설정 요약)**를 클릭합니다.

그림 13-31. PIM-SM RP Set Summary(PIM-SM RP 설정 요약)



PIM-SM RP Set Summary(PIM-SM RP 설정 요약) 페이지에는 다음 필드가 표에 표시됩니다.

Group Address(그룹 주소) — IP 멀티캐스트 그룹 주소를 표시합니다.

Group Mask(그룹 마스크) — 멀티캐스트 그룹 주소 마스크를 표시합니다.

Address(주소) — 후보 RP의 IP 주소를 표시합니다.

Hold Time(지속 시간) (hh:mm:ss) — 후보 RP의 지속 시간입니다. 로컬 라우터가 BSR이 아닌 경우 이 값은 0입니다.

Expiry Time(만료 시간) (hh:mm:ss) — 후보 RP가 다운된 것으로 선언되기 이전에 남아 있는 최소 시간입니다.

Component(구성 요소) — 구성 요소를 고유하게 식별하는 번호입니다. 개별 도메인에 연결된 각 프로토콜 인스턴스는 색인 값이 서로 달라야 합니다.

CLI 명령을 사용하여 RP 설정 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

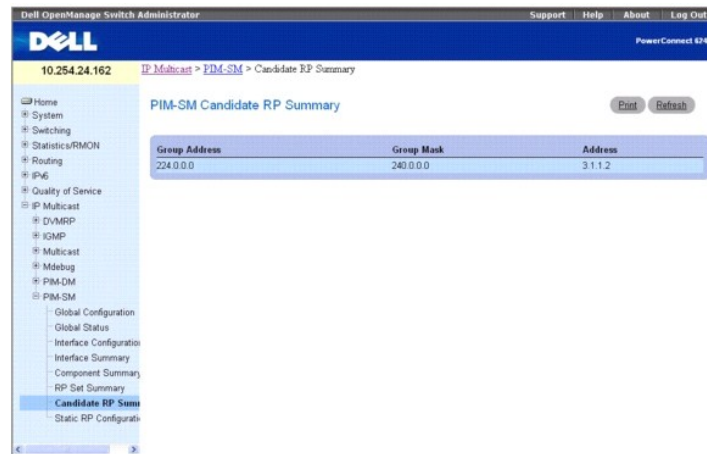
- 1 PIM-SM 명령

후보 RP 요약

PIM-SM Candidate RP Summary(PIM-SM 후보 RP 요약) 페이지를 사용하여 각 IP 멀티캐스트 그룹의 후보 집합 지정(RP)에 대한 PIM 정보를 표시합니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→PIM-SM→Candidate RP Summary(후보 RP 요약)**를 클릭합니다.

그림 13-32. PIM-SM Candidate RP Summary(PIM-SM 후보 RP 요약)



Group Address	Group Mask	Address
224.0.0.0	240.0.0.0	3.1.1.2

PIM-SM Candidate RP Summary(PIM-SM 후보 RP 요약) 페이지에는 다음 필드가 표시됩니다.

Group Address(그룹 주소) — 후보 RP 알림에서 전송되는 그룹 주소입니다.

Group Mask(그룹 마스크) — 집합 지정(RP)으로 선택된 경우 라우터가 지원하는 전체 그룹 범위를 식별하기 위해 후보 RP 알림에서 전송된 그룹 주소 마스크입니다.

Address(주소) — 후보 RP로 알려지는 인터페이스의 유니캐스트 주소를 표시합니다.

CLI 명령을 사용하여 PIM-SM 후보 RP 요약 표시

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

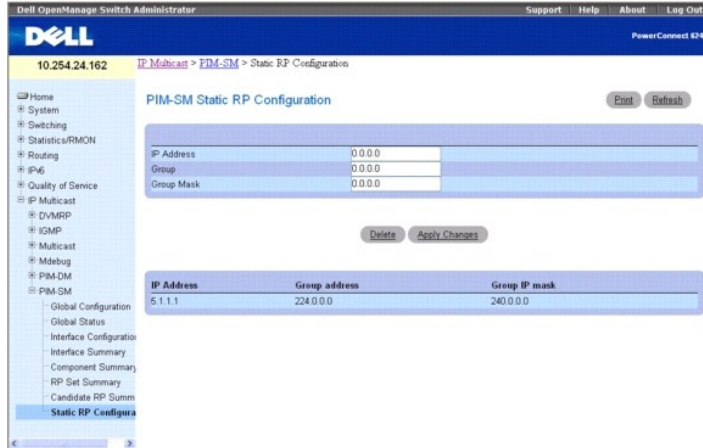
- 1 PIM-SM 명령

정적 RP 구성

Static RP Configuration(정적 RP 구성) 페이지를 사용하여 PIM-SM 라우터에 대해 지정된 정적 RP IP 주소를 만듭니다.

이 페이지를 표시하려면 디렉터리 화면에서 **Multicast(멀티캐스트)→PIM-SM→Static RP Configuration(정적 RP 구성)**를 클릭합니다.

그림 13-33. Static RP Configuration(정적 RP 구성)



Static RP Configuration(정적 RP 구성) 페이지에는 다음 필드가 포함되어 있습니다.

IP Address(IP 주소) — 만들 RP의 IP 주소입니다.

Group(그룹) — 만들 RP의 그룹 주소입니다.

Group Mask(그룹 마스크) — 만들 RP의 그룹 IP 마스크입니다.

기존 구성이 페이지 아래쪽의 표에 표시됩니다.

정적 RP 구성

1. Static RP Configuration(정적 RP 구성) 페이지를 엽니다.
2. IP Address(IP 주소), Group(그룹)에 대한 IP 주소 및 정적 RP 구성에 대한 Group Mask(그룹 마스크)를 입력합니다.
3. Apply Changes(변경사항 적용)를 클릭하십시오.

PIM-SM 라우터에 대해 지정된 정적 RP IP 주소가 생성되고 장치가 업데이트됩니다.

CLI 명령을 사용하여 정적 RP 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 *CLI 참조 안내서*의 다음 장을 참조하십시오.

- 1 PIM-SM 명령

[목록 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

Dell™ PowerConnect™ 구성


Dell™ PowerConnect™ M6220 사용 설명서

- [CLI 시작](#)
- [일반 구성 정보](#)
- [스위치 부팅](#)
- [구성 개요](#)
- [고급 구성](#)
- [소프트웨어 다운로드 및 재부팅](#)
- [부팅 메뉴 기능](#)
- [샘플 구성 프로세스](#)


이 장에서는 초기 스위치 구성에 대해 설명합니다. 이 항목에서 다루는 내용은 다음과 같습니다.

- 1 [CLI 시작](#)
- 1 [일반 구성 정보](#)
- 1 [스위치 부팅](#)
- 1 [구성 개요](#)
- 1 [고급 구성](#)
- 1 [소프트웨어 다운로드 및 재부팅](#)
- 1 [부팅 메뉴 기능](#)
- 1 [샘플 구성 프로세스](#)

모든 외부 연결을 완료한 후 터미널을 스위치에 연결하여 부팅 및 기타 절차를 모니터링합니다.

 **주:** 스위치 스택을 설치할 경우 터미널을 마스터 스위치에 연결하십시오. 스택에 처음 전원을 공급하면 스위치에서 마스터 스위치(스택에서의 위치는 상관 없음)를 선택합니다. 이 스위치는 마스터 스위치 LED를 켭니다. 터미널을 종속 스위치에 연결하면 CLI를 사용하지 못합니다.

그런 다음 [그림 5-1](#)에 설명된 설치 및 구성 절차의 순서를 따릅니다. 처음 구성하는 경우 표준 스위치 구성을 수행합니다. 기타 기능 수행은 이 단원의 뒷부분에서 설명합니다.

 **주의사항:** 진행하기 전에 이 제품의 릴리즈 노트를 확인하십시오. Dell 지원 웹 사이트(support.dell.com)에서 릴리즈 노트를 다운로드할 수 있습니다.

CLI 시작

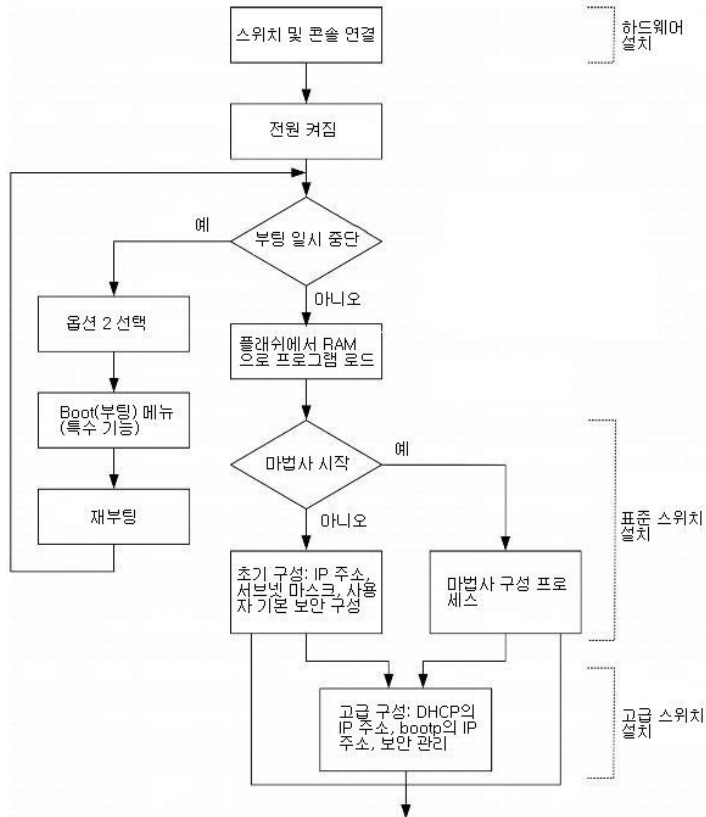
CLI 실행을 시작하려면 다음 단계를 수행하십시오.

 **주:** 다음 단계는 콘솔 라인에서만 사용합니다.

1. 스위치를 시작하고 시작 절차가 완료될 때까지 대기합니다. **Easy Setup Wizard** 시작 메시지가 표시됩니다.
2. **Easy Setup Wizard**를 사용하여 스위치를 구성하고 필요한 명령을 입력하여 필요한 작업을 완료합니다.
3. 완료되면 **quit** 또는 **exit** 명령을 사용하여 세션을 종료합니다.

스위치 콘솔 포트에 대한 직접 연결 또는 텔넷 연결을 통해 스위치 또는 스택을 관리할 수 있습니다. 스위치에 직접 연결하지 않은 경우 사용자 계정 없이 스위치에 액세스할 수 있습니다. 그러나 텔넷을 통해 스위치에 액세스하려면 하나 이상의 사용자 계정을 정의해야 합니다. 또한 텔넷 연결을 통해 액세스하는 경우에는 CLI 명령을 사용하기 전에 스위치에 IP 주소가 정의 되어 있고 해당되는 관리 액세스 권한이 부여되어 있으며 워크스테이션이 연결되어 있어야 합니다.

그림 5-1. Installation and Configuration Flow Chart(설치 및 구성 흐름 차트)



일반 구성 정보

6200 시리즈 스위치에는 스위치 운영 체제가 포함된 바이너리 파일과, 스위치와 네트워크 환경과의 관계를 정의하는 ASCII 구성 파일이 함께 제공됩니다. 구성 프로세스에서는 각 스위치가 고유 네트워크 토폴로지에 적합하도록 ASCII 구성 파일을 조정합니다.

자동 교섭

자동 교섭을 사용하여 스위치(또는 단일 장치로 작동하는 스택)는 작동 모드를 알리고 지정된 링크 세그먼트를 공유하는 다른 스위치와 정보를 공유할 수 있습니다. 이렇게 하면 두 스위치를 모두 자동으로 구성하여 기능을 최대한 활용할 수 있습니다.

자동 교섭은 MAC 또는 상위 프로토콜 계층에 대한 추가 오버헤드 없이 링크 초기화 동안 물리적 계층 내에서 완벽하게 수행됩니다. 자동 교섭을 사용하면 포트는 다음을 수행할 수 있습니다.

- 1 기능 알림
- 1 수신 승인 및 두 스위치가 공유하는 공통 작업 모드 이해
- 1 두 스위치가 공유하지 않는 작동 모드 사용 거부
- 1 두 포트가 모두 지원할 수 있는 최상위 수준의 작동 모드에 대해 각 포트 구성

주: 장애적 문제를 피하려면 링크의 양쪽에서 가능한 경우 항상 자동 교섭을 사용해야 합니다.

스위치의 포트를 자동 교섭을 지원하지 않거나 자동 교섭으로 설정되지 않은 워크스테이션 또는 서버의 네트워크 인터페이스 카드(NIC)에 연결하는 경우 여러 추가 단계가 필요합니다. 스위칭 포트와 NIC 모두 수동으로 동일한 속도 및 이중 모드로 설정해야 합니다. 이 작업은 웹 브라우저 인터페이스 또는 CLI 명령을 사용하여 수행할 수 있습니다.

주의사항: 링크 반대편의 스테이션이 전이중으로 수동 구성된 포트를 통해 자동 교섭을 시도하면 결과적으로 스테이션이 반이중 작동을 시도하게 되며 이러한 불일치로 인해 상당한 프레임 손실이 발생합니다. 이러한 현상은 자동 교섭 표준의 속성입니다.

터미널 연결 구성

스위치를 구성하려면 다음 터미널 연결 매개 변수가 필요합니다.

- 1 패리티 없음

- 1 | 정지 비트: 1
- 1 | 데이터 비트: 8
- 1 | 흐름 제어 없음


보드율

보드율을 다음 값으로 수동으로 변경할 수 있습니다.

- 1 | 2400
- 1 | 4800
- 1 | 9600(기본 보드율)
- 1 | 19200
- 1 | 38400
- 1 | 57600
- 1 | 115200

다음은 CLI 명령을 사용하여 기본 보드율을 변경하기 위한 구성의 예입니다.

```
console#configure
console(config)#line console
console(config-line)#speed 115200
```

 **주:** 워크스테이션의 터미널 에뮬레이터 소프트웨어에서 스위치 속도와 일치하도록 보드율을 설정해야 합니다.

기타 구성 요구 사항

내장된 소프트웨어를 다운로드하고 스위치를 구성하려면 다음이 필요합니다.

- 1 | 장치 뒤쪽의 직렬 포트(교차 케이블)에 연결된 ASCII 터미널(또는 에뮬레이션)
- 1 | 텔넷, SSH 등의 원격 제어를 위해 스위치에 할당된 IP 주소

스위치 부팅

로컬 터미널을 연결한 상태에서 전원을 켜면 스위치에서 POST(Power-In Self-Test)가 수행됩니다. POST는 스위치가 시작될 때마다 실행되어 부팅이 완료되기 전에 하드웨어 구성요소를 검사하여 스위치가 작동 가능한지 여부를 확인합니다.

중요한 문제가 발견되면 프로그램 흐름이 중지됩니다. POST를 통과하면 실행 가능한 유효 이미지가 RAM에 로드됩니다.

POST 메시지가 터미널에 표시되어 테스트 성공 여부를 알려줍니다.

스위치를 부팅하려면 다음 단계를 수행하십시오.

1. 직렬 케이블이 터미널에 연결되어 있는지 확인합니다.
2. 전원 공급 장치를 스위치에 연결합니다.
3. 스위치 전원을 켭니다.

스위치가 부팅되면 먼저 부팅 테스트를 통해 스위치 메모리 가용성을 계산한 다음 부팅을 계속합니다.

4. 부팅하는 동안 특별한 절차를 실행해야 하는 경우 **Boot(부팅)** 메뉴를 사용할 수 있습니다. **Boot(부팅)** 메뉴로 이동하려면 다음 메시지가 나타난 후 10초 이내에 **2**를 누릅니다.

```
Select an option. If no selection in 10 seconds then
operational code will start.
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
```

Boot(부팅) 메뉴에 대한 자세한 내용은 "[부팅 메뉴 기능](#)"을 참조하십시오. 다음 텍스트는 전체 표시된 POST의 예입니다.

```
CPU Card ID: 0x508541

volume descriptor ptr (pVolDesc): 0xffefd00
cache block I/O descriptor ptr (cbio): 0xffefde0
auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0
# of different files in use: 0
# of descriptors for deleted files: 0
# of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240

FAT handler information:
-----
- allocation group size: 2 clusters
- free space on volume: 15,335,424 bytes

Boot Menu Version: 22 Dec 2006

Select an option. If no selection in 10 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.

Select (1, 2):2

Boot Menu Version: 22 Dec 2006

Options available


1 - Start operational code
2 - Change baud rate
3 - Retrieve event log using XMODEM
4 - Load new operational code using XMODEM
```

- 5 - Display operational code vital product data
- 6 - Run flash diagnostics
- 7 - Update boot code
- 8 - Delete backup image
- 9 - Reset the system
- 10 - Restore configuration to factory defaults (delete config files)
- 11 - Activate Backup Image
- 12 - Password Recovery Procedure

[Boot Menu]

부팅 프로세스는 약 60초가 소요됩니다.

POST 후반부에 나타나는 자동 부팅 메시지(마지막 행 참조)는 부팅 중에 문제가 발생하지 않았음을 표시합니다. [Boot Menu] 프롬프트에서 작업 코드로 돌아가려면 **1**을 누릅니다.

 **주:** 다음 출력은 구성의 예입니다. 주소, 버전, 날짜 등과 같은 항목은 스위치가 다를 수 있습니다.

Operational Code Date: Fri May 4 07:44:08 2007

Uncompressing.....

50% 100%

|||||

Attaching interface lo0...done

Adding 36263 symbols for standalone.

volume descriptor ptr (pVolDesc): 0xffc0650

cache block I/O descriptor ptr (cbio): 0xffc0730

auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

of different files in use: 0

of descriptors for deleted files: 0

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector:)

- volume Id: 0x0

- total number of sectors: 60,716

- bytes per sector: 512

- # of sectors per cluster: 4

- # of reserved sectors: 1

- FAT entry size: FAT16

- # of sectors per FAT copy: 60

- # of FAT table copies: 2

- # of hidden sectors: 4

- first cluster is in sector # 136

- Update last access date for open-read-close = FALSE

- directory structure: VFAT

- root dir start sector: 121

```

- # of sectors per root: 15

- max # of entries in root: 240

FAT handler information:
-----

- allocation group size: 2 clusters

- free space on volume: 15,337,472 bytes

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533.33332

8 MHz

SOC unit 0 attached to PCI device BCM56314_A0

SOC unit 1 attached to PCI device BCM56314_A0

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

hpc - No stack ports. Starting in stand-alone mode.

(Unit 1 - Waiting to select management unit)>

<188> JAN 01 00:00:08 0.0.0.0-1 POE[254746256]: broad_poe.c(286) 4 % Unable to set POE Power bank 73

Applying configuration, please wait ...

No Potential unit to configure as Standby when unit 1 joined

<187> JAN 01 00:00:13 192.168.2.1-1 UNITMGR[244207968]: unitmgr.c(4490) 15 % No

Potential unit to configure as Standby when unit 1 joined

....

console>

```

스위치가 성공적으로 부팅된 후 프롬프트가 나타나고 로컬 터미널을 사용하여 스위치 구성을 시작할 수 있습니다. 그러나 스위치를 구성하기 전에 스위치에 설치된 소프트웨어 버전이 최신 버전인지 확인하십시오. 최신 버전이 아닌 경우 최신 버전을 다운로드하여 설치하십시오. "[소프트웨어 다운로드 및 재부팅](#)"을 참조하십시오.


구성 개요

스위치를 구성하기 전에 네트워크 관리자로부터 다음 정보를 받으십시오.

- 1 네트워크의 IP 서브넷 마스크
- 1 기본 경로를 구성하기 위한 기본 게이트웨이(다음 홉 라우터) IP 주소

다음과 같이 두 가지 유형의 구성이 있습니다.

- 1 초기 구성에는 기본 보안 고려 사항과 함께 구성 기능이 포함되어 있습니다.
- 1 고급 구성에는 동적 IP 구성 및 추가 고급 보안 고려 사항이 포함되어 있습니다.

 **주의사항:** 구성을 변경한 후 새 구성을 저장한 다음 재부팅해야 합니다. 구성을 저장하려면 다음과 같이 입력합니다.

```
console#copy running-config startup-config
```

Easy Setup Wizard

Easy Setup Wizard는 구성 없이 또는 출하 시 기본 구성만으로 시스템이 부팅되는 경우 표시됩니다. **Easy Setup Wizard**는 몇 가지 초기 단계를 통해 기본 시스템 구성 및 보안을 설정하고 스위치를 관리할 수 있도록 설계되었습니다. **Easy Setup Wizard**를 사용하려면 스위치 전원을 켜고 새 관리자 계정을 설정해야 합니다. 마법사에 의해 설정된 이 관리자 계정은 최상위 권한 수준(수준15)을 가집니다.

Easy Setup Wizard는 웹, CLI 및 원격 Dell 네트워크 관리자를 통해 즉시 배포 및 작동되고 완벽하게 관리할 수 있도록 새로 설치된 스위치의 기본적인 초기 구성을 진행합니다. 초기 설정 후 시스템으로 이동하여 추가 고급 구성을 설정할 수 있습니다.

기본적으로 스위치는 출하 시 IP 주소 192.168.2.1 및 넷마스크 255.255.255.0 상태로 제공됩니다. 시스템은 기본 관리 LAN ID=1 상태로 설정됩니다. IP 주소 없이는 다른 관리 인터페이스에 액세스할 수 없기 때문에 직렬 인터페이스를 통해 초기 부팅을 수행해야 합니다.

이 마법사를 이용하여 스위치에 대해 다음 구성을 설정할 수 있습니다.

- 1 초기 권한 사용자 계정을 유효한 암호와 함께 설정합니다. 마법사는 설정 과정 동안 하나의 권한 사용자 계정을 구성합니다. 초기 계정에 최상위 권한 수준(수준 15)이 제공됩니다.
- 1 로컬 인증 설정만을 사용하기 위한 CLI 로그인 및 HTTP/HTTPS 액세스를 활성화합니다. 나중에 Radius 또는 TACACS+를 구성할 수 있습니다.
- 1 관리 VLAN용 IP 주소를 설정합니다.
- 1 해당 IP 주소에서 SNMP 관리자가 사용할 SNMP 커뮤니티 문자열을 설정합니다. 스위치에 SNMP 관리를 사용하지 않을 경우에는 이 단계를 건너뛸 수 있습니다. 이 항목이 구성될 경우 기본 액세스 레벨이 SNMP 관리 인터페이스에 사용할 수 있는 가장 높은 액세스로 설정됩니다. 초기에는 SNMPv1/2c만 활성화됩니다. SNMPv3은 SNMPv3용 보안 액세스 구성으로 돌아갈 때까지 비활성화됩니다(예: 엔진 ID, view 등). SNMP 커뮤니티 문자열에 공백이 포함될 수 있습니다. 마법사에서 커뮤니티 문자열에 공백을 입력하려면 따옴표를 사용해야 합니다. 커뮤니티 문자열에 공백이 허용되지만 가능한 사용하지 않는 것이 좋습니다. 기본 커뮤니티 문자열에는 공백이 없습니다.
- 1 관리 서버 IP를 지정하거나 모든 IP 주소에서 SNMP 액세스를 허용하도록 지정할 수 있습니다.
- 1 기본 게이트웨이 IP 주소를 설정합니다.

