

Broadcom[®] NetXtreme[®] BCM57XX

사용 설명서

마지막 수정 날짜: 2015년 2월

2CS57XX-CDUM513-R

이 문서에 있는 정보는 예고 없이 변경될 수 있습니다.
© 2014 Broadcom Corporation. All rights reserved.

본 사용 설명서는 저작권법에 의해 보호되며 이의 사용, 복사, 배포, 개조를 제한하는 라이선스 하에서 배포됩니다. 본 사용 설명서를 어떠한 형식 또는 방법으로 복제하는 경우 Broadcom Corporation으로부터 서면 승인을 미리 받아야 합니다. 관련 문서는 비침해 행위에 대한 명시적 또는 묵시적 보증을 비롯한 상업성이나 특정 목적의 적합성에 대한 묵시적 보증 등, 어떠한 보증 없이 "있는 그대로" 제공됩니다.

Broadcom Corporation은 신뢰도, 기능, 디자인 등, 관련 품질을 높이기 위해 사전 통보 없이 제품을 비롯한 본 사용 설명서의 내용을 변경할 수 있습니다. Broadcom Corporation이 제공하는 정보는 정확성과 신뢰성이 있는 것으로 간주됩니다. 그러나, Broadcom Corporation은 이와 같은 정보를 비롯한 본 설명서에서 언급된 제품 또는 회로를 응용하거나 사용하여 발생하는 문제에 대해 아무런 책임을 지지 않습니다. 또한, 특허권 등 기타 권리에 따라 사용권이 양도되지 않습니다.

Broadcom, Pulse 로고, Connecting everything, Connecting everything 로고, NetXtreme, Ethernet@Wirespeed, LiveLink 및 Smart Load Balancing은 미국, 특정 국가 및/또는 EU에서 Broadcom Corporation 및/또는 지사의 상표입니다. Microsoft 및 Windows는 Microsoft Corporation의 상표입니다. Linux는 Linus Torvalds의 상표입니다. Intel은 Intel Corporation의 상표입니다. Magic Packet은 Advanced Micro Devices, Inc.의 상표입니다. Red Hat은 Red Hat, Inc.의 상표입니다. PCI Express은 PCI-SIG는 상표입니다. 그 밖에 언급된 모든 상표 및 상호는 해당 소유자의 자산입니다.

마지막 수정 날짜: 2015년 2월

2CS57XX-CDUM513-R

목차

1. 기능 및 특징	11
기능 설명	11
특징	12
전원 상태 관리	12
적응 인터럽트 주파수	13
이중 DMA 채널	13
내장 RISC 프로세서가 있는 ASIC	13
Broadcom Advanced Control Suite	13
지원되는 운영 환경	14
네트워크 링크 및 활동 표시	14
2. 팀 구성	15
개요	16
로드 균형 조정 및 결함 허용	16
팀 유형	16
Smart Load Balancing™ 및 장애 조치	17
링크 집계(802.3ad)	17
일반 트렁킹(FEC/GEC)/802.3ad-Draft Static	17
SLB(Auto-Fallback Disable)	18
Smart Load Balancing 및 장애 조치/SLB(Auto-Fallback Disable) 팀 유형의 제한 사항	18
LiveLink™ 기능	19
팀 구성 및 Large Send Offload/Checksum Offload 지원	19
3. Broadcom Gigabit Ethernet 팀 구성 서비스	20
시작	21
용어	21
팀 구성의 개념	23
네트워크 주소 지정	23
팀 구성 및 네트워크 주소	23
팀 구성 유형 설명	24

소프트웨어 구성 요소	26
하드웨어 요구 사항	28
Ethernet 스위치	28
라우터	28
팀 유형별 지원 기능	28
팀 유형 선	30
팀 구성 메커니즘	31
아키텍처	31
아웃바운드 트래픽 흐름	32
인바운드 트래픽 흐름(SLB에만 해당)	32
프로토콜 지원	32
성능	33
운영 체제별 드라이버 지원	34
지원되는 팀 구성 속도	35
팀 구성 및 기타 고급 네트워크 속성	36
Checksum Offload	37
IEEE 802.1p QoS 태그	37
Large Send Offload	37
대용량 프레임	37
IEEE 802.1Q VLAN	37
Wake On LAN	38
PXE(Preboot Execution Environment)	38
일반 네트워크 고려 사항	39
스위치 간의 팀 구성	39
스위치 링크 결함 허용	39
스패닝 트리 알고리즘	41
TCN(Topology Change Notice)	42
Port Fast/Edge Port	42
Microsoft NLB/WLBS를 사용한 팀 구성	42
응용 프로그램 고려 사항	43
팀 구성 및 클러스터링—Microsoft 클러스터 소프트웨어	43
팀 구성 및 네트워크 백업	44
로드 균형 조정 및 장애 조치	44

결함 허용	45
팀 구성 문제 해결	47
팀 구성 팁	47
문제 해결 지침	48
FAQ	49
이벤트 로깅 메시지	52
Windows 시스템 이벤트 로깅 메시지	52
기본 드라이버(물리적 어댑터/미니포트)	52
중급 드라이버(가상 어댑터/팀)	54
4. 가상 LAN(VLAN)	56
VLAN 개요	56
팀에 VLAN 추가	58
5. 관리	59
CIM	59
SNMP	60
BASP Subagent	60
BASP 확장형 에이전트	60
6. 하드웨어 설치	62
안전 주의 사항	62
사전 설치 검사 목록	63
어댑터 설치	63
네트워크 케이블 연결	64
구리	64
7. 드라이버 디스크 작성	65
8. Broadcom Boot Agent 드라이버 소프트웨어	66
개요	66
클라이언트 환경에서 MBA 설정	67
MBA 드라이버 구성	67
BIOS 설정	68

9. iSCSI 프로토콜	69
iSCSI 부트	69
iSCSI 부트용으로 지원되는 운영 체제.....	69
iSCSI 부트 설정	69
iSCSI 대상 구성	69
iSCSI 부트 매개 변수 구성	70
MBA 부트 프로토콜 구성.....	71
iSCSI 부트 구성	71
CHAP 인증 활성화	74
DHCP 서버가 iSCSI 부트를 지원하도록 구성	74
IPv4를 위한 DHCP iSCSI 부트 구성.....	74
IPv6을 위한 DHCP iSCSI 부트 구성.....	76
DHCP 서버 구성	76
iSCSI 부트 이미지 준비	77
부팅	83
기타 iSCSI 부트 고려 사항.....	83
Windows 환경에서 Speed & Duplex 설정 변경	83
Locally Administered Address	83
가상 LAN(VLAN)	84
iSCSI 부트 문제 해결.....	84
iSCSI Crash Dump	84
10. Linux 드라이버 및 관리 응용 프로그램 설치	85
패키지	85
TG3 드라이버 소프트웨어 설치	86
소스 RPM 패키지 설치	86
소스 TAR 파일로 드라이버 구축.....	87
네트워크 설치	87
TG3 드라이버 언로드/제거	87
RPM 설치에서 드라이버 언로드/제거	87
TAR 설치에서 드라이버 제거	87
드라이버 메시지	88
채널 본딩을 사용하여 팀 구성	88

Linux 관리 응용 프로그램 설치	89
개요	89
통신 프로토콜	89
Linux 서버에 WS-MAN 또는 CIM-XML 설치	90
1단계: OpenPegasus 설치	90
2단계: 서버에서 CIM 서버 시작	92
3단계: 서버에서 OpenPegasus 구성	92
4단계: Broadcom CMPI 공급자 설치	94
5단계: 필요 시 Linux 방화벽 구성 수행	94
6단계: BACS 및 관련 관리 응용 프로그램 설치	95
Linux 클라이언트에 WS-MAN 또는 CIM-XML 설치	96
Linux 클라이언트에서 HTTPS 구성	96
Broadcom Advanced Control Suite 응용 프로그램 설치	98
11. VMware 드라이버 소프트웨어	99
패키지	99
드라이버	99
드라이버 다운로드, 설치 및 업데이트	99
드라이버 매개 변수	99
드라이버 매개 변수	100
드라이버 기본값	100
드라이버 메시지	101
12. Windows 드라이버 및 관리 응용 프로그램 설치	102
드라이버 소프트웨어 설치	103
설치 프로그램 사용	103
자동 설치 사용	104
드라이버 소프트웨어 수정	105
드라이버 소프트웨어 복구 또는 다시 설치	106
장치 드라이버 제거	106
어댑터의 속성 확인 또는 변경	107
전원 관리 옵션 설정	107
BACS4와 함께 사용할 통신 프로토콜 구성	108

WS-MAN 사용	108
WS-MAN Windows Server 구성	108
WS-MAN Windows 클라이언트 설치	115
WMI 사용	117
1단계: WMI 컨트롤을 사용하여 네임스페이스 보안 설정	117
2단계: DCOM 원격 실행 및 활성화 사용 권한 부여	117
각기 다른 시스템의 WMI를 위한 특수 구성	118
13. Broadcom Advanced Control Suite 4 사용	119
Broadcom Advanced Control Suite 개요	119
Broadcom Advanced Control Suite 시작	120
BACS 인터페이스	120
탐색기 보기 창	121
컨텍스트 보기 선택기	122
필터 보기	122
컨텍스트 보기 창	122
메뉴 모음	122
설명 창	123
Windows에서 기본 설정 구성	123
호스트에 연결	124
호스트 관리	125
정보 탭: 호스트 정보	125
네트워크 어댑터 관리	127
어댑터 정보 확인	127
드라이버 정보 보기	128
리소스 정보 보기	129
하드웨어 정보 보기	130
네트워크 테스트	131
진단 테스트 실행	132
케이블 분석	133
어댑터 속성 설정	134
통계 보기	136
일반 통계	136

팀 구성	137
팀 유형	137
Broadcom 팀 구성 마법사 사용	138
전문가 모드 사용	150
팀 생성	150
팀 수정	152
VLAN 추가	153
VLAN 속성 및 통계 보기 및 VLAN 테스트 실행	154
VLAN 삭제	155
Smart Load Balancing 및 장애 조치와 SLB(Auto-Fallback Disable) 팀에 대한 LiveLink 구성	156
구성 저장 및 복원	157
BASP 통계 보기	158
명령줄 인터페이스 유틸리티를 사용하여 구성	159
BACS 문제 해결	159
14. 사양	160
10/100/1000BASE-T 케이블 사양	160
성능 사양	160
15. 규정	161
FCC Class B 표시	161
VCCI Class B 표시	162
VCCI Class B 규정(일본)	162
CE 표시	162
캐나다 규정 정보(캐나다만 해당)	166
Industry Canada, Class B	166
Industry Canada, classe B	166
MIC 표시(대한민국만 해당)	167
CLASS B 장치	167
BSMI	168
16. 문제 해결 단계	169
하드웨어 진단	169
BACS 진단 테스트 실패	169

BACS 네트워크 테스트 실패	170
문제 해결 검사 목록.....	171
네트워크 링크 및 활동 상태 검사.....	171
최신 드라이버가 로드되었는지 검사.....	172
Windows.....	172
Linux.....	172
케이블 길이 테스트 실행.....	172
네트워크 연결 테스트	173
Windows	173
Linux	173
Broadcom Boot Agent	173
BASP(Broadcom Advanced Server Program)	174
이더넷을 통한 커널 디버깅	174
기타.....	174

1 절: 기능 및 특징

- 기능 설명
- 특징
- 지원되는 운영 환경
- 네트워크 링크 및 활동 표시

기능 설명

Broadcom NetXtreme Gigabit Ethernet 어댑터는 Gigabit Ethernet 네트워크에 PCI Express™ 호환 시스템을 연결합니다. Broadcom NetXtreme Gigabit Ethernet 어댑터에는 데이터를 1초당 최고 1기가비트의 속도(Fast Ethernet 어댑터 속도의 10 배)로 전송하는 기술을 채택하고 있습니다.

Broadcom 팀 구성 소프트웨어를 사용하면 네트워크를 가상 LAN(VLAN)으로 분할하고 여러 네트워크 어댑터를 팀으로 그룹화하여 네트워크 로드 균형 조정 및 결함 허용 기능을 제공할 수 있습니다. 팀 구성에 대한 자세한 내용은 [팀 구성](#) 및 [Broadcom Gigabit Ethernet 팀 구성 서비스](#)를 참조하십시오. VLAN에 대한 설명은 [가상 LAN](#)을 참조하십시오. Windows 운영 체제에서 팀을 구성하고 VLAN을 생성하는 방법은 [팀 구성](#)을 참조하십시오.

특징

지원되는 모든 운영 체제의 Broadcom NetXtreme Gigabit Ethernet 어댑터 기능 목록은 다음과 같습니다.

- 통합 쿼드 10/100/1000BASE-T 및 쿼드 1000BASE-X/SGMII 1.25Gbaud SerDes 트랜시버
- IEEE Std 802.3az-2010과 호환되는 Energy Efficient Ethernet™
- IEEE 802.3ap 제73절 자동 협상
- 쿼드 10/100/1000BASE-T 전이중/반이중 MAC
- 쿼드 1000BASE-X/SGMII 전이중/반이중 MAC
- 5GT/s 또는 2.5GT/s에서 자동 MDI Crossover
- x4 PCI Express v2.0
- MSI 및 MSI-X 기능-최대17 MSI-X 벡터
- VMware NetQueue 및 Microsoft VMQ에 대해 입출력(I/O) 가상화 지원
 - 수신 대기열 17개 및 전송 대기열 16개
 - 대기열당 호스트 인터럽트를 지원하는 17 MSI-X 벡터
- 대기열 연결을 전송/수신하는 유연한 MSI-X 벡터
- PCI Express 기본 사양 v2.0에 대한 TPH(TLP Processing Hint) ECN
- 기능 수준 재설정
- 대기열당 MSI-X 벡터가 지원되는 RSS(Receive Side Scaling) 및 UDP RSS 해시 유형 지원
- 대기열당 MSI-X 벡터가 지원되는 TSS(Transmit Side Scaling) 및 다중 Tx 대기열
- 최대 9600바이트 페이로드에 대해 대용량 프레임 지원
- 가상 LAN(VLAN) 지원— IEEE 802.1q VLAN 태그
- TCP, IP, UDP Checksum Offload
- LSO(Large Send Offload), TSO(TCP Segmentation Offload)
- IEEE 1588에 대한 하드웨어 지원 및 IEEE 802.1AS 시간 동기화 구현
- IEEE 802.3x 흐름 제어
- SMBus 2.0 인터페이스
- SNMP MIB II, Ethernet-like MIB 및 Ethernet MIB(IEEE 802.3z, 제30절) 통계
- ACPI 전원 관리 준수
- CPMU(Central Power Management Unit)를 통한 고급 전원 관리
- 효율적인 통합 스위칭 레귤레이터 컨트롤러
- 칩 내장 온도 모니터
- PCI Express CLKREQ 지원
- 전원 관리 Offload(PM Offload)
- 직렬 플래시 및 EEPROM NVRAM 지원(플래시 자동 구성)
- 내부 SRAM에서 ECC 오류 탐지 및 수정
- JTAG 범위 스캔 지원

전원 상태 관리

Wake on LAN(Magic Packet, Wake Up Frame, 특정 패턴)을 지원합니다.



참고: 어댑터 연결 속도는 시스템이 절전 모드 해제 신호 대기 중에 종료될 때 10Mbps 또는 100Mbps지만, 시스템이 가동되어 실행 중인 경우 1000Mbps 가능 스위치에 연결되면 1000Mbps로 되돌아올 수 있습니다. WOL(Wake on LAN)을 사용하는 시스템은 1000Mbps 및 10Mbps 또는 100Mbps의 속도를 낼 수 있는 스위치에 연결되어야 합니다.

적응 인터럽트 주파수

어댑터 드라이버는 트래픽 상태 기반의 호스트 인터럽트 주파수를 지능적으로 조정하여 전체적인 응용 프로그램 처리율을 높여줍니다. 트래픽이 낮은 경우 어댑터 드라이버는 수신된 각 패킷에 대한 호스트를 인터럽트하여 지연을 최대한 줄여주고, 트래픽이 높은 경우 어댑터는 지속적으로 수신되는 여러 패킷에 대해 한 개의 호스트 인터럽트를 발생시켜 호스트 CPU 주기를 유지합니다.

이중 DMA 채널

Broadcom NetXtreme Gigabit Ethernet 어댑터의 PCIe 인터페이스에는 읽기 및 쓰기 작업에 각각 사용되는 DMA 채널이 두 개 있습니다.

내장 RISC 프로세서가 있는 ASIC

Broadcom NetXtreme Gigabit Ethernet 어댑터의 핵심적인 제어 기능은 완전 통합된 고성능 ASIC에 있습니다. ASIC에는 RISC 프로세서가 내장됩니다. 따라서 ASIC를 통해 카드에 새 기능을 추가할 수 있을 뿐만 아니라 소프트웨어 다운로드를 통해 이후 네트워크 요구 사항에 맞게 구성할 수 있습니다.

Broadcom NetXtreme 관리 작업(DMTF, SMASH, DASH 및 NC-SI 통과 등)은 기존 네트워크 처리 엔진과는 다른 고성능 APE(Application Processor Engine)에서 실행됩니다.

Broadcom Advanced Control Suite

Broadcom 팀 구성 소프트웨어의 구성 요소인 Broadcom Advanced Control Suite(BACS)는 시스템에 설치된 각 네트워크 어댑터에 대한 유용한 정보를 제공하는 통합형 유틸리티입니다. BACS 유틸리티를 사용하면 속성 값을 수정하고 각 어댑터의 트래픽 통계를 확인할 수 있으며 상세 테스트, 진단 및 분석을 수행할 수 있습니다. Windows 운영 체제에서 팀을 구성하고 VLAN을 추가하려면 BACS가 사용됩니다. 자세한 내용과 지침은 [Broadcom Advanced Control Suite 사용](#)을 참조하십시오.