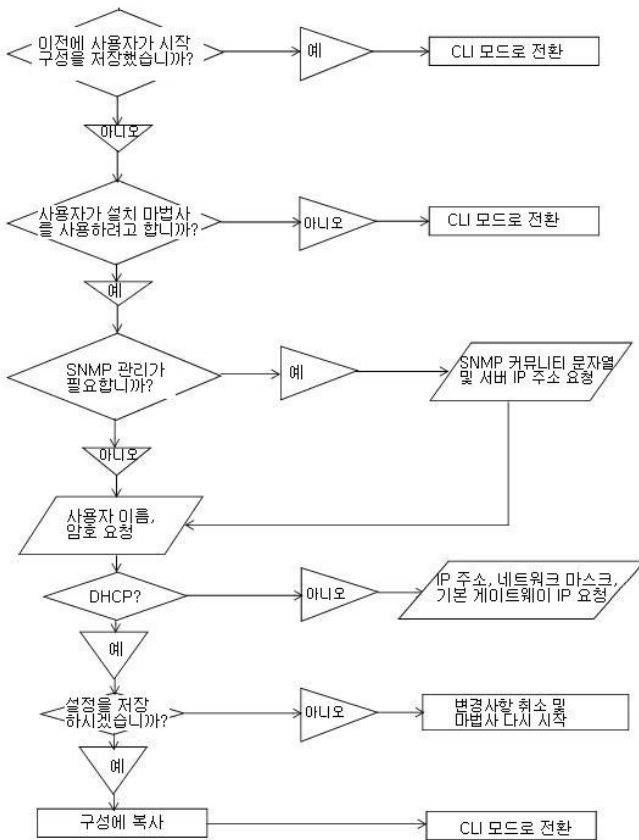
초기에 마법사를 사용하지 않는 경우 세션은 CLI 모드로 기본값으로 설정합니다. 설치 마법사는 구성을 저장할 때까지 로그인할 때마다 계속해서 표시됩니다. 저장한 후에는 스위치를 출하 시 기본 설정으로 재설정하는 경우에만 마법사 옵션이 다시 표시됩니다.

현장에서는 직렬 연결 없이 스위치 전원을 켜므로 스위치가 아직 구성되지 않은 경우 스위치는 설치 프롬프트에 응답할 때까지 60초 동안 대기합니다. 응답이 없는 경우 스위치는 출하 시 기본 구성을 사용하여 계속해서 정상적으로 작동합니다. 다음에 시스템을 재부팅할 때 설치 마법사를 실행할 수 있습니다.

기능 흐름

다음 기능 흐름도에서는 Easy Setup Wizard 절차에 대해 설명합니다.

그림 5-2. Setup Wizard Flow Chart(설치 마법사 흐름 차트)



Easy Setup Wizard 세션 예


아래에서는 Easy Setup Wizard 세션을 설명합니다. 일반적인 흐름의 경우 이전 절의 상태 다이어그램을 참조하십시오. 다음 세션에 사용된 값은 하나의 예입니다. 네트워크 관리자에게 실제 값을 요청하십시오.

- 1 관리 VLAN용 IP 주소: 192.168.1.1:255.255.255.0
- 1 사용자 이름은 *admin*, 암호는 *admin123*입니다.

- 1 네트워크 관리 시스템 IP 주소: 192.168.1.10
- 1 기본 게이트웨이: 192.168.1.100.
- 1 사용할 SNMP 커뮤니티 문자열: *Dell_Network_Manager*.

설치 마법사에서 초기 값을 위와 같이 구성합니다. 마법사를 완료하면 시스템은 다음과 같이 구성됩니다.

- 1 SNMPv1/2c가 활성화되고 커뮤니티 문자열은 상기에서 정의된 대로 설정됩니다. SNMPv3이 비활성화됩니다.
- 1 admin 사용자 계정은 정의된 대로 설정됩니다.
- 1 네트워크 관리 시스템이 구성됩니다. 이 관리 시스템에서 SNMP, HTTP 및 CLI 인터페이스를 액세스할 수 있습니다. 또한 (0.0.0.0) IP 주소를 선택하여 모든 IP 주소에서 이 관리 인터페이스들을 액세스할 수 있도록 선택할 수도 있습니다.
- 1 기본 관리 VLAN (1)에 대해 IP 주소가 구성됩니다.
- 1 기본 게이트웨이 주소가 구성됩니다.

 **주:** 아래 예에서 선택 가능한 사용자 옵션은 []로 표시됩니다. 또한 가능한 경우 기본 값은 { }로 제공됩니다. 아무런 옵션을 정의하지 않고 <Return>을 입력하면 기본 값이 사용됩니다. 도움말 텍스트는 괄호 안에 표시됩니다.

다음 예에는 위에 나열된 입력 값을 사용하여, Dell **Easy Setup Wizard** 예제 세션을 실행하는 것과 관련된 일련의 프롬프트와 응답이 포함되어 있습니다.

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. 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. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the set up wizard (you must answer this question within 60 seconds)? [Y/N] **y**

1단계:

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

- o Set up the initial SNMP version 2 account now.
- o Return later and set up other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

Would you like to set up the SNMP management interface now? [Y/N] **y**

To set up 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 other management interfaces to change this setting and to add additional management system later. 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 {public}:

>> *Dell_Network_Manager*<Return>

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}:

>> *192.168.1.10*<Return>

2단계:


Now we need to set up your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To set up a user account:

Please enter the user name {admin}: *admin*<Return>

Please enter the user password: *******<Return>

Please reenter the user password: *******<Return>

 **주:** 첫 번째 및 두 번째 암호 항목이 동일하지 않을 경우 동일해질 때까지 프롬프트가 표시됩니다.

3단계:

Next, an IP address is set up. 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. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this require that you have a DHCP server running on the network).

To set up an IP address:


Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network

DHCP server (192.168.2.1):

>> 192.168.2.1<Return>


Please enter the IP subnet mask (A.B.C.D or /nn){255.255.255.0}:

>> 255.255.255.0<Return>

 주: 위의 DHCP를 선택한 경우 이 정보는 DHCP 서버에서 제공되므로 시스템에서 IP 서브넷 마스크를 요청하지 않습니다.

4단계:

Finally, set up the default gateway. Please enter the IP address of the gateway from which this network is reachable (for example 0.0.0.0): >> 192.168.2.100<Return>

 주: 위의 DHCP를 선택한 경우 이 정보는 DHCP 서버에서 제공되므로 시스템에서 IP 기본 게이트웨이를 요청하지 않습니다.

This is the configuration information that has been collected:

SNMP Interface = "Dell_Network_Manager"@192.168.1.10

User Account set up = admin

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 192.168.2.100

5단계:

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**

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode.

고급 구성

CLI 기본 사항

사용자 EXEC 모드 및 권한이 있는 EXEC 모드에서 help 명령을 통해 키보드 단축 키를 표시합니다. 다음은 help 명령의 표시 예입니다.

```
Console>help
HELP:
Special keys:
DEL, BS .... delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-T .... transpose previous character
Ctrl-P .... go to previous line in history buffer
Ctrl-R .... rewrites or pastes the line
Ctrl-N .... go to next line in history buffer
Ctrl-Y .... print last deleted character
```



```
Ctrl-Z .... return to root command prompt

Ctrl-Q .... enables serial flow

Ctrl-S .... disables serial flow

Tab, <SPACE> command-line completion

Exit .... go to next lower command prompt

? .... list choices
```

상황에 맞는 도움말

? 명령을 사용하여 CLI에서 상황에 맞는 도움말을 확인합니다. 가능한 하위 명령 목록을 가져오거나 일부만 입력된 명령으로 시작하는 명령을 나열하는 데 사용할 수 있습니다. 빈 행에 ? 명령을 지정하면 명령 트리의 지정된 레벨에 가능한 명령 목록이 제공됩니다. 또한 명령 입력 내에서 ?를 사용하여 명령을 완료하는 데 필요한 매개 변수 목록을 반환할 수 있습니다. 사용자에 의해 이미 제공된 매개 변수는 명령 목록에서 제외시켜 누락된 매개 변수만 나열되도록 합니다.

인터페이스 명령 규정

업계 표준 CLI 구현에는 CLI의 인터페이스를 명명하는 승인된 규정이 있습니다. Dell 장치의 인터페이스 명령 규정은 다음과 같습니다.

- 1 **장치 번호/인터페이스 ID** — 각 인터페이스는 **장치 번호** 및 /**기호**가 오고 그 다음에 **인터페이스 ID**로 표시됩니다(아래 참조). 예를 들어 **2/g10**는 스택의 두 번째 장치 내에서 기가비트 포트 10을 표시합니다.
- 1 **장치 번호** — 장치 번호는 여러 스위치를 중첩하여 가상 장치로 구성하는 스택형 솔루션에서만 사용됩니다. 이 경우 **장치 번호**는 스택 내의 물리적 장치 식별자입니다.
- 1 **인터페이스 ID** — 인터페이스 유형과 인터페이스 번호로 구성됩니다. 현재 사전 정의된 **인터페이스 유형** 목록(아래 참조)이 있습니다. 추가 인터페이스 유형을 정의하려면 Dell에 등록해야 합니다. 예를 들어 **2/g10**은 두 번째 장치의 기가비트 포트 10을 표시합니다.
- 1 **인터페이스 유형** — 다음 인터페이스 유형이 6200 시리즈 스위치에 정의되어 있습니다.
 - o **g** — 기가비트 이더넷 포트(예: 1/g2는 기가비트 이더넷 포트 2).
 - o **xg** — 10 기가비트 이더넷 포트(예: 1/xg2는 10 기가비트 이더넷 포트 2).

PowerConnect 6200 시스템 CLI 참조 안내서

6200 시리즈 스위치에 사용 가능한 모든 CLI 명령에 대한 자세한 내용은 **CLI 참조 안내서**를 참조하십시오.

이 절에서는 다음과 같은 공통 작업에 대한 요약 정보를 제공합니다.

- 1 [스위칭 포트 기본 설정 수정](#)
- 1 [DHCP 서버에서 IP 주소 검색](#)
- 1 [초기 콘솔 암호 구성](#)
- 1 [초기 텔넷 암호 구성](#)
- 1 [초기 HTTP 암호 구성](#)
- 1 [초기 HTTPS 암호 구성](#)

스위칭 포트 기본 설정 수정

DHCP 및 BOOTP를 통해 IP 주소를 구성/수신하는 경우 이러한 서버에서 수신한 구성에는 IP 주소가 포함되고 서브넷 마스크 및 기본 게이트웨이가 포함될 수 있습니다.

처음으로 로그인하는 경우 CLI는 명령 계층 구조의 루트로 이동합니다. 다른 레벨의 명령 계층 구조로 이동하려면 **configure**과 같은 명령을 입력하여 CLI가 **config** 하위 트리로 이동하도록 합니다. 명령 계층 구조의 이전 레벨로 이동하려면 **exit** 명령을 사용합니다.

```
SwitchA#configure
SwitchA(config)#exit
SwitchA#
```

다음 예에서는 6200 시리즈 스위치에 사용되는 시스템 프롬프트에 대해 설명합니다.

- 1 **SwitchA>** — 장치 이름이 **SwitchA**임을 표시하고 CLI는 현재 명령 계층 구조의 최상위 레벨에 있습니다. 또한 CLI는 **사용자 EXEC 모드**에 있습니다.
- 1 **SwitchA#** — 이 프롬프트는 CLI가 권한이 있는 EXEC 모드에 있음(사용자 EXEC 모드가 아님)을 표시하는 #을 제외하고 위의 프롬프트와 유사합니다.
- 1 **SwitchA(config)#** — CLI가 현재 명령 계층 구조의 **현재 구성 모드**에 있음을 나타냅니다. 최상위 레벨에서 **configure**를 입력하여 이 모드로 들어갑니다.
- 1 **SwitchA(config-if)#** — 이 프롬프트는 CLI가 현재 **interface** 구성 모드에 있음을 나타냅니다. 구성 모드에서 **interface range ethernet**, **interface range port-channel** 또는 **interface range vlan**을 입력하여 시작합니다. 이 경우 시스템이 일반 인터페이스 집합에서 작동하기 때문에 특정 인터페이스를 참조하지 않습니다.
- 1 **SwitchA(config-if-1/g1)#** — CLI가 현재 기가비트 이더넷 인터페이스 1에서 작동 중임을 나타냅니다.

스위칭 포트 기본 설정

다음 표에서는 스위치 포트 기본 설정에 대해 설명합니다.

표 5-1. Port Default Settings(포트 기본 설정)

기능	기본 설정
포트 속도 및 모드	1000M 자동 교섭
포트 전송 상태	Enabled
회선 차단 방지 헤드	켜짐(사용)
흐름 제어	꺼짐
배알	꺼짐

다음은 CLI 명령을 사용하여 포트 1/g1에서 포트 속도를 변경하는 예입니다.


```
console(config)#interface ethernet 1/g1  
  
console(config-if-1/g1)#speed 100
```

DHCP 서버에서 IP 주소 검색

DHCP 프로토콜을 사용하여 IP 주소를 검색하는 경우 스위치가 DHCP 클라이언트 역할을 수행합니다.

DHCP 서버에서 IP 주소를 검색하려면 다음 단계를 수행하십시오.

포트를 선택하여 DHCP 서버 또는 DHCP 서버가 있는 서브네트에 연결하여 IP 주소를 검색합니다.

 **주:** DHCP 서버의 IP 주소를 검색하기 위해 스위치 구성을 삭제할 필요가 없습니다.

1. IP 주소 검색을 위해 선택한 포트를 사용하려면 다음 명령을 입력합니다.

1 동적 IP 주소 지정:

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

인터페이스가 자동으로 IP 주소를 검색합니다.

2. IP 주소를 확인하려면 다음 예에 표시된 것처럼 시스템 프롬프트에 **show ip interface** 명령을 입력합니다.

```
console#show ip interface  
  
Management Interface:  
  
IP Address..... 10.240.4.125  
  
Subnet Mask..... 255.255.255.0  
  
Default Gateway..... 10.240.4.1  
  
Burned In MAC Address..... 00:10:18:82:04:35  
  
Network Configuration Protocol Current..... DHCP  
  
Management VLAN ID..... 1  
  
Routing Interfaces:  
  
Netdir Multi  
Interface IP Address IP Mask Bcast CastFwd  
  
-----  
  
vlan1      192.168.10.10 255.255.255.0 Disable Disable  
  
vlan2      0.0.0.0 0.0.0.0 Enable Disable  
  
loopback2 0.0.0.0 0.0.0.0 Disable Disable
```

보안 관리 및 암호 구성


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

시스템은 기본 암호 구성 없이 전달되며 모든 암호는 사용자가 정의합니다. 사용자 정의 암호를 보실할 경우 **Boot(부팅) 메뉴**에서 암호 복구 절차를 호출할 수 있습니다. 이 절차는 로컬 터미널에만 해당하며 암호 입력 없이 로컬 터미널에서 한 번에 스위치에 액세스할 수 있습니다.

보안 암호 구성

다음 서비스에 대해 보안 암호를 구성할 수 있습니다.

- 1 콘솔
- 1 Telnet(텔넷)
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **주:** 사용자 이름을 만든 경우 기본 우선 순위는 "1"이며 액세스할 수 있지만 구성 권한은 없습니다. 스위치에 대한 액세스 및 구성 권한을 사용하려면 우선 순위를 "15"로 설정해야 합니다.

초기 콘솔 암호 구성

초기 콘솔 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 secret123
```

- 1 콘솔 세션을 통해 처음으로 로그인하는 경우 암호 프롬프트에 **secret123**을 입력합니다.
- 1 스위치 모드를 사용하도록 설정하는 경우 암호 프롬프트에 **secret123**을 입력합니다.

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 pass1234
```

- 1 텔넷 세션을 통해 처음으로 로그인하는 경우 암호 프롬프트에 **pass1234**을 입력합니다.
- 1 스위치 모드를 사용하도록 설정하는 경우 **pass1234**를 입력합니다.

초기 HTTP 암호 구성


초기 HTTP 암호를 구성하려면 다음 명령을 입력하십시오.

```
console(config)#ip http authentication local
console(config)#username admin password user1234 level 15
```

초기 HTTPS 암호 구성

초기 HTTPS 암호를 구성하려면 다음 명령을 입력하십시오.

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


 **주:** 스위치에서 제어 소프트웨어 응용프로그램을 업그레이드(새 버전 설치)할 때마다 새 암호화 인증서를 만들어야 합니다.

콘솔, 텔넷 또는 SSH 세션을 통해 HTTPS 세션을 사용하도록 구성하는 경우 다음 명령을 입력하십시오.

 **주:** 웹 브라우저에 페이지 내용이 나타나도록 하려면 SSL 2.0 이상을 사용해야 합니다.

```
console(config)#crypto certificate 1 generate
```


```
console(config)#ip https server
```

 **주:** Http 및 Https 서비스의 경우 레벨 15 액세스가 필요하며 구성 레벨 액세스에 직접 연결합니다.

소프트웨어 다운로드 및 재부팅

XModem을 통한 소프트웨어 다운로드

이 절에서는 백업 구성 파일 업데이트를 위한 데이터 전송 프로토콜인 XModem을 사용하여 스위치 소프트웨어(시스템 및 부팅 이미지)를 다운로드하는 방법에 대해 설명합니다.

 **주:** xmodem 다운로드 는 외부에서 작동되지 않기 때문에 다운로드하는 경우 직렬 콘솔 인터페이스에 연결해야 합니다.

XModem을 사용하여 소프트웨어 이미지 파일을 다운로드하려면 다음을 수행하십시오.

전송 프로세스를 시작할 소스 파일 경로를 지정합니다.

다음 보기와 같은 정보가 화면에 표시될 수 있습니다.

```
console#copy xmodem image
```

```
Mode..... XMODEM
```

```
Data Type..... Code
```

```
Destination Filename..... image2
```

```
Management access will be blocked for the duration of the transfer
```


```
Are you sure you want to start? (y/n) y
```

```
console#boot system image2
```

TFTP 서버를 통한 소프트웨어 다운로드

이 절에서는 TFTP 서버를 통한 스위치 소프트웨어(시스템 및 부팅 이미지)의 다운로드 방법에 대해 설명합니다. 소프트웨어를 다운로드하기 전에 TFTP 서버를 네트워크에서 사용할 수 있어야 합니다.

스위치는 시스템 이미지의 복사본이 저장되는 플래시 메모리 영역에서 시스템 이미지의 압축을 풀 때 부팅되어 실행됩니다.

 **주의사항:** boot system 명령을 실행하여 새로 다운로드한 이미지를 활성화해야 합니다.

별도의 설정을 선택한 경우가 아니라면 다음 부팅 시 스위치에서 현재 활성 시스템 이미지의 압축을 풀어서 실행합니다.

TFTP 서버를 통해 이미지를 다운로드하려면 다음을 수행하십시오.

1. IP 주소가 스위치 포트 중 하나에서 구성되고 ping이 TFTP 서버로 전송될 수 있는지 확인합니다.
2. 다운로드할 파일이 TFTP 서버(.stk 파일)에 저장되어 있는지 확인합니다.
3. show version 명령을 입력하여 스위치에서 현재 실행 중인 소프트웨어 버전을 확인합니다.

다음 보기와 같은 정보가 화면에 표시될 수 있습니다.

```

console>show version

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash

-----unit image1 image2 current-active next-active
-----

1 0.15.0.0 0.15.0.0 image1 image1

```

4. **show bootvar** 명령을 입력하여 어느 시스템 이미지가 현재 활성화되어 있는지 확인합니다. 다음 보기와 같은 정보가 화면에 표시될 수 있습니다.

```

console>show bootvar

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash

-----unit image1 image2 current-active next-active
-----

1 0.15.0.0 0.15.0.0 image1 image1

```

5. **copy tftp://{ tftp address }/{ file name} image2** 명령을 입력하여 새 시스템 이미지를 스위치에 복사합니다.

새 이미지가 다운로드되면 시스템 이미지의 다른 복사본(예의 경우 image2)용으로 할당된 영역에 저장됩니다. 다음 보기와 같은 정보가 화면에 표시될 수 있습니다.

```

console#copy tftp://10.254.24.64/pc62xxr0v34.stk image2

Mode..... TFTP

Set TFTP Server IP..... 10.254.24.64

TFTP Path..... ./

TFTP Filename..... pc62xxr0v34.stk

Data Type..... Code

Destination Filename..... image2

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) y

```

느낌표 기호는 복사 프로세스가 진행 중임을 나타냅니다. 마침표는 복사 프로세스의 제한 시간이 만료되었음을 나타냅니다. 한 행에 마침표가 여러 개 있으면 복사 프로세스가 실패했음을 의미합니다.

6. **boot system** 명령을 입력하여 다음 부팅을 위한 이미지를 선택합니다. 이 명령 후에 **show bootvar** 명령을 입력하여 **boot system** 명령의 매개변수가 다음 부팅에 선택되어 있는 것처럼 복사가 지정되어 있는지 확인합니다.

다음 보기와 같은 정보가 화면에 표시될 수 있습니다.

```

console#boot system image2

Activating image image2 ..

console>show bootvar

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash

-----unit image1 image2 current-active next-active
-----

```

1 0.15.0.0 0.15.0.0 image1 image2

boot system 명령을 입력하여 다음 부팅을 위한 이미지를 선택하지 않은 경우 현재 활성 이미지(예의 경우 image1)에서 시스템이 부팅됩니다.

7. **reload** 명령을 입력합니다. 다음과 같은 메시지가 표시됩니다.

```
console#reload  
  
Management switch has unsaved changes.  
  
Are you sure you want to continue? (y/n)
```

8. Enter **y**. 다음과 같은 메시지가 표시됩니다.

```
Configuration Not Saved!  
  
Are you sure you want to reload the stack? (y/n)
```

9. 스위치를 다시 부팅하려면 **y**를 입력합니다.

부팅 코드 업데이트

update bootcode 명령을 사용하여 모든 스위치의 부팅 코드를 업데이트합니다. 각 스위치에 대해 부팅 코드는 활성 이미지에서 추출되어 플래시를 수행하도록 프로그래밍됩니다. 특정 스위치의 부팅 코드를 업데이트하려면 명령에 장치를 지정합니다(다음 예 참조).

스위치에 있는 부팅 코드를 표시하려면 스위치를 재부팅합니다. 부팅하는 동안 초기 날짜가 표시됩니다.

1. 다음 명령을 입력합니다. 여기서 2는 장치 번호입니다.

```
console# update bootcode 2  
  
Updating boot code ...  
  
Boot code update completed successfully.
```

2. **reload** 명령을 입력합니다.

```
console#reload  
  
Are you sure you want to reload the stack? (y/n)
```

3. 스위치를 다시 부팅하려면 **y**를 입력합니다.

부팅 메뉴 기능

POST의 첫 번째 부분이 완료된 후 호출할 수 있는 **Boot(부팅)** 메뉴를 통해 많은 구성 작업을 수행할 수 있습니다.

Boot(부팅) 메뉴를 표시하려면 다음을 수행하십시오.

1. 부팅하는 동안 다음 메시지가 표시된 후 10초 이내에 **2**를 누릅니다.

```
Boot Menu Version: Oct 20 2004  
  
Select an option. If no selection in 10 seconds then  
operational code will start.  
  
1 - Start operational code.  
2 - Start Boot Menu.  
  
Select (1, 2):
```

Boot(부팅) 메뉴가 표시되고 다음 구성 기능이 제공됩니다.

```
1 - Start operational code  
2 - Change baud rate
```

- 3 - Retrieve event log using XMODEM
- 4 - Load new operational code using XMODEM
- 5 - Display operational code vital product data
- 6 - Run flash diagnostics
- 7 - Update boot code
- 8 - Delete backup image
- 9 - Reset the system
- 10 - Restore configuration to factory defaults (delete config files)
- 11 - Activate Backup Image
- 12 - Password Recovery Procedure

다음 절에서는 **Boot(부팅)** 메뉴 옵션에 대해 설명합니다.

Start Operational Code(작업 코드 시작)

옵션 1을 사용하여 작업 코드 로딩을 시작합니다.

Boot(부팅) 메뉴에서 부팅 프로세스를 다시 시작하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **1**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
Operational Code Date: Thu Jun 8 12:51:44 2006

Uncompressing....

50% 100%

|||||
1 File: bootos.c Line: 462 Task: fffff000 EC: 2863311530 (0xaaaaaaaa)

(0 d 0 hrs 0 min 13 sec)

Timebase: 24.750275 MHz, MEM: 99.001100 MHz, PCI: 33.000366 MHz, CPU: 198.002200 MHz

PCI device BCM5675_A0 attached as unit 0.
PCI device BCM5695_B0 attached as unit 1.
PCI device BCM5695_B0 attached as unit 2.
PCI device BCM5673_A1 attached as unit 3.
PCI device BCM5673_A1 attached as unit 4.