지원되는 운영 환경

Broadcom NetXtreme Gigabit Ethernet 어댑터의 소프트웨어는 다음 운영 체제에서 사용할 수 있습니다.

- Microsoft® Windows®(32비트 및 64비트 확장형)
- Linux®(32비트 및 64비트 확장형)
- VMware
- Oracle Solaris

네트워크 링크 및 활동 표시

구리선 기반 Ethernet 연결의 경우 표 1: 14페이지의 “RJ-45 포트 LED로 알 수 있는 네트워크 링크 및 활동 상태”에 설명되어 있는 바와 같이 네트워크 링크 및 활동 상태가 RJ-45 커넥터에 있는 LED를 통해 표시됩니다. Broadcom Advanced Control Suite는 네트워크 링크 및 활동 상태 정보도 알려줍니다([어댑터 정보 확인](#) 참조).

표 1. RJ-45 포트 LED로 알 수 있는 네트워크 링크 및 활동 상태

포트 LED	LED 상태	네트워크 상태
링크 LED	OFF	링크 없음(케이블 연결 안 됨)
	켜져 있음	연결됨
활동 LED	OFF	네트워크 활동 없음
	깜박임	네트워크 활동

2 절: 팀 구성

- [개요](#)
- [로드 균형 조정 및 결함 허용](#)



참고: 다음 항목에 대한 자세한 내용은 [Broadcom Gigabit Ethernet 팀 구성 서비스](#)를 참조하십시오.

- 용어 및 약어 목록
- 팀 구성의 개념
- 소프트웨어 구성 요소
- 하드웨어 요구 사항
- 팀 유형별 지원 기능
- 팀 유형을 선택합니다.
- 팀 구성 메커니즘
- 아키텍처
- 팀 유형
- 운영 체제별 드라이버 지원
- 지원되는 팀 구성 속도
- 팀 구성 및 기타 고급 네트워크 특징
- 일반 네트워크 고려 사항
- 응용 프로그램 고려 사항
- 팀 구성 문제 해결
- FAQ
- 이벤트 로깅 메시지

개요

어댑터 팀 구성 기능을 사용하면 한 팀으로 작동하도록 네트워크 어댑터를 함께 그룹화할 수 있습니다. 이를 통해 VLAN에 멤버십을 허용할 수 있으므로 어댑터 간 로드 균형을 조정하고 결함 허용을 제공하는 이점이 있습니다. 로드 균형 조정 멤버를 위한 로드 균형 조정 기능과 팀이 서로 다른 VLAN에 참여하게 되는 장애 조치 채용 기능을 결부시킬 수 있도록 이러한 이점을 결합할 수 있습니다.

BASP(Broadcom Advanced Server Program)는 Broadcom 팀 구성 소프트웨어입니다. Windows 운영 체제의 경우 BASP는 **Broadcom Advanced Control Suite(BACS)** 유틸리티를 통해 구성됩니다. Linux 운영 체제에서의 팀 구성은 채널 본딩을 통해 수행됩니다([채널 본딩을 사용하여 팀 구성 참조](#)).

BASP에서 지원하는 4가지 로드 균형 조정 팀 유형은 다음과 같습니다.

- Smart Load Balancing과 장애 조치
- 링크 집계(802.3ad)
- 일반 트렁킹(FEC/GEC)/802.3ad-Draft Static
- SLB(Auto-Fallback Disable)

로드 균형 조정 및 결함 허용

팀 구성은 트래픽 로드 균형 조정 및 결함 허용을 제공합니다(네트워크 연결 실패 시 중복 어댑터 작업 제공). 여러 어댑터가 동일한 시스템에 설치된 경우, 최대 16개의 팀으로 그룹화할 수 있습니다.

각 팀은 최대 8개의 어댑터로 구성할 수 있으며, 이들 중 하나는 SLB(Smart Load Balancing 및 장애 조치) 또는 SLB(Auto-Fallback Disabled) 팀 유형을 위한 대기 어댑터로 사용됩니다. 어댑터, 케이블 또는 스위치 오류로 인해 어댑터 팀 멤버 연결 부분에서 트래픽이 확인되지 않는 경우 현재 연결되어 있는 나머지 팀 멤버에게 로드가 분산됩니다. 기본 어댑터에 모두 오류가 발생한 경우에는 대기 어댑터로 트래픽이 분산됩니다. 기존 세션은 사용자에게 영향을 미치지 않고 유지됩니다.

팀 유형

지원되는 운영 체제에 사용 가능한 팀 유형은 다음 표에 설명되어 있습니다.

표 2. 팀 유형

운영 체제	사용 가능한 팀 유형
Windows Server 2008 및 Windows Server 2012	Smart Load Balancing과 장애 조치 링크 집계(802.3ad) 일반 트렁킹(FEC/GEC)/802.3ad-Draft Static SLB(Auto-Fallback Disable)
	참고: Windows Server 2012는 NIC 팀이라고 하는 내부 팀 구성 지원을 제공합니다. 사용자가 동일한 어댑터에서 동시에 NIC 팀 및 BASP를 통해 팀을 활성화하는 것은 권장되지 않습니다.
Linux	본딩 커널 모듈과 채널 본딩 인터페이스를 사용하는 팀 어댑터. 자세한 내용은 Linux 설명서를 참조하십시오.

Smart Load Balancing™ 및 장애 조치

Smart Load Balancing™ 및 장애 조치는 Broadcom이 IP 흐름을 기반으로 구현한 로드 균형 조정입니다. 이 기능은 여러 어댑터(팀 멤버)에 대한 IP 트래픽의 균형 조정을 양방향으로 지원합니다. 이 유형에서 팀 내의 모든 어댑터에는 별도의 MAC 주소가 있습니다. 이는 다른 팀 멤버 또는 상시 대기 멤버에 자동 결함 감지 및 동적 장애 조치를 제공합니다. 계층 3 프로토콜(IP)에 별도로 수행하며 이는 기존 계층 2 및 계층 3 스위치와 작동합니다. 팀이 작동하는 데 스위치 구성(예, 트렁크, 링크 집계)은 필요하지 않습니다.



설명:

- SLB 팀 구성 시 LiveLink™를 활성화하지 않는 경우 스위치 또는 포트에서 스페닝 트리 프로토콜(STP)을 비활성화하는 것이 좋습니다. 그러면 장애 조치 시 스페닝 트리 루프 결정으로 인한 시스템 종료 시간이 최소화됩니다. LiveLink는 이러한 문제를 완화합니다.
- 팀 멤버가 1000Mbit/s의 속도로 링크되어 있고 다른 팀 멤버가 100Mbit/s의 속도로 링크되어 있는 경우 대부분의 트래픽은 1000Mbit/s 속도의 팀 멤버에서 처리됩니다.

링크 집계(802.3ad)

이 모드는 링크 집계를 지원하고 IEEE 802.3ad(LACP) 사양에 맞습니다. 구성 소프트웨어를 사용하여 지정된 팀에 참여하려는 어댑터를 동적으로 구성할 수 있습니다. 링크 파트너가 802.3ad 링크 구성에 대해 올바르게 구성되지 않은 경우 오류가 감지되어 기록됩니다. 이 모드에서 팀에 구성된 모든 어댑터는 동일한 MAC 주소에 대해 패킷을 수신합니다. 아웃바운드 로드 균형 조정 체계는 BASP 드라이버로 결정됩니다. 팀의 링크 파트너는 인바운드 패킷에 대해 로드 균형 조정 스키마를 결정합니다. 이 팀 유형에서는 링크 파트너 하나 이상이 활성 모드여야 합니다.

일반 트렁킹(FEC/GEC)/802.3ad-Draft Static

일반 트렁킹(FEC/GEC)/802.3ad-Draft Static 팀 유형은 팀의 모든 어댑터가 동일한 MAC 주소에 대한 패킷을 수신하도록 구성된다는 점에서 링크 집계(802.3ad)와 매우 유사합니다. 그러나, 일반 트렁킹(FEC/GEC)/802.3ad-Draft Static 팀 유형은 LACP 또는 마커 프로토콜 지원을 제공하지 않습니다. 이 유형은 어댑터 링크 파트너가 독립적인 트렁킹 메커니즘을 지원하기 위해 정적으로 구성되는 다양한 환경을 지원합니다. 예를 들어, 이 유형은 Lucent의 OpenTrunk 또는 Cisco의 Fast EtherChannel(FEC)을 지원하는 데 사용할 수 있습니다. 기본적으로 이 모드는 링크 집계(802.3ad) 팀 유형의 라이트 버전입니다. 이 접근법은 공식화된 링크 집계 제어 프로토콜(LACP)이 아니라는 점에서 보다 단순합니다. 다른 유형에서와 마찬가지로, 팀 만들기과 다양한 팀에 물리적인 어댑터 할당은 사용자 구성 소프트웨어를 통해 정적으로 수행됩니다.

일반 트렁킹(FEC/GEC)/802.3ad-Draft Static 팀 지원 유형은 아웃바운드 및 인바운드 트래픽 모두에 대한 로드 균형 조정 및 장애 조치를 지원합니다.

SLB(Auto-Fallback Disable)

SLB(Auto-Fallback Disable) 팀 유형은 Smart Load Balancing 및 장애 조치와 동일하지만 다음과 같은 예외가 있습니다. 상시 대기 멤버가 활성화된 경우 기본 멤버가 복원되면 팀은 기본 멤버로 다시 스위칭하지 않고 상시 대기 멤버를 사용하여 계속 진행합니다.

팀에 할당된 기본 어댑터를 비활성화하면 팀은 자동 고장 대체가 수행되는 Smart Load Balancing 및 장애 조치 팀 유형으로 작동합니다.

팀의 모든 기본 인터페이스는 전체 트래픽의 일부를 송수신하면서 로드 균형 조정 작업에 참여하게 됩니다. 대기 인터페이스는 모든 기본 인터페이스의 해당 링크가 해제될 경우 기본 인터페이스를 대신하여 그 임무를 수행합니다.

장애 조치 팀 구성은 네트워크 연결 실패 시 중복 어댑터 작업(결함 허용)을 제공합니다. 어댑터, 케이블 또는 스위치 포트의 실패로 인해 팀에 있는 기본 어댑터가 해제된 경우 보조 팀 멤버는 기본 어댑터에 원래 할당된 인바운드 및 아웃바운드 트래픽을 다시 연결하여 활성화됩니다. 기존 세션이 유지되고 사용자에게는 아무런 영향이 없습니다.

Smart Load Balancing 및 장애 조치/SLB(Auto-Fallback Disable) 팀 유형의 제한 사항

Smart Load Balancing™(SLB)은 프로토콜별 스키마입니다.

표 3. Smart Load Balancing

운영 체제	장애 조치/고장 대체 — 모두 Broadcom	장애 조치/고장 대체 — 여러 공급업체
프로토콜	IP	IP
Windows Server 2008	Y	Y
Windows Server 2008 R2	Y	Y
Windows Server 2012	Y	Y
운영 체제	로드 균형 조정 — 모두 Broadcom	로드 균형 조정 — 여러 공급업체
프로토콜	IP	IP
Windows Server 2008	Y	Y
Windows Server 2008 R2	Y	Y
Windows Server 2012	Y	Y
Windows Server 2012 R2	Y	Y

범례 : Y = 예
 N = 아니오
 N/S = 지원 안 함

Smart Load Balancing 팀 유형은 스위치 포트를 특수 트렁킹 모드에 구성할 필요 없이 모든 **Ethernet** 스위치와 작동합니다. IP 트래픽만 인바운드 및 아웃바운드 방향으로 모두 로드 균형 조정이 가능합니다. 기타 프로토콜 패킷은 하나의 기본 인터페이스를 통해서만 전송 및 수신됩니다. IP가 아닌 트래픽의 장애 조치는 **Broadcom** 네트워크 어댑터로만 지원됩니다. 일반 트렁킹 유형에서 일부 포트 트렁킹 모드 형식을 지원하려면 **Ethernet** 스위치가 필요합니다(예, **Cisco**의 **Gigabit EtherChannel** 또는 기타 스위치 공급업체의 링크 집계 모드). 일반 트렁킹 팀 유형은 프로토콜과 무관하고 모든 트래픽은 로드 균형 조정과 결함 허용이 가능합니다.



참고 : 팀 구성 시 **LiveLink™**를 활성화하지 않는 경우 스위치에서 스페닝 트리 프로토콜 (STP)을 비활성화하는 것이 좋습니다. 그러면 장애 조치 시 스페닝 트리 루프 결정으로 인한 시스템 종료 시간이 최소화됩니다. **LiveLink**는 이러한 문제를 완화합니다.

LiveLink™ 기능

LiveLink™ 기능은 **Smart Load Balancing™** 및 장애 조치 팀 구성 유형에서만 사용 가능한 **BASP**의 기능입니다. **LiveLink**는 해당 스위치 이외의 네트워크 연결을 감지하고 라이브 링크가 있는 팀 멤버를 통해서만 트래픽을 돌아가게 합니다. 이 기능을 사용하려면 팀 구성 소프트웨어를 설치해야 합니다(**Smart Load Balancing 및 장애 조치와 SLB(Auto-Fallback Disable) 팀에 대한 LiveLink 구성 참조**). 팀 구성 소프트웨어는 하나 이상의 지정된 대상 네트워크 어댑터를 정기적으로 검사합니다(각 팀 멤버의 링크 패킷 발생). 링크 패킷이 수신되면 조사 대상이 응답합니다. 팀 멤버가 지정한 재시도 횟수 이후의 특정 시간 내에 응답을 감지하지 않는 경우 팀 구성 소프트웨어는 해당 팀 멤버를 통한 트래픽 통과를 중단합니다. 나중에 팀 멤버가 검색 대상에서 응답을 감지하기 시작하면 이는 링크가 다시 복구되어 팀 구성 소프트웨어가 팀 멤버를 통해 다시 자동으로 트래픽을 통과시키기 시작했다는 것을 나타냅니다. **LiveLink**는 **TCP/IP**에만 작동합니다.

LiveLink™ 기능은 **32비트** 및 **64비트 Windows** 운영 체제에서 모두 지원됩니다. **Linux** 운영 체제의 유사한 기능은 **Linux** 설명서의 채널 본딩을 참조하십시오.

팀 구성 및 Large Send Offload/Checksum Offload 지원

모든 멤버가 해당 기능을 지원하고 이를 위해 구성된 경우에만 **LSO(Large Send Offload)** 및 **Checksum Offload** 속성을 팀을 위해 사용할 수 있습니다.

3 절: Broadcom Gigabit Ethernet 팀 구성 서비스

- 시작
- 팀 구성 메커니즘
- 팀 구성 및 기타 고급 네트워크 속성
- 일반 네트워크 고려 사항
- 응용 프로그램 고려 사항
- 팀 구성 문제 해결
- FAQ
- 이벤트 로깅 메시지

시작

- 용어
- 팀 구성의 개념
- 소프트웨어 구성 요소
- 하드웨어 요구 사항
- 팀 유형별 지원 기능
- 팀 유형 선

이 절에서는 시스템과 함께 제공되는 Broadcom 소프트웨어의 네트워크 팀 구성 서비스를 작업할 때 적용되는 기술 및 구현 고려 사항에 대해 설명합니다. Broadcom 팀 구성 서비스는 둘 이상의 어댑터로 구성된 팀에 결함 허용 및 링크 집계를 제공하기 위한 것입니다. 이 문서에 제공된 정보는 IT 전문가가 네트워크 결함 허용 및 로드 균형 조정이 필요한 시스템 응용 프로그램을 배포하고 제반 문제를 해결하는 과정에 도움을 주기 위한 것입니다.

용어

표 4. 용어

항목	정의
ARP	Address Resolution Protocol(주소 분석 프로토콜)
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program(중급 소프트웨어)
DNS	Domain Name Service(도메인 이름 서비스)
G-ARP	Gratuitous Address Resolution Protocol
일반 트래킹(FEC/GEC)/802.3ad-Draft Static	중급 드라이버가 나가는 트래픽을 관리하고 스위치가 들어오는 트래픽을 관리하는 스위치 종속형 로드 균형 조정 및 장애 조치 유형의 팀
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
링크 집계(802.3ad)	중급 드라이버가 나가는 트래픽을 관리하고 스위치가 들어오는 트래픽을 관리하는 스위치 종속형 로드 균형 조정 및 장애 조치 유형의 팀(LACP 지원)
LOM	LAN on Motherboard
MAC	Media Access Control
NDIS	Network Driver Interface Specification
NLB	Network Load Balancing(Microsoft)
PXE	Preboot Execution Environment
RAID	RAID(Redundant Array of Inexpensive Disk)
Smart Load Balancing 및 장애 조치	기본 팀 멤버가 들어오고 나가는 트래픽을 모두 처리하고 대기 팀 멤버는 장애 조치 이벤트(예: 링크 손실)가 끝날 때까지 유휴 상태를 유지하는 스위치 독립형 장애 조치 유형의 팀. 중급 드라이버(BASP)에서 들어오는 트래픽과 나가는 트래픽을 관리합니다.

표 4. 용어

항목	정의
SLB(Smart Load Balancing)	중급 드라이버에서 들어오고 나가는 트래픽을 관리하는 스위치 독립형 로드 균형 조정 및 장애 조치 유형의 팀.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WINS	Windows Name Service
WLBS	Windows Load Balancing Service

팀 구성의 개념

- 네트워크 주소 지정
- 팀 구성 및 네트워크 주소
- 팀 구성 유형 설명

네트워크 주소 지정

팀 구성의 작동 원리를 이해하려면 이더넷 네트워크에서 노드의 통신이 이루어지는 방식을 이해해야 합니다. 이 문서는 독자가 IP 및 이더넷 네트워크 통신의 기본 원리에 익숙하다는 가정을 기반으로 하고 있습니다. 아래 정보는 이더넷 네트워크에 사용되는 네트워크 주소 지정 개념의 상위 레벨 개요를 설명합니다.

컴퓨터 시스템 같은 호스트 플랫폼의 모든 이더넷 네트워크 인터페이스에는 글로벌 고유 계층 2 주소와 하나 이상의 글로벌 고유 계층 3 주소가 있어야 합니다. 계층 2는 데이터 링크 계층이며 계층 3은 OSI 모델에 정의된 네트워크 계층입니다. 계층 2 주소는 하드웨어에 할당되며 대개 MAC 주소 또는 물리적 주소라고 합니다. 이 주소는 출고 시 사전에 프로그래밍되어 네트워크 인터페이스 카드 또는 내장형 LAN 인터페이스용 시스템 마더보드의 NVRAM에 저장됩니다. 계층 3 주소는 소프트웨어 스택에 할당되는 프로토콜 또는 논리적 주소입니다. IP는 계층 3 프로토콜의 예입니다. 또한 계층 4(전송 계층)는 Telnet 또는 FTP 같은 네트워크 상위 수준 프로토콜마다 포트 번호를 사용합니다. 이러한 포트 번호는 응용 프로그램 간에 트래픽 흐름을 구분하는 데 사용됩니다. 오늘날 네트워크에서 가장 일반적으로 사용되는 계층 4 프로토콜에는 TCP 또는 UDP가 있습니다. IP 주소와 TCP 포트 번호의 조합을 소켓이라고 합니다.

이더넷 장치는 IP 주소가 아니라 MAC 주소를 사용하여 다른 이더넷 장치와 통신합니다. 그러나 대부분의 응용 프로그램은 WINS 및 DNS 같은 이름 서비스에 의해 IP 주소로 변환되는 호스트 이름으로 작동합니다. 따라서 IP 주소에 할당된 MAC 주소를 식별하는 방식이 필요한 것입니다. 이러한 메커니즘은 IP 네트워크의 ARP(주소 분석 프로토콜)에서 제공됩니다. 여기서 유니캐스트 주소는 단일 MAC 주소 또는 단일 IP 주소에 해당됩니다. 브로드캐스트 주소는 네트워크상의 모든 장치에 전송됩니다.

팀 구성 및 네트워크 주소

어댑터 팀은 단일 가상 네트워크 인터페이스 역할을 수행하며 팀 구성이 안된 어댑터와는 달리 다른 네트워크 장치와 구분되지 않습니다. 가상 네트워크 어댑터는 하나의 계층 2와 하나 이상의 계층 3 주소를 보급합니다. 팀 구성 드라이버는 초기화 시 팀 MAC 주소가 되도록 팀을 구성하는 물리적 어댑터 중 하나에서 MAC 주소를 한 개 선택합니다. 이 주소는 보통 드라이버가 초기화하는 첫 번째 어댑터에서 가져옵니다. 팀을 호스트하는 시스템은 ARP 요청을 받으면 ARP Reply의 소스 MAC 주소로 사용할 MAC 주소 한 개를 팀의 실제 어댑터에서 선택합니다. Windows 운영 체제에서 IPCONFIG /all 명령을 실행하면 가상 서버의 IP 및 MAC 주소가 표시되며 개별 물리적 어댑터는 표시되지 않습니다. 프로토콜 IP 주소는 가상 네트워크 인터페이스로 할당되며 개별 물리적 어댑터에는 할당되지 않습니다.

스위치 독립형 팀 구성 모드의 경우 가상 어댑터를 구성하는 모든 물리적 어댑터는 각각 할당된 고유한 MAC 주소를 사용하여 데이터를 전송해야 합니다. 즉, 팀의 각 물리적 어댑터에서 전송하는 프레임은 IEEE 호환을 위해 고유한 MAC 주소를 사용해야 합니다. ARP 캐시 항목은 수신된 프레임이 아닌 ARP 요청 및 ARP Reply에서만 확인할 수 있습니다.

팀 구성 유형 설명

- Smart Load Balancing과 장애 조치
- 일반 트렁킹
- 링크 집계(IEEE 802.3ad LACP)
- SLB(Auto-Fallback Disable)

다음과 같은 세 가지 방법을 사용하여 지원되는 팀 구성 유형을 분류할 수 있습니다.

- 첫 번째는 스위치 포트 구성도 어댑터 팀 구성 유형과 일치해야 하는지 여부를 기준으로 합니다.
- 두 번째는 팀 기능이 로드 균형 조정과 장애 조치를 모두 지원하는지, 아니면 장애 조치만 지원하는지 여부를 기준으로 합니다.
- 세 번째는 링크 집계 제어 프로토콜 사용 여부를 기준으로 합니다.

표 5는 팀 구성 유형 및 해당 분류 요약을 보여 줍니다.

표 5. 사용 가능한 팀 구성 유형

팀 구성 유형	스위치 종속형 (스위치가 특정 팀 유형을 지원해야 함)	스위치에 링크 집계 제어 프로토콜 지원이 필요함	로드 균형 조정	장애 조치
Smart Load Balancing 및 장애 조치(2~8명의 로드 균형 조정 팀 멤 버)			●	●
SLB(Auto-Fallback Disable)				●
링크 집계(802.3ad)	●	●	●	●
일반 트렁킹(FEC/ GEC)/802.3ad-Draft Static	●		●	●

Smart Load Balancing과 장애 조치

Smart Load Balancing™ 및 장애 조치 팀 유형은 로드 균형에 대해 구성된 경우에는 로드 균형 조정 및 장애 조치를, 결함 허용에 대해 구성된 경우에는 장애 조치만을 지원합니다. 이 팀 유형은 모든 Ethernet 스위치에 사용할 수 있으며 스위치에 대한 트렁킹 구성이 필요하지 않습니다. 이 유형의 팀은 여러 MAC 주소와 하나 이상의 IP 주소(보조 IP 주소를 사용하는 경우)를 보급합니다. 팀 MAC 주소는 로드 균형 조정 멤버 목록에서 선택합니다. 시스템에서 ARP 요청을 수신하면 소프트웨어 네트워킹 스택은 항상 팀 MAC 주소가 포함된 ARP Reply를 보냅니다. 로드 균형 조정 과정을 시작할 때 팀 구성 드라이버는 물리적 어댑터 중 하나와 일치하도록 소스 MAC 주소를 변경함으로써 이 ARP Reply를 수정합니다.

Smart Load Balancing을 사용하면 계층 3/계층 4 IP 주소 및 TCP/UDP 포트 번호를 기반으로 로드 균형 조정을 전송 및 수신할 수 있습니다. 즉, 로드 균형 조정은 바이트 또는 프레임 수준이 아닌 TCP/UDP 세션을 기준으로 수행됩니다. 같은 소켓 대화에 속하는 프레임을 순서대로 전달하려면 이 방법을 사용해야 합니다. 로드 균형 조정은 2~8개 사이의 포트에서 지원됩니다. 이러한 포트에는 애드 인 어댑터 및 LOM(LAN on Motherboard) 장치 조합이 포함될 수 있습니다. 전송 로드 균형 조정은 소스 및 대상 IP 주소와 TCP/UDP 포트 번호를 사용하여 해시 테이블을 작성하는 방법으로 수행합니다. 동일한 소스와 대상 IP 주소 및 TCP/UDP 포트 번호의 조합은 보통 동일한 해시 인덱스를 사용하므로 팀에서 동일한 포트를 가리킵니다. 지정된 소켓의 모든 프레임을 전송하기 위해 포트를 선택하면 물리적 어댑터의 고유한 MAC 주소가 프레임에 포함되며 팀 MAC 주

소는 포함되지 않습니다. 이는 IEEE 802.3 표준 호환을 위해 필요합니다. 두 어댑터가 동일한 MAC 주소를 사용해 전송하는 경우 MAC 주소가 중복될 수 있으며 이는 스위치가 처리할 수 없습니다.

수신 로드 균형 조정은 각 클라이언트의 유니캐스트 주소를 ARP 요청(전용 ARP라고도 함)의 대상 주소로 사용하여 클라이언트별로 ARP를 무작위로 전송함으로써 중급 드라이버를 통해 수행됩니다. 이는 트래픽 로드 균형 조정이 아닌 클라이언트 로드 균형 조정으로 간주됩니다. 중급 드라이버는 SLB 팀의 물리적 어댑터 간에 중요한 로드 불균형을 발견하면 G-ARP를 생성하여 들어오는 프레임을 재배포합니다. 중급 드라이버(BASP)는 ARP 요청에 응답하지 않으며, 소프트웨어 프로토콜 스택만이 필요한 ARP Reply를 제공합니다. 수신 로드 균형 조정은 팀 인터페이스를 통해 시스템에 연결하는 클라이언트 기능입니다.

SLB는 팀의 물리적 포트에 걸쳐 클라이언트 컴퓨터의 들어오는 트래픽을 균형 조정하려는 로드 균형 조정 시도를 수신합니다. 이때 SLB는 수정된 무작위 ARP를 사용하여 보낸 사람의 물리적 및 프로토콜 주소에 있는 팀 IP 주소에 대해 다른 MAC 주소를 보급합니다. 이 G-ARP는 각각 물리적 대상 및 프로토콜 주소에 있는 클라이언트 컴퓨터의 MAC 및 IP 주소와 함께 유니캐스트됩니다. 이로 인해 새 MAC 주소 맵이 포함된 대상 클라이언트의 ARP 캐시가 팀 IP 주소로 업데이트됩니다. G-ARP는 브로드캐스트되지 않습니다. 브로드캐스트되는 경우 모든 클라이언트가 해당 트래픽을 동일한 포트에 보내기 때문입니다. 그러면 클라이언트 로드 균형 조정 사용 시의 이점을 활용할 수가 없으며 프레임 전달이 제대로 작동하지 않습니다. 이 수신 로드 균형 조정 체계는 모든 클라이언트 및 팀 구성 시스템이 동일한 서브넷 또는 브로드캐스트 도메인에 있어야 작동합니다.

클라이언트 및 시스템이 다른 서브넷에 있고 들어오는 트래픽이 라우터를 거쳐야 하는 경우 시스템용으로 수신된 트래픽이 로드 균형 조정되지 않습니다. 중급 드라이버가 IP 흐름을 전달하기 위해 선택한 물리적 어댑터는 모든 트래픽을 전달하게 됩니다. 라우터는 특정 프레임을 팀 IP 주소로 보낼 때 ARP 캐시에 있지 않은 경우 ARP 요청을 브로드캐스트합니다. 서버 소프트웨어 스택은 팀 MAC 주소가 포함된 ARP Reply를 생성하지만, 중급 드라이버가 ARP Reply를 수정하여 특정 물리적 어댑터로 보내 해당 세션에 대한 흐름을 설정합니다.

이는 ARP가 라우팅 가능한 프로토콜이 아니기 때문입니다. ARP에는 IP 헤더가 없으므로 라우터 또는 기본 게이트웨이로 전송되지 않습니다. ARP는 로컬 서브넷 프로토콜일 뿐입니다. 특히 G-ARP는 브로드캐스트 패킷이 아니기 때문에 라우터가 처리하지 않으며 해당 ARP 캐시도 업데이트하지 않습니다.

라우터가 다른 네트워크 장치에 사용되는 ARP를 처리하는 경우는 프록시 ARP를 활성화하고 호스트에 기본 게이트웨이가 없는 경우 뿐입니다. 그러나 이러한 경우는 거의 없으며 대부분의 응용 프로그램에 권장되지 않습니다.

전송 로드 균형 조정은 소스 및 대상 IP 주소와 TCP/UDP 포트 번호를 기반으로 하므로 라우터를 통한 전송 트래픽은 로드 균형 조정됩니다. 라우터는 소스 및 대상 IP 주소를 변경하지 않으므로 로드 균형 조정 알고리즘은 예상대로 작동합니다.

HSRP(Hot Standby Routing Protocol)에 대해 라우터를 구성하면 로드 균형 조정을 어댑터 팀에서 받을 수 없습니다. 보통 HSRP는 두 개의 라우터가 하나의 라우터로 작동하도록 허용하여 가상 IP 및 가상 MAC 주소를 보급합니다. 이 두 물리적 라우터 중 하나는 활성 인터페이스이고 다른 하나는 대기 인터페이스입니다. HSRP는 호스트 노드의 서로 다른 기본 게이트웨이를 사용하여 HSRP 그룹의 여러 라우터에 걸쳐 노드를 공유할 수는 있지만 항상 팀의 기본 MAC 주소를 가리킵니다.

일반 트렁킹

일반 트렁킹은 링크의 양쪽 끝, 즉 서버 인터페이스 및 스위치 포트에서 포트를 구성해야 하는 스위치 보조 팀 구성 모드입니다. 이를 보통 Cisco Fast EtherChannel 또는 Gigabit EtherChannel이라고도 합니다. 또한 일반 트렁킹은 Extreme Networks Load Sharing 및 Bay Networks 또는 IEEE 802.3ad 링크 집계 등의 다른 스위치 OEM에 의한 유사 구현도 지원합니다. 이 모드에서 팀은 프로토콜 스택이 ARP 요청에 응답할 때 하나의 MAC 주소 및 하나의 IP 주소를 보급합니다. 또한 팀의 각 물리적 어댑터는 프레임을 전송할 때 동일한 팀 MAC 주소를 사용합니다. 이러한 작업이 가능한 이유는 링크의 반대쪽 끝에 있는 스위치가 팀 구성 모드를 인식하여 팀의 모든 포트에서 이루어지는 단일 MAC 주소 사용을 처리하기 때문입니다. 스위치의 전달 테이블은 트렁크를 단일 가상 포트로 반영합니다.

이 팀 구성 모드에서 중급 드라이버는 나가는 트래픽에 대해서만 로드 균형 조정 및 장애 조치를 제어하는 반면, 들어오는 트래픽은 스위치 펌웨어 및 하드웨어에 의해 제어됩니다. Smart Load Balancing의 경우와 마찬가지로, BASP 중급 드라이버는

IP/TCP/UDP 소스 및 대상 주소를 사용하여 서버의 전송 트래픽을 균형 조정합니다. 대부분의 스위치는 소스의 XOR 해시 및 대상 MAC 주소를 구현합니다.

링크 집계(IEEE 802.3ad LACP)

링크 집계는 링크 집계 제어 프로토콜을 사용하여 팀을 구성할 포트를 협상한다는 점을 제외하고는 일반 트렁킹과 유사합니다. 팀이 작동하려면 LACP를 링크의 양쪽 끝에서 활성화해야 합니다. LACP를 링크의 양쪽 끝에서 사용할 수 없는 경우 802.3ad는 링크의 양쪽 끝이 연결 상태이기만 하면 되는 수동 집계를 제공합니다. 수동 집계는 LACP 메시지 교환을 수행하지 않고 구성원 링크를 활성화하기 위해 제공되므로, 신뢰할 수 있으며 강력한 LACP 협상 링크로 간주해서는 안 됩니다. LACP는 집계할 수 있는 구성원 링크를 자동으로 결정하여 해당 링크를 집계합니다. LACP는 프레임이 손실되거나 중복되지 않도록 링크 집계를 위한 물리적 링크를 제어된 방식으로 추가 또는 제거하기 위해 제공됩니다. 집계 링크 구성원 제거는 LACP(링크 집계 제어 프로토콜) 사용 집계 링크에 대해 선택적으로 활성화할 수 있는 마커 프로토콜에 의해 제공됩니다.

링크 집계 그룹은 트렁크의 모든 포트에 대해 단일 MAC 주소를 보급합니다. 집계의 MAC 주소는 그룹을 구성하는 MAC 중 하나의 MAC 주소일 수 있습니다. LACP 및 마커 프로토콜은 멀티캐스트 대상 주소를 사용합니다.

링크 집계 제어 기능을 통해 집계할 링크가 결정되면 포트가 시스템의 집계 함수로 바인딩되며 집계 그룹을 변경해야 하는지를 결정하기 위해 상태가 모니터링됩니다. 링크 집계는 여러 링크의 개별 기능을 결합하여 보다 성능이 뛰어난 가상 링크를 형성합니다. LACP 트렁크의 링크에 오류가 발생하거나 링크를 대체해도 연결은 끊어지지 않습니다. 이 경우 트래픽은 트렁크의 나머지 링크로 장애 조치됩니다.

SLB(Auto-Fallback Disable)

이 팀 유형은 Smart Load Balancing 및 장애 조치 팀 유형과 동일하지만, 대기 멤버가 활성화된 경우 기본 멤버가 복원되면 팀은 기본 멤버로 다시 스위칭하지 않고 대기 멤버를 사용하여 계속 진행한다는 예외가 있습니다. 이 팀 유형은 네트워크 케이블이 네트워크 어댑터에 지속적으로 연결되고 해제되는 경우에만 지원되며, 어댑터가 장치 관리자 또는 핫 플러그 PCI를 통해 제거/설치된 경우에는 지원되지 않습니다.

팀에 할당된 기본 어댑터를 비활성화하면 팀은 자동 고장 대체가 수행되는 Smart Load Balancing 및 장애 조치 팀 유형으로 작동합니다.