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

st_state(0) = 0x0

st_state(1) = 0x3

st_state(2) = 0x2
```

Change baud rate(보드율 변경)


옵션 2를 사용하여 직렬 인터페이스의 보드율을 변경합니다.

Boot(부팅) 메뉴에서 보드율을 변경하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **2**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu]2
Select baud rate:
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
7 - 57600
8 - 115200
0 - no change
```

 주: 선택한 보드율이 즉시 적용됩니다.

- 부팅 프로세스가 재개됩니다.

Retrieve Event Log using XMODEM(XMODEM을 사용하여 이벤트 로그 검색)

옵션 3을 사용하여 이벤트 로그를 검색하고 ASCII 터미널에 다운로드합니다.

Boot(부팅) 메뉴에서 이벤트 로그를 검색하려면 다음을 수행하십시오.

- Boot(부팅) 메뉴**에서 **3**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu] 3
Sending event log, start XMODEM receive....
File asciilog.bin Ready to SEND in binary mode
Estimated File Size 169K, 1345 Sectors, 172032 Bytes
Estimated transmission time 3 minutes 20 seconds
Send several Control-X characters to cancel before transfer starts.
```

- 부팅 프로세스가 재개됩니다.

Load New Operational Code Using XMODEM(XMODEM을 사용하여 새 작업 코드 로드)

새 소프트웨어 버전을 다운로드해야 하는 경우 옵션 4를 사용하여 손상된 파일을 바꾸고 시스템 소프트웨어를 업데이트 또는 업그레이드합니다.

Boot(부팅) 메뉴에서 소프트웨어를 다운로드하려면 다음을 수행하십시오.

- Boot(부팅) 메뉴**에서 **4**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC...
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cancel before transfer starts.
```

- 하이퍼터미널을 사용하는 경우 **HyperTerminal(하이퍼터미널)** 메뉴 모음에서 **Transfer(전송)**를 클릭합니다.

3. **Transfer(전송)** 메뉴에서 **Send File(파일 전송)**을 클릭합니다.

Send File(파일 전송) 창이 나타납니다.

4. 다운로드할 파일의 파일 경로를 입력합니다.

5. 프로토콜이 Xmodem으로 정의되어 있는지 확인합니다.

6. **Send**를 클릭합니다.

소프트웨어가 다운로드됩니다. 소프트웨어를 다운로드하는 데 몇 분이 걸립니다. 하이퍼터미널과 같은 터미널 에뮬레이션 응용프로그램에 로딩 프로세스 진행률이 표시됩니다.

Display Operational Code Vital Product Data(작업 코드 필수 제품 데이터 표시)

옵션 5를 사용하여 부팅 이미지 정보를 표시합니다.

Boot(부팅) 메뉴에서 부팅 이미지 정보를 표시하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **5**를 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu]5
The following image is in the Flash File System:
File Name.....image1
CRC.....0xb017 (45079)
Target Device.....0x00508541
Size.....0x8ec50c (9356556)
Number of Components.....2
Operational Code Size.....0x7ec048 (8306760)
Operational Code Offset.....0x74 (116)
Operational Code FLASH flag.....1
Operational Code CRC.....0x9B4D
Boot Code Version.....1
Boot Code Size.....0x100000 (1048576)
Boot Code Offset.....0x7ec0bc (8306876)
Boot Code FLASH flag.....0
Boot Code CRC.....0x1CB8
VPD - rel 0 ver 31 maint_lvl 0
Timestamp - Thu Jun 8 12:51:44 2006
File - pc62xxr0v31.stk
```

2. 부팅 프로세스가 재개됩니다.

Run Flash Diagnostics(플래쉬 진단 실행)

옵션 6을 사용하여 플래쉬 진단을 실행합니다. 명령을 실행하기 전에 Y/N 질문을 통해 사용자 작업을 확인합니다.

Boot(부팅) 메뉴에서 플래쉬 메모리의 전체 테스트를 수행하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **6**를 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu]6

Do you wish to run flash diagnostics? (Boot code region will not be tested.) (y/n): y

Input number of diagnostic iterations -> 1

Testing 2 x 28F128J3 base: 0xfe000000

Iterations remaining = 1

Erasing sector 0

Verify sector 0 erased

Writing sector 0

Erasing sector 1

Verify sector 1 erased

Writing sector 1

Erasing sector 2

Verify sector 2 erased

Writing sector 2

Erasing sector 3

Verify sector 3 erased

Writing sector 3

Erasing sector 4

Verify sector 4 erased

Writing sector 4

Erasing sector 5


Verify sector 5 erased

Writing sector 5

Erasing sector 6

Verify sector 6 erased

Writing sector 6
```

 주: 이 프로세스는 모든 섹터를 지우고 지웠는지 확인한 다음 기록할 때까지 실행됩니다.

```
Flash Diagnostics passed
```

```
[Boot Menu]
```

2. 부팅 프로세스가 재개됩니다.

Update Boot Code(부팅 코드 업데이트)

옵션 7을 사용하여 플래시 메모리의 부팅 코드를 업데이트합니다. 이 옵션은 부팅 메뉴 옵션 4를 사용하여 새 부팅 코드를 로드한 후에만 유효합니다. 사용자는 명령을 실행하기 전에 Y/N 질문에 대답합니다.

Boot(부팅) 메뉴에서 소프트웨어를 다운로드하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 7을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
Do you wish to update Boot Code? (y/n) y
```

```
Erasing Boot Flash.....Done.
```

```
Wrote 0x10000 bytes.
```

```
Wrote 0x20000 bytes.  
  
Wrote 0x30000 bytes.  
  
Wrote 0x40000 bytes.  
  
Wrote 0x50000 bytes.  
  
Wrote 0x60000 bytes.  
  
Boot code updated
```

2. 부팅 프로세스가 재개됩니다.

Delete Backup Image(백업 이미지 삭제)

옵션 8을 사용하여 플래쉬 메모리에서 백업 이미지를 삭제합니다. 명령을 실행하기 전에 Y/N 질문을 통해 사용자 작업을 확인합니다.

Boot(부팅) 메뉴에서 백업 이미지를 삭제하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **8**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
Are you SURE you want to delete backup image : image2 ? (y/n):y  
  
Backup image deleted...  
  
[Boot Menu]
```

2. 부팅 프로세스가 재개됩니다.

Reset the System(시스템 재설정)

옵션 9를 사용하여 모든 플래쉬를 지우고 시스템을 기본 설정으로 재설정합니다. 명령을 실행하기 전에 Y/N 질문을 통해 사용자 작업을 확인합니다.

Boot(부팅) 메뉴에서 시스템을 재설정하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **9**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
[Boot Menu] 9  
  
Are you SURE you want to reset the system? (y/n):y
```

2. The bootup process starts over.

Restore Configuration to Factory Defaults (Delete Configuration Files)(출하 시 기본값으로 구성 복원(Configuration 파일 삭제))

옵션 10을 사용하여 시스템 기본 구성을 통해 로드하고 현재 시작 구성 사용 없이 부팅합니다. Boot(부팅) 메뉴에서 10을 선택하면 시스템 기본값으로 복원됩니다. 그런 다음 Boot(부팅) 메뉴에서 1을 선택하여 부팅 시퀀스를 시작할 수 있습니다.

Boot(부팅) 메뉴에서 소프트웨어를 다운로드하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **10**을 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 나타납니다.

```
Are you SURE you want to delete the configuration? (y/n):y
```

2. 부팅 프로세스가 재개됩니다.

Activate Backup Image(백업 이미지 활성화)

옵션 11을 사용하여 백업 이미지를 활성화합니다. 이 옵션을 선택하면 활성화 이미지가 백업됩니다.

백업 이미지를 활성화하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **11**를 선택하고 <Enter> 키를 누릅니다.

다음과 같은 메시지가 표시됩니다.

```
Backup image - image2 activated(백업 이미지 - image2가 활성화됨)
```

2. 부팅 프로세스가 재개됩니다.

Password Recovery Procedure(암호 복구 절차)

암호를 분실한 경우 옵션 12를 사용합니다. 이를 통해 스위치가 콘솔 암호를 묻는 메시지 표시 없이 한 번 부팅할 수 있습니다. *enable* 암호는 이 모드에서 표시되지 않습니다.

로컬 터미널에서만 분실된 암호를 복구하려면 다음을 수행하십시오.

1. **Boot(부팅) 메뉴**에서 **12**를 선택하고 <Enter> 키를 누릅니다.

암호가 삭제됩니다.

2. 부팅 프로세스가 재개됩니다.

3. 스위치 보안을 강화하려면 해당 관리 방법에 대한 암호를 다시 구성합니다.

샘플 구성 프로세스

이 절에서는 스위치를 통한 원격 네트워크 관리 연결을 설정하는 데 필요한 기본 단계에 대해 설명합니다. 스위치 또는 관련 명령에서 사용할 수 있는 다양한 구성에 대해서는 이 절에서 설명하지 않습니다.

또한 이 절에서는 기본 구성 및 정의를 통해 처음으로 스위치에 액세스하는 절차에 대해 설명합니다. 이전에 입력한 구성에 문제가 있는 경우 전원을 켜고 스위치를 구성하는 시작 구성 파일을 지우고 스위치를 재부팅해야 합니다. "[장치 기본 설정](#)"을 참조하십시오.

스위치 설정 요구 사항

이 예를 설명하기 위해 다음 구성 요소가 필요합니다.

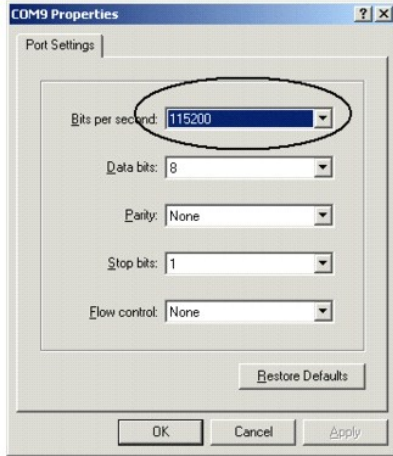
1. PowerConnect 6200 시리즈 스위치
1. 다음 구성 요소가 설치된 워크스테이션:
 - o 네트워크 어댑터 카드
 - o ASCII 터미널 응용프로그램(예: Microsoft® Windows® HyperTerminal 또는 Procomm Plus™ Terminal)
 - o 브라우저 응용프로그램
1. 널 모델 F2F 케이블 1개
1. 직선 또는 크로스 UTP (category 5) 케이블

초기 연결

1. RS-232 포트를 사용하여 스위치를 워크스테이션에 연결합니다.
2. ASCII 터미널을 다음과 같이 설정하고 적절한 COM 포트를 선택합니다.

샘플 화면에서는 하이퍼터미널을 사용합니다.

그림 5-3. HyperTerminal Properties Window(하이퍼터미널 속성 창)



주: 9600은 새 스위치의 기본 보드율입니다. 스위치가 다른 보드율을 가질 수 있습니다. 기본 보드율을 사용하여 스위치 터미널을 볼 수 없는 경우 다른 보드율을 사용합니다.

3. F2F 널 모뎀 케이블을 사용하여 워크스테이션을 스위치에 연결합니다.

주: 스택을 구성하는 경우 워크스테이션을 마스터 스위치에 연결합니다.

4. 스위치 전원 코드를 연결하고 스위치 전원을 켭니다. 시스템이 부팅 프로세스를 시작합니다. 다음이 표시되면 **2**를 선택하여 **Boot(부팅) 메뉴**로 이동할 수 있으며 필요한 경우 특수 절차를 실행합니다.

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):**2**

Boot(부팅) 메뉴로 이동하지 않는 경우 시스템은 RAM에 코드의 압축을 풀어 작업을 계속합니다. 코드가 RAM에서 실행하기 시작하고 사용 가능한 포트 번호 목록 및 상태(up 또는 down)가 표시됩니다.

주: 다음 화면은 구성의 예입니다. 주소, 버전, 날짜 등과 같은 항목은 스위치마다 다를 수 있습니다.

```
current volume configuration:
- volume label: NO LABEL ; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240
```

FAT handler information:

- allocation group size: 2 clusters
- free space on volume: 21,348,352 bytes

Boot Menu Version: 27 Apr 2006

Select an option. If no selection in 10 seconds then
operational code will start.

- 1 - Start operational code.
- 2 - Start Boot Menu.

Select (1, 2):1

Operational Code Date: Wed May 17 10:54:19 2006

Uncompressing.....

50% 100%

||||||||||||||||||||||||||||||||||||||||||||||||||||||||

volume descriptor ptr (pVolDesc): 0xfd7e6c0
cache block I/O descriptor ptr (cbio): 0xfd7fe40
auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

of different files in use: 0

of descriptors for deleted files: 0

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector:)
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240

FAT handler information:

```

- allocation group size: 2 clusters

- free space on volume: 21,350,400 bytes

File: unitmgr.c, Line: 3419, Error 0 (0x0)

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533.333328 MHz

SOC unit 0 attached to PCI device BCM56304_B0

SOC unit 1 attached to PCI device BCM56304_B0

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

hpc - No stack ports. Starting in stand-alone mode.

(Unit 1 - Waiting to select management unit)>

```

장치 기본 설정

장치 기본 설정으로 돌아가려면 권한이 있는 모드 프롬프트(#)에서 `delete startup-config` 명령을 사용하여 장치를 재부팅합니다. 장치가 재부팅되면 기본 설정으로 설정됩니다.

```

console>

console>enable

console#delete startup-config

Startup file was deleted

console#reload

Management switch has unsaved changes.

Are you sure you want to continue? (y/n) y

Configuration Not Saved!

Are you sure you want to reload the stack? (y/n) y

Reloading all switches..

```

원격 관리 활성화

1. 콘솔에서 `enable` 명령을 입력하여 다음과 같이 권한이 있는 EXEC 화면 모드로 들어갑니다.

```

console>enable

console#

```

2. CA5 케이블을 사용하여 이더넷 포트 중 하나를 통하여 스위치에 연결된 네트워크를 통해 스위치에 관리 스테이션을 연결합니다.

이 예에서는 포트 `1/g1`를 사용합니다.

3. 아래에 표시된 대로 인터페이스 상태가 "up(작동)"로 변경되고 STP 상태가 30초 후 전달되는지 ASCII 터미널에서 확인합니다.

```

console#

01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1

01-Jan-2000 01:43:03 %LINK-I-Up: 1/g1

01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/g1: STP status Forwarding

```

4. 콘솔에서 `config` 명령을 입력하여 다음과 같이 구성 화면 모드로 들어갑니다.

```

console#config

```

5. 다음 명령을 사용하여 IP 주소를 DHCP로 설정합니다.

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

6. 다음 명령을 사용하여 기본 게이트웨이를 설정합니다.

```
console(config)#ip default-gateway 10.254.24.162
```

7. 관리 스테이션이 원격 네트워크의 구성원이고 인터페이스에 직접 연결되지 않은 경우 정적 경로를 구성합니다.

구성된 IP 주소는 스위치 IP 인터페이스 중 하나와 동일한 서브네트에 속해야 합니다. 이 예에서 정적 주소는 192.168.20.100입니다.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1 200
```

8. 스위치에서 관리 스테이션을 ping하여 연결이 이루어졌는지 확인합니다.

관리 스테이션을 ping하기 전에 포트가 STP 전송 중에 있도록 30초 대기합니다. 이 예에서 관리 스테이션 IP는 50.1.1.2입니다.

```
console>ping 50.1.1.2
```

```
64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms
```

```
---50.1.1.2 PING Statistics---
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip (ms) min/avg/max = 0/0/0
```

9. 원격 사용자(HTTP 및 HTTPS)에 대해 권한 레벨 15 스위치 액세스가 허용되도록 사용자 이름 및 암호를 정의합니다.

이 예에서 사용자 이름은 **Dell**이고 암호도 **Dell1234**이며 권한 레벨은 15입니다. 권한 레벨의 범위는 1-15이고 최상위 레벨은 15입니다. 레벨 15 액세스는 웹 인터페이스의 액세스 레벨입니다.

```
console#config
```

```
console(config)#username Dell password Dell1234 level 15
```

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

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

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

```
Generating RSA private key, 1024 bit long modulus
```

```
console(config)#ip https server
```

10. 사용자 이름 및 암호를 정의하여 로컬 사용자(예: 콘솔, 텔넷 또는 웹 서버)의 액세스를 허용합니다.

이 예에서 사용자 이름 및 암호는 **Dell**이고 암호는 **Dell1234**이며, 권한 레벨은 15입니다.

```
console(config)#username Dell password Dell1234 level 15
```

```
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 tommy123
```

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

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

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

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



```
console(config-line)#password bobby123

console(config-line)#exit

console(config)#line ssh

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password jones123

console(config-line)#exit
```

11. **running-config** 파일을 **startup-config** 파일에 저장합니다.

이렇게 하면 스위치를 재부팅하는 경우 방금 완료된 구성이 동일합니다.

```
console(config)#exit

console#copy running-config startup-config
```

이제 스위치가 구성되었으며 텔넷, 웹 브라우저 인터페이스 등과 같은 서로 다른 옵션을 통해 관리할 수 있습니다.

보안 관리 액세스 구성(HTTPS)

표준 웹 브라우저를 통해 스위치를 안전하게 관리하려는 경우 SSL(Secure Socket Layer) 보안 프로토콜이 사용됩니다.

표준 웹 브라우저를 통해 스위치를 안전하게 관리하려면 다음을 수행하십시오.

1. HTTPS 서버를 허용하고 보안 키를 작성하도록 스위치를 구성하려면 **ip https server** 및 **crypto certificate 1 generate** 명령을 사용합니다.

```
console#configure

console(config)#crypto certificate 1 generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server

console(config)#
```

2. 관리 스테이션을 정규 HTTP 연결과 동일하게 구성합니다.
3. 브라우저 창에서 **https://장치 IP** 주소 주소를 입력하여 HTTPS 를 통해 스위치에 연결합니다(**https**를 반드시 입력해야 함).

Security Alert(보안 경고) 창이 나타납니다.

4. 보안 인증을 적용하려면 **Yes(예)**를 클릭합니다(타사에 의해 인증되지 않은 경우).

Login Screen(로그인 화면)이 표시됩니다.

5. 지정한 사용자 이름 및 암호를 입력합니다.

Dell OpenManage™ 스위치 관리자가 표시됩니다.

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

도움말 얻기


Dell™ PowerConnect™ M6220 사용 설명서


- [지원 얻기](#)
- [Dell Enterprise Training and Certification](#)
- [주문 관련 문제](#)
- [제품 정보](#)
- [수리 또는 신용 보증에 따른 제품 반환](#)
- [문의하기 전에](#)
- [Dell에 문의하기](#)

지원 얻기

컴퓨터에 문제가 발생할 경우 다음 단계에 따라 문제를 진단 및 해결할 수 있습니다.

1. [진단 체크리스트](#)를 작성합니다.
2. Dell 지원 웹사이트(support.dell.com)에서 제공하는 설치 및 문제 해결 절차와 관련된 Dell의 다양한 온라인 서비스를 받을 수 있습니다. 보다 다양한 Dell 지원 온라인 목록은 [온라인 서비스](#)를 참조하십시오.
3. 앞 단계에서 문제를 해결하지 못한 경우 [Dell에 문의하기](#)를 참조하십시오.

 **주:** Dell 기술 지원부에 전화로 문의하는 경우 필요한 절차를 수행할 수 있도록 컴퓨터 옆이나 가까운 곳에서 전화하십시오.

 **주:** Dell 특급 서비스 코드 시스템은 모든 국가에 지원되지는 않습니다.

Dell 자동 응답 시스템에 연결되면, 특급 서비스 코드를 입력하십시오. 그러면 해당 지원 담당자와 직접 연결됩니다. 특급 서비스 코드가 없는 경우, **Dell Accessories** 폴더에서 **Express Service Code(특급 서비스 코드)** 아이콘을 더블 클릭한 다음 화면에 나타나는 지침을 따르십시오.

Dell 지원 서비스 사용에 대한 지침은 [지원 서비스](#)를 참조하십시오.

 **주:** 미국 이외의 지역에서는 다음 서비스 중 일부가 지원되지 않습니다. 사용가능성 여부를 확인하려면, 해당 지역의 Dell 지사로 문의하십시오.

온라인 서비스

다음 웹 사이트를 통해 Dell 제품 및 서비스를 확인할 수 있습니다.

www.dell.com

www.dell.com/ap(아시아/태평양 지역 국가 전용)

www.dell.com/jp(일본 전용)

www.euro.dell.com(유럽 전용)

www.dell.com/la(라틴 아메리카 및 카리브해 연안 국가)

www.dell.ca(캐나다 전용)

다음 웹 사이트 및 전자 우편 주소를 통해 Dell 지원 서비스를 이용할 수 있습니다.

- 1 Dell 지원 웹 사이트

support.dell.com

support.jp.dell.com(일본 전용)

support.euro.dell.com(유럽 전용)

- 1 Dell 지원 전자 우편 주소

mobile_support@us.dell.com

support@us.dell.com

la-techsupport@dell.com(라틴 아메리카 및 카리브해 연안 국가)

apsupport@dell.com (아시아/태평양 지역 국가 전용)

- 1 Dell 마케팅 및 판매 전자 우편 주소

apmarketing@dell.com (아시아/태평양 지역 국가 전용)

sales_canada@dell.com(캐나다 전용)

- 1 Anonymous FTP(File Transfer Protocol)

ftp.dell.com

사용자 (anonymous)로 로그인하고 암호로 전자 우편 주소를 사용합니다.

자동 주문 현황 서비스

주요한 Dell 제품 현황을 확인하려면 support.dell.com 또는 자동화된 주문 상대 서비스로 문의하십시오. 자동 응답 시스템을 이용하는 경우, 녹음된 안내 내용을 통해 주문 확인에 필요한 여러 정보를 묻습니다. 해당 지역의 전화 번호는 [Dell에 문의하기](#)를 참조하십시오.

지원 서비스

이 서비스는 연중무휴로 제공되며 Dell 하드웨어에 대해 질문하고 응답하는 Dell만의 업계 선두적인 하드웨어 기술 지원 서비스입니다. Dell의 기술 지원부 직원들은 컴퓨터 기반 진단 프로그램을 사용하여 보다 빠르고 정확하게 답변해드리고 있습니다.

Dell의 기술 지원 서비스에 문의하려면 [문의하기 전에](#)를 참조한 다음 해당 지역의 연락처 정보를 참조하십시오.

Dell Enterprise Training and Certification

이제 Dell Enterprise Training and Certification을 이용할 수 있습니다. 자세한 내용은 www.dell.com/training을 참조하십시오. 지역에 따라 이 서비스가 제공되지 않을 수도 있습니다.

주문 관련 문제

부품의 누락 및 결함, 또는 잘못된 청구서 발송과 같은 주문상의 문제가 발생하는 경우에는 Dell 고객 지원부로 문의하십시오. 문의할 때에는 제품 구매서나 포장재를 사용할 수 있도록 준비하십시오. 해당 지역의 전화 번호는 [Dell에 문의하기](#)를 참조하십시오.

제품 정보

Dell에서 추가로 구입할 수 있는 제품에 대한 정보가 필요하거나 제품을 주문하려면 Dell 웹 사이트(www.dell.com)를 방문하십시오. 해당 지역의 전화 번호를 알고 싶거나 영업 담당자와 통화하려면 [Dell에 문의하기](#)를 참조하십시오.

수리 또는 신용 보증에 따른 제품 반환


수리 또는 신용 보증에 따라 제품을 반환하는 경우, 다음 사항을 준비하십시오.