소프트웨어 구성 요소

팀 구성은 Windows 운영 체제 환경의 NDIS 중급 드라이버를 통해 구현됩니다. 이 소프트웨어 구성 요소는 미니포트 드라이버, NDIS 계층 및 프로토콜 스택에 작동하여 팀 구성 아키텍처를 활성화합니다(그림 1 참조). 미니포트 드라이버는 호스트 LAN 컨트롤러를 직접 제어하여 송신, 수신 및 인터럽트 처리 등의 기능을 활성화합니다. 중급 드라이버는 미니포트 드라이버 및 프로토콜 계층 사이에 장착되어 여러 미니포트 드라이버 인스턴스를 멀티플렉싱하고 단일 어댑터처럼 보이는 가상 어댑터를 NDIS 계층에 만듭니다. NDIS는 라이브러리 기능 집합을 통해 미니포트 드라이버 간 또는 중급 드라이버 및 프로토콜 스택 간의 통신을 활성화합니다. IP 주소 등의 프로토콜 주소가 각 미니포트 장치 인스턴스에 할당됩니다. 그러나 중급 드라이버가 설치되는 경우 프로토콜 주소는 팀을 구성하는 개별 미니포트 장치가 아닌 가상 팀 어댑터에 할당됩니다.

Broadcom 제공 팀 구성 자원은 함께 작동하며 패키지로 제공되는 세 개의 개별 소프트웨어 구성 요소에 의해 제공됩니다. 한 구성 요소가 업그레이드되면 모든 나머지 구성 요소도 지원되는 버전으로 업그레이드해야 합니다. 표 6에서는 이 세 가지 소프트웨어 구성 요소 및 지원되는 운영 체제용 해당 연결 파일에 대해 설명합니다.

표 6. Broadcom 팀 구성 소프트웨어 구성 요소

소프트웨어 구성 요소	Broadcom 이름	Windows	Linux
미니포트 드라이버	Broadcom 기본 드라이버	b57nd60X.sys	tg3
중급 드라이버	BASP(Broadcom Advanced Server Program)	Basp.sys	본딩
구성 사용자 인터페이스	Broadcom Advanced Control Suite(BACS)	BACS	BACS CLI
NDIS 6 드라이버	Windows Vista 이상 x86 드라이버	b57nd60x.sys	없음
	Windows Vista 이상 x64 드라이버	b57nd60a.sys	

Broadcom Advanced Control Suite(BACS) 유틸리티는 32비트와 64비트 Windows Server 운영 체제에서 실행됩니다. BACS는 로드 균형 조정 및 결함 허용 팀 구성 그리고 VLAN 구성에 사용됩니다. 또한 각 네트워크 어댑터의 MAC 주소, 드라이버 버전 및 상태 정보를 표시합니다. BACS에는 하드웨어 진단, 케이블 테스트 및 네트워크 토폴로지 테스트 등의 다양한 진단 도구도 포함됩니다.

하드웨어 요구 사항

- [Ethernet 스위치](#)
- [라우터](#)

이 문서에 설명되어 있는 다양한 팀 구성 모드에는 클라이언트를 팀 구성 시스템에 연결하는 데 사용되는 네트워킹 장치에 대한 특정 제한이 있습니다. 각 네트워크 상호 연결 기술 유형은 팀 구성에 대해 다음 절에 설명되어 있는 것과 같은 영향을 줍니다.

Ethernet 스위치

Ethernet 스위치를 사용하면 Ethernet 네트워크를 여러 브로드캐스트 도메인으로 나눌 수 있습니다. 스위치는 Ethernet MAC 주소만을 기반으로 하여 호스트 간에 Ethernet 패킷을 전달합니다. 스위치에 연결되어 있는 물리적 네트워크 어댑터는 반이중 또는 전이중 모드로 동작할 수 있습니다.

일반 트렁킹 및 802.3ad 링크 집계를 지원하려면 스위치는 그와 같은 특정 기능을 지원해야 합니다. 스위치가 이러한 프로토콜을 지원하지 않는 경우에도 Smart Load Balancing 용으로는 사용할 수 있습니다.

라우터

라우터는 계층 3 이상의 프로토콜에서 네트워크 트래픽을 라우팅하기 위한 것이지만, 스위칭 기능이 있는 계층 2 장치에도 사용할 수 있습니다. 라우터에 직접 연결된 포트의 팀 구성 포트는 지원되지 않습니다.

팀 유형별 지원 기능

표 7에는 Broadcom NIC에서 지원하는 각 팀 유형의 기능이 비교되어 있습니다. 이 표를 사용하여 사용자의 응용 프로그램에 가장 적절한 팀 유형을 결정할 수 있습니다. 팀 구성 소프트웨어는 단일 팀에서 최대 8개 포트, 그리고 단일 시스템에서 최대 16개 팀을 지원합니다. 이러한 팀은 지원되는 팀 구성 유형의 조합일 수 있지만 이 경우 각 팀은 별도의 네트워크 또는 서브넷에 있어야 합니다.

표 7. 팀 유형 비교

팀 유형	결함 허용	로드 균형 조정	스위치 종속형 정적 트렁킹	스위치 독립형 동적 링크 집계 (IEEE 802.3ad)
기능	SLB(대기 지원) ^a	SLB	일반 트렁킹	링크 집계
팀당 포트 수(동일한 브로드캐스트 도메인)	2-8	2-8	2-8	2-8
팀 수	16	16	16	16
어댑터 결함 허용	예	예	예	예
스위치 링크 결함 허용(동일한 브로드캐스트 도메인)	예	예	스위치 종속형	스위치 종속형
TX 로드 균형 조정	아니오	예	예	예
RX 로드 균형 조정	아니오	예	예(스위치가 수행함)	예(스위치가 수행함)
호환 스위치 필요	아니오	아니오	예	예

표 7. 팀 유형 비교 (계속)

팀 유형	결함 허용	로드 균형 조정	스위치 종속형 정적 트렁킹	스위치 독립형 동적 링크 집계 (IEEE 802.3ad)
연결 확인을 위한 하트비트	아니오	아니오	아니오	아니오
혼합 매체(서로 다른 매체가 있는 어댑터)	예	예	예(스위치 종속형)	예
혼합 속도(일반 속도를 지원하지 않지만 서로 다른 속도로 작동할 수 있는 어댑터)	예	예	아니오	아니오
혼합 속도(일반 속도를 지원하며 서로 다른 속도에서 작동할 수 있는 어댑터)	예	예	아니오(속도가 같아야 함)	예
TCP/IP 로드 균형 조정	아니오	예	예	예
혼합 공급업체 팀 구성	예 ^b	예 ^b	예 ^b	예 ^b
비 IP 로드 균형 조정	아니오	예(IPX 아웃바운드 트래픽에만 해당)	예	예
모든 팀 구성원에 대해 동일한 MAC 주소	아니오	아니오	예	예
모든 팀 구성원에 대해 동일한 IP 주소	예	예	예	예
IP 주소별 로드 균형 조정	아니오	예	예	예
MAC 주소별 로드 균형 조정	아니오	예(비 IP/IPX에 사용)	예	예

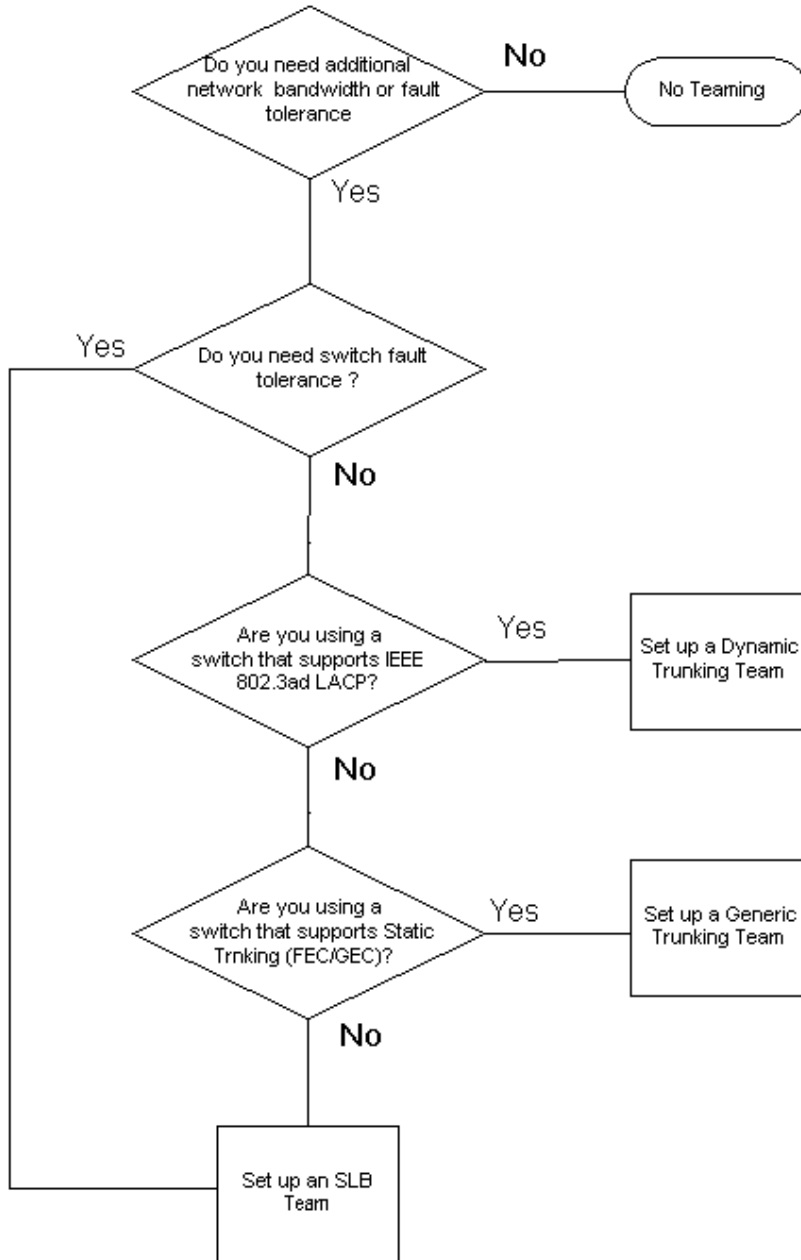
^a 기본 및 대기 구성원이 각각 하나씩 있는 SLB

^b 팀에 적어도 하나의 Broadcom 어댑터가 있어야 함

팀 유형 선

다음 흐름도에는 팀 구성 계획 시의 의사 결정 흐름이 나와 있습니다. 팀 구성을 수행하는 가장 큰 이유는 추가 네트워크 대역폭 및 결함 허용이 필요하기 때문입니다. 팀 구성은 이러한 두 요구 사항을 모두 충족할 수 있도록 링크 집계 및 결함 허용을 제공합니다. 기본 설정 팀 구성 시의 선택 순서는 링크 집계를 첫 번째, 일반 트렁킹을 두 번째로 선택하며, 이 두 옵션을 지원하지 않는 관리되지 않는 스위치를 사용하는 경우에는 SLB 팀 구성을 세 번째로 선택합니다. 스위치 결함 허용이 필수 요구 사항인 경우에는 SLB밖에 선택할 수가 없습니다(그림 1 참조).

그림 1: 팀 유형 선택 과정



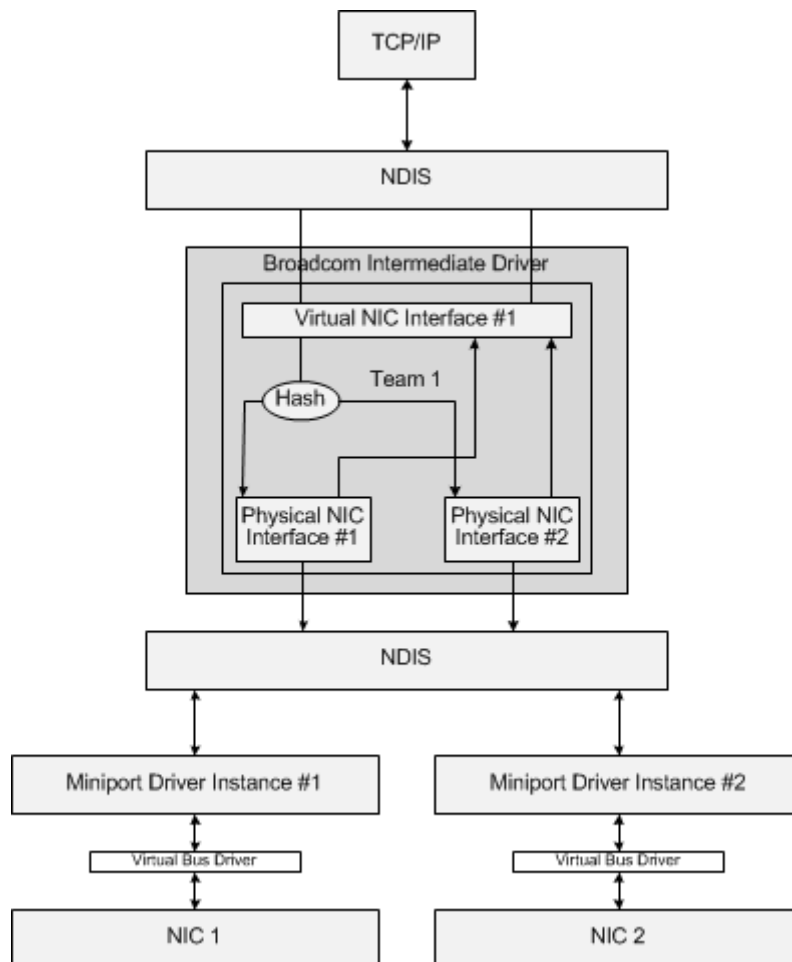
팀 구성 메커니즘

- 아키텍처
- 운영 체제별 드라이버 지원
- 지원되는 팀 구성 속도

아키텍처

Broadcom Advanced Server Program은 NDIS 중급 드라이버로 구현됩니다(그림 2 참조). 이 프로그램은 TCP/IP 등의 프로토콜 스택 하위에서 운영되며 가상 어댑터로 표시됩니다. 이 가상 어댑터는 팀에서 초기화된 첫 번째 포트의 MAC 주소를 상속합니다. 계층 3 주소도 가상 어댑터에 대해 구성해야 합니다. BASP의 기본 기능은 팀 구성을 위해 선택한 시스템에 설치된 물리적 어댑터 간의 인바운드(SLB용) 및 아웃바운드 트래픽(모든 팀 구성 모드용) 균형 조정입니다. 인바운드 및 아웃바운드 알고리즘은 상호 독립적이면서 대칭적입니다. 특정 세션의 아웃바운드 트래픽을 특정 포트에, 그리고 그에 해당하는 인바운드 트래픽을 또 다른 포트에 할당할 수 있습니다.

그림 2: 중급 드라이버



아웃바운드 트래픽 흐름

Broadcom 중급 드라이버는 모든 팀 구성 모드의 아웃바운드 트래픽 흐름을 관리합니다. 아웃바운드 트래픽의 경우 모든 패킷은 먼저 흐름으로 분류된 다음 전송을 위해 선택한 물리적 어댑터로 배포됩니다. 흐름 분류 작업에는 알려진 프로토콜 필드에 대한 효율적인 해시 계산이 포함됩니다. 계산 결과로 생성되는 해시 값은 아웃바운드 흐름 해시 테이블로의 인덱싱에 사용됩니다. 선택한 아웃바운드 흐름 해시 항목에는 이 흐름을 전송하는 선택한 물리적 어댑터의 인덱스가 포함됩니다. 그런 후에 패킷의 소스 MAC 주소는 선택한 물리적 어댑터의 MAC 주소로 수정됩니다. 이렇게 수정된 패킷은 전송을 위해 선택한 물리적 어댑터로 전달됩니다.

아웃바운드 TCP 및 UDP 패킷은 계층 3 및 계층 4 헤더 정보를 사용하여 분류됩니다. 이 체계를 사용하면 HTTP 및 FTP 등의 널리 알려진 포트를 사용하는 일반적인 인터넷 프로토콜 서비스에 대한 로드 배포가 향상됩니다. 그러므로 BASP는 패킷별이 아닌 TCP 세션별로 로드 균형 조정을 수행합니다.

아웃바운드 흐름 해시 항목에서 통계 카운터도 분류 후에 업데이트됩니다. 로드 균형 조정 엔진은 이러한 카운터를 사용하여 팀 구성 포트 간의 흐름을 주기적으로 배포합니다. 아웃바운드 코드 경로는 아웃바운드 흐름 해시 테이블에 대해 복수 동시 액세스가 허용되는 경우 최상의 동시 액세스를 보장할 수 있도록 디자인되었습니다.

TCP/IP 외의 프로토콜의 경우 아웃바운드 패킷에 대해 항상 첫 번째 물리적 어댑터가 선택됩니다. 이 경우의 예외는 인바운드 로드 균형 조정을 위해 다른 방식으로 처리되는 ARP(주소 분석 프로토콜)입니다.

인바운드 트래픽 흐름(SLB에만 해당)

Broadcom 중급 드라이버는 SLB 팀 구성 모드의 인바운드 트래픽 흐름을 관리합니다. 아웃바운드 로드 균형 조정과는 달리 인바운드 로드 균형 조정은 로드 균형 조정 서버와 동일한 서브넷에 있는 IP 주소에만 적용할 수 있습니다. 인바운드 로드 균형 조정은 각 IP 호스트가 고유한 ARP 캐시를 사용하여 IP 데이터그램을 Ethernet 프레임으로 캡슐화하는 주소 분석 프로토콜(RFC0826)의 독특한 특성을 사용합니다. BASP는 ARP 응답을 주의 깊게 조정하여 각 IP 호스트가 인바운드 IP 패킷을 올바른 물리적 어댑터로 보내도록 지시합니다. 그러므로 인바운드 로드 균형 조정은 인바운드 흐름의 통계 기록을 기반으로 하는 선형 계획 체계입니다. 클라이언트의 서버에 대한 새 연결은 항상 기본 물리적 어댑터에서 발생합니다. 이는 운영 체제 프로토콜 스택에 의해 생성된 ARP Reply는 항상 논리 IP 주소를 기본 물리적 어댑터의 MAC 주소와 연결하기 때문입니다.

아웃바운드의 경우와 마찬가지로 인바운드 흐름 헤드 해시 테이블도 있습니다. 이 테이블 내의 각 항목에는 단일 링크 목록이 있으며 각 링크(인바운드 흐름 항목)는 동일한 서브넷에 있는 IP 호스트를 나타냅니다.

인바운드 IP 데이터그램이 도착하면 IP 데이터그램의 소스 IP 주소를 해시하여 해당 인바운드 흐름 헤드 항목을 찾습니다. 선택한 항목에 저장된 두 개의 통계 카운터도 업데이트됩니다. 이 카운터는 로드 균형 조정 엔진이 주기적으로 흐름을 물리적 어댑터에 재할당하는 방식으로 아웃바운드 카운터처럼 사용됩니다.

인바운드 코드 경로에서 인바운드 흐름 헤드 해시 테이블도 동시 액세스를 허용합니다. 인바운드 흐름 항목의 링크 목록은 ARP 패킷 처리 및 주기적인 로드 균형 조정 작업에서만 참조됩니다. 인바운드 흐름 항목에 대한 패킷당 참조는 없습니다. 링크 목록은 바인딩되지 않지만 각 ARP 패킷이 아닌 패킷 처리 과정의 오버헤드는 항상 상수입니다. 그러나 ARP 패킷 처리(인바운드 및 아웃바운드)는 해당 링크 목록 내의 링크 수에 따라 달라집니다.

인바운드 처리 경로에서는 브로드캐스트 패킷이 다른 물리적 어댑터에서 시스템을 통해 다시 루프되지 않도록 필터링도 사용됩니다.

프로토콜 지원

ARP 및 IP/TCP/UDP 흐름은 로드 균형 조정됩니다. 패킷이 IP 프로토콜 전용(예: ICMP 또는 IGMP)인 경우 특정 IP 주소로 흐르는 모든 데이터는 동일한 물리적 어댑터를 통해 나갑니다. 패킷이 L4 프로토콜용 TCP 또는 UDP를 사용하는 경우에는 포트 번호가 해시 알고리즘에 추가되어 두 개의 개별 L4 흐름이 두 개의 개별 물리적 어댑터를 통해 동일한 IP 주소로 나갈 수 있습니다.

예를 들어, 클라이언트의 IP 주소가 10.0.0.1이면 IP 주소만 해시에 사용되므로 모든 IGMP 및 ICMP 트래픽은 동일한 물리적 어댑터를 통해 나갑니다. 이 흐름은 다음과 같습니다.

IGMP -----> PhysAdapter1 -----> 10.0.0.1

ICMP -----> PhysAdapter1 -----> 10.0.0.1

이 서버에서 동일한 10.0.0.1 주소로 TCP 및 UDP 흐름도 보내는 경우, 이 흐름은 IGMP 및 ICMP와 동일한 물리적 어댑터에 있을 수도 있고 IGMP 및 ICMP와는 완전히 다른 물리적 어댑터에 있을 수도 있습니다. 이 스트림은 다음과 같습니다.

IGMP -----> PhysAdapter1 -----> 10.0.0.1

ICMP -----> PhysAdapter1 -----> 10.0.0.1

TCP-----> PhysAdapter1 -----> 10.0.0.1

UDP-----> PhysAdatper1 -----> 10.0.0.1

또는 스트림이 다음과 같을 수도 있습니다.

IGMP -----> PhysAdapter1 -----> 10.0.0.1

ICMP -----> PhysAdapter1 -----> 10.0.0.1

TCP-----> PhysAdapter2 -----> 10.0.0.1

UDP-----> PhysAdatper3 -----> 10.0.0.1

어댑터 간의 실제 할당은 시간이 지나면서 변경될 수 있지만, 해시에서는 IP 주소만이 사용되므로 TCP/UDP 기반이 아닌 모든 프로토콜은 동일한 물리적 어댑터를 통과합니다.

성능

현재 사용되는 네트워크 인터페이스 카드는 CPU를 많이 사용하는 특정 작업을 Offload하여 CPU 사용량을 줄이는 여러 가지 하드웨어 기능을 제공합니다(팀 구성 및 기타 고급 네트워크 속성 참조). 반면, BASP 중급 드라이버는 프로토콜 스택에서 수신되는 모든 패킷을 검사하여 특정 물리적 인터페이스를 통해 해당 패킷을 보내기 전에 내용을 확인하여 처리해야 하는 순수한 소프트웨어 기능입니다. BASP 드라이버에서 거의 일정한 시간에 나가는 각 패킷을 처리할 수는 있지만, 이 경우 이미 CPU 바인딩된 일부 응용 프로그램을 팀 구성 인터페이스에서 작동하는 경우 오류가 발생할 수 있습니다. 이와 같은 응용 프로그램은 로드 균형 조정 기능보다는 중급 드라이버의 장애 조치 기능을 사용해야 하는 경우에 더 적절하거나, Large Send Offload 등의 특정 하드웨어 기능을 제공하는 단일 물리적 어댑터에 대해 보다 효율적으로 작동할 수도 있습니다.

운영 체제별 드라이버 지원

앞서 설명한 것처럼, BASP는 Windows Server 2008 및 2012 운영 체제 환경에서 지원됩니다.

아래 표에는 다양한 팀 구성 모드 기능이 요약되어 있습니다.

표 8. 팀 구성 모드 기능

특징	Windows 지원
Smart Load Balancing™	
사용자 인터페이스	BACS ^a
팀 수	16
팀당 어댑터 수	8
즉시 교체	예
즉시 추가	예
즉시 제거	예
링크 속도 지원	다른 속도
프레임 프로토콜	IP
들어오는 패킷 관리	BASP
나가는 패킷 관리	BASP
장애 조치 이벤트	링크 손실 또는 LiveLink 이벤트
장애 조치 시간	500ms 이하
대체 시간	약 1.5s ^b
LiveLink 지원	예
MAC 주소	다름
여러 공급업체 팀 구성	예
일반 트렁킹	
사용자 인터페이스	BACS
팀 수	16
팀당 어댑터 수	8
즉시 교체	예
즉시 추가	예
즉시 제거	예
링크 속도 지원	다른 속도
프레임 프로토콜	모두
들어오는 패킷 관리	스위치
나가는 패킷 관리	BASP
장애 조치 이벤트	링크 손실의 경우만
장애 조치 시간	500ms
대체 시간	약 1.5s ^b
MAC 주소	모든 어댑터에 대해 동일

표 8. 팀 구성 모드 기능 (계속)

특징	Windows 지원
여러 공급업체 팀 구성	예
동적 트렁킹	
사용자 인터페이스	BACS
팀 수	16
팀당 어댑터 수	8
즉시 교체	예
즉시 추가	예
즉시 제거	예
링크 속도 지원	다른 속도
프레임 프로토콜	모두
들어오는 패킷 관리	스위치
나가는 패킷 관리	BASP
장애 조치 이벤트	링크 손실의 경우만
장애 조치 시간	500ms 이하
대체 시간	약 1.5s ^b
MAC 주소	모든 어댑터에 대해 동일
여러 공급업체 팀 구성	예

^a Broadcom Advanced Control Suite

^b Port Fast 또는 Edge Port가 활성화되어 있어야 합니다.

지원되는 팀 구성 속도

각 팀 유형에 지원되는 다양한 링크 속도는 표 9에 나열되어 있습니다. 혼합 속도란 서로 다른 링크 속도로 실행되는 팀 구성 어댑터 기능을 말합니다.

표 9. 팀 구성의 링크 속도

팀 유형	링크 속도	트래픽 방향	속도 지원
SLB	10/100/1000	들어오는 트래픽/나가는 트래픽	혼합 속도
FEC	100	들어오는 트래픽/나가는 트래픽	동일한 속도
GEC	1000	들어오는 트래픽/나가는 트래픽	동일한 속도
IEEE 802.3ad	10/100/1000	들어오는 트래픽/나가는 트래픽	혼합 속도

팀 구성 및 기타 고급 네트워크 속성

- Checksum Offload
- IEEE 802.1p QoS 태그
- Large Send Offload
- 대용량 프레임
- IEEE 802.1Q VLAN
- Wake On LAN
- PXE(Preboot Execution Environment)

팀을 만들거나 팀 구성원을 추가 또는 제거하거나 팀 구성원의 고급 설정을 변경하기 전에 각 팀 구성원을 유사하게 구성했는지 확인하십시오. 확인할 설정에는 VLAN 및 QoS 패킷 태그, 대용량 프레임 및 다양한 Offload 등이 포함됩니다. 고급 어댑터 속성 및 팀 구성 지원은 표 10에 나열되어 있습니다.

표 10. 고급 어댑터 속성 및 팀 구성 지원

어댑터 속성	팀 구성 가상 어댑터의 지원 여부
Checksum Offload	예
IEEE 802.1p QoS 태그	아니오
Large Send Offload	예 ^a
대용량 프레임	예 ^b
IEEE 802.1Q VLAN	예
Wake On LAN	아니오
PXE(Preboot Execution Environment)	예 ^c

^a 팀의 모든 어댑터가 이 기능을 지원해야 합니다. IPMI도 활성화되어 있는 경우 일부 어댑터는 이 기능을 지원하지 않을 수도 있습니다.

^b 팀의 모든 어댑터가 지원해야 합니다.

^c 클라이언트가 아닌 PXE 서버로만 사용 가능합니다.

Checksum Offload

Checksum Offload는 송신 및 수신 트래픽의 TCP/IP/UDP Checksum을 호스트 CPU가 아닌 어댑터 하드웨어가 계산하도록 하는 Broadcom 네트워크 어댑터 속성입니다. 트래픽 사용량이 높은 상태에서 이 속성은 시스템이 호스트 CPU가 Checksum을 계산하도록 지정된 경우보다 더 많은 연결을 보다 효율적으로 처리할 수 있도록 합니다. 이 속성은 기본적으로 하드웨어 속성이므로 소프트웨어 전용 구현의 이점은 사용할 수 없습니다. Checksum Offload를 지원하는 어댑터는 이 기능을 운영 체제로 보급하여 Checksum을 프로토콜 스택에서 계산하지 않아도 되도록 합니다. 중급 드라이버는 프로토콜 계층과 미니포트 드라이버 바로 사이에 있기 때문에 프로토콜 계층에서는 Checksum을 Offload할 수 없습니다.

IEEE 802.1p QoS 태그

IEEE 802.1p 표준에는 최대 8개의 우선 순위 수준을 지원하는 3비트 필드가 포함됩니다. 이 필드를 사용하여 트래픽 우선 순위를 지정할 수 있습니다. BASP 중급 드라이버는 IEEE 802.1p QoS 태그를 지원하지 않습니다.

Large Send Offload

LSO(Large Send Offload)는 TCP 등의 상위 수준 프로토콜이 대형 데이터 패킷을 헤더가 포함된 보다 작은 패킷 집합으로 분해하지 못하도록 하는, Broadcom 네트워크 어댑터에서 제공되는 기능입니다. 프로토콜 스택은 데이터 패킷에 대해 최대 64KB의 단일 헤더만 생성하면 되며, 어댑터 하드웨어는 원래 제공된 단일 헤더를 기준으로 하여 데이터 버퍼를 크기가 대략적으로 지정되며 순서가 올바른 헤더를 포함하는 Ethernet 프레임으로 분해합니다.

대용량 프레임

BASP 중급 드라이버는 팀의 모든 물리적 어댑터도 대용량 프레임을 지원하고 팀의 모든 어댑터에 크기가 동일하게 설정되어 있는 경우 대용량 프레임을 지원합니다.

IEEE 802.1Q VLAN

IEEE 802.3ac 표준은 IEEE 802.1Q 사양에 지정되어 있는 Ethernet 네트워크에 대한 가상 브리지 LAN 태그를 지원하기 위한 프레임 형식 확장을 정의합니다. VLAN 프로토콜에서는 태그를 Ethernet 프레임에 삽입하여 프레임이 속하는 VLAN을 식별할 수 있습니다. 4바이트 VLAN 태그(있는 경우)가 소스 MAC 주소 및 길이/유형 필드 사이의 Ethernet 프레임에 삽입됩니다. VLAN 태그의 첫 2바이트는 IEEE 802.1Q 태그 유형으로 구성되며 다음 2바이트는 사용자 우선 순위 필드와 VID(VLAN 식별자)를 포함합니다. 가상 LAN(VLAN)을 사용하면 사용자는 물리적 LAN을 논리적 하위 부분으로 분할할 수 있습니다. 정의된 각 VLAN은 별도의 네트워크로 동작하며 해당 트래픽과 브로드캐스트도 다른 트래픽 및 브로드캐스트와 격리되어 있으므로 각 논리 그룹 내의 대역폭 효율성이 높아집니다. VLAN은 또한 관리자가 적절한 보안 및 QoS(Quality of Service) 정책을 적용할 수 있도록 합니다. BASP는 팀 또는 어댑터당 64개의 VLAN, 즉 태그가 지정된 63개 VLAN 및 태그가 지정되지 않은 1개 VLAN을 만들 수 있도록 합니다. 그러나 운영 체제 및 시스템 리소스로 인해 실제 VLAN 수는 제한됩니다. VLAN 지원은 IEEE 802.1q에 따라 제공되며 팀 구성 환경은 물론 단일 어댑터에 대해서도 지원됩니다. VLAN은 같은 유형의 팀 구성에 대해서만 지원되며 여러 공급업체 팀 구성 환경에서는 지원되지 않습니다. BASP 중급 드라이버는 VLAN 태그를 지원합니다. 하나 이상의 VLAN이 중급 드라이버의 단일 인스턴스로 바인딩될 수 있습니다.

Wake On LAN

WOL(Wake on LAN)은 Ethernet 인터페이스를 통해 특정 패킷이 도착하면 시스템이 절전 모드에서 해제되도록 하는 기능입니다. 가상 어댑터는 소프트웨어 전용 장치로 구현되므로 **Wake on LAN** 기능을 구현할 수 있는 하드웨어 기능이 없기 때문에, 가상 어댑터를 통해 시스템을 절전 상태에서 해제할 수 없습니다. 그러나 물리적 어댑터는 어댑터가 팀의 일부인 경우에도 이 속성을 지원합니다.

PXE(Preboot Execution Environment)

PXE(Preboot Execution Environment)를 사용하면 시스템이 네트워크를 통해 운영 체제 이미지에서 부팅되도록 할 수 있습니다. PXE는 운영 체제가 로드되기 전에 호출되도록 정의되어 있으므로 **BASP** 중급 드라이버가 팀을 로드 및 활성화하지는 못합니다. 따라서, 운영 체제가 로드될 때 팀에 참여하는 물리적 어댑터를 **PXE** 클라이언트로 사용할 수 있기는 하지만 팀 구성은 **PXE** 클라이언트로는 지원되지 않습니다. 팀 구성 어댑터를 **PXE** 클라이언트로는 사용할 수 없지만 **PXE** 서버로는 사용할 수 있습니다. **PXE** 서버는 **DHCP**(동적 호스트 제어 프로토콜) 및 **TFTP**(Trivial File Transfer Protocol) 조합을 사용하여 운영 체제 이미지를 **PXE** 클라이언트에 제공합니다. 이 두 프로토콜은 모두 IP를 통해 작동되며 모든 팀 구성 모드에서 지원됩니다.

일반 네트워크 고려 사항

- 스위치 간의 팀 구성
- 스페닝 트리 알고리즘
- Microsoft NLB/WLBS를 사용한 팀 구성

스위치 간의 팀 구성

SLB 팀 구성을 스위치 간에 구성할 수 있습니다. 그러나 이 경우 스위치를 서로 연결해야 합니다. 일반 트렁킹 및 링크 집계는 스위치 간에 작동하지 않습니다. 이러한 각 구현의 경우에는 팀의 모든 물리적 어댑터가 동일한 Ethernet MAC 주소를 공유해야 하기 때문입니다. SLB는 팀의 포트와 해당 포트의 직접 링크 파트너 간의 링크 손실만을 감지할 수 있습니다. 즉, SLB는 스위치의 다른 하드웨어 오류에 대응할 수 없으며 다른 포트의 링크 손실을 감지할 수도 없습니다.