1. Dell에 전화를 걸어 제품 반환 승인 번호를 받으십시오. 이 번호를 상자 바깥쪽에 알기 쉽고 잘 보이도록 적어 놓으십시오.
해당 지역의 전화 번호는 [Dell에 문의하기](#)를 참조하십시오.
2. 제품 구매서 사본 및 반환 사유를 첨부하십시오.
3. 실행한 테스트 및 Dell 진단 프로그램에서 보고한 모든 오류 메시지를 나타내는 진단 체크리스트([진단 체크리스트](#) 참조)의 복사본을 포함하십시오.
4. 신용 반환인 경우는 반환 제품과 함께 부속품(전원 케이블, CD 및 디스켓과 같은 미디어 및 설명서)도 반환하십시오.
5. 원래의 포장 용기에 제품을 담아 반환하십시오.


반환 운송료는 사용자가 부담하게 됩니다. 제품을 안전하게 반환해야 하며 제품 운송 중 발생한 손실에 대해서는 사용자가 책임을 지야 합니다. 수신자 부담 배달(C.O.D.)로 운송된 제품은 접수하지 않습니다.

앞에서 설명한 조건이 하나라도 누락된 경우 Dell은 반환된 제품을 다시 반송합니다.

문의하기 전에

 **주:** 전화를 걸어 문의하기 전에 특급 서비스 코드를 알아두십시오. Dell 자동 응답 지원 전화 시스템은 이 코드를 사용하여 보다 효율적으로 고객의 전화 문의를 처리합니다.


진단 체크리스트 ([진단 체크리스트 참조](#))를 반드시 작성하십시오. 가능한 경우 기술 지원을 Dell에 문의하기 전에 컴퓨터를 켜고, 컴퓨터 가까이에서 전화하십시오. 키보드로 명령을 입력하거나 작동상의 세부사항을 알려주거나 컴퓨터 자체적인 문제 해결 절차를 수행하도록 요청받을 수 있기 때문입니다. 컴퓨터 설명서도 준비하십시오.

 **주의:** 컴퓨터 내부 작업 전에 제품 정보 안내의 안전 지침을 따르십시오.

진단 체크리스트
이름:
날짜:
주소:
전화 번호:
서비스 태그(컴퓨터의 후면 또는 밑면의 바 코드):
특급 서비스 코드:
제품 반환 승인 번호(Dell 지원부 기술자 제공):
운영 체제 및 버전:
장치:
확장 카드:
네트워크에 연결되어 있습니까? 예/아니오
네트워크, 버전 및 네트워크 어댑터:
프로그램 및 버전:
시스템의 시작 파일 내용을 확인하려면 운영 체제 설명서를 참조하십시오. 컴퓨터가 프린터에 연결되어 있는 경우 각 파일을 인쇄하십시오. 아니면 Dell에 문의하기 전에 각 파일의 내용을 기록해 두십시오.
오류 메시지, 경고음 코드 또는 진단 코드:
문제 설명 및 수행한 문제 해결 절차:

Dell에 문의하기

미국 고객의 경우 800-WWW.DELL(800.999.3355)로 문의하십시오.

 **주:** 인터넷 연결이 활성화되어 있지 않을 경우 제품 구매서, 포장재, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 찾아보십시오.

Dell은 여러 종류의 온라인 및 전화 기반의 기술 지원과 서비스 옵션을 제공합니다. 사용 가능성 여부는 국가 및 제품에 따라 다르며, 일부 서비스를 이용하지 못할 수도 있습니다. 판매, 기술 지원 또는 고객 서비스 문제로 Dell에 문의하려면:

1. support.dell.com을 방문하십시오.
2. 페이지의 **Choose A Country/Region** 드롭다운 메뉴에서 해당 국가 또는 지역을 확인하십시오.
3. 페이지 왼쪽의 **Contact Us**를 클릭하십시오.
4. 원하는 서비스 또는 링크를 선택하십시오.
5. Dell에 편리하게 문의할 수 있는 방법을 선택하십시오.

[목록 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

Dell™ OpenManage™ 스위치 관리자 사용

Dell™ PowerConnect™ M6220 사용 설명서

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

스위치의 IP 주소 설정

IP 주소를 설정하는 두 가지 방법은 DHCP를 사용하거나 정적으로 주소를 할당하는 것입니다. CLI를 시작하려면 [CLI를 통해 스위치 액세스](#)를 참조하십시오.

DHCP를 사용한 IP 주소 설정

1. > 프롬프트에 enable를 입력하고 <Enter> 키를 누릅니다.
2. console# 프롬프트에 config를 입력하고 <Enter> 키를 누릅니다.
3. ip address dhcp를 입력하고 <Enter> 키를 누릅니다.
4. exit를 입력합니다.
5. console# 프롬프트에서 show ip interface management를 입력합니다.


정적 주소 설정

1. > 프롬프트에 enable를 입력하고 <Enter> 키를 누릅니다.
2. console# 프롬프트에 config를 입력하고 <Enter> 키를 누릅니다.
3. ip address none
를 입력합니다.
4. 255.255.248.0의 넷마스크와 10.256.24.1 게이트웨이로 10.256.24.64의 IP 주소를 구성하려면 다음을 입력하십시오.
ip address 10.256.24.64 255.255.248.0
ip default-gateway 10.256.24.1
5. exit를 입력합니다.
6. show ip interface management를 입력합니다.

응용프로그램 시작

1. 웹 브라우저를 엽니다.
2. 주소 표시줄에 스위치 IP 주소를 입력하고(CLI에 정의된 대로) <Enter> 키를 누릅니다.

스위치에 IP 주소를 할당하는 데 대한 자세한 내용은 "[구성 개요](#)"를 참조하십시오.
3. Login(로그인) 창이 표시되면 사용자 이름 및 암호를 입력합니다.

 **주:** 콘솔 포트를 사용하여 CLI에 연결할 때 스위치가 기본 암호로 구성되어 있지 않으므로 암호를 입력하지 않고도 스위치를 구성할 수 있습니다. 암호는 대소문자를 구분하며 영숫자입니다. 분실된 암호의 복구에 대한 자세한 내용은 "[암호 복구 절차](#)"를 참조하십시오.

4. **OK (확인)**를 클릭합니다.
5. Dell OpenManage 스위치 관리자 홈페이지가 표시됩니다.

인터페이스 이해

홈페이지(그림 3-1 참조)에는 다음과 같은 보기가 포함되어 있습니다.

1. **디렉터리 화면** — 홈페이지 왼쪽에 위치한 디렉터리 화면에서는 기능 및 해당 구성 요소에 대한 확장 가능한 보기를 제공합니다.
1. **장치 보기** — 홈페이지 오른쪽에 위치한 장치 보기는 장치 보기, 정보 또는 표 영역 및/또는 구성 지침과 같은 사항을 표시하는 데 사용됩니다.

그림 3-1. 스위치 관리자 구성 요소

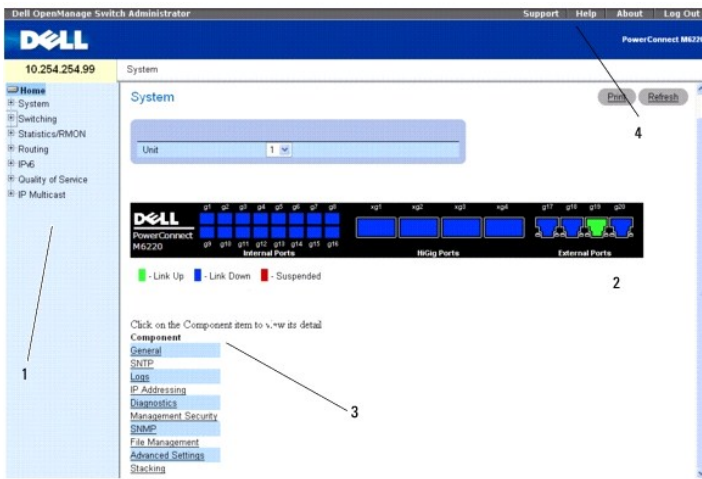


표 3-1에는 해당 번호와 함께 인터페이스 구성 요소가 나열되어 있습니다.

표 3-1. 인터페이스 구성 요소

구성 요소	이름
1	디렉터리 화면에는 다양한 장치 기능에 대한 목록이 포함되어 있습니다. 디렉터리 화면의 버튼을 확장하여 특정 기능의 모든 구성 요소를 보거나 축소하여 기능의 구성 요소를 숨길 수 있습니다. 수직 막대를 오른쪽으로 끌어 트리 영역을 확장하여 구성 요소의 전체 이름을 볼 수 있습니다.
2	장치 보기에서는 장치 포트, 현재 구성 및 상태, 표 정보 및 기능 구성 요소에 대한 정보를 제공합니다. 포트 색상은 포트가 현재 활성 상태인지 여부를 표시합니다. 녹색은 포트가 활성화되었음을 표시하고 빨간색은 포트에 오류가 발생했음을 표시하며 파란색은 링크가 비활성화되었음을 표시합니다. 주: LED 상태는 장치 보기에 나타나지 않습니다. 실제 스위치를 살펴봐야만 LED 상태를 확인할 수 있습니다. LED에 대한 자세한 내용은 " LED 정의 "를 참조하십시오. 선택한 옵션에 따라 장치 보기 하단 영역에 다른 장치 정보 및/또는 매개변수 구성을 위한 대화상자가 표시됩니다.
3	구성 요소에는 기능 구성 요소 목록이 포함되어 있습니다. 또한 디렉터리 화면에서 기능을 확장하여 구성 요소를 볼 수 있습니다.
4	정보 단추는 스위치 정보에 대한 액세스 및 Dell 지원에 대한 액세스를 제공합니다. 자세한 내용은 " 정보 단추 "를 참조하십시오.

스위치 관리자 단추 사용

정보 단추

표 3-2. 정보 단추

--	--

단추	설명
지원	Dell 지원 페이지(support.dell.com)를 엽니다.
도움말	스위치 구성 및 관리에 도움을 주는 정보가 포함된 온라인 도움말입니다. 온라인 도움말 페이지는 상황별 도움말입니다. 예를 들어 IP Addressing(IP 주소) 페이지를 열고 Help(도움말) 를 클릭하면 해당 페이지에 대한 도움말 항목이 표시됩니다.
정보	버전 및 빌드 번호와 Dell 저작권 정보가 포함되어 있습니다.
Log Out(로그아웃)	응용프로그램에서 로그아웃합니다.

장치 관리 단추

표 3-3. 장치 관리 단추

단추	설명
Apply Changes(변경사항 적용)	장치에 설정 변경사항을 적용합니다.
추가	표 또는 대화상자에 정보를 추가합니다.
Telnet(텔넷)	텔넷 세션을 시작합니다.
Query(쿼리)	표를 쿼리합니다.
Show All(모두 표시)	장치 표를 표시합니다.
좌측 화살표/우측 화살표	목록 간에 정보를 이동합니다.
새로 고침	장치 정보를 새로 고칩니다.
Reset All Counters(모든 카운터 재설정)	통계 카운터를 지웁니다.
인쇄	네트워크 관리 시스템 페이지 및/또는 표 정보를 인쇄합니다.
Draw(그리기)	신속히 통계 차트를 만듭니다.

확인란

표 3-4. 확인란

확인란 유형	설명
추가	구성 페이지로 이동하는 하이퍼링크입니다.
제거	선택한 항목을 제거합니다.
General selection(일반 선택)	구성 항목을 활성화할 때(예: 로그 파일 민감도 조정, diffserv에 대한 일치 기준 선택 및 ACL 규칙 매개변수 선택) 사용됩니다.

필드 정의

Dell OpenManage 스위치 관리자 웹 페이지에 다른 지침이 없는 한 사용자 정의 필드에는 1-159자가 포함될 수 있습니다.

다음은 제외한 모든 문자를 사용할 수 있습니다.


```

1 \
1 /
1 :
1 *
1 ?
1 <
1 >
1 |

```

CLI를 통해 스위치 액세스

콘솔 포트에 대한 직접 연결 또는 텔넷 연결을 통해 스위치를 관리할 수 있습니다.


 **주:** 스택을 관리하는 경우 직렬 인터페이스 케이블이 스택의 마스터 스위치에 연결되어 있는지 확인합니다.

CLI 사용은 Linux 시스템에서 명령을 입력하는 것과 비슷합니다. 텔넷 연결을 통해 액세스하는 경우 장치에 IP 주소가 정의되어 있고 장치를 액세스하는 데 사용된 워크스테이션이 CLI 명령을 사용하기 전에 장치에 연결되어 있는지 확인합니다.


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

콘솔 연결

1. 스위치 또는 스택 전원을 켜고 시작이 완료될 때까지 대기합니다.

 **주:** 스위치 스택을 설치할 경우 터미널을 마스터 스위치에 연결하십시오. 이 스위치는 마스터 스위치 LED를 켭니다. 스택에 처음 전원을 공급하면 스위치에서 마스터 스위치(스택에서의 위치는 상관 없음)를 선택합니다. 터미널을 종속 스위치에 연결한 경우 종속 직렬 인터페이스를 통해 CLI를 사용할 수 없습니다.

2. 관리자가 로그인 인증 방법을 구성하지 않은 경우 스위치가 부팅될 때 `console>` 프롬프트가 표시됩니다. 그렇지 않은 경우 사용자에게 User: 로그인 프롬프트가 표시됩니다.

 **주:** 다음 단계는 관리자 사용자 및 암호가 시스템 구성되어 있는 것으로 가정합니다.

3. 프롬프트에 `admin`을 입력하고 <Enter> 키를 누릅니다.

그러면 `Password:` 프롬프트가 표시됩니다.

4. 암호를 입력하면 별표(*)로 표시됩니다.

그러면 `console#` 프롬프트가 표시됩니다.

5. 장치를 구성하고 필요한 명령을 입력하여 요구되는 작업을 완료합니다.

6. 완료되면 `quit` 또는 `exit` 명령을 사용하여 세션을 종료합니다.

텔넷 연결

텔넷은 터미널 에뮬레이션 TCP/IP 프로토콜입니다. ASCII 터미널은 TCP/IP 프로토콜 네트워크를 통해 로컬 장치에 가상적으로 연결할 수 있습니다. 텔넷은 원격 로그인이 필요한 로컬 로그인 터미널에 대한 대안입니다.

스위치는 최대 4개의 동시 텔넷 세션을 지원합니다. 모든 CLI 명령은 텔넷 세션을 통해 사용할 수 있습니다.

CLI 사용

명령 모드 개요

CLI는 명령 모드로 구분됩니다. 각 명령 모드에는 특정 명령 세트가 있습니다. 콘솔 프롬프트에 물음표를 입력하면 해당 특정 명령 모드에 대해 사용 가능한 명령 목록이 표시됩니다.

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

CLI 세션이 초기화되는 동안 CLI 모드는 사용자 EXEC 모드입니다. 명령의 제한된 하위 집합만 사용자 EXEC 모드에서 사용할 수 있습니다. 이 레벨은 스위치 구성을 변경하지 않는 작업에 대해 유지되고 구성 하위 시스템에 액세스하는 데 사용됩니다. `enable` 암호가 구성된 경우 권한이 있는 EXEC 모드에 암호가 필요할 수 있습니다. `enable` 암호 설정에 대한 자세한 내용은 [보안 관리 및 암호 구성](#)을 참조하십시오.

권한이 있는 EXEC 모드에서는 장치 전역 구성에 대한 액세스를 제공합니다. 장치 내의 특정 전역 구성에 대해 다음 레벨인 전역 구성 모드를 입력합니다. 암호가 필요하지 않습니다.


전역 구성 모드 모드는 전역 레벨에서 장치 구성을 관리합니다.

인터페이스 구성 모드는 물리적 인터페이스 레벨에서 장치를 구성합니다. 하위 명령이 필요한 인터페이스 명령에는 하위 인터페이스 구성 모드라고 하는 또 다른 레벨이 있습니다.

사용자 EXEC 모드

사용자 EXEC 레벨 프롬프트는 꼭시 괄호(>) 다음에 호스트 이름을 붙여 구성됩니다. 예:

```
console>
```

 **주:** 기본 호스트 이름은 초기 구성 동안 수정되지 않는 `console`입니다.

사용자 EXEC 명령은 원격 장치로의 연결, 일시적인 터미널 설정 변경, 기본 검사 수행 및 시스템 정보 나열을 허용합니다.

사용자 EXEC 명령을 나열하려면 명령 프롬프트에 물음표를 입력합니다.

권한이 있는 EXEC 모드

무단 액세스를 방지하고 작동 매개변수를 확인하도록 권한이 있는 액세스를 보호할 수 있습니다. 암호는 대/소문자를 구분하며 암호의 각 문자는 화면에 별표로 표시됩니다.

권한이 있는 EXEC 모드 명령에 액세스하고 나열하려면 다음을 수행합니다.

1. 프롬프트에 `enable`를 입력하고 <Enter> 키를 누릅니다.
2. 암호 프롬프트가 표시되면 암호를 입력하고 <Enter> 키를 누릅니다.

권한이 있는 EXEC 모드 프롬프트에는 # 다음에 장치 호스트 이름이 표시됩니다. 예:

```
console#
```

3. 권한이 있는 EXEC 명령을 나열하려면 명령 프롬프트에 물음표를 입력하십시오.
4. 권한이 있는 EXEC 모드에서 사용자 EXEC 모드로 돌아가려면 `exit` 명령을 입력하고 <Ctrl><Z> 키를 누릅니다.

다음 예에서는 권한이 있는 EXEC 모드에 액세스한 다음 사용자 EXEC 모드로 돌아가는 상황을 보여 줍니다.

```
console>enable
Enter Password: *****
console#
console#exit
console>
```

`exit` 명령을 사용하여 이전 모드로 돌아갑니다. 예를 들어 인터페이스 구성 모드에서 전역 구성 모드로 이동하거나 전역 구성 모드에서 권한이 있는 EXEC 모드로 이동할 수 있습니다.

전역 구성 모드

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

전역 구성 모드에 액세스하려면 다음을 수행합니다.

1. 권한이 있는 EXEC 모드 프롬프트에서 `configure`를 입력하고 <Enter> 키를 누릅니다. 전역 구성 모드에는 장치 호스트 이름 다음에 (`config`) 및 숫자 기호(#)가 표시됩니다.
- ```
console(config)#
```
2. 전역 구성 명령을 나열하려면 명령 프롬프트에 물음표를 입력합니다.
  3. 전역 구성 모드에서 권한이 있는 EXEC 모드로 돌아가려면 `exit` 명령을 입력하거나 <Ctrl><Z> 명령을 사용합니다.

다음 예에서는 전역 구성 모드에 액세스하고 권한이 있는 EXEC 모드로 돌아가는 방법에 대해 설명합니다.

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

## 인터페이스 구성 모드

인터페이스 구성 명령은 브리지-그룹, 설명 등을 포함한 특정 IP 인터페이스 설정을 수정합니다. 인터페이스 구성 모드는 다음과 같습니다.

1. **VLAN** — 예를 들어 VLAN을 만들고 IP 주소를 VLAN에 적용하는 명령과 같이 VLAN을 만들고 구성하기 위한 전반적인 명령이 포함되어 있습니다.
1. **포트 채널** — 링크 결합 그룹(LAG)을 구성하기 위한 명령이 포함되어 있습니다.
1. **이더넷** — 이더넷 포트 구성을 관리하기 위한 명령이 포함되어 있습니다.

1 **루프백** — 루프백 인터페이스 구성을 관리하기 위한 명령이 포함되어 있습니다.

1 **터널** — 터널 인터페이스 구성을 관리하기 위한 명령이 포함되어 있습니다.

---

[목차 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

## 하드웨어 설명

### Dell™ PowerConnect™ M6220 사용 설명서

- [포트 설명](#)
- [기타 특성](#)
- [LED 정의](#)

이 절에서는 장치의 특성과 모듈 하드웨어 구성에 관한 정보를 제공합니다. 이 항목에서 다루는 내용은 다음과 같습니다.

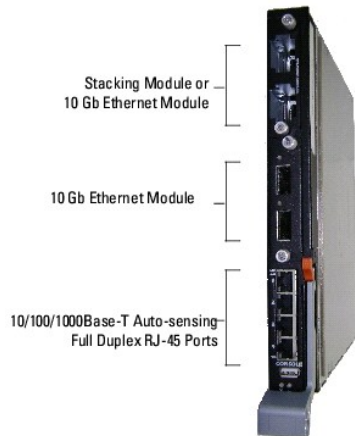
- 1 [Dell™ PowerConnect™ M6220 전면 패널](#)
- 1 [콘솔\(RS-232\) 포트](#)
- 1 [물리적 크기](#)
- 1 [전원 공급 장치](#)
- 1 [통풍 시스템](#)
- 1 [스택형 배치](#)
- 1 [LED 정의](#)

## 포트 설명

### Dell™ PowerConnect™ M6220 전면 패널

PowerConnect M6220 전면 패널에는 4개의 10/100/1000 Base-T RJ-45 포트와 4개의 10기가비트 이더넷 포트가 있습니다. 각 서버 블레이드에 연결된 내장 포트도 16개가 있습니다.

그림 2-1. PowerConnect M6220



- 1 이 스위치는 RJ-45 포트에서 교차 케이블과 직통 케이블의 차이점을 자동으로 감지합니다.
- 1 RJ-45 포트는 반이중 및 전이중 모드를 지원합니다.

## 콘솔(RS-232) 포트

콘솔(RS-232) 포트는 직렬 인터페이스를 통해 관리하는 경우에만 사용됩니다. 이 포트는 스위치에 직접 연결되며, EIA/TIA-232 포트에 연결된 콘솔 터미널에서 CLI를 액세스하는 데 사용됩니다.

M6220의 콘솔 포트에서 터미널로 연결하려면 한쪽 끝에는 USB 유형 A 커넥터를, 다른 쪽 끝에는 암 DB-9 커넥터를 사용하여 제공된 직렬 케이블을 사용하십시오. M6220의 콘솔 포트는 전면 패널 밑면에 위치한 USB 포트입니다.

콘솔 포트는 데이터 비트(8개), 정지 비트(1개), 패리티 비트(없음) 및 흐름 제어(없음)의 비동기 데이터를 지원합니다. 기본 보드율은 9600bps입니다.

- **주:** 스위치 스택을 설치할 경우 스택의 전원을 켜고 구성하기 전에 스택을 조립하고 케이블을 연결해야 합니다. 스택에 처음 전원을 공급하면 스위치에서 마스터 스위치(스택에서의 위치는 상관 없음)를 선택합니다. 터미널을 마스터 스위치에 연결합니다. 터미널을 종속 스위치에 연결하면 CLI를 사용하지 못합니다.

## 콘솔 재지정

Dell Blade Server 새시의 콘솔 재지정 기능을 사용하여 단일 직렬 연결에서 새시까지 각 M6220 모듈을 관리할 수 있습니다. 콘솔 재지정에 대한 자세한 내용은 *Dell Blade Server CMC 사용 설명서*를 참조하십시오.

**주:** 콘솔 재지정 기능을 사용하여 모듈을 액세스하면 해당 모듈의 외부 콘솔이 비활성화되고 현재 활성 중인 콘솔 세션이 모두 종료됩니다.

## 기타 특성

### 물리적 크기

PowerConnect M6220의 물리적 크기에 대한 자세한 내용은 *Dell Blade Server 새시 하드웨어 소유자 설명서*를 참조하십시오.

### 전원 공급 장치

PowerConnect M6220 전원 공급 장치에 대한 자세한 내용은 *Dell Blade Server 새시 하드웨어 소유자 설명서*를 참조하십시오.

### 통풍 시스템

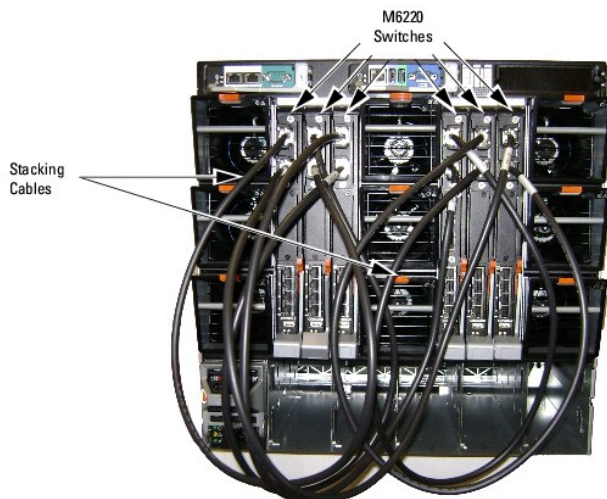
PowerConnect M6220의 통풍 시스템에 대한 자세한 내용은 *Dell Blade Server 새시 하드웨어 소유자 설명서*를 참조하십시오.