스위치 링크 결함 허용

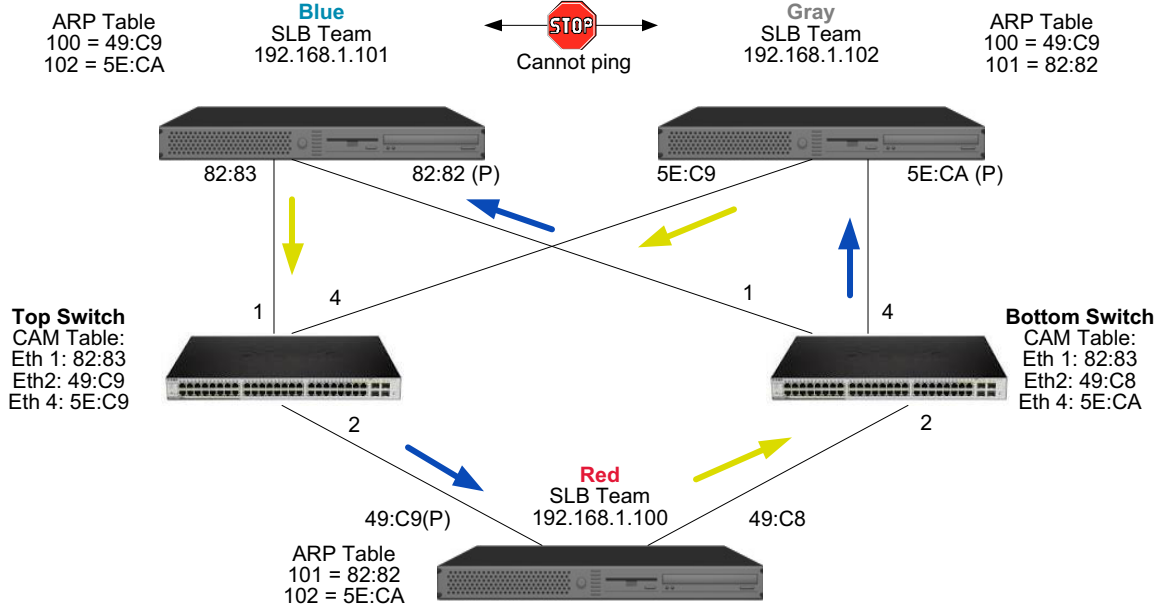
아래 다이어그램에는 스위치 결함 허용 구성의 SLB 팀 작동이 설명되어 있습니다. 두 활성 구성원이 있는 SLB 팀의 ping 요청 및 ping 응답 매핑이 표시되어 있습니다. 모든 서버(Blue, Gray 및 Red)에는 서로에 대한 지속적인 ping이 있습니다. 그림 3은 두 스위치 간에 상호 연결 케이블이 없는 설정입니다. 그림 4는 상호 연결 케이블이 있는 설정이며, 그림 5는 상호 연결 케이블이 있는 경우의 장애 조치 이벤트 예제입니다. 이러한 시나리오는 두 스위치 간의 팀 구성 동작 및 상호 연결 링크의 중요성을 설명합니다.

다이어그램에는 ICMP 반향 요청(노란색 화살표)을 보내는 보조 팀 구성원이 나와 있습니다. 기본 팀 구성원은 개별 ICMP 반향 응답(파란색 화살표)을 받습니다. 이는 팀 구성 소프트웨어의 주요 특성을 보여 줍니다. 로드 균형 조정 알고리즘은 프레임이 송신 또는 수신될 때 로드 균형 조정되는 방법을 동기화하지 않습니다. 다시 말해, 특정 대화의 프레임은 팀의 서로 다른 인터페이스에서 송신 및 수신될 수 있습니다. 이는 Broadcom에서 지원하는 모든 팀 구성 유형에 대해 적용됩니다. 그러므로 동일한 팀의 포트에 연결되는 스위치 간에는 상호 연결 링크가 제공되어야 합니다.

상호 연결이 없는 구성에서, Blue에서 Gray로 이동하는 ICMP 요청은 Gray 포트 5E:CA로 이동하는 포트 82:83으로 나갑니다. 그러나 위쪽 스위치는 Gray의 5E:C9 포트를 통과할 수 없으므로 이 요청을 보낼 수 없습니다. Gray가 Blue에 대해 ping을 수행하는 경우에도 유사한 시나리오가 발생합니다. ICMP 요청이 Blue 82:82로 이동하는 5E:C9로 나가지만 목적지에 도달할 수 없습니다. 위쪽 스위치와 아래쪽 스위치가 상호 연결되어 있지 않으므로 위쪽 스위치의 CAM 테이블에 82:82에 대한 입구가 없습니다. 그러나 Red 및 Blue, 그리고 Red 및 Gray 간에는 ping이 제대로 진행됩니다.

또한 장애 조치 이벤트로 인해 연결이 추가로 손실될 수 있습니다. 위쪽 스위치 포트 4에서 케이블 연결이 끊어지는 경우, Gray는 ICMP 요청을 Red 49:C9로 보내지만 아래쪽 스위치의 CAM 테이블에 49:C9에 대한 입구가 없으므로 프레임이 모든 해당 포트에 플러드되지만 49:C9로 이동할 수는 없습니다.

그림 3: 상호 스위치 링크를 사용하지 않는 스위치 간 팀 구성



스위치 간에 링크를 추가하면 Blue 및 Gray 간의 트래픽이 아무런 문제 없이 이동할 수 있습니다. 두 스위치의 CAM 테이블에서 추가 항목을 확인하십시오. 팀이 제대로 작동하려면 링크 상호 연결이 필수적입니다. 따라서 링크 집계 트렁크가 두 스위치를 상호 연결하여 연결을 효율적으로 사용할 수 있도록 해야 합니다.

그림 4: 상호 연결을 사용하는 스위치 간 팀 구성

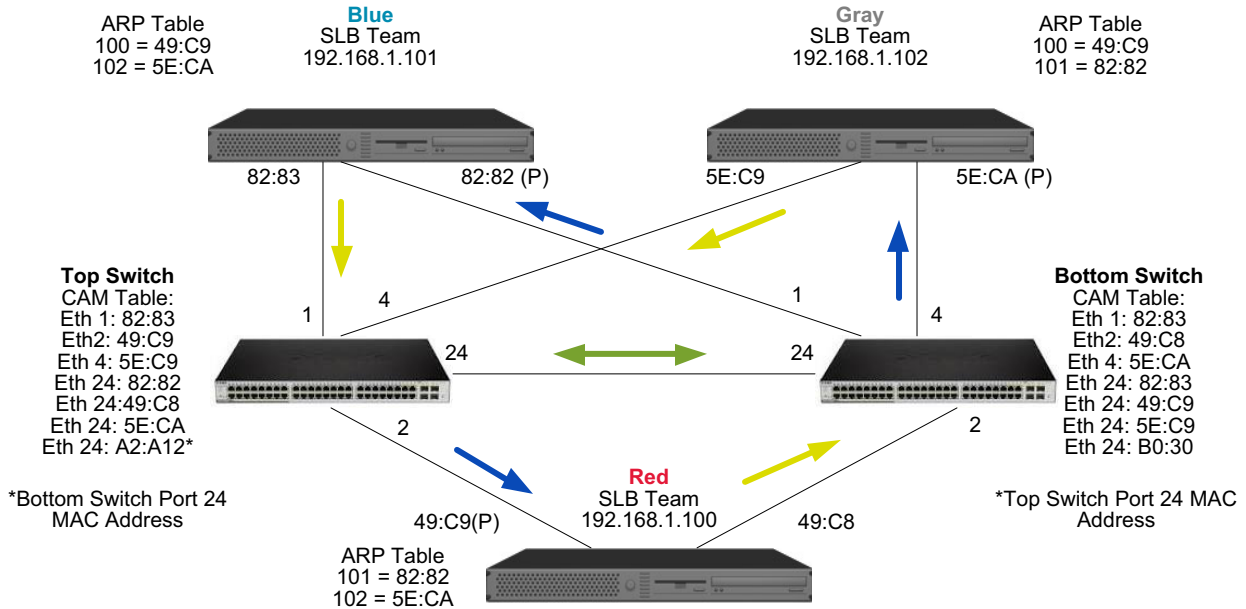
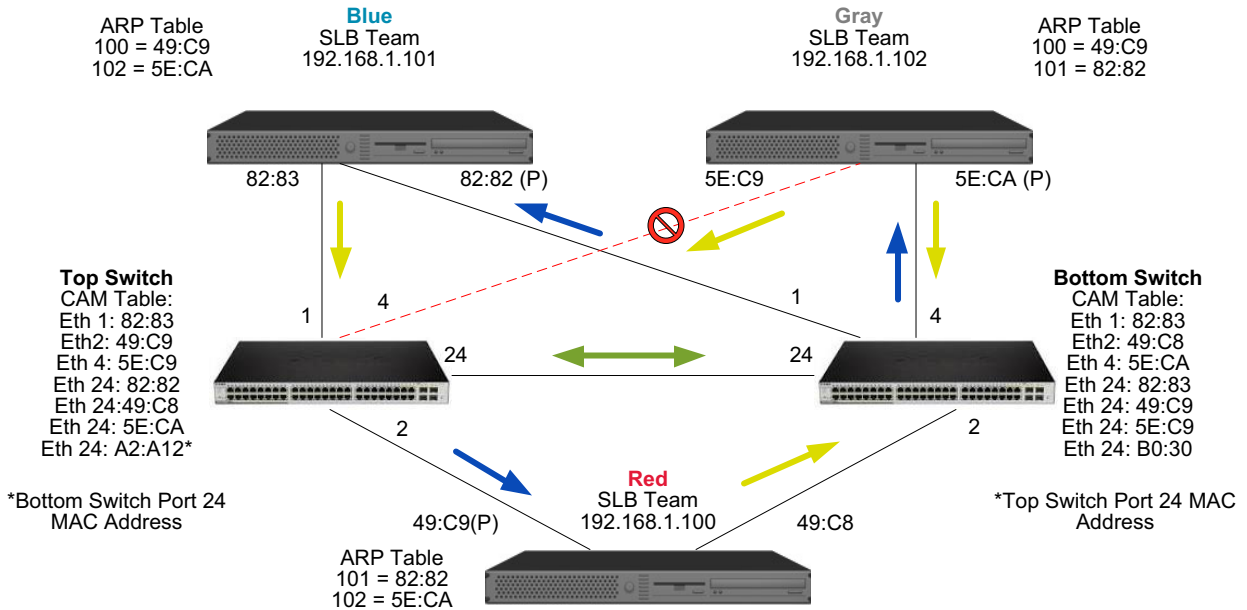


그림 5 는 위쪽 스위치 포트 4 에서 케이블 연결이 끊어진 경우의 장애 조치 이벤트를 보여 줍니다 . 이 이벤트는 모든 스테이션이 연결 끊김 없이 서로에 대해 ping 을 수행하는 성공적인 장애 조치입니다 .

그림 5: 장애 조치 이벤트



스패닝 트리 알고리즘

- TCN(Topology Change Notice)
- Port Fast/Edge Port

Ethernet 네트워크에서는 두 브리지 또는 스위치 간에 활성 경로가 하나만 있을 수 있습니다. 스위치 간에 활성 경로가 여러 개 있으면 네트워크에 루프가 발생할 수 있습니다. 루프가 발생하면 일부 스위치가 스위치의 양쪽에 있는 스테이션을 모두 인식합니다. 그러면 전달 알고리즘이 잘못 작동되어 중복 프레임이 전달될 수 있습니다. 스패닝 트리 알고리즘에서는 확장 네트워크의 모든 스위치에 스패닝 트리를 정의한 다음 특정 중복 데이터 경로를 대기(차단) 상태로 설정함으로써 중복 경로를 제공합니다. 네트워크의 스위치는 일정한 간격으로 경로를 식별하는 데 사용하는 스패닝 트리 패킷을 송신 및 수신합니다. 한 네트워크 세그먼트에 연결할 수 없거나 스패닝 트리 시간이 변경되면 스패닝 트리 알고리즘은 스패닝 트리 토폴로지를 재구성하며 대기 경로를 활성화하여 링크를 재설정합니다. 중점 스테이션에서는 스패닝 트리 작업을 인식할 수 없으며, 이 작업은 중점 스테이션이 단일 LAN 세그먼트에 연결되어 있는지 여러 세그먼트의 스위치 LAN에 연결되어 있는지 여부를 감지하지 않습니다.

STP(스패닝 트리 프로토콜)는 브리지 및 스위치에서 실행하도록 디자인된 계층 2 프로토콜입니다. STP 사양은 IEEE 802.1d 에 정의되어 있습니다. STP의 주요 목적은 사용자의 네트워크에 중복 경로가 있을 때 루프 상황이 발생하지 않도록 하는 것입니다. STP는 네트워크 루프를 감지 및 비활성화하여 스위치 또는 브리지 간에 백업 경로를 제공합니다. STP를 사용하면 장치가 네트워크의 다른 STP 호환 장치와 상호 작용하여 네트워크의 두 스테이션 간에 경로가 하나만 존재하도록 할 수 있습니다.

안정적인 네트워크 토폴로지를 설정하고 나면 모든 브리지가 루트 브리지에서 전송된 BPDU 메시지(브리지 프로토콜 데이터 단위)를 수신 대기합니다. 지정된 기간(최대 에이징 기간)이 지나도 BPDU 메시지를 수신하지 못하는 경우 브리지는 루트 브리지에 대한 링크가 다운된 것으로 가정합니다. 그런 다음 이 브리지는 다른 브리지와의 협상을 시작하여 네트워크를 재구

성해 올바른 네트워크 토폴로지를 재설정합니다. 새 토폴로지를 만드는 과정은 최대 50초가 걸립니다. 이 시간 동안 중단 간 통신은 인터럽트됩니다.

중점 스테이션에 연결된 포트에 대해서는 스페닝 트리를 사용하지 않는 것이 좋습니다. 기본적으로 중점 스테이션은 Ethernet 세그먼트 내에 루프를 만들지 않도록 정의되어 있기 때문입니다. 또한 팀 구성 어댑터가 스페닝 트리가 활성화된 포트에 연결되어 있으면 사용자에게 예기치 않은 연결 문제가 발생할 수 있습니다. 예를 들어 해당 물리적 어댑터 중 하나의 링크가 손실된 팀 구성 어댑터를 가정해 봅니다. 물리적 어댑터를 재연결(대체라고도 함)하는 경우 중급 드라이버가 링크 재설정을 감지하여 포트를 통해 트래픽을 전달하기 시작합니다. 스페닝 트리 프로토콜에 의해 포트가 일시적으로 차단되는 경우 트래픽이 손실됩니다.

TCN(Topology Change Notice)

브리지/스위치는 특정 포트에서 수신된 소스 MAC 주소를 파악하여 MAC 주소 및 포트 번호의 전달 테이블을 만듭니다. 이 테이블은 프레임을 모든 포트에 플러드하는 대신 특정 포트에 전달하는 데 사용됩니다. 일반적인 테이블 항목 최대 에이징 기간은 5분입니다. 즉, 호스트에서 5분 동안 아무런 작업이 수행되지 않을 때 해당 항목이 테이블에서 제거됩니다. 에이징 기간을 줄이는 것이 효과적인 경우도 있습니다. 전달 링크가 차단으로 이동하고 또 다른 링크는 차단에서 전달로 이동하는 경우를 그 예로 들 수 있습니다. 이 기간을 변경하는 데는 최대 50초가 걸립니다. STP 재계산이 끝나면 중점 스테이션 간에 새 경로를 사용하여 통신할 수 있습니다. 그러나 전달 테이블에 이전 토폴로지를 기반으로 하는 항목이 여전히 존재하므로, 변경 내용이 적용된 포트 항목이 테이블에서 제거된 후 5분이 지나야 통신이 재설정되는 경우도 있습니다. 그러면 트래픽은 모든 포트에 플러드되어 다시 확인됩니다. 이 경우에는 에이징 기간을 줄이는 것이 좋습니다. TCN(Topology Change Notice) BPDU는 이러한 용도로 사용할 수 있습니다. TCN은 변경 내용이 적용된 브리지/스위치에서 루트 브리지/스위치로 전송됩니다. 브리지/스위치는 토폴로지 변경 내용(링크가 아래로 이동하거나 포트가 전달로 이동)을 감지하면 해당 루트 포트를 통해 TCN을 루트 브리지로 전송합니다. 그러면 루트 브리지는 토폴로지 변경 내용이 적용된 BPDU를 전체 네트워크로 보급합니다. 이로 인해 모든 브리지의 MAC 테이블 에이징 기간이 지정된 시간 동안 15초로 줄어듭니다. 그러면 STP가 통합되는 즉시 스위치가 MAC 주소를 다시 확인할 수 있습니다.

전달 포트가 차단 포트에 변경되거나 전환 포트가 포워딩 포트에 변경되면 Topology Change Notice BPDU가 전송됩니다. TCN BPDU는 STP 재계산을 시작하지 않으며 스위치의 전달 테이블 항목 에이징 기간에만 영향을 줍니다. 또한 TCN BPDU는 네트워크 토폴로지를 변경하거나 루프를 만들지도 않습니다. 서버 또는 클라이언트 등의 중단 노드가 꺼졌다가 다시 켜지면 토폴로지 변경이 실행됩니다.

Port Fast/Edge Port

네트워크에 대한 TCN의 영향을 줄이려면(예: 스위치 포트에 대한 플러드를 늘림) 자주 켜고 끄는 중단 노드에서는 연결되어 있는 스위치 포트에 대해 Port Fast 또는 Edge Port 설정을 사용해야 합니다. Port Fast 또는 Edge Port는 특정 포트에 적용되며 다음과 같은 효과를 발생하는 명령입니다.

- 하위 링크에서 상위 링크로 이동하는 포트는 수신 대기 상태에서 수신 상태로, 그런 다음 전달로 이동하는 대신 전달 STP 모드로 설정됩니다. STP는 여전히 이러한 포트에서 실행됩니다.
- 포트가 위쪽 또는 아래쪽으로 이동할 때 스위치는 Topology Change Notice를 생성하지 않습니다.

Microsoft NLB/WLBS를 사용한 팀 구성

SLB 팀 구성 모드는 Microsoft NLB(네트워크 균형 조정) 유니캐스트 모드에서 작동하지 않으며 멀티캐스트 모드에서만 작동합니다. NLB 서비스에서 사용하는 메커니즘으로 인해 로드 균형 조정을 NLB에서 관리하므로 이 환경에서는 팀 구성을 장애 조치(대기 NIC가 있는 SLB)로 하는 것이 좋습니다.