### 스택형 배치

최대 240개 1-Gb 포트를 지지하면서 최대 12 스위치 높이까지 PowerConnect M6220 장치를 스택형으로 적재할 수 있습니다. 스위치 패널 위에 있는 스택 포트를 사용하는 인접 장치를 연결하여 스택을 만드십시오. [그림 2-2](#)를 참조하십시오.

1. 스택의 각 스위치에 있는 후면 "베이 1"에 별도로 구입한 스택링 모듈을 설치합니다.
2. 스택의 각 스위치의 경우, 스위치의 스택형 포트 1에서 다음 스위치의 스택형 포트 2까지 짧은 스택링 케이블 중 하나를 연결하십시오.
3. 필요한 경우 별도로 구입한 3m의 긴 스택링 케이블을 스위치에 연결합니다. 모든 장치가 연결될 때까지 이 과정을 반복합니다.
4. 남은 스택링 케이블을 사용하여 마지막 스위치의 포트 1에서 첫 번째 스위치의 포트 2까지 비어 있는 포트에 연결하십시오.

**그림 2-2. Connecting a Stack of Switches(스위치 스택 연결)**



[그림 2-2](#)에서 스택에 스택링 포트를 통해 연결된 PowerConnect M6220 스위치가 6개 있습니다. 각 M6220의 첫 번째 스택링 포트는 실제로 스택링 케이블을 통해 다음 M6220의 두 번째 스택링 포트에 연결됩니다. 스위치 6의 첫 번째 스택링 포트는 스위치 1의 두 번째 스택링 포트에 연결됩니다.

## 스태킹 대기

스태킹 기능은 스택의 마스터 장치에 문제가 있을 경우 마스터 장치 역할을 하게 될 "대기" 또는 백업을 지원합니다. 스택에 마스터 장애가 발견되자마자 대기 장치는 제어 플레인을 초기화하고 현재 구성으로 다른 모든 스택 장치를 활성화합니다. 대기 장치는 스택에 실행 중인 구성의 동기화 복사본을 그대로 유지합니다. 전환하는 도중 루프가 발생하지 않도록 모든 포트가 위아래로 움직이며 새 마스터 소프트웨어 응용프로그램을 일관적인 상태로 둡니다.

대기 장치는 스택에 미리 구성되어 있지만 CLI를 사용하여 다른 스택 구성원을 대기 장치로 선택할 수 있습니다. 자세한 내용은 *CLI 참조 안내서*를 참조하십시오.

## LED 정의

전면 패널에는 링크, 내장 1Gb 포트 및 시스템 상태를 나타내는 발광 다이오드(LED)가 있습니다.

그림 2-3. Front Panel LEDs(전면 패널 LED)

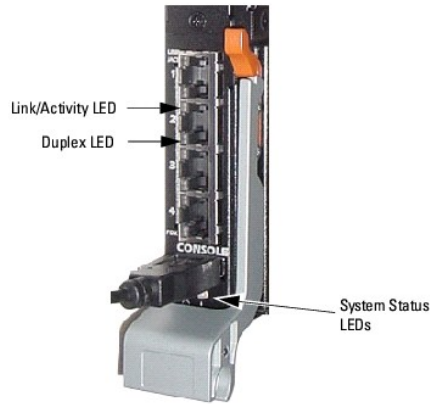


표 2-1에는 시스템 LED 정의가 포함되어 있습니다.

표 2-1. M6220 Status LEDs Definitions(M6220 상태 LED 정의)

| LED | 색상 | 정의                       |
|-----|----|--------------------------|
| ①   | 녹색 | M6220 모듈에 전원을 공급하는 중입니다. |
|     | 꺼짐 | M6220에 전원이 없습니다.         |
| ⚡   | 청색 | 스위치가 현재 스택 마스터입니다.       |
|     | 꺼짐 | 스위치가 현재 스택 마스터가 아닙니다.    |
|     | 황색 | 장애가 발생했습니다.              |

## XFP 모듈 포트 LED

XFP 커넥터는 M6220에 삽입될 때 XFP 모듈에 있습니다. 표 2-2에는 XFP 포트 LED 정의가 포함되어 있습니다.

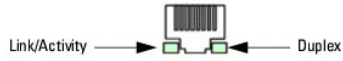
표 2-2. XFP Port LEDs Definitions(XFP 포트 LED 정의)

| LED | 색상           | 정의                             |
|-----|--------------|--------------------------------|
| XFP | 녹색           | 포트가 연결되어 있습니다.                 |
|     | 녹색들이 깜박이는 경우 | 포트가 네트워크 트래픽을 전송 및/또는 수신 중입니다. |
|     | 꺼짐           | 포트가 연결되어 있지 않습니다.              |

## 10/100/1000 Base-T 포트 LED

각 10/100/1000 Base-T 포트에는 LED가 두 개씩 있습니다. 다음 그림은 10/100/100 Base-T 포트 LED를 보여줍니다.

그림 2-4. 10/100/1000 Base-T Port LEDs(10/100/1000 Base-T 포트 LED)



[표 2-3](#)에는 10/100/1000 Base-T 포트 LED 정의가 포함되어 있습니다.

표 2-3. 10/100/1000 Base-T Port Definitions(10/100/1000 Base-T 포트 LED)

| LED   | 색상  | 정의                          |
|-------|-----|-----------------------------|
| 연결/작동 | 녹색  | 포트가 1000Mbps에서 작동하고 있습니다.   |
|       | 황색  | 포트가 10/100Mbps에서 작동하고 있습니다. |
|       | 켜짐  | 연결되었지만 작동하지 않습니다.           |
|       | 깜박임 | 연결되어 있고 작동 중입니다.            |
|       | 꺼짐  | 링크가 없습니다.                   |
| 이중    | 녹색  | 전이중 모드                      |
|       | 꺼짐  | 반이중 모드                      |

[목록 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

## 소개

### Dell™ PowerConnect™ M6220 사용 설명서

- [기능](#)
- [CLI 설명서](#)

🔍 **주의사항:** 진행하기 전에 이 제품의 릴리즈 노트를 확인하십시오. Dell 지원 웹 사이트([support.dell.com](http://support.dell.com))에서 릴리즈 노트를 다운로드할 수 있습니다.

Dell™ PowerConnect™ M6220은 Dell Blade Server 새시에서 사용할 수 있는 Layer 3, 기가비트 이더넷 스위치 블레이드입니다. PowerConnect M6220은 Dell PowerConnect 6200 시리즈 구조에 기반을 두고 있습니다.

## 기능

이 절에서는 사용자 구성 가능한 스위치 기능에 대해 설명합니다. 전체 기능 목록을 보려면 소프트웨어 버전 릴리즈 노트를 참조하십시오.

### 포트 기반 기능

#### 정보 프레임 지원

정보 프레임을 사용하면 더 적은 수의 프레임으로 동일한 데이터를 전송할 수 있으므로 오버헤드가 줄어들고, 처리 시간이 단축되며, 인터럽트 수가 감소합니다.

#### 자동 MDI/MDIX 지원

이 스위치는 교차 케이블과 스트레이트 스루 케이블 간의 자동 감지를 지원합니다.

종단국의 표준 배선은 MDI(Media-Dependent Interface)이고 허브 및 스위치의 표준 배선은 MDIX(Media-Dependent Interface with Crossover)라고 합니다.

포트 또는 LAG에 대해 MDI/MDIX를 구성하는 방법에 대한 자세한 내용은 "[포트 구성](#)" 또는 "[LAG 구성](#)"을 참조하십시오.

#### 자동 교섭

자동 교섭을 통해 스위치는 동작 모드를 알릴 수 있습니다. 자동 교섭 기능은 지정대 지정 연결 세그먼트를 공유하는 두 스위치 간에 정보를 교환하는 방법과 전송 기능을 최대한 활용하도록 두 개의 스위치를 자동으로 구성하는 방법을 제공합니다.

PowerConnect 6200 시리즈는 포트 알림을 제공하여 자동 교섭 기능을 향상시킵니다. 포트 알림에서 시스템 관리자는 포트 알림 속도를 구성할 수 있습니다.

자동 교섭에 대한 자세한 내용은 "[포트 구성](#)" 또는 "[LAG 구성](#)"을 참조하십시오.

#### 흐름 제어 지원(IEEE 802.3x)

흐름 제어를 사용하면 고속의 스위치가 패킷을 보내는 것을 잠시 중단하도록 요청하는 방식으로 저속의 스위치와 고속의 스위치가 통신할 수 있습니다. 버퍼 오버플로가 발생하지 않도록 전송이 일시적으로 중지됩니다.

포트 또는 LAG에 대해 흐름 제어를 구성하는 방법에 대한 자세한 내용은 "[포트 구성](#)" 또는 "[LAG 구성](#)"을 참조하십시오.

#### HOL(Head of Line) 블로킹 방지

HOL(Head of Line) 블로킹 방지 기능은 동일한 출력 포트 자원에 대해 경쟁하는 트래픽으로 인해 발생하는 트래픽 지연 및 프레임 손실을 방지합니다. HOL 블로킹은 패킷을 대기시키고 대기열의 맨 앞에 있는 패킷이 대기열의 끝에 있는 패킷보다 먼저 전달됩니다.

#### 백 프레셔 지원

반이중 링크에서 수신기는 추가 트래픽에 사용하지 못하도록 링크를 점유하여 버퍼 오버플로를 방지할 수 있습니다.

#### ASF(Alternate Store and Forward)

ASF(Alternate Store and Forward) 기능은 대용량 패킷에 대한 대기 시간을 줄일 수 있습니다. ASF가 활성화되어 있으면 CBP(Cell Buffer Pool) 메모리에 전체를 수신하기 전에 MMU(Memory Management Unit)가 전송 포트에 패킷을 전달할 수 있습니다. 침투 모드로도 알려져 있는 ASF는 명령줄 인터페이스를 통해 구성할 수 있습니다. ASF 기능 구성 방법에 대한 자세한 내용은 CLI 참조 안내서를 참조하십시오.

## MAC 주소 지원 기능

### MAC 주소 지원

이 스위치는 최대 8,000개의 MAC 주소를 지원하고 시스템에서 사용하도록 2개의 MAC 주소를 예약합니다.

### MAC 주소 자동 학습

이 스위치는 들어오는 패킷에서 MAC 주소를 자동으로 학습할 수 있습니다.

### MAC 주소 자동 에이징

지정된 기간 동안 트래픽이 없는 MAC 주소가 소멸되어 브리지 표가 오버플로되지 않도록 방지합니다.

MAC 주소 소멸 기간을 구성하는 방법에 대한 자세한 내용은 "[동적 주소 표](#)"를 참조하십시오.

### 정적 MAC 항목

사용자 정의 MAC 항목은 자동 학습된 주소와 함께 브리지 표에 저장됩니다.

정적 MAC 주소를 구성하는 방법에 대한 자세한 내용은 "[정적 주소 표](#)"를 참조하십시오.

## VLAN 인식 MAC 기반 스위칭

알 수 없는 소스 주소에서 도착된 패킷은 CPU로 보내지고 하드웨어 표에 추가됩니다. 이후에 이 주소에서 송/수신되는 패킷은 보다 효율적으로 전달됩니다.

## MAC 멀티캐스트 지원

멀티캐스트 서비스는 일대다 및 다대다 연결을 허용하는 제한된 브로드캐스트 서비스입니다. 계층 2 멀티캐스트 서비스에서 특정 멀티캐스트 주소로 전송된 단일 프레임이 수신되고 관련된 각 포트에서 전송할 프레임의 복사본이 생성됩니다.

MAC 멀티캐스트 지원을 구성하는 방법에 대한 자세한 내용은 "[멀티캐스트 지원 관리](#)"를 참조하십시오.

## 계층 2 기능

### IGMP 스누핑

IGMP 스누핑은 스테이션에서 스위치를 통해 임스트림 멀티캐스트 라우터로 전달되는 IGMP 프레임의 내용을 검사합니다. 스위치는 스누핑 기능을 통해 멀티캐스트 세션과 관련된 스테이션과 멀티캐스트 프레임을 보내는 멀티캐스트 라우터를 식별할 수 있습니다.

### 포트 미러링

포트 미러링은 최대 4개의 소스 포트에서 들어오는 패킷과 나가는 패킷의 복사본을 모니터링 포트에 전달하여 네트워크 트래픽을 모니터링하고 미러링합니다.

### 브로드캐스트 뇌우 제어

계층 2 프레임이 전달되면 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 프레임이 관련 VLAN(Virtual Local Area Network)의 모든 포트에 플러딩됩니다. 플러딩은 대역폭을 사용하고 모든 포트에 연결된 모든 노드를 로드합니다. 뇌우 제어는 스위치에서 송/수신되는 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 프레임의 양을 제한합니다.

### 연결 종속성 기능



연결 종속성 기능은 하나 이상의 포트 연결 상태에 따라 하나 이상의 포트를 활성화 또는 비활성화할 수 있는 기능입니다.

연결 종속성에 대한 자세한 내용은 "[연결 종속성 만들기](#)"를 참조하십시오.

## VLAN(Virtual Local Area Network)이 지원되는 기능

### VLAN 지원

VLAN은 단일 브로드캐스트 도메인을 구성하는 스위칭 포트의 모음입니다. 패킷은 VLAN 태그 또는 수신 포트와 패킷 내용의 조합을 기반으로 VLAN에 속하는 것으로 분류됩니다. 공통 속성을 공유하는 패킷은 동일한 VLAN의 그룹이 될 수 있습니다.

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

### 포트 기반 VLAN

포트 기반 VLAN은 해당 수신 포트에 기반하여 들어오는 패킷을 VLAN으로 분류합니다.

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

### IEEE 802.1v 프로토콜 기반 VLAN

VLAN 분류 규칙은 데이터 링크 계층(계층 2) 프로토콜 확인 시 정의됩니다. 프로토콜 기반 VLAN은 계층 3 프로토콜과의 구분을 위해 계층 2 트래픽을 격리하는 데 사용됩니다.

프로토콜 기반 VLAN을 정의하는 방법에 대한 자세한 내용은 "[프로토콜 그룹](#)"을 참조하십시오.

### 전체 802.1Q VLAN 태깅 규약

IEEE 802.1Q는 가상 브리지 LAN의 구조, VLAN에 제공된 서비스, 이러한 서비스 규정과 관련된 프로토콜 및 알고리즘 등을 정의합니다.

### GVRP 지원

GVRP(GARP VLAN Registration Protocol)는 IEEE 802.1Q 호환 VLAN 삭제 및 802.1Q 트렁크 포트에서 동적 VLAN 생성 등을 제공합니다. GVRP가 활성화되면 스위치는 활성 기본 스페닝 트리 프로토콜 토폴로지의 일부인 모든 포트에 대한 VLAN 멤버십을 등록하고 전파합니다.

GVRP 구성에 대한 자세한 내용은 "[GVRP 매개변수](#)"를 참조하십시오.

### 보호된 포트(사설 VLAN 예지)

PVE(사설 VLAN 예지) 포트는 동일한 VLAN의 구성원인 포트 간에 포트 기반 보안을 제공하는 계층 2 보안 기능으로 일반 VLAN의 확장입니다. 보호된 포트에서 들어오는 트래픽은 업링크 포트에만 전송되며 VLAN 내의 다른 포트로는 전송될 수 없습니다.

### 서브넷 기반 VLAN

이 기능을 사용하면 태그되지 않은 수신 패킷을 패킷의 소스 IP 주소를 기반으로 VLAN 및 트래픽 클래스에 할당할 수 있습니다.

서브넷 기반 VLAN을 구성하는 방법에 대한 자세한 내용은 "[IP 서브넷을 VLAN에 바인드](#)"를 참조하십시오.

### MAC 기반 VLAN

이 기능을 사용하면 태그 없는 수신 패킷을 패킷의 소스 MAC 주소를 기반으로 VLAN 및 트래픽 클래스에 할당할 수 있습니다.

MAC 기반 VLAN을 구성하는 방법에 대한 자세한 내용은 "[MAC를 VLAN에 바인드](#)"를 참조하십시오.

### 스패닝 트리 프로토콜 기능

### 스위치당 STP(스패닝 트리 프로토콜)

802.1d STP는 브리지기 자동으로 L2 전달 루프를 방지하고 해결하도록 하는 계층 2 스위치의 표준 요구 사항입니다. 스위치는 포트상에서 특별히 포맷된 프레임과 선택적인 전달을 사용하여 구성 메시지를 교환합니다.

STP(Spanning Tree Protocol) 구성 방법에 대한 자세한 내용은 "[스패닝 트리 프로토콜 구성](#)"을 참조하십시오.

## IEEE 802.1w 빠른 스패닝 트리

RSTP(빠른 스패닝 트리 프로토콜)는 전달 루프를 생성하지 않고 네트워크 토폴로지를 감지한 후 사용하여 컨버전스를 가속화합니다.

RSTP(Rapid Spanning Tree Protocol) 구성 방법에 대한 자세한 내용은 "[빠른 스패닝 트리](#)"를 참조하십시오.

## 다중 스패닝 트리

MSTP(다중 스패닝 트리) 작업은 VLAN을 스패닝 트리 인스턴스에 매핑합니다. MSTP는 다른 로드 밸런싱 시나리오를 제공합니다. 다양한 VLAN에 할당되는 패킷은 MSTP 영역(MST 영역) 내에서 서로 다른 경로를 따라 전송됩니다. 영역은 동일한 MSTP 설정을 가진 하나 이상의 상호 연결된 MSTP 브리지입니다. 관리자는 이 표준을 사용하여 VLAN 트래픽을 고유한 경로에 할당합니다.

다중 스패닝 트리 구성에 대한 자세한 내용은 "[MSTP 설정](#)"을 참조하십시오.

## 스패닝 트리 루트 가드

스패닝 트리 루트 가드는 스패닝 트리 인스턴스의 루트가 예기치 않게 변경되지 않도록 하는 데 사용됩니다. 브리지 ID의 우선 순위는 0으로 설정될 수 있지만 더 낮은 MAC 주소를 가진 다른 브리지 ID의 우선 순위를 0으로 설정하여 루트로 사용할 수도 있습니다.

## 브리지 프로토콜 데이터 유닛 가드

스패닝 트리 BPDU 가드는 새 장치가 기존의 STP 토폴로지를 시작하려고 할 때 포트를 비활성화하는 데 사용됩니다. 따라서 원래 STP의 일부가 아닌 장치는 STP 토폴로지에 영향을 줄 수 없습니다.

## 링크 결합 기능

### 링크 결합

최대 8개의 포트를 결합하여 단일 LAG(Link Aggregated Group)를 형성할 수 있습니다. 이렇게 함으로써 실제 링크 붕괴로부터 결합 허용 보호, 높은 대역폭 연결, 항상된 대역폭 세분화 등이 가능해집니다.

LAG는 속도가 동일하며 전이중 방식 작동으로 설정된 포트로 구성됩니다.

LAG 구성에 대한 자세한 내용은 "[LAG 구성](#)"을 참조하십시오.

### 링크 결합 및 LACP

LACP(Link Aggregate Control Protocol)는 링크 사이에서 피어 교환을 사용하여 지속적으로 다양한 링크의 결합 기능을 결정하고 지정된 두 시스템 사이에서 얻을 수 있는 최대 수준의 결합 기능을 제공합니다. LACP는 시스템 내에서 결합자에 바인딩된 포트를 자동으로 결정, 구성, 바인드 및 모니터링합니다.

LACP에 대한 자세한 내용은 "[LACP 매개변수](#)"를 참조하십시오.

## IPv4 라우팅 기능

### ARP(Address Resolution Protocol)

PowerConnect 6200은 ARP 프로토콜을 사용하여 계층 2 MAC 주소를 계층 3 IPv4 주소에 연결합니다. 관리자는 ARP 표에 항목을 정적으로 추가할 수 있습니다.

### OSPF(Open Shortest Path First)

OSPF 라우팅 프로토콜은 일반 OSPF 영역과 OSPF 스템 영역의 두 영역 유형을 정의합니다. OSPF 내부 및 외부 경로 정보는 일반 OSPF 영역을 통해 전파될 수 있으며, 전송 트래픽 및 가상 링크를 지원할 수 있습니다. OSPF 스템 영역은 외부 경로 정보를 수신하지 않습니다. 스템 영역을 구성하도록 자극하면 제한된 리소스를 가진 해당 라우터에 대한 영역 데이터베이스의 크기가 제한됩니다.

## BOOTP/DHCP 릴레이 에이전트

BootP 프로토콜을 사용하면 장치에서 해당 서버에 구성 데이터 및 매개변수를 요청하여 수신할 수 있습니다. DHCP는 시스템 시작에 따라 추가 설정 매개 변수를 네트워크 서버에서 수신할 수 있도록 해주는 BootP의 확장입니다. BootP는 IP 주소가 확인되면 작동을 중지하지만 DHCP 서비스는 계속 처리됩니다. 예를 들어, 시스템에 할당된 IP 주소의 '리스 시간'이 만료될 수 있으므로 즉시 갱신할 수 있습니다.

## RIP(Routing Information Protocol)

자차 인터넷 시스템에서 사용되는 라우팅 프로토콜을 내부 게이트웨이 프로토콜 또는 IGP(Interior Gateway Protocol)라고 합니다. RIP는 중간 규모 네트워크에서 작동하도록 고안된 IGP입니다.

## VRRP(Virtual Routing Redundancy Protocol)

VRRP(Virtual Routing Redundancy Protocol)는 여러 라우터가 있는지 확인하거나 호스트를 재구성하지 않고 네트워크 토폴로지에서 중복 라우터를 호스트에 제공하는 데 사용됩니다.

## IPv6 라우팅 기능

### DHCPv6

DHCPv6은 "상대 비저장" 서버 개념을 통합합니다. 여기서는 DHCPv6가 클라이언트에 대한 IP 주소 할당에 사용되지 않고, DNS, NTP(Network Time Protocol), SIP(Session Initiation Protocol) 정보 등과 같은 다른 네트워킹 정보만 제공합니다.

### OSPFv3

OSPFv3은 IPv6 네트워킹을 위한 라우팅 프로토콜을 제공합니다. OSPFv3은 OSPF 버전 2 구성 요소를 기반으로 하는 새로운 라우팅 구성 요소입니다. 듀얼 스택 IPv6에서 OSPF 및 OSPFv3 구성 요소를 둘 다 구성 및 사용할 수 있습니다.

### IPv6 경로

IPv4와 IPv6이 네트워크에 공존할 수 있기 때문에 그런 네트워크에 있는 라우터는 두 가지 트래픽 유형을 모두 전달해야 합니다. 두 경로가 공존할 경우 PowerConnect 6200은 두 라우팅 표 rto 및 rto6을 유지하여 동일한 인터페이스를 통해 전달할 수 있습니다. IPv6 인터페이스는 IPv4 인터페이스와 비슷한 방식으로 관리됩니다.

## QoS(서비스 품질) 기능

### QoS(서비스 품질) 지원

예상치 못한 네트워크 트래픽을 수용하고 성능을 최적화하려면 네트워크 전체에서 QoS(서비스 품질)를 적용하여 특정 기준에 따라 네트워크 트래픽의 우선 순위를 지정할 수 있습니다. 이 순위치는 구분된 서비스와 서비스 클래스의 두 가지 QoS를 지원합니다.

### 구분된 서비스

QoS 기능은 트래픽을 스트림으로 분류하고 정의된 출발 동작에 따라 특정 QoS를 처리할 수 있는 구분된 서비스(DiffServ)를 지원합니다.

### 서비스 클래스

CoS(서비스 클래스) 대기열 기능을 사용하면 스위치 대기열의 특정 부분을 직접 구성할 수 있습니다. 복잡한 DiffServ가 필요하지 않은 경우 네트워크 트래픽 유형별로 원하는 QoS 동작을 제공합니다.