응용 프로그램 고려 사항

- 팀 구성 및 클러스터링—Microsoft 클러스터 소프트웨어
- 팀 구성 및 네트워크 백업

팀 구성 및 클러스터링—Microsoft 클러스터 소프트웨어

각 클러스터 노드에서 사용자는 최소한 2개의 네트워크 어댑터를 설치하는 것이 좋습니다. 보드 일체형 어댑터를 사용해도 됩니다. 이러한 인터페이스는 두 가지 용도로 사용됩니다. 한 어댑터는 내부 클러스터 *하트비트* 통신 전용으로 사용됩니다. 이 어댑터를 *개인 어댑터*라고 하며, 보통 별도의 개인 하위 네트워크에 위치합니다. 다른 어댑터는 클라이언트 통신에 사용되며, *공용 어댑터*라고 합니다.

이러한 각 목적, 즉 개인(클러스터 내부 통신) 및 공용(외부 클라이언트 통신)에 여러 어댑터를 사용할 수도 있습니다. 모든 Broadcom 팀 구성 모드는 공용 어댑터에 대해서만 Microsoft 클러스터 소프트웨어를 지원합니다. 개인 네트워크 어댑터 팀 구성은 지원되지 않습니다. Microsoft는 서버 클러스터의 개인 상호 연결 환경에서는 팀 구성을 사용할 수 없음을 명시하고 있습니다. 이는 노드 간의 하트비트 패킷 전송 및 수신 과정에서 발생할 수 있는 지연 때문입니다. 최적의 결과를 위해서는 개인 상호 연결에 대한 중복성을 원하는 경우 팀 구성을 비활성화하고 사용 가능한 포트를 사용하여 두 번째 개인 상호 연결을 형성하면 됩니다. 그러면 동일한 결과를 얻을 수 있으며, 통신할 노드에 대해 강력한 2중 통신 경로가 제공됩니다.

클러스터된 환경의 팀 구성에 대해서는 동일한 브랜드의 어댑터를 사용하는 것이 좋습니다.



참고 : Microsoft 클러스터 소프트웨어는 Microsoft 네트워크 로드 균형 조정을 지원하지 않습니다 .

팀 구성 및 네트워크 백업

- 로드 균형 조정 및 장애 조치
- 결함 허용

팀 구성이 없는 환경에서 네트워크 백업을 수행할 때는 과도한 트래픽 및 어댑터 오버로드로 인해 백업 서버 어댑터의 전체 처리율이 쉽게 영향을 받을 수 있습니다. 백업 서버 수, 데이터 스트림 및 테이프 드라이브 속도에 따라 백업 트래픽은 높은 비율의 네트워크 링크 대역폭을 사용하기가 쉬우며, 이로 인해 프로덕션 데이터 및 테이프 백업 성능이 영향을 받을 수 있습니다. 네트워크 백업에는 보통 NetBackup, Galaxy 또는 Backup Exec 등의 테이프 백업 소프트웨어를 실행하는 전용 백업 서버가 포함됩니다. 백업 서버에는 SCSI 테이프 백업 장치가 직접 연결되어 있거나 테이프 라이브러리가 파이버 채널 SAN을 통해 연결되어 있습니다. 네트워크를 통해 백업되는 시스템은 보통 클라이언트 또는 원격 서버라고 하며, 테이프 백업 소프트웨어 에이전트가 설치되어 있습니다.

4개의 클라이언트 서버가 있으므로 백업 서버는 클라이언트당 하나씩 4개의 백업 작업을 동시에 다중 드라이브 자동 로더로 스트림할 수 있습니다. 그러나 스위치와 백업 서버 간에는 링크가 하나 뿐이므로, 4개 스트림 백업으로 인해 어댑터와 링크는 쉽게 포화 상태가 될 수 있습니다. 백업 서버의 어댑터가 1Gbps(125MB/s)로 작동하고 각 클라이언트가 테이프 백업 동안 20MB/s로 데이터를 스트림할 수 있다면 백업 서버와 스위치 간의 처리율은 80MB/s(20MB/s x 4)가 되며, 이는 네트워크 대역폭의 64%에 해당됩니다. 이 64%는 네트워크 대역폭 범위 내에서는 우리가 없지만, 특히 다른 응용 프로그램도 동일한 링크를 공유하는 경우 매우 높은 비율입니다.

로드 균형 조정 및 장애 조치

백업 스트림 수가 증가하면 전체 처리율도 증가합니다. 그러나 각 데이터 스트림은 25MB/s의 단일 백업 스트림과 동일한 성능을 유지하지 못할 수도 있습니다. 즉, 백업 서버가 단일 클라이언트의 데이터를 25MB/s로 스트림할 수 있다고 해도 4개의 동시 실행 백업 작업이 100MB/s(20MB/s x 4)로 스트림할 수 있는 것은 아닙니다. 백업 스트림 수가 늘어나면 전체 처리율도 증가하는 것은 사실이지만, 각 백업 스트림은 테이프 소프트웨어 또는 네트워크 스택 제한에 의해 영향을 받습니다.

테이프 백업 서버가 클라이언트를 백업할 때 안정적으로 어댑터 성능 및 네트워크 대역폭을 사용하도록 하려면 네트워크 인프라에서 로드 균형 조정 및 결함 허용 등의 팀 구성을 구현해야 합니다. 데이터 센터는 중복 스위치, 링크 집계 및 트렁킹을 결함 허용 솔루션으로 통합합니다. 팀 구성 장치 드라이버가 팀 구성 인터페이스 및 장애 조치 경로를 통해 데이터가 흐르는 방식을 조정하지만, 테이프 백업 응용 프로그램은 이를 인식하지 못하므로 네트워크를 통해 원격 시스템을 백업할 때 테이프 백업 과정이 인터럽트되지 않습니다. 그림 6에서는 Broadcom 팀 구성 환경의 테이프 백업 및 Smart Load Balancing이 팀 구성 어댑터 간에 테이프 백업 데이터를 로드 균형 조정하는 방법을 설명하는 네트워크 토폴로지를 볼 수 있습니다.

클라이언트 서버가 데이터를 백업 서버로 보내는 데 사용할 수 있는 경로에는 네 가지가 있지만, 데이터 전송 중에 이러한 경로 중 하나만 지정됩니다. 클라이언트 서버가 데이터를 백업 서버로 보내는 데 사용할 수 있는 경로 중 하나는 다음과 같습니다.

경로 예: 클라이언트 서버 Red가 어댑터 A, 스위치 1, 백업 서버 어댑터 A를 통해 데이터를 보냅니다.

지정되는 경로는 다음과 같은 두 가지 요인에 의해 결정됩니다.

1. 백업 서버 MAC 주소를 가리키는 클라이언트 서버 ARP 캐시. 이 캐시는 Broadcom 중급 드라이버 인바운드 로드 균형 조정 알고리즘에 의해 결정됩니다.
2. 클라이언트 서버 Red의 물리적 어댑터 인터페이스가 데이터 전송에 사용됩니다. Broadcom 중급 드라이버 아웃바운드 로드 균형 조정 알고리즘이 이를 결정합니다(아웃바운드 트래픽 흐름 및 인바운드 트래픽 흐름(SLB에만 해당) 참조).

백업 서버의 팀 구성 인터페이스는 G-ARP(무작위 주소 분석 프로토콜)를 클라이언트 서버 Red로 전송하고, 그러면 Red는 클라이언트 서버 ARP가 백업 서버 MAC 주소로 업데이트되도록 합니다. 팀 구성 인터페이스 내의 로드 균형 조정 메커니즘에 따라 G-ARP에 포함되는 MAC 주소가 결정됩니다. 선택된 MAC 주소는 기본적으로 클라이언트 서버의 데이터를 전송하는 대상입니다. 클라이언트 서버 Red에서 SLB 팀 구성 알고리즘은 두 어댑터 인터페이스 중 데이터 전송에 사용할 인터페이스

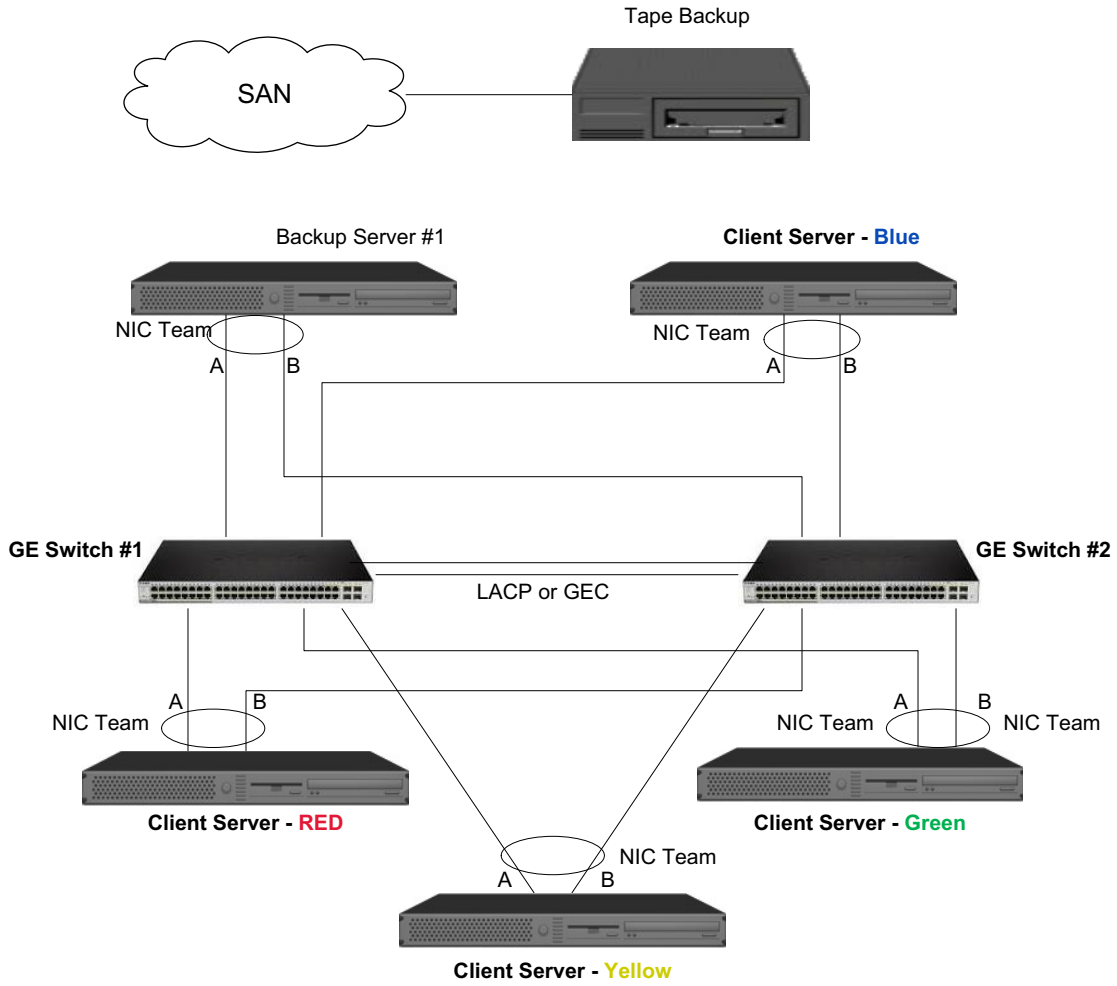
스를 결정합니다. 이 예에서 클라이언트 서버 **Red**의 데이터는 백업 서버 어댑터 **A** 인터페이스에서 수신됩니다. 팀 구성 인터페이스에 추가적인 로드가 더해질 때의 **SLB** 메커니즘을 설명하기 위해, 백업 서버가 두 번째 백업 작업을 시작하는 시나리오를 가정해 봅니다. 첫 번째 백업 작업은 클라이언트 서버 **Red**에 대한 작업이며 두 번째는 클라이언트 서버 **Blue**에 대한 작업입니다. 클라이언트 서버 **Blue**가 데이터를 백업 서버로 보내는 데 사용하는 경로는 해당 **ARP** 캐시에 있으며, 백업 서버 **MAC** 주소를 가리킵니다. 백업 서버의 어댑터 **A**가 이미 클라이언트 서버 **Red**의 백업 작업으로 인해 로드되어 있기 때문에, 백업 서버는 **SLB** 알고리즘을 호출하여 클라이언트 서버 **Blue**에 백업 서버 어댑터 **B** **MAC** 주소를 반영하도록 해당 **ARP** 캐시를 업데이트할 것을 **G-ARP**를 통해 *알립니다*. 클라이언트 서버 **Blue**는 데이터를 전송해야 하는 경우 자체 **SLB** 알고리즘에 의해 결정되는 해당 어댑터 인터페이스 중 하나를 사용합니다. 여기서 클라이언트 서버 **Blue**의 데이터를 백업 서버 어댑터 **A** 인터페이스가 아닌 어댑터 **B** 인터페이스가 수신한다는 것이 중요합니다. 두 백업 스트림이 동시에 실행 중인 경우 백업 서버는 서로 다른 클라이언트의 데이터 스트림을 *로드 균형 조정*해야 하기 때문입니다. 두 백업 스트림이 모두 실행 중일 때 백업 서버의 각 어댑터 인터페이스는 같은 양의 로드를 처리하므로 두 어댑터 인터페이스 간의 데이터가 로드 균형 조정되는 것입니다.

세 번째 및 네 번째 백업 작업이 백업 서버에서 시작되는 경우에도 이와 동일한 알고리즘이 적용됩니다. 백업 서버의 팀 구성 인터페이스는 유니캐스트 **G-ARP**를 백업 클라이언트로 전송하여 해당 **ARP** 캐시를 업데이트하도록 알립니다. 그런 다음 각 클라이언트는 경로를 통해 백업 데이터를 백업 서버의 대상 **MAC** 주소로 전송합니다.

결함 허용

테이프 백업 작업 중 네트워크 링크에 오류가 발생하는 경우 백업 서버 및 클라이언트 간의 모든 트래픽이 중지되고 백업 작업이 실패합니다. 그러나 **Broadcom SLB** 및 스위치 결함 허용에 대해 모두 네트워크 토폴로지를 구성한 경우에는 링크 오류가 발생해도 테이프 백업 작업을 중단하지 않고 계속 수행할 수 있습니다. 테이프 백업 소프트웨어 응용 프로그램은 네트워크 내의 모든 장애 조치 과정을 인식할 수 없습니다. 네트워크 장애 조치 과정 동안 백업 데이터 스트림이 이동하는 방법을 이해하려면 **그림 6**의 토폴로지를 살펴보십시오. 클라이언트 서버 **Red**가 경로 **1**을 통해 데이터를 백업 서버로 전송했지만 백업 서버 및 스위치 간에 링크 오류가 발생했습니다. 데이터를 더 이상 스위치 **#1**에서 백업 서버의 어댑터 **A** 인터페이스로 보낼 수 없기 때문에, 이 데이터는 스위치 **#1**에서 스위치 **#2**를 통해 백업 서버의 어댑터 **B** 인터페이스로 리디렉션됩니다. 모든 결함 허용 작업은 스위치의 어댑터 팀 인터페이스 및 트렁크 설정이 처리하므로 백업 응용 프로그램은 이를 인식하지 못합니다. 클라이언트 서버의 경우 원래 경로로 데이터가 전송되는 것처럼 그대로 작동합니다.

그림 6: 두 스위치 간에 SLB 팀을 구성한 네트워크 백업



팀 구성 문제 해결

- 팀 구성 팀
- 문제 해결 지침

가상 어댑터 팀 구성 인터페이스를 통해 프로토콜 분석기를 실행할 때 전송된 프레임에 표시된 MAC 주소가 올바르지 않을 수 있습니다. 분석기에는 BASP에 의해 구성된 프레임이 그대로 표시되지 않으며, 프레임을 전송하는 인터페이스의 MAC 주소가 아닌 팀의 MAC 주소가 표시됩니다. 그러므로 팀을 모니터링하는 데 다음과 같은 과정을 사용하는 것이 좋습니다.

1. 스위치에서 팀의 모든 uplink 포트를 미러링합니다.
2. 팀에 스위치가 두 개 있는 경우에는 interlink 트렁크도 미러링합니다.
3. 모든 미러 포트를 독립적으로 샘플링합니다.
4. 분석기에서 QoS 및 VLAN 정보를 필터링하지 않는 어댑터 및 드라이버를 사용합니다.

팀 구성 팀

네트워크 연결 또는 팀 구성 기능 관련 문제를 해결할 때는 현재 구성에 다음 정보가 해당되는지를 확인하십시오.