## IPv4 멀티캐스트 기능

## DVMRP(Distance Vector Multicast Routing Protocol)

DVMRP는 탐침 패킷을 모든 DVMRP 사용 라우터와 교환하며, 양방향 인접 관계를 설정하고 인접 표를 구성합니다. 또한 멀티캐스트 라우팅 표를 생성하는 데 사용되는 보고서 패킷을 교환하고 유니캐스트 토폴로지 표를 만듭니다. 그런 다음 이 멀티캐스트 경로 표를 사용하여 멀티캐스트 패킷을 라우팅합니다.

## IGMP(Internet Group Management Protocol)

IGMP(Internet Group Management Protocol)는 IPv4 시스템(호스트 및 라우터)이 IP 멀티캐스트 그룹 멤버십을 인정한 멀티캐스트 라우터에 보고하는 데 사용됩니다. PowerConnect 6200은 IGMP 프로토콜의 "멀티캐스트 라우터 부분"을 수행합니다. 즉, 활성 멀티캐스트 라우팅에 필요한 멤버십 정보를 수집합니다.

## PIM-DM(Protocol Independent Multicast-Dense Mode)

PIM(Protocol Independent Multicast)은 특정 유니캐스트 라우팅 프로토콜에서 제공되는 메커니즘에 관계 없이 인터넷을 통해 확장 가능한 도메인 간 멀티캐스트 라우팅을 제공하는 표준 멀티캐스트 라우팅 프로토콜입니다. PIM-DM 프로토콜은 기존 유니캐스트 라우팅 표와 Join/Prune/Graft(연결/정리/결합) 메커니즘을 사용하여 트리를 작성합니다. PIM-DM은 RPF(Reverse Path Forwarding)를 사용하여 소스 기반 최단 경로 배포 트리를 생성합니다.

## PIM-SM(Protocol Independent Multicast-Sparse Mode)

PIM-SM을 사용하면 멀티캐스트 트래픽을 멀티캐스트 그룹으로 효과적으로 라우팅하여 WAN을 확장할 수 있지만, 대역폭이 제한됩니다. PIM-SM에서는 기본적으로 공유 트리를 사용하고 효율성을 위해 소스 기반 트리를 구현합니다. 이 데이터 임계값은 트리 간을 전환하는 데 사용됩니다.

## 스위치 관리 기능

### SNMP 경보 및 트랩 로그

심각도 코드 및 타임스탬프가 있는 시스템 로그 이벤트입니다. 이벤트는 트랩 수신자 목록에 SNMP 트랩으로 전송됩니다.

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

### 웹 기반 관리

모든 웹 브라우저에서 시스템을 관리할 수 있습니다. 스위치에는 시스템을 모니터링 및 구성하는 데 사용할 수 있는 HTML 페이지 역할을 하는 내부 웹 서버가 포함되어 있습니다.

### 구성 파일 다운로드

스위치의 구성 파일에는 시스템 전체 장치 구성 데이터와 포트별 장치 구성 데이터가 모두 포함되어 있습니다. CLI(Command-line Interface) 명령을 사용하여 구성 파일을 표시할 수 있습니다.

구성 파일 다운로드에 대한 자세한 내용은 "[파일 다운로드](#)"를 참조하십시오.

### 소프트웨어 다운로드

소프트웨어 다운로드를 백업 펌웨어 이미지 스토리지를 활성화합니다. 소프트웨어 다운로드에 대한 자세한 내용은 "[소프트웨어 다운로드 및 재부팅](#)"을 참조하십시오.

## TFTP(Trivial File Transfer Protocol)

PowerConnect 6200 시리즈는 TFTP를 통한 부트 이미지, 펌웨어 및 구성 업로드/다운로드를 지원합니다.

## RMON(Remote Monitoring)

RMON(Remote Monitoring)은 현재 및 기존의 MAC 계층 통계 및 제어 개체를 정의하는 표준 MIB로서 전체 네트워크에서 실시간 정보를 수집할 수 있도록 해줍니다.

## SNMP(Simple Network Management Protocol) 버전 1, 2 및 3

MIB(Management Information Base) 변수를 조합하여 시스템을 완벽하게 관리할 수 있습니다. 결합된 변수 값은 모든 시스템 상태를 나타내며, 또한 이러한 값을 조사 및 수정 가능한 SNMP를 나타냅니다. SNMP v1/v2c/v3 over the UDP/IP 전송 프로토콜이 지원됩니다.

## 명령줄 인터페이스

CLI(Command Line Interface) 구문 및 의미는 일반적인 업계 규정을 최대한 준수합니다. CLI는 필수 요소와 선택 요소로 구성됩니다. 문자열 도움말은 현재 명령에 허용되는 형식 및 값 범위를 제공하고, CLI 인터프리터는 명령 및 키워드를 완성합니다.

## Syslog

Syslog는 이벤트 알림을 원하는 원격 서버로 전송하여 저장, 조사 및 처리할 수 있도록 해주는 프로토콜입니다.

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

## SNTP

SNTP(Simple Network Time Protocol)를 사용하면 네트워크 스위치 클럭 시간을 밀리초까지 정확하게 동기화할 수 있습니다. 시간 동기화는 네트워크 SNTP 서버에서 수행됩니다.

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

## 보안 기능

### ACL(액세스 제어 목록)

ACL(액세스 제어 목록)을 사용하면 권한 있는 사용자만 특정 리소스에 액세스하도록 허용하고 네트워크 리소스에 연결하려는 무단 시도를 차단할 수 있습니다. ACL은 트래픽 흐름 제어를 제공하고, 라우팅 업데이트 내용을 제한하고, 전달 또는 차단할 트래픽 유형을 결정하고, 네트워크에 보안을 제공(가장 중요한 역할)하는 데 사용됩니다.

ACL 정의에 대한 자세한 내용은 "[IP ACL 구성](#)" 및 "[MAC ACL 구성](#)"을 참조하십시오.

### 포트 기반 인증(802.1x)

포트 기반 인증을 사용하면 외부 서버를 통해 포트 단위로 시스템 사용자를 인증할 수 있습니다. 인증되고 승인된 시스템 사용자만 데이터를 전송/수신할 수 있습니다. 포트는 RADIUS(Remote Authentication Dial In User Service) 서버에서 EAP(Extensible Authentication Protocol)를 사용하여 인증됩니다. PEAP, EAP-TTL, EAP-TTLS, EAP-TLS 등도 지원합니다.

### 잠긴 포트 지원

잠긴 포트 기능은 특정 MAC 주소에 있는 사용자만 포트에 액세스할 수 있도록 제한합니다. 이러한 주소는 수동으로 정의되거나 해당 포트에서 학습한 것입니다. 잠긴 포트에 프레임이 있으며 프레임 소스 MAC 주소가 해당 포트에 연결되지 않는 경우 보호 메커니즘이 호출됩니다.

잠긴 포트 보안 사용에 대한 자세한 내용은 "[포트 보안](#)"을 참조하십시오.

### 암호 관리 보안

암호 관리를 사용하면 네트워크 보안이 향상되고 암호 제어 기능이 강화됩니다. SSH, 텔넷, HTTP, HTTPS 및 SNMP 액세스를 위한 암호는 할당된 보안 기능입니다.

암호 관리에 대한 자세한 내용은 "[암호 관리](#)"를 참조하십시오.

### TACACS+

TACACS+는 스위치에 액세스하는 사용자 확인을 위한 중앙 집중식 보안을 제공합니다. TACACS+는 RADIUS 및 기타 인증 프로세스와의 일관성을 유지하면서 중앙 집중식 사용자 관리 시스템을 제공합니다.

### RADIUS 클라이언트

RADIUS는 사용자 이름, 암호, 계정 정보 등의 사용자별 인증 정보가 들어 있는 사용자 데이터베이스를 서버에서 유지 관리하는 클라이언트/서버 기반 프로토콜입니다.

### SSH/SSL

SSH(Secure Shell)는 장치로의 안전한 원격 연결을 제공하는 프로토콜입니다. 이 연결은 인바운드 텔넷 연결과 유사한 기능을 제공합니다.

SSL(Secure Sockets Layer) 프로토콜을 사용하면 두 스테이션 간의 암호화된 연결을 추출할 수 있습니다. 그런 연결은 보안되지 않은 연결을 사용하는 것과 실제로 차이가 없습니다.

---

## CLI 설명서

Dell PowerConnect 6200 시리즈에 대한 다른 자료로는 *CLI 참조 안내서*가 있습니다. 이 설명서에서는 스위치와 스택을 구성 및 관리하는 데 사용되는 CLI 명령에 대한 정보를 제공합니다. 또한 자세한 CLI 설명, 구문, 기본값 및 예제를 제공합니다.

---

[목록 페이지로 돌아가기](#)

[목차 페이지로 돌아가기](#)

## 연결 종속성 만들기

### Dell™ PowerConnect™ M6220 사용 설명서

#### ● [연결 종속성 요약](#)

연결 종속성 기능은 하나 이상의 다른 포트의 연결 상태에 따라 하나 이상의 포트를 활성화 또는 비활성화할 수 있는 기능입니다. 연결 종속성이 포트에 활성화되어 있으면 해당 포트의 연결 상태는 다른 포트의 연결 상태에 따라 달라집니다. 예를 들어, 포트 A는 포트 B에 따라 달라지는 상태에서 스위치가 포트 B의 연결 손실을 감지할 경우 스위치는 자동으로 포트 A의 연결을 종료합니다. 포트 B의 연결이 복구되면 스위치는 자동으로 포트 A의 연결을 복구합니다.

최대 16개의 종속성 그룹을 만들 수 있습니다. 연결 종속성에 참여하는 포트는 모든 스택 장치(관리자/구성원 장치)에서 사용할 수 있습니다.

연결 종속성 기능은 다음 시나리오를 지원합니다.

- 1 포트 간의 종속 — 포트 연결이 끊어질 경우 스위치가 다른 포트의 연결을 종료합니다.
- 1 LAG에 종속되는 포트 — 채널 그룹의 모든 포트의 연결이 끊어질 경우 스위치가 다른 포트의 연결을 종료합니다.
- 1 포트에 종속되는 LAG — 포트 연결이 끊어질 경우 스위치가 채널 그룹의 모든 연결을 종료합니다.
- 1 다중 포트 명령 — 포트의 그룹 연결이 끊어질 경우 스위치가 다른 포트 그룹의 연결을 종료합니다.
- 1 포트 검침 — 다른 그룹의 포트가 검침된 종속 포트가 모두 연결이 끊어질 경우에만 종료됩니다.

Link Dependency(연결 종속성) 메뉴 페이지에는 [연결 종속성 요약](#) 페이지의 링크가 포함되어 있습니다.

## 연결 종속성 요약

Link Dependency Summary(연결 종속성 요약) 페이지를 사용하여 시스템의 모든 연결 종속성을 검토하고 Link Dependency Configuration(연결 종속성 구성) 페이지를 액세스합니다. 최대 16개의 종속성 그룹을 만들 수 있습니다. 페이지에 해당 그룹의 구성 여부가 표시됩니다.

Link Dependency Summary(연결 종속성 요약) 페이지를 표시하려면 디렉터리 화면에서 Switching(스위칭) → Link Dependency(연결 종속성) → Link Dependency Summary(연결 종속성 요약)를 클릭합니다.

그림 8-1. Link Dependency Summary(연결 종속성 요약)

| Group ID | Member Ports    | Ports Depended On | Remove                                          |
|----------|-----------------|-------------------|-------------------------------------------------|
| 1        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 2        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 3        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 4        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 5        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 6        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 7        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 8        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 9        | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 10       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 11       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 12       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 13       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 14       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 15       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |
| 16       | Not configured. | Not configured.   | <input type="checkbox"/> <a href="#">Modify</a> |

Link Dependency Summary(연결 종속성 요약) 페이지에는 다음 필드가 포함되어 있습니다.

Group ID(그룹 ID) — 그룹의 ID 번호입니다.

Member Ports(구성원 포트) — 해당 그룹에 속하는 구성원 포트 목록입니다.

Ports Depended On(종속 대상 포트) — 그룹이 종속하는 포트 목록입니다.

Remove(제거) — 그룹의 구성을 제거하기 위한 확인란입니다.

Modify(수정) — 그룹의 구성을 수정하기 위한 링크입니다. Modify(수정) 링크를 클릭하여 해당 그룹에 대한 구성을 액세스합니다.

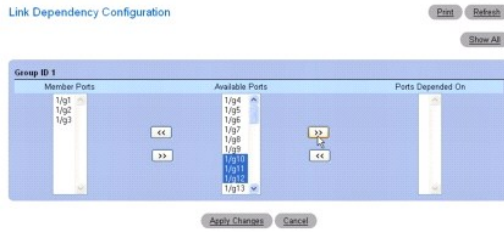
## 연결 종속성 그룹 수정

1. Link Dependency Summary(연결 종속성 요약) 페이지를 엽니다.

2. 구성할 연결 종속성 그룹에 대한 그룹 ID 행에서 **Modify(수정)** 링크를 클릭합니다.

Link Dependency Group Configuration(연결 종속성 그룹 구성) 페이지가 표시됩니다.

그림 8-2. Link Dependency Group Configuration(연결 종속성 그룹 구성)



3. **Member Ports(구성원 포트)** 열에 포트를 추가하려면 **Available Ports(사용 가능한 포트)** 열에서 해당 포트를 클릭한 다음 **Available Ports(사용 가능한 포트)** 열 왼쪽의 << 단추를 클릭합니다. 포트를 여러 개 선택하려면 Ctrl 키를 누른 상태에서 마우스를 클릭합니다.
4. **Ports Depended On(종속 대상 포트)** 열에 포트를 추가하려면 **Available Ports(사용 가능한 포트)** 열에서 해당 포트를 클릭한 다음 **Available Ports(사용 가능한 포트)** 열 오른쪽의 >> 단추를 클릭합니다.
5. **Apply Changes(변경사항 적용)**를 클릭합니다.  
그룹의 연결 종속성 설정이 수정되고 해당 장치가 업데이트됩니다.
6. **Link Dependency Summary(연결 종속성 요약)** 페이지를 반환하려면 **Show All(모두 표시)**을 클릭합니다.

### 연결 종속성 그룹에서 모든 포트 제거

1. **Link Dependency Summary(연결 종속성 요약)** 페이지를 엽니다.
2. 제거할 연결 종속성 그룹에 대한 그룹 ID 행에서 **Remove(제거)** 확인란을 선택합니다.
3. **Apply Changes(변경사항 적용)**를 클릭합니다.  
연결 종속성 그룹에서 모든 포트가 제거되고 해당 장치가 업데이트됩니다.

### CLI 명령으로 연결 종속성 그룹 구성

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 연결 종속성 명령

---

[목차 페이지로 돌아가기](#)



[목차 페이지로 돌아가기](#)

## Dell™ PowerConnect™ M6220 사용 설명서



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



**주의사항:** "주의사항"은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.



**주의:** "주의"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 나타냅니다.

**본 설명서에 수록된 정보는 사전 통보 없이 변경될 수 있습니다.  
© 2007 Dell Inc. 저작권 본사 소유.**

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

본 설명서에 사용된 상표인 Dell, Dell OpenManage, DELL 로고, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet 및 Latitude는 Dell Inc.의 상표이며, Microsoft, Windows 및 Windows Vista는 미국 및 기타 국가에서 Microsoft Corporation의 상표 또는 등록 상표입니다. Procomm Plus는 미국 및 기타 국가에서 Symantec Corporation 또는 계열 회사의 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 상표 이름에 대한 어떠한 소유권도 보유하지 않습니다.

모델 M6220

2007년 9월 Rev. A00

---

[목차 페이지로 돌아가기](#)

[목록 페이지로 돌아가기](#)

## 통계/RMON 보기


### Dell™ PowerConnect™ M6220 사용 설명서

- [표 보기](#)
- [RMON](#)
- [차트](#)

원격 모니터링(RMON)을 사용하면 네트워크 관리자는 원격 액세스를 통해 네트워크 성능 및 상태에 대한 정보를 얻을 수 있습니다. RMON 표준의 일부로 정의된 4개의 모니터링 그룹(통계, 기록, 경고 및 이벤트)이 지원됩니다.

이 절에서는 **Statistics/RMON(통계/RMON)** 메뉴 페이지에서 사용 가능한 RMON 옵션에 대해 설명합니다. 이러한 옵션에는 표 형식으로 통계 보기, RMON 통계 편집 및 보기와 포트 및 LAG 통계 차트가 포함됩니다. **Statistics/RMON(통계/RMON)** 메뉴 페이지에서는 다음 메뉴 페이지를 통해 이러한 옵션에 대한 액세스를 제공합니다.

- 1 [표 보기](#)
- 1 [RMON](#)
- 1 [차트](#)

 **주:** CLI 명령은 일부 Statistics/RMON(통계/RMON) 페이지에서 사용할 수 없습니다.

## 표 보기

**Table Views(표 보기)** 메뉴 페이지에는 표 형식으로 통계를 표시하는 웹 페이지에 대한 링크가 포함되어 있습니다. 이 페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→Table Views(표 보기)**를 클릭합니다. 이 메뉴 페이지에서 액세스 가능한 웹 페이지는 다음과 같습니다.

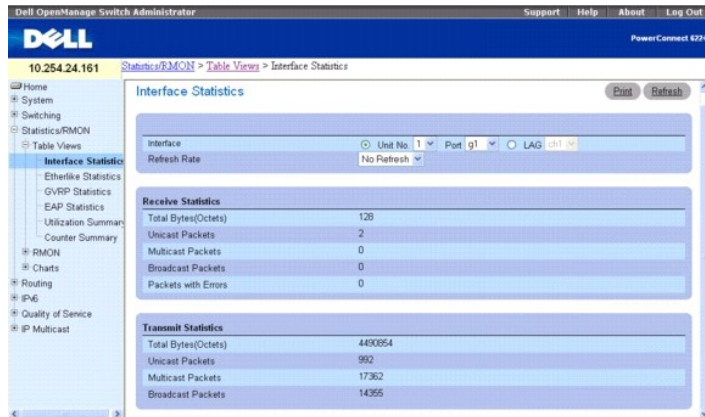
- 1 [인터페이스 통계](#)
- 1 [Etherlike 통계](#)
- 1 [GVRP 통계](#)
- 1 [EAP 통계](#)
- 1 [사용 요약](#)
- 1 [카운터 요약](#)

## 인터페이스 통계

**Interface Statistics(인터페이스 통계)** 페이지를 사용하여 수신 및 전송된 패킷 모두에 대한 통계를 표시합니다. 수신 및 전송된 패킷 모두에 대한 필드는 동일합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→Table Views(표 보기)→Interface Statistics(인터페이스 통계)**를 클릭합니다.

그림 9-1. 인터페이스 통계



**Interface Statistics(인터페이스 통계)** 페이지에는 다음 필드가 포함되어 있습니다.

**Interface(인터페이스)** — 통계를 표시할 물리적 인터페이스(장치, 포트) 또는 LAG 인터페이스를 선택합니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

## 수신된 통계

**Total Bytes (Octets)(전체 바이트(옥텟))** — 선택한 인터페이스에서 수신된 전체 옥텟 수를 표시합니다.

**Unicast Packets(유니캐스트 패킷)** — 선택한 인터페이스에서 수신된 전체 유니캐스트 패킷 수를 표시합니다.

**Multicast Packets(멀티캐스트 패킷)** — 선택한 인터페이스에서 수신된 전체 멀티캐스트 패킷 수를 표시합니다.

**Broadcast Packets(브로드캐스트 패킷)** — 선택한 인터페이스에서 수신된 전체 브로드캐스트 패킷 수를 표시합니다.

**Packets with Errors(오류가 있는 패킷)** — 선택한 인터페이스에서 수신된 오류가 있는 전체 패킷 수를 표시합니다.

## 전송 통계

**Total Bytes (Octets)(전체 바이트(옥텟))** — 선택한 인터페이스에서 송신한 전체 옥텟 수를 표시합니다.

**Unicast Packets(유니캐스트 패킷)** — 선택한 인터페이스에서 송신한 전체 유니캐스트 패킷 수를 표시합니다.

**Multicast Packets(멀티캐스트 패킷)** — 선택한 인터페이스에서 송신한 전체 멀티캐스트 패킷 수를 표시합니다.

**Broadcast Packets(브로드캐스트 패킷)** — 선택한 인터페이스에서 송신한 전체 브로드캐스트 패킷 수를 표시합니다.

## 인터페이스 통계 표시

1. **Interface Statistics(인터페이스 통계)** 페이지를 엽니다.

2. 인터페이스를 지정합니다.

지정된 인터페이스에 대한 통계를 표시합니다.

## CLI 명령을 사용하여 인터페이스 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

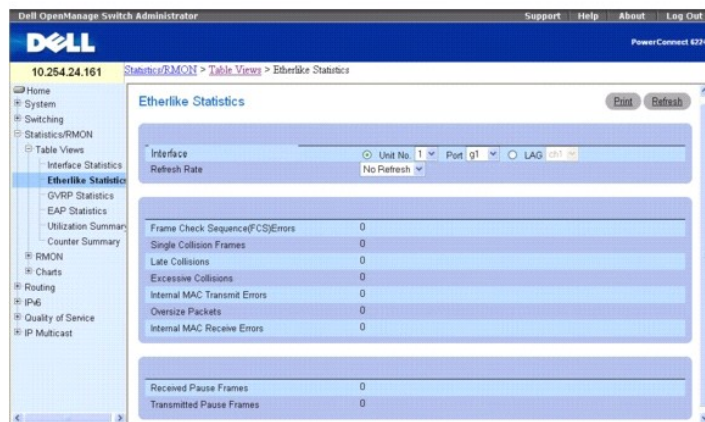
- 1 이더넷 구성 명령

## Etherlike 통계

**Etherlike Statistics(Etherlike 통계)** 페이지를 사용하여 인터페이스 통계를 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→ Table Views(표 보기)→ Etherlike Statistics(Etherlike 통계)**를 클릭합니다.

그림 9-2. Etherlike 통계



**Etherlike Statistics(Etherlike 통계)** 페이지에는 다음 필드가 포함되어 있습니다.

**Interface(인터페이스)** — 통계를 표시할 물리적 인터페이스(장치, 포트) 또는 LAG 인터페이스를 선택합니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

**Frame Check Sequence (FCS) Errors(프레임 점검 시퀀스(FCS) 오류)** — 선택한 인터페이스에서 수신된 FCS 오류 수를 표시합니다.

**Signal Collision Frames(신호 충돌 프레임)** — 선택한 인터페이스에서 수신된 신호 충돌 프레임 오류 수를 표시합니다.

**Late Collisions(최종 충돌)** — 선택한 인터페이스에서 수신된 최종 충돌 수를 표시합니다.

**Excessive Collisions(과도한 충돌)** — 선택한 인터페이스에서 수신된 과도한 충돌 수를 표시합니다.

**Internal MAC Transmit Errors(내부 MAC 전송 오류)** — 선택한 인터페이스에서의 내부 MAC 전송 오류 수를 표시합니다.

**Oversize Packets(크기 초과 패킷)** — 1518옥테트(프레이밍 비트 제외, FCS 옥텟 포함)보다 길지만 올바른 형식으로 수신된 총 패킷 수를 표시합니다.

**Internal MAC Receive Errors(내부 MAC 수신 오류)** — 선택한 인터페이스에서의 내부 MAC 수신 오류 수를 표시합니다.

**Received Pause Frames(수신된 일시 중지 프레임)** — 선택한 인터페이스에서 수신된 일시 중지된 프레임 수를 표시합니다.

**Transmitted Pause Frames(전송된 일시 중지 프레임)** — 선택한 인터페이스에서 전송된 일시 중지된 프레임 수를 표시합니다.

## 인터페이스의 Etherlike 통계 표시

1. Etherlike Statistics(Etherlike 통계) 페이지를 엽니다.
2. 인터페이스를 지정합니다.

지정된 인터페이스에 대한 통계가 표시됩니다.

## GVRP 통계

**GVRP Statistics(GVRP 통계)** 페이지를 사용하여 GVRP의 스위치 통계를 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON) → Table Views(표 보기) → GVRP Statistics(GVRP 통계)**를 클릭합니다.

그림 9-3. GVRP 통계

| GVRP Statistics Table Attribute(Counter) |  | Received | Transmitted |
|------------------------------------------|--|----------|-------------|
| Join Empty                               |  | 0        | 0           |
| Empty                                    |  | 0        | 0           |
| Leave Empty                              |  | 0        | 0           |
| Join In                                  |  | 0        | 0           |
| Leave In                                 |  | 0        | 0           |
| Leave All                                |  | 0        | 0           |

| Error Statistics        |  | Received |
|-------------------------|--|----------|
| Invalid Protocol ID     |  | 0        |
| Invalid Attribute Type  |  | 0        |
| Invalid Attribute Value |  | 0        |

**GVRP Statistics(GVRP 통계)** 페이지에는 다음 필드가 포함되어 있습니다.

**Interface(인터페이스)** — 통계를 표시할 물리적 인터페이스(장치, 포트) 또는 LAG 인터페이스를 선택합니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

## GVRP 통계 표 속성(카운터) - 수신 및 전송

**Join Empty(빈 항목 연결)** — GVRP 빈 항목 연결 스위치 통계를 표시합니다.

**Empty(빈 항목)** — GVRP 빈 항목 스위치 통계를 표시합니다.

**Leave Empty(빈 항목으로 두기)** — GVRP 빈 항목으로 두기 스위치 통계를 표시합니다.

Join In(연결) — GVRP 연결 스위치 통계를 표시합니다.

Leave In(그대로 두기) — GVRP 그대로 두기 스위치 통계를 표시합니다.

Leave All(모두 그대로 두기) — GVRP 모두 그대로 두기 스위치 통계를 표시합니다.

오류 통계 - 수신

Invalid Protocol ID(잘못된 프로토콜 ID) — GVRP 잘못된 프로토콜 ID 스위치 통계를 표시합니다.

Invalid Attribute Type(잘못된 속성 유형) — GVRP 잘못된 속성 유형 스위치 통계를 표시합니다.

Invalid Attribute Value(잘못된 속성 값) — GVRP 잘못된 속성 값 스위치 통계를 표시합니다.

Invalid Attribute Length(잘못된 속성 길이) — GVRP 잘못된 속성 길이 스위치 통계를 표시합니다.

Invalid Event(잘못된 이벤트) — GVRP 잘못된 이벤트 스위치 통계를 표시합니다.

### 인터페이스에 대한 GVRP 통계 표시

1. GVRP Statistics(GVRP 통계) 페이지를 엽니다.
2. Interface(인터페이스) 필드에서 인터페이스를 선택합니다.

지정된 인터페이스에 대해 GVRP 통계가 표시됩니다.

### CLI 명령을 사용하여 GVRP 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

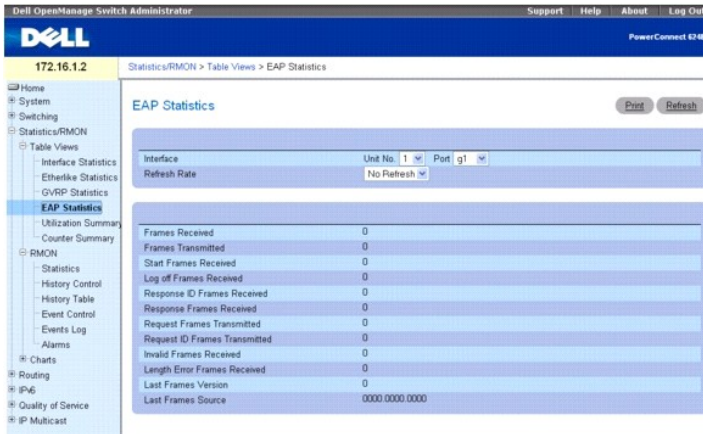
1. GVRP 명령

### EAP 통계

EAP Statistics(EAP 통계) 페이지를 사용하여 특정 포트에서 수신되는 EAP 패킷에 대한 정보를 표시합니다. EAP에 대한 자세한 내용은 "포트 기반 인증"을 참조하십시오.

EAP Statistics(EAP 통계) 페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON) → Table Views(표 보기) → EAP Statistics(EAP 통계)를 클릭합니다 .

그림 9-4. EAP 통계



Interface(인터페이스) — 통계를 위해 폴링된 인터페이스를 지정합니다.

Refresh Rate(재생률) — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

Frames Received(프레임 수신) — 포트에서 수신된 유효한 EAPOL 프레임 수를 표시합니다.

Frames Transmit(프레임 전송) — 포트를 통해 전송된 EAPOL 프레임 수를 표시합니다.

Start Frames Received(시작 프레임 수신) — 포트에서 수신된 EAPOL 시작 프레임 수를 표시합니다.

Log off Frames Received(로그 오프 프레임 수신) — 포트에서 수신된 EAPOL 로그 오프 프레임 수를 표시합니다.

Respond ID Frames Received(응답 ID 프레임 수신) — 포트에서 수신된 EAP 응답 ID 프레임 수를 표시합니다.

Respond Frames Received(응답 프레임 수신) — 포트에서 수신된 유효한 EAP 응답 프레임 수를 표시합니다.

Request ID Frames Received(요청 ID 프레임 수신) — 포트에서 수신된 EAP 요청 ID 프레임 수를 표시합니다.

Request Frames Transmitted(요청 프레임 전송) — 포트를 통해 전송된 EAP 요청 프레임 수를 표시합니다.

Request Frames Transmitted(요청 프레임 전송) — 포트를 통해 전송된 EAP 요청 ID 프레임 수를 표시합니다.

Invalid Frames Received(잘못된 프레임 수신) — 이 포트에서 수신된 인식되지 않은 EAPOL 프레임 수를 표시합니다.

Length Error Frames Receive(길이 오류 프레임 수신) — 이 포트에서 수신된 잘못된 패킷 본문 길이를 가진 EAPOL 프레임 수를 표시합니다.

Last Frames Version(최신 프레임 버전) — 가장 최근에 수신된 EAPOL 프레임에 연결된 프로토콜 버전 번호를 표시합니다.

Last Frames Source(최신 프레임 소스) — 가장 최근에 수신된 EAPOL 프레임에 연결된 소스 MAC 주소를 표시합니다.

### 인터페이스에 대한 EAP 통계 표시

1. EAP Statistics(EAP 통계) 페이지를 엽니다.
2. Interface(인터페이스) 필드에서 인터페이스를 선택합니다.

선택된 인터페이스에 대한 EAP 통계가 표시됩니다.

### CLI 명령을 사용하여 EAP 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

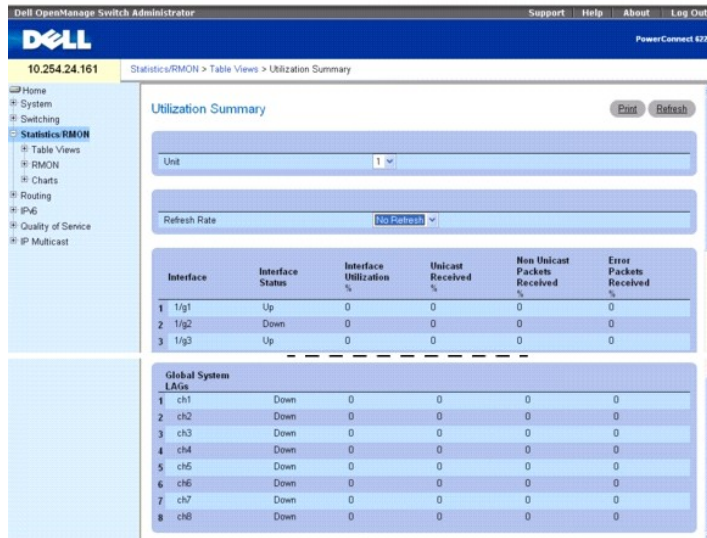
- 1 802.1X 명령

### 사용 요약

Utilization Summary(사용 요약) 페이지를 사용하여 인터페이스 사용 통계를 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON) → Table Views(표 보기) → Utilization Summary(사용 요약)**를 클릭합니다.

그림 9-5. 사용 요약



Utilization Summary(사용 요약) 페이지에는 다음 필드가 포함되어 있습니다.

Unit(장치) — 통계를 표시할 장치를 지정합니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

**Interface(인터페이스)** — 통계를 표시할 인터페이스를 지정합니다.

**Interface Status(인터페이스 상태)** — 인터페이스 상태를 표시합니다.

**Interface Utilization % (인터페이스 사용률(%))** — 인터페이스의 이중 모드를 기반으로 네트워크 인터페이스 사용률(%)을 표시합니다. 이 값의 범위는 0 ~ 200%입니다. 전이 중 연결의 최대 측정값 200%는 수신 및 송신 연결의 100% 대역폭이 인터페이스를 통해 전달되는 트래픽에 의해 사용됨을 표시합니다. 반이중 연결의 최대 측정값은 100%입니다.

**Unicast Received % (유니캐스트 수신율(%))** — 인터페이스에서 수신된 유니캐스트 패킷의 백분율을 표시합니다.

**Non Unicast Packets Received % (비유니캐스트 패킷 수신율(%))** — 인터페이스에서 수신된 비유니캐스트 패킷의 백분율을 표시합니다.

**Error Packets Received % (오류 패킷 수신율)** — 인터페이스에서 수신된 오류가 있는 패킷 수를 표시합니다.

## CLI 명령을 사용하여 인터페이스 사용 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. RMON 명령

## 카운터 요약

**Counter Summary(카운터 요약)** 페이지를 사용하여 백분율이 아닌 숫자 합계로 인터페이스 사용 통계를 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)** → **Table Views(표 보기)** → **Counter Summary(카운터 요약)**를 클릭합니다.

그림 9-6. 카운터 요약

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'Counter Summary' page. At the top, there are fields for 'Unit' (set to 1) and 'Refresh Rate' (set to 'No Refresh'). Below these is a table with columns: Interface, Interface Status, Received Unicast Packets, Transmit Unicast Packets, Received Non Unicast Packets, Transmit Non Unicast Packets, Received Errors, and Transmit Errors. The table lists three interfaces: 1/g1 (Up), 2/g2 (Down), and 3/g3 (Down). Below this table is a section for 'Global System LAGs' with a table listing LAGs from ch1 to ch8, all of which are Down.

| Interface | Interface Status | Received Unicast Packets | Transmit Unicast Packets | Received Non Unicast Packets | Transmit Non Unicast Packets | Received Errors | Transmit Errors |
|-----------|------------------|--------------------------|--------------------------|------------------------------|------------------------------|-----------------|-----------------|
| 1/g1      | Up               | 6639523                  | 6339                     | 365892                       | 133900                       | 0               | 0               |
| 2/g2      | Down             | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 3/g3      | Down             | 0                        | 0                        | 0                            | 0                            | 0               | 0               |

| LAG   | Status | Received Unicast Packets | Transmit Unicast Packets | Received Non Unicast Packets | Transmit Non Unicast Packets | Received Errors | Transmit Errors |
|-------|--------|--------------------------|--------------------------|------------------------------|------------------------------|-----------------|-----------------|
| 1 ch1 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 2 ch2 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 3 ch3 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 4 ch4 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 5 ch5 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 6 ch6 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 7 ch7 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |
| 8 ch8 | Down   | 0                        | 0                        | 0                            | 0                            | 0               | 0               |

**Counter Summary(카운터 요약)** 페이지에는 다음 필드가 포함되어 있습니다.

**Unit(장치)** — 통계를 표시할 장치를 지정합니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.

**Interface(인터페이스)** — 통계를 표시할 인터페이스를 지정합니다.

**Interface Status(인터페이스 상태)** — 인터페이스 상태를 표시합니다.

**Received Unicast Packets(수신된 유니캐스트 패킷)** — 인터페이스에서 수신된 유니캐스트 패킷 수를 표시합니다.

**Transmit Unicast Packets(전송된 유니캐스트 패킷)** — 인터페이스에서 전송된 유니캐스트 패킷 수를 표시합니다.

**Received Non Unicast Packets(수신된 비유니캐스트 패킷)** — 인터페이스에서 수신된 비유니캐스트 패킷 수를 표시합니다.

**Transmit Non Unicast Packets(전송된 비유니캐스트 패킷)** — 인터페이스에서 전송된 비유니캐스트 패킷 수를 표시합니다.

**Received Errors(수신된 오류)** — 인터페이스에서 수신된 오류 수를 표시합니다.



Transmit Errors(전송된 오류) — 인터페이스에서 전송된 오류 수를 표시합니다.

## 재생을 설정

1. Counter Summary(카운터 요약) 페이지를 엽니다.
2. 드롭다운 메뉴에서 Refresh Rate(재생률)를 선택합니다.  
표시된 인터페이스에 대한 통계가 선택한 주기에 재생됩니다.

## CLI 명령을 사용하여 숫자 포트 사용 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

1. RMON 명령

## RMON

원격 모니터링(RMON)을 사용하면 네트워크 관리자는 원격 액세스를 통해 네트워크 성능 및 상태에 대한 정보를 얻을 수 있습니다.

RMON 메뉴 페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON)→RMON을 클릭합니다. RMON 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

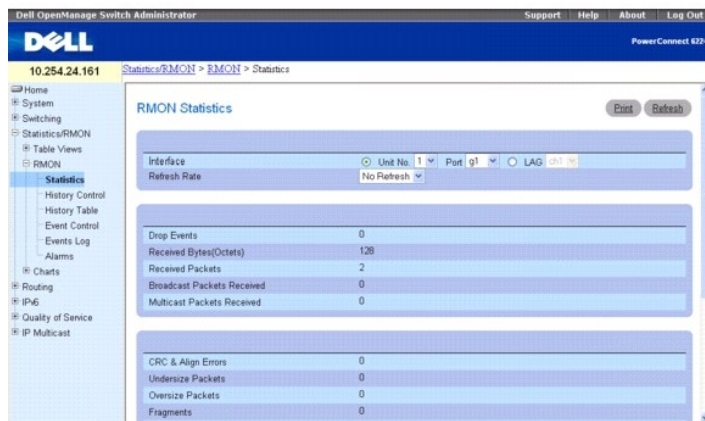
1. [RMON 통계](#)
1. [RMON 기록 제어 통계](#)
1. [RMON 기록 표](#)
1. [RMON 이벤트 제어](#)
1. [RMON 이벤트 로그](#)
1. [RMON 경고](#)

## RMON 통계

RMON Statistics(RMON 통계) 페이지를 사용하여 패킷 처리 통계 및 스위치에서 발생된 오류와 같은 스위치 사용에 대한 세부사항을 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON)→RMON→Statistics(통계)를 클릭합니다.

그림 9-7. RMON 통계



RMON Statistics(RMON 통계) 페이지에는 다음 필드가 포함되어 있습니다.

Interface(인터페이스) — 단위/LAG 표시 여부 뿐만 아니라 단위 또는 LAG에 대한 통계 표시 여부를 지정합니다.

Refresh Rate(재생률) — 통계를 재생하는 간격을 지정합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 No Refresh(재생 안 함)입니다.



**Drop Events(드롭 이벤트)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 발생한 드롭 이벤트 수를 표시합니다.

**Received Bytes (Octets)(수신된 바이트(옥텟))** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 옥텟 수를 표시합니다. 이 값에는 불량 패킷 및 FCS 옥텟은 포함되지 않 프레임 비트는 제외됩니다.

**Received Packets(수신된 패킷)** — 스위치가 마지막으로 재생된 이후 불량 패킷, 멀티캐스트 및 브로드캐스트 패킷을 포함하여 인터페이스에서 수신된 패킷 수를 표시합니다.

**Broadcast Packets Received(수신된 브로드캐스트 패킷)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 양호한 브로드캐스트 패킷 수를 표시합니다. 멀티캐스트 패킷은 이 값에 포함되지 않습니다.

**Multicast Packets Received(수신된 멀티캐스트 패킷)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 양호한 멀티캐스트 패킷 수를 표시합니다.

**CRC & Align Errors(CRC 및 정렬 오류)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 발생한 CRC 및 정렬 오류 수를 표시합니다.

**Undersize Packets(크기 부족 패킷)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 크기 부족 패킷(64 옥텟 이하) 수를 표시합니다.

**Oversize Packets(크기 초과 패킷)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 크기 초과 패킷(1518옥텟 이상) 수를 표시합니다.

**Fragments(조각)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 조각(프레이밍 비트 제외, FCS 옥텟 포함, 64옥텟 이하의 패킷) 수를 표시합니다.

**Jabbers(재버)** — 샘플링 세션 동안 1518옥텟 이상의 길이이며 FCS를 가진 수신 패킷 수를 표시합니다.

**Collisions(충돌)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 충돌 수를 표시합니다.

**Frames of 64Bytes(64바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 64 바이트 프레임 수를 표시합니다.

**Frames of 65 to 127 Bytes(65 - 127바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 65 - 127바이트 프레임 수를 표시합니다.

**Frames of 128 to 255 Bytes(128 - 255 바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 128- 255바이트 프레임 수를 표시합니다.

**Frames of 256 to 511 Bytes(256 - 511 바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 256 - 511바이트 프레임 수를 표시합니다.

**Frames of 512 to 1023 Bytes(512 - 1023 바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 512 - 1023바이트 프레임 수를 표시합니다.

**Frames of 1024 to 1518 Bytes(1024 - 1518 바이트 프레임)** — 스위치가 마지막으로 재생된 이후 인터페이스에서 수신된 1024 - 1518바이트 프레임 수를 표시합니다.

## 인터페이스 통계 보기

1. **RMON Statistics Group(RMON 통계 그룹)** 페이지를 엽니다.
2. **Interface(인터페이스)** 필드에서 인터페이스를 선택합니다.

선택된 인터페이스에 대한 통계가 표시됩니다.

## CLI 명령을 사용하여 RMON 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

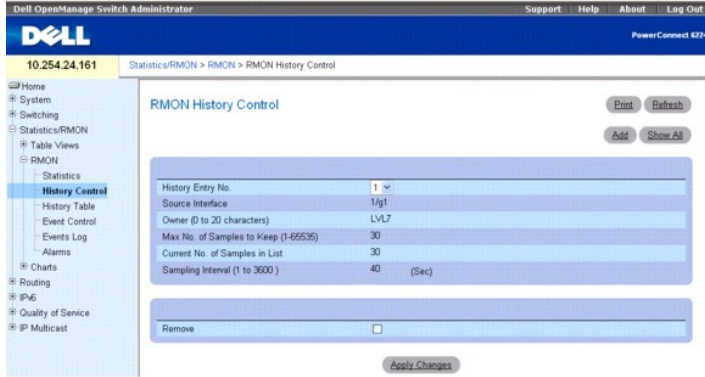
- 1 RMON 명령

## RMON 기록 제어 통계

**RMON History Control(RMON 기록 제어)** 페이지를 사용하여 각 포트에 대한 통계 기록을 관리합니다. 각 인터페이스(물리적 포트 또는 포트 채널)에 대해 존재하는 버킷 수 및 각 버킷 스냅샷 간의 시간 간격을 정의할 수 있습니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→RMON→History Control(기록 제어)**을 클릭합니다.

그림 9-8. RMON 기록 제어



RMON History Control(기록 제어) 페이지에는 다음 필드가 포함되어 있습니다.

History Entry(기록 항목) — RMON History Control(기록 제어) 표에서 항목 번호를 선택합니다.

Source Interface(소스 인터페이스) — 가져온 기록 샘플에서 인터페이스를 지정합니다.

Owner (0-20 characters)(소유자(0-20자)) — RMON 스테이션 또는 RMON 정보를 요청한 사용자를 표시합니다.

Max No. of Samples to Keep (1-65535)(보존할 최대 샘플 수(1-65535)) — 이 인터페이스에 대한 기록 버킷 수를 설정합니다.

Current No. of Samples in List(목록에서 현재 샘플 번호) — 가져온 샘플의 현재 번호를 표시합니다.

Sampling Interval (1-3600)(샘플링 간격(1-3600)) — 포트에서 샘플링을 가져올 주기를 설정합니다. 유효한 값은 1 ~ 3600초입니다. 기본값은 1800초(30분)입니다.

Remove(제거) — 선택한 경우 표시되는 RMON History Control Table(기록 제어) 표 항목을 제거합니다.

## 기록 제어 항목 추가

1. RMON History Control(RMON 기록 제어) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add History Entry(기록 항목 추가) 페이지가 표시됩니다.

그림 9-9. 기록 항목 추가



3. 이 페이지의 필드를 완료하고 Apply Changes(변경사항 적용)를 클릭합니다.

항목이 RMON History Control(기록 제어) 표에 추가됩니다.

## RMON 기록 제어 표 표시

1. RMON History Control(RMON 기록 제어) 페이지를 엽니다.
2. Show All(모두 표시)를 클릭합니다.

RMON History Control(기록 제어) 표가 표시됩니다.

그림 9-10. RMON 기록 제어 표

History Control Table Print Refresh

| History Entry No. | Source Interface | Sampling Interval | Current Number of Samples | Owner | Remove                   |
|-------------------|------------------|-------------------|---------------------------|-------|--------------------------|
| 1                 | 1/g1             | 1000              | 10                        |       | <input type="checkbox"/> |

Apply Changes Back

## 기록 제어 표 항목 제거

1. RMON History Control(RMON 기록 제어) 페이지를 엽니다.
  2. 기록 항목의 행에서 Remove(제거) 확인란을 선택하여 제거합니다.
  3. Apply Changes(변경사항 적용)를 클릭합니다.
- 표 항목이 제거되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 RMON 기록 제어 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 RMON 명령

## RMON 기록 표

RMON History Table(RMON 기록 표) 페이지를 사용하여 인터페이스별 통계 네트워크 샘플링을 표시합니다. 각 표 항목은 단일 샘플링 시 모든 카운터 값을 표시합니다.

RMON History Table(RMON 기록 표) 페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON)→RMON→History Table(기록 표)을 클릭합니다.

그림 9-11. RMON 기록 표

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'RMON History Table' configuration page. At the top, there are 'Print' and 'Refresh' buttons. Below that, a configuration table is shown with the following values: History Entry No. 3, Owner RTP, Source Interface 1/g1, Max No. of Samples to Keep 15, and Sampling Interval 45 (sec). Below the configuration table is a data table with the following columns: Sample Drop No., Events, Received Bytes (Octets), Received Packets, Broadcast Packets, Multicast Packets, CRC Align Errors, Undersize Packets, Oversize Packets, Fragments, Jabbers, Collisions, and Utilization. The data row shows: 1, 0, 40595, 210, 42, 13, 0, 0, 0, 0, 0, 0, 0, 0.

RMON History Table(RMON 기록 표) 페이지에는 다음 필드가 포함되어 있습니다.

**History Entry No.(기록 항목 번호)** — RMON 기록 표 에 표시할 기록 항목 번호를 선택합니다.

**Owner(소유자)** — 사용 가능한 경우 RMON 통계 그룹 소유자 이름을 표시합니다.

**Source Interface(소스 인터페이스)** — 통계를 수집 중인 인터페이스 또는 LAG를 표시합니다.

**Max No. of Samples to Keep(보존할 최대 샘플 수)** — 각 기록 항목 번호마다 기록 표의 목록 길이를 결정합니다.

**Sampling Interval(샘플링 간격)** — 연속 샘플 간의 시간(초)을 설정합니다.

**Sample No.(샘플 번호)** — 표의 정보가 적용되는 특정 샘플을 표시합니다.

**Drop Events(드롭 이벤트)** — 자원 부족으로 인해 포트에 의해 패킷이 드롭된 전체 이벤트 수를 표시합니다. 이 값은 반드시 드롭된 패킷 수는 아니며 이 조건이 감지된 횟수일 뿐입니다.

**Received Bytes (Octets)(수신된 바이트(옥텟))** — 네트워크에서 수신된 데이터(불량 패킷의 데이터 포함)의 전체 옥텟 수를 표시합니다(프레이밍 비트 제외, 프레임 정경 시퀀스(FCS) 옥텟 포함).