1. SLB 팀의 경우 모든 어댑터가 동일한 링크 속도를 가지는 것이 좋습니다.
2. LiveLink가 활성화되어 있지 않은 경우 팀에 연결되어 있는 스위치 포트에 대해 스페닝 트리 프로토콜을 비활성화하거나 초기 단계를 무시하는 STP 모드(예: Port Fast, Edge Port)를 활성화하십시오.
3. 팀이 직접 연결하는 모든 스위치의 지원 예정 하드웨어, 펌웨어 및 소프트웨어의 개정 버전은 같아야 합니다.
4. 팀으로 구성하려면 어댑터는 동일한 VLAN의 구성원이어야 합니다. 여러 팀을 구성한 경우 각 팀은 별도의 네트워크에 있어야 합니다.
5. Locally Administered Address 필드에 멀티캐스트 또는 브로드캐스트 주소를 입력하지 마십시오.
6. Locally Administered Address를 팀 구성원인 물리적 어댑터에 할당하지 마십시오.
7. 모든 팀의 모든 물리적 구성원에 대해 전원 관리가 비활성화되어 있는지 확인하십시오. 어댑터 속성의 전원 관리 탭에서 전원을 절약하기 위해 컴퓨터가 이 장치를 끌 수 있음 확인란이 선택 해제되어 있어야 합니다. "Windows 드라이버 및 응용 프로그램"에서 전원 관리 옵션 설정을 참조하십시오.
8. 팀을 구축하기 전에 개별 물리적 팀 구성원에서 정적 IP 주소를 제거합니다.
9. 최대 처리율을 필요로 하는 팀은 LACP 또는 GEC/FEC를 사용해야 합니다. 이러한 경우 중급 드라이버는 아웃바운드 로드 균형 조정만 수행하면 되며, 스위치는 인바운드 로드 균형 조정을 수행합니다.
10. 집계된 팀(802.3ad \ LACP 및 GEC/FEC)은 IEEE 802.3a, LACP 또는 GEC/FEC를 지원하는 단일 스위치에만 연결해야 합니다.
11. 허브는 반이중만 지원하므로 팀을 허브에 연결해서는 안 됩니다. 허브는 문제 해결을 위해서만 팀에 연결해야 합니다. LACP 또는 GEC/FEC 팀에 참여하는 네트워크 어댑터의 장치 드라이버를 비활성화하면 네트워크 연결에 나쁜 영향을 미칠 수 있습니다. 네트워크 연결이 끊어지는 것을 막기 위해 장치 드라이버를 비활성화하기 전에 먼저 스위치에서 어댑터를 물리적으로 분리하는 것이 좋습니다.
12. 기본(미니포트) 및 팀(중급) 드라이버가 동일한 릴리스 패키지의 것인지 확인합니다.
13. 팀 구성 전에 각 물리적 어댑터 연결을 테스트합니다.
14. 프로덕션 환경에 배치하기 전에 팀의 장애 조치 및 대체 동작을 테스트합니다.
15. 프로덕션 네트워크가 아닌 네트워크에서 프로덕션 네트워크로 이동할 때는 장애 조치 및 대체를 다시 테스트하는 것이 좋습니다.
16. 프로덕션 환경에 배치하기 전에 팀의 성능 동작을 테스트합니다.

문제 해결 지침

서버가 어댑터 팀 구성을 사용하는 경우 지원을 요청하기 전에 네트워크 연결 문제를 해결하기 위한 다음 단계를 완료했는지 확인하십시오.

1. 모든 어댑터의 **Ethernet** 링크 표시등이 켜져 있고 모든 케이블이 연결되어 있는지 확인합니다.
2. 기본 및 중급 드라이버가 동일한 패키지의 것이며 제대로 로드되었는지 확인합니다.
3. **Windows ipconfig** 명령을 사용하여 IP 주소가 올바른지 확인합니다.
4. 팀에 연결된 스위치 포트에서 **STP** 포트가 비활성화되었거나 **Edge Port/Port Fast**가 활성화되었는지, 또는 **LiveLink**를 사용 중인지 확인합니다.
5. 어댑터 및 스위치가 링크 속도 및 이중에 대해 동일하게 구성되어 있는지 확인합니다.
6. 가능한 경우 팀을 분해하여 각 어댑터에 대한 연결을 독립적으로 확인하는 방법을 통해 문제가 팀 구성과 직접 관련되어 있는지 확인합니다.
7. 팀에 연결된 모든 스위치 포트가 동일한 **VLAN**에 있는지 확인합니다.
8. 스위치 포트가 일반 트렁킹(**FEC/GEC**)/**802.3ad-Draft Static** 팀 구성 유형용으로 올바르게 구성되어 있으며 어댑터 팀 구성 유형과 일치하는지 확인합니다. 시스템이 **SLB** 팀 유형용으로 구성된 경우에는 해당 스위치 포트가 일반 트렁킹(**FEC/GEC**)/**802.3ad-Draft Static** 팀 유형용으로 구성되지 않았는지 확인합니다.

FAQ

Q:	어떤 상황에서 트래픽이 로드 균형 조정되지 않습니까? 왜 모든 트래픽이 팀 구성원 간에 균등하게 로드 균형 조정되지 않습니까?
A:	대량 트래픽이 IP/TCP/UDP를 사용하지 않거나 많은 수의 클라이언트가 다른 네트워크에 있습니다. 수신 로드 균형 조정은 트래픽 로드와 관련된 것이 아니라 시스템에 연결되어 있는 클라이언트 수와 관련되어 있습니다.
Q:	팀에서 로드 균형 조정되는 네트워크 프로토콜은 어떤 것입니까?
A:	Broadcom의 팀 구성 소프트웨어는 IP/TCP/UDP 트래픽만을 지원합니다. 다른 트래픽은 모두 기본 어댑터로 전달됩니다.
Q:	SLB를 통해 로드 균형 조정할 수 있는 프로토콜과 그렇지 않은 프로토콜에는 어떤 것이 있습니까?
A:	IP/TCP/UDP 프로토콜만 양쪽 방향(송신 및 수신)에서 로드 균형 조정됩니다.
Q:	100Mbps로 실행되는 포트와 1000Mbps로 실행되는 포트를 팀으로 구성할 수 있습니까?
A:	팀 내의 링크 속도 혼합은 앞서 언급한 것과 같이 Smart Load Balancing™ 팀 및 802.3ad 팀에 대해서만 지원됩니다.
Q:	파이버 어댑터를 구리 Gigabit Ethernet 어댑터와 팀으로 구성할 수 있습니까?
A:	SLB를 사용하는 경우, 그리고 스위치가 FEC/GEC 및 802.3ad에서 허용하는 경우 가능합니다.
Q:	어댑터 로드 균형 조정 및 Microsoft의 NLB(네트워크 로드 균형 조정) 간의 차이점은 무엇입니까?
A:	어댑터 로드 균형 조정은 네트워크 세션 수준에서 수행되고 NLB는 시스템 응용 프로그램 수준에서 수행됩니다.
Q:	팀 구성 어댑터를 라우터의 포트에 연결할 수 있습니까?
A:	아니오. 팀의 모든 포트는 동일한 네트워크에 있어야 합니다. 그러나 라우터에서 각 포트는 별도의 네트워크로 정의되어 있습니다. 모든 팀 구성 모드에서는 링크 파트너가 계층 2 스위치여야 합니다.
Q:	Microsoft 클러스터 서비스에 팀 구성을 사용할 수 있습니까?
A:	예를 클릭합니다. 팀 구성은 공용 네트워크에서만 지원되며, 하트비트 링크에 사용되는 개인 네트워크에서는 지원되지 않습니다.
Q:	PXE가 가상 어댑터(팀)에서 작동합니까?
A:	PXE 클라이언트는 운영 체제가 로드되기 전, 즉 가상 서버가 아직 활성화되기 전에 환경에서 작동합니다. PXE를 지원하는 물리적 어댑터를 PXE 클라이언트로 사용할 수 있습니다. 운영 체제가 로드될 때 이 클라이언트가 가상 어댑터의 일부인지 여부는 관계가 없습니다. PXE 서버는 가상 어댑터에 대해 작동할 수 있습니다.

Q:	WOL이 가상 어댑터(팀)에서 작동합니까?
A:	Wake-on-LAN 기능은 운영 체제가 로드되기 전에 환경에서 작동합니다. WOL은 시스템이 꺼져 있거나 대기 상태일 때 발생하므로 팀이 구성되지 않습니다.
Q:	팀으로 구성할 수 있는 최대 포트 수는 몇 개입니까?
A:	하나의 팀에는 포트를 최대 8개까지 할당할 수 있습니다.
Q:	동일한 시스템에 구성할 수 있는 최대 팀 수는 몇 개입니까?
A:	동일한 시스템에는 팀을 최대 16개까지 구성할 수 있습니다.
Q:	기본 어댑터가 복원된 후(고장 대체) 30~50초 동안 팀의 연결이 끊어지는 이유는 무엇입니까?
A:	스패닝 트리 프로토콜이 포트를 차단에서 전달 상태로 전환하기 때문입니다. 팀에 연결된 스위치 포트에 대해 Port Fast 또는 Edge Port를 활성화하거나 STP 지연용 계정에 LiveLink를 사용해야 합니다.
Q:	여러 스위치 간에 팀을 연결할 수 있습니까?
A:	시스템의 각 물리적 어댑터가 고유한 Ethernet MAC 주소를 사용하기 때문에 Smart Load Balancing을 여러 스위치에 사용할 수 있습니다. 링크 집계 및 일반 트렁킹을 사용하려면 모든 물리적 어댑터가 동일한 Ethernet MAC 주소를 공유해야 하므로 링크 집계 및 일반 트렁킹은 여러 스위치 간에 작동하지 않습니다.
Q:	중급 드라이버(BASP)는 어떻게 업그레이드합니까?
A:	중급 드라이버는 LAN 속성을 통해서만 업그레이드할 수 없습니다. 설치 프로그램을 사용하여 업그레이드해야 합니다.
Q:	가상 서버(팀)에서 성능 통계를 어떻게 확인할 수 있습니까?
A:	Broadcom Advanced Control Suite에서 가상 어댑터의 BASP 통계 탭을 클릭하면 됩니다.
Q:	NLB 및 팀 구성을 동시에 구성할 수 있습니까?
A:	예, 그러나 NLB를 멀티캐스트 모드로 실행 중이어야 합니다. NLB는 MS 클러스터 서비스에는 지원되지 않습니다.
Q:	백업 시스템 및 백업한 클라이언트 시스템을 모두 팀으로 구성해야 합니까?
A:	백업 시스템에 대한 데이터 로드가 가장 크므로, 백업 시스템은 항상 링크 집계 및 장애 조치와 팀으로 구성해야 합니다. 그러나 완전 중복 네트워크의 경우에는 스위치 및 백업 클라이언트를 모두 결합 허용 및 링크 집계와 팀으로 구성해야 합니다.
Q:	백업 작업 중 어댑터 팀 구성 알고리즘이 데이터를 바이트 수준에서 로드 균형 조정합니까, 세션 수준에서 조정합니까?
A:	어댑터 팀 구성을 사용하는 경우 데이터는 프레임의 오동작을 방지하기 위해 세션 수준에서만 로드 균형 조정되며 바이트 수준에서는 조정되지 않습니다. 어댑터 팀 구성 로드 균형 조정은 EMC PowerPath 등의 기타 스토리지 로드 균형 조정 메커니즘과 동일한 방식으로 작동하지 않습니다.
Q:	테이프 백업 소프트웨어를 어댑터 팀 구성에 사용하려면 특수한 구성이 필요합니까?

A: 팀 구성에 사용하기 위해 테이프 소프트웨어를 특수하게 구성할 필요는 없습니다. 테이프 백업 응용 프로그램은 팀 구성을 인식할 수 없습니다.

Q: 현재 사용 중인 드라이버는 어떻게 확인합니까?

A: 모든 운영 체제에서 드라이버 개정 버전을 확인하는 가장 정확한 방법은 물리적으로 드라이버 파일을 찾아 속성을 확인하는 것입니다.

Q: 스위치 결함 허용 구성에서 SLB가 스위치 오류를 감지할 수 있습니까?

A: 아니오. SLB는 팀 구성 포트 및 해당 직접 연결 파트너 간의 링크 손실만을 감지할 수 있습니다. 그러므로 다른 포트에서 발생한 링크 오류는 감지할 수 없습니다. 자세한 내용은 [LiveLink™ 기능](#)을 참조하십시오.

Q: Windows 시스템에서 어댑터의 실시간 통계는 어디서 모니터링할 수 있습니까?

A: Broadcom Advanced Control Suite(BACS)를 사용하여 일반, IEEE 802.3 및 사용자 정의 카운터를 모니터링하십시오.

이벤트 로깅 메시지

- [Windows 시스템 이벤트 로깅 메시지](#)
- [기본 드라이버\(물리적 어댑터/미니포트\)](#)
- [중급 드라이버\(가상 어댑터/팀\)](#)

Windows 시스템 이벤트 로깅 메시지

다음 섹션에는 알려진 Broadcom NetXtreme Gigabit Ethernet 어댑터에 대한 기본 드라이버 및 중급 드라이버 Windows 시스템 이벤트 로깅 상태 메시지가 나열되어 있습니다. Broadcom 어댑터 드라이버가 로드되면 Windows는 시스템 이벤트 뷰어에 상태 코드를 표시합니다. 두 드라이버, 즉 기본 또는 미니포트 드라이버용으로 설정된 드라이버와 중급 또는 팀 구성 드라이버용으로 설정된 드라이버가 모두 로드되어 있는지 여부에 따라 이러한 이벤트 코드에는 최대 두 개의 항목 클래스가 있을 수 있습니다.

기본 드라이버(물리적 어댑터/미니포트)

표 11에는 기본 드라이버에서 지원하는 이벤트 로깅 메시지가 나열되어 있고 해당 메시지의 원인이 설명되어 있으며, 권장 조치가 제공되어 있습니다.

표 11. 기본 드라이버 이벤트 로깅 메시지

메시지 번호	메시지	원인	수정 조치
1	장치 블록에 대해 메모리를 할당하지 못했습니다. 시스템 메모리 리소스 사용량을 확인하십시오.	드라이버에서 운영 체제의 메모리를 할당할 수 없습니다.	실행 중인 응용 프로그램을 닫아 메모리를 확보하십시오.
2	맵 레지스터를 할당하지 못했습니다.	드라이버에서 운영 체제의 맵 레지스터를 할당할 수 없습니다.	맵 레지스터를 할당하는 다른 드라이버를 언로드하십시오.
3	구성 정보에 액세스하지 못했습니다. 네트워크 드라이버를 다시 설치하십시오.	드라이버에서 어댑터의 PCI 구성 공간 레지스터에 액세스할 수 없습니다.	애드 인 어댑터의 경우: 슬롯에서 드라이버의 사용자를 다시 지정하거나 어댑터를 다른 PCI 슬롯으로 옮기거나 어댑터를 교체하십시오.
4	네트워크 링크가 다운되었습니다. 네트워크 케이블이 제대로 연결되어 있는지 확인하십시오.	해당 링크 파트너에 대한 어댑터 연결이 끊어졌습니다.	네트워크 케이블이 연결되어 있고 올바른 유형이며, 링크 파트너(예: 스위치 또는 허브)가 제대로 작동 중인지 확인하십시오.
5	네트워크 링크가 작동되는 상태입니다.	어댑터가 링크를 설정했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
6	네트워크 컨트롤러를 10MB 반이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.

표 11. 기본 드라이버 이벤트 로깅 메시지 (계속)

메시지 번호	메시지	원인	수정 조치
7	네트워크 컨트롤러를 10MB 전이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
8	네트워크 컨트롤러를 100MB 반이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
9	네트워크 컨트롤러를 100MB 전이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
10	네트워크 컨트롤러를 1GB 반이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
11	네트워크 컨트롤러를 1GB 전이중 링크에 대해 구성했습니다.	선택한 회선 속도 및 이중 설정으로 어댑터를 수동 구성했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
12	매체가 지원되지 않습니다.	운영 체제에서 IEEE 802.3 매체를 지원하지 않습니다.	운영 체제를 다시 부팅하고 바이러스 검사 및 디스크 검사 (chkdsk)를 실행한 다음 운영 체제를 다시 설치하십시오.
13	인터럽트 서비스 루틴을 등록할 수 없습니다.	장치 드라이버가 인터럽트 처리기를 설치할 수 없습니다.	운영 체제를 다시 부팅하고 동일한 IRQ를 공유하는 다른 장치 드라이버를 제거합니다.
14	I/O 공간을 매핑할 수 없습니다.	장치 드라이버가 드라이버 레지스터에 액세스하기 위해 메모리 매핑 I/O를 할당할 수 없습니다.	시스템에서 다른 어댑터를 제거하고 설치되어 있는 실제 메모리 양을 줄인 다음 어댑터를 교체하십시오.
15	드라이버를 초기화했습니다.	드라이버가 로드되었습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
16	NDIS가 미니포트 드라이버를 재설정하는 중입니다.	NDIS 계층에서 패킷 송신/수신의 문제를 감지하여 문제 해결을 위해 드라이버를 재설정하는 중입니다.	Broadcom Advanced Control Suite 진단을 실행하여 네트워크 케이블 상태가 정상인지 확인하십시오.
18	알 수 없는 PHY가 감지되었습니다. 기본 PHY 초기화 루틴을 사용 중입니다.	드라이버에서 PHY ID를 읽을 수 없습니다.	어댑터를 교체하십시오.
19	이 드라이버는 이 장치를 지원하지 않습니다. 최신 드라이버로 업그레이드하십시오.	드라이버가 설치된 어댑터를 인식하지 않습니다.	해당 어댑터를 지원하는 드라이버 버전으로 업그레이드하십시오.
20	드라이버를 초기화하지 못했습니다.	드라이버 초기화 중 알 수 없는 오류가 발생했습니다.	드라이버를 다시 설치하거나 최신 드라이버로 업데이트하거나 Broadcom Advanced Control Suite 진단을 실행하거나 어댑터를 교체하십시오.

표 11. 기본 드라이버 이벤트 로깅 메시지 (계속)

메시지 번호	메시지	원인	수정 조치
21	Ethernet@WireSpeed가 활성화되고 최대 링크 속도를 협상할 수 없습니다.	케이블 또는 연결에 결함이 있을 수 있습니다.	케이블을 다시 연결하거나 케이블을 변경합니다.
22	이 운영 체제의 이전 네트워크 컨트롤러에 대한 장치 드라이버를 설치할 수 없습니다.	최신 Outbox 드라이버는 더 이상 이전 장치를 지원하지 않습니다.	OS Inbox 드라이버를 사용하거나 최신 장치로 교체하십시오.
256	통합 처리 풀을 위한 실제 메모리가 부족합니다.	드라이버가 통합 처리 패킷 버퍼