**Received Packets(수신된 패킷)** — 샘플링 간격 동안 수신된 전체 패킷 수(불량 패킷, 브로드캐스트 패킷 및 멀티캐스트 패킷 포함)를 표시합니다.

**Broadcast Packets(브로드캐스트 패킷)** — 브로드캐스트 주소로 전달된 양호한 전체 수신 패킷 수를 표시합니다. 멀티캐스트 패킷은 포함되지 않습니다.

**Multicast Packets(멀티캐스트 패킷)** — 멀티캐스트 주소로 전달된 양호한 전체 수신 패킷 수를 표시합니다. 브로드캐스트 주소로 전달된 패킷은 이 값에 포함되지 않습니다.

**CRC Align Errors(CRC 정렬 오류)** — 64 ~ 1518옥텟 사이의 길이(프레이밍 비트 제외, FCS 옥텟 포함)이고 정수 옥텟의 불량 FCS(FCS 오류) 또는 비정수 옥텟의 불량 FCS(정렬 오류)를 가진 전체 수신 패킷 수를 표시합니다.

**Undersize Packets(크기 부족 패킷)** — 64옥텟(프레이밍 비트 제외, FCS 옥텟 포함)보다 짧지만 올바른 형식으로 수신된 전체 수신 패킷 수를 표시합니다.

**Oversize Packets(크기 초과 패킷)** — 1518옥텟(프레이밍 비트 제외, FCS 옥텟 포함)보다 길지만 올바른 형식으로 수신된 총 패킷 수를 표시합니다.

**Fragments(조각)** — 64옥텟(프레이밍 비트 제외, 정수 옥텟의 불량 FCS(FCS 오류) 또는 비정수 옥텟의 불량 FCS(정렬 오류) 포함)보다 짧은 전체 수신 패킷 수를 표시합니다.

**Jabbers(재버)** — 1518옥텟(프레이밍 비트 제외, FCS 옥텟 포함)보다 길고 정수 옥텟의 불량 프레임 정경 시퀀스(FCS)(FCS 오류) 또는 비정수 옥텟의 불량 FCS(정렬 오류)를 가진 전체 수신 패킷 수를 표시합니다.

**Collisions(충돌)** — 이 이더넷 세그먼트의 총 충돌 수를 가장 적절하게 측정된 값을 표시합니다.

**Utilization(사용)** — 세션 샘플링 동안 인터페이스에서 기본 물리 층 네트워크 사용을 측정합니다. 값은 100분의 1%로 표시됩니다.

## 특정 기록 항목에 대한 통계 보기

1. **RMON History Table(RMON 기록 표)** 페이지를 엽니다.
2. **History Entry No.(기록 항목 번호)** 필드에서 항목을 선택합니다.

항목 통계가 화면에 표시됩니다.

## CLI 명령을 사용하여 RMON 기록 제어 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

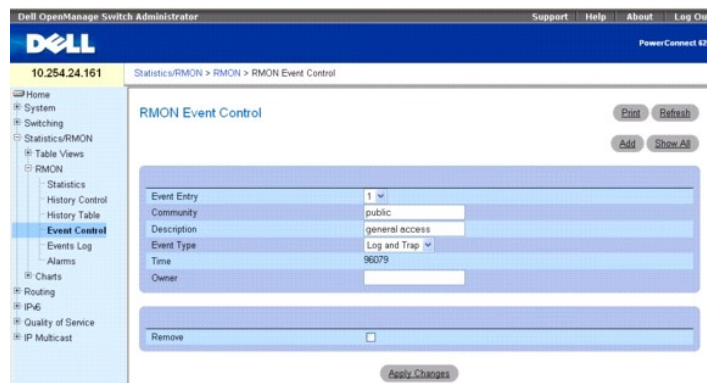
- 1 RMON 명령

## RMON 이벤트 제어

**RMON Events Control(RMON 이벤트 제어)** 페이지를 사용하여 RMON 이벤트를 정의합니다. 이벤트는 특정 RMON 카운터의 임계값을 초과할 경우 강제로 일부 조치를 수행하도록 하기 위해 RMON 경고에 의해 사용됩니다. 이벤트 정보는 로그에 저장하고 트랩으로 트랩 수신기에 보낼 수 있습니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→RMON→Event Control(이벤트 제어)**을 클릭합니다.

그림 9-12. RMON 이벤트 제어



**RMON Event Control(RMON 이벤트 제어)** 페이지에는 다음 필드가 포함되어 있습니다.

**Event Entry(이벤트 항목)** — 이벤트를 선택합니다.

**Community(커뮤니티)** — 이벤트에 속한 커뮤니티를 지정합니다.

**Description(설명)** — 사용자 정의 이벤트를 설명합니다.

**Event Type(이벤트 유형)** — 이벤트 유형을 선택합니다. 가능한 값은 다음과 같습니다.

**Log(로그)** — 이벤트 유형이 로그 항목입니다.

**Trap(트랩)** — 이벤트 유형이 트랩입니다.

**Log and Trap(로그 및 트랩)** — 이벤트 유형이 로그 항목 및 트랩입니다.

**None(없음)** — 이벤트가 없습니다.

**Time(시간)** — 이벤트가 발생한 시간을 표시합니다.

**Owner(소유자)** — 이벤트를 정의한 스위치 또는 사용자를 나열합니다.

**Remove(제거)** — 선택한 경우 이벤트 표에서 이벤트를 제거합니다.

## RMON 이벤트 추가

1. **RMON Event Control(RMON 이벤트 제어)** 페이지를 엽니다.

2. **Add(추가)**를 클릭합니다.

**Add an Event Entry(이벤트 항목 추가)** 페이지가 표시됩니다.

그림 9-13. 이벤트 항목 추가

The screenshot shows a web form titled "Add an Event Entry". It contains the following fields and controls:

- Event Entry:** A text input field containing the number "2".
- Community:** An empty text input field.
- Description:** An empty text input field.
- Event Type:** A dropdown menu with "None" selected.
- Owner:** An empty text input field.
- Buttons:** "Post", "Refresh", "Apply Changes", and "Back".

3. 이 페이지의 필드를 완료합니다.

4. **Apply Changes(변경사항 적용)**를 클릭합니다.

**이벤트**가 **RMON 이벤트 표**에 추가되고 장치가 업데이트됩니다.

## RMON 이벤트 수정

1. **RMON Event Control(RMON 이벤트 제어)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭하여 **Event Control Table(이벤트 제어 표)** 페이지를 표시합니다.

3. 이벤트 항목을 변경하려면 **Edit(편집)** 확인란을 선택합니다.

4. 필요에 따라 페이지의 필드를 수정합니다.

5. **Apply Changes(변경사항 적용)**를 클릭합니다.

**RMON 이벤트 표** 항목이 수정되고 장치가 업데이트됩니다.

## RMON 이벤트 제어 표 표시

1. **RMON Event Control(RMON 이벤트 제어)** 페이지를 엽니다.

2. **Show All(모두 표시)**를 클릭합니다.

**Event Control Table(이벤트 제어 표)**가 표시됩니다.

그림 9-14. 이벤트 제어 표

The screenshot shows a table titled "Event Control Table". The table has the following columns:

| Event Entry | Community | Description | Event Type | Time | Owner | Remove | Edit |
|-------------|-----------|-------------|------------|------|-------|--------|------|
|-------------|-----------|-------------|------------|------|-------|--------|------|

Buttons: "Post", "Refresh", "Apply Changes", "Back".

## RMON 이벤트 항목 제거

1. RMON Event Control(RMON 이벤트 제어) 페이지를 엽니다.
2. Event Entry(이벤트 항목) 필드의 드롭다운 메뉴에서 제거할 이벤트를 선택하고 Remove(제거)를 선택합니다.
3. Apply Changes(변경사항 적용)를 클릭합니다.

표 항목이 제거되고 장치가 업데이트됩니다.

## CLI 명령을 사용하여 스위치 이벤트 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

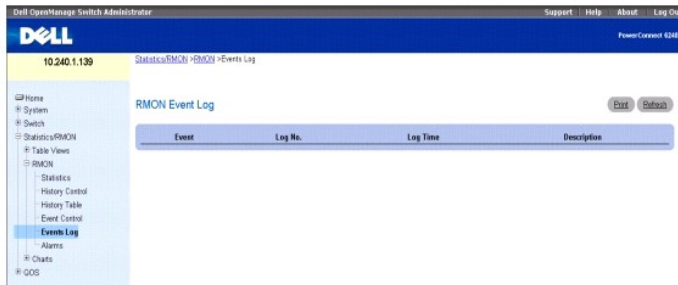
- 1 RMON 명령

## RMON 이벤트 로그

RMON Event Log(RMON 이벤트 로그) 페이지를 사용하여 RMON 이벤트 목록을 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→ RMON→ Events Log(이벤트 로그)**을 클릭합니다.

그림 9-15. RMON 이벤트 로그



RMON Event Log(RMON 이벤트 로그) 페이지에는 다음 필드가 포함되어 있습니다.

**Event(이벤트)** — RMON 이벤트 로그 항목 번호를 표시합니다.

**Log No.(로그 번호)** — 로그 번호를 표시합니다.

**Log Time(로그 시간)** — 그 항목을 입력한 시간을 표시합니다.

**Description(설명)** — 로그 항목을 설명합니다.

## CLI 명령을 사용하여 스위치 이벤트 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

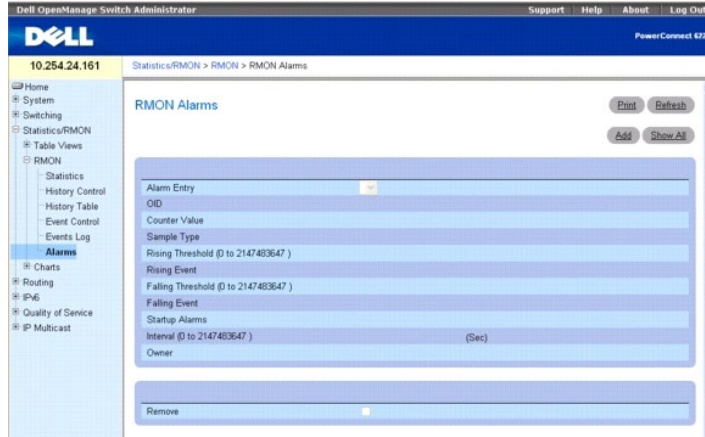
- 1 RMON 명령

## RMON 경고

**RMON Alarms(RMON 경고)** 페이지를 사용하여 네트워크 경고를 설정합니다. 경고는 구성된 RMON 카운터의 특정 임계값을 초과하는 경우 발생합니다. 경고로 인해 이벤트가 발생합니다. 이벤트는 RMON 이벤트 그룹의 일부로 구성할 수 있습니다. 이벤트에 대한 자세한 내용은 ["RMON 이벤트 로그"](#)를 참조하십시오.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→ RMON→ Alarms(경고)**를 클릭합니다.

그림 9-16. RMON 경고



RMON Alarms(RMON 경고) 페이지에는 다음 필드가 포함되어 있습니다.

**Alarm Entry(경고 항목)** — 드롭다운 메뉴에서 특정 경고를 선택합니다.

**OID** — 개체 식별자를 지정합니다.

**Counter Value(카운터 값)** — 선택한 이벤트를 계산한 수를 표시합니다.

**Sample Type(샘플 유형)** — 선택한 변수에 대한 샘플링 방법을 표시하고 값을 임계값과 비교합니다. 가능한 필드 값은 다음과 같습니다.

**Delta(델타)** — 현재 값에서 마지막 샘플 값을 뺍니다. 값의 차이를 임계값과 비교합니다.

**Absolute(절대)** — 샘플링 간격 후반부의 값을 임계값과 직접 비교합니다. 기본 설정입니다.

**Rising Threshold (0-2147483647)(상승 임계값(0-2147483647))** — 상승 임계값 경고를 실행하는 상승 카운터 값을 표시합니다. 상승 임계값은 그래프 막대의 상단에 표시됩니다. 모니터링 각 변수에 색상이 지정됩니다. 기본값은 100입니다.

**Rising Event(상승 이벤트)** — 로그, 트랩 또는 둘 다를 포함하여 경고가 보고되는 메커니즘을 표시합니다. 로그를 선택할 때 스위치 또는 관리 시스템에 저장 메커니즘이 없습니다. 하지만 스위치를 다시 설정하지 않으면 이벤트가 스위치 로그 표에 그대로 남아 있습니다. 트랩을 선택하면 SNMP 트랩이 생성되어 트랩 메커니즘을 통해 보고됩니다. 동일한 메커니즘을 사용하여 트랩을 저장할 수 있습니다.

**Falling Threshold (0-2147483647)(하강 임계값(0-2147483647))** — 하강 임계값 경고를 실행하는 하강 카운터 값을 표시합니다. 하강 임계값은 그래프 막대의 상단에 표시됩니다. 모니터링 각 변수에 색상이 지정됩니다. 기본값은 20입니다.

**Falling Event(하강 이벤트)** — 로그, 트랩 또는 둘 다를 포함하여 경고가 보고되는 메커니즘을 표시합니다. 로그를 선택할 때 스위치 또는 관리 시스템에 저장 메커니즘이 없습니다. 하지만 스위치를 다시 설정하지 않으면 이벤트가 스위치 로그 표에 그대로 남아 있습니다. 트랩을 선택하면 SNMP 트랩이 생성되어 트랩 메커니즘을 통해 보고됩니다. 동일한 메커니즘을 사용하여 트랩을 저장할 수 있습니다.

**Startup Alarms(시작 경고)** — 이벤트 유형을 표시합니다. 옵션은 상승, 상승-하강 및 하강입니다.

**Interval (0-2147483647)(간격(0-2147483647))** — 경고 간격 시간을 표시합니다. 기본값은 100입니다.

**Owner(소유자)** — 경고를 정의한 스위치 또는 사용자를 표시합니다.

**Remove(제거)** — 선택한 경우 RMON 경고를 제거합니다.

## 경고 표 항목 추가

1. RMON Alarms(RMON 경고) 페이지를 엽니다.
2. Add(추가)를 클릭합니다.

Add an Alarm Entry(경고 항목 추가) 페이지가 표시됩니다.

## 그림 9-17. 경고 항목 추가

Add an Alarm Entry Exit Refresh

|                                     |          |
|-------------------------------------|----------|
| Alarm Entry                         | 1        |
| OID                                 |          |
| Sample Type                         | Absolute |
| Rising Threshold (0 to 2147483647)  |          |
| Rising Event                        |          |
| Falling Threshold (0 to 2147483647) |          |
| Falling Event                       |          |
| Startup Alarms                      | Rising   |
| Interval (0 to 2147483647)          | (Sec)    |
| Owner                               |          |

Apply Changes Back

3. 필요에 따라 이 페이지의 필드를 완료합니다.
4. **Apply Changes(변경사항 적용)**를 클릭합니다.  
RMON 경고가 추가되고 장치가 업데이트됩니다.

### 경고 표 표시

1. **RMON Alarms(RMON 경보)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.  
RMON Alarms Table(RMON 경고 표)의 왼쪽이 표시됩니다.

그림 9-18. RMON 경고 표

RMON Alarms Table Exit Refresh

| Alarm Entry | OID | Counter Value | Sample Type | Rising Threshold | Rising Event | Falling Threshold | Falling Event |
|-------------|-----|---------------|-------------|------------------|--------------|-------------------|---------------|
| 1           | 1   | 0             | Absolute    | 100              | 1            | 20                | 2             |

Apply Changes Back

3. 표의 오른쪽을 보려면 화면의 아래쪽에 있는 오른쪽 화살표를 클릭합니다.

### 단일 경고 표 항목 제거

1. **RMON Alarms(RMON 경보)** 페이지를 엽니다.
2. **Alarm Entry(경보 항목)** 드롭다운 메뉴에서 항목을 선택합니다.
3. **Remove(제거)** 확인란을 선택하고 **Apply Changes(변경사항 적용)**를 클릭합니다.  
항목이 제거되고 장치가 업데이트됩니다.

### 여러 경고 표 항목 제거

1. **RMON Alarms(RMON 경보)** 페이지를 엽니다.
2. **Show All(모두 표시)**를 클릭합니다.  
RMON 경고 표가 표시됩니다.
3. 제거할 각 경고 항목에 대해 **Remove(제거)**를 선택합니다.
4. **Apply Changes(변경사항 적용)**를 클릭하십시오.  
항목이 제거되고 장치가 업데이트됩니다.

### CLI 명령을 사용하여 스위치 경고 정의

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.



## 차트

Chart(차트) 메뉴 페이지에는 그래프에 통계를 차트로 표시할 수 있는 웹 페이지에 대한 링크가 포함되어 있습니다. Chart(차트) 메뉴 페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON)→Charts(차트)를 클릭합니다. Charts(차트) 메뉴 페이지에는 다음 기능에 대한 링크가 포함되어 있습니다.

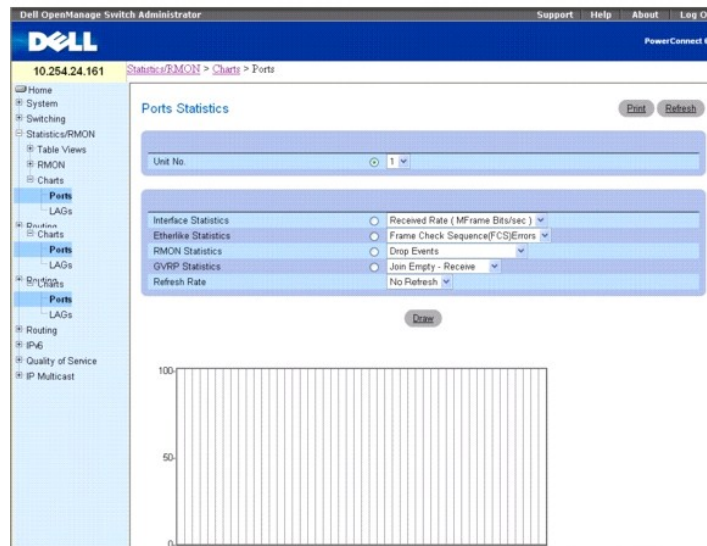
- 1 [포트 통계](#)
- 1 [LAG 통계](#)

## 포트 통계

Ports Statistics(포트 통계) 페이지를 사용하여 그래프에 포트 관련 통계를 차트로 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 Statistics/RMON(통계/RMON)→Charts(차트)→Ports(포트)를 클릭합니다.

그림 9-19. 포트 통계



Ports Statistics(포트 통계) 페이지에는 다음 필드가 포함되어 있습니다.

**Unit No.(장치 번호)** — 표시할 포트를 선택합니다.

**Interface Statistics(인터페이스 통계)** — 클릭할 때 Interface Statistics(인터페이스 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 인터페이스 통계 유형을 지정합니다. 기본값은 Received Rate(수신률)(MFrame 비트/초)입니다.

**Etherlike Statistics(Etherlike 통계)** — 클릭할 때 Etherlike Statistics(Etherlike 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 etherlike 통계 유형을 지정합니다. 기본값은 Frame Check Sequence (FCS) Errors(프레임 정경 시퀀스(FCS) 오류)입니다.

**RMON Statistics(RMON 통계)** — 클릭할 때 RMON Statistics(RMON 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 RMON 통계 유형을 지정합니다. 기본값은 Drop Events(드롭 이벤트)입니다.

**GVRP Statistics(GVRP 통계)** — 클릭할 때 GVRP Statistics(GVRP 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 GVRP 통계 유형을 지정합니다. 기본값은 Join Empty - Receive(빈 항목 연결 - 수신)입니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 선택합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본 비율은 재생 안 함입니다.

## 포트 통계 표시

1. Port Statistics(포트 통계) 페이지를 엽니다.
2. 통계를 차트로 표시할 포트를 선택합니다.
3. 차트로 표시할 통계와 연결된 라디오 단추를 클릭합니다.

4. 관련 드롭다운 메뉴에서 통계 유형을 선택합니다.
5. **Refresh Rate(재생률)** 드롭다운 메뉴에서 원하는 재생률을 선택합니다.
6. **Draw(그리기)**를 클릭합니다.

선택된 통계가 그래프에 차트로 표시됩니다.

## CLI 명령을 사용하여 포트 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

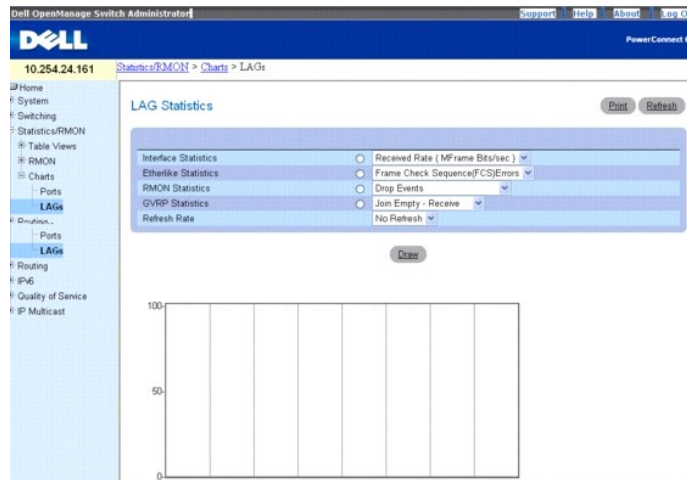
- 1 시스템 관리 명령
- 1 RMON 명령
- 1 GVRP 명령

## LAG 통계

**LAG Statistics(LAG 통계)** 페이지를 사용하여 그래프에 LAG 관련 통계를 차트로 표시합니다.

페이지를 표시하려면 디렉터리 화면에서 **Statistics/RMON(통계/RMON)→Charts(차트)→LAGs(LAG)**를 클릭합니다.

그림 9-20. LAG 통계



**LAG Statistics(LAG 통계)** 페이지에는 다음 필드가 포함되어 있습니다.

**Interface Statistics(인터페이스 통계)** — 클릭할 때 Interface Statistics(인터페이스 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 인터페이스 통계 유형을 지정합니다. 기본값은 Received Rate(수신률)입니다.

**Etherlike Statistics(Etherlike 통계)** — 클릭할 때 Etherlike Statistics(Etherlike 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 etherlike 통계 유형을 지정합니다. 기본값은 Frame Check Sequence Errors(프레임 점검 시퀀스 오류)입니다.

**RMON Statistics(RMON 통계)** — 클릭할 때 RMON Statistics(RMON 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 RMON 통계 유형을 지정합니다. 기본값은 Drop Events(드롭 이벤트)입니다.

**GVRP Statistics(GVRP 통계)** — 클릭할 때 GVRP Statistics(GVRP 통계)를 선택하고 드롭다운 메뉴에서 그래프로 나타낼 GVRP 통계 유형을 지정합니다. 기본값은 Join Empty - Receive(빈 항목 연결 - 수신)입니다.

**Refresh Rate(재생률)** — 통계를 재생하는 간격을 선택합니다. 가능한 필드 값은 No Refresh(재생 안 함), 15, 30 및 60초입니다. 기본값은 15초입니다.

## LAG 통계 표시

1. **LAG Statistics(LAG 통계)** 페이지를 엽니다.

2. 차트로 표시할 통계와 연결된 라디오 단추를 클릭합니다.
  3. 관련 드롭다운 메뉴에서 통계 유형을 선택합니다.
  4. **Refresh Rate(재생률)** 드롭다운 메뉴에서 원하는 재생률을 선택합니다.
  5. **Draw(그리기)**를 클릭합니다.
- 선택된 통계가 그래프에 차트로 표시됩니다.

## CLI 명령을 사용하여 LAG 통계 보기

이 기능을 수행하는 CLI 명령에 대한 자세한 내용은 CLI 참조 안내서의 다음 장을 참조하십시오.

- 1 시스템 관리 명령
- 1 RMON 명령
- 1 GVRP 명령

---

[목록 페이지로 돌아가기](#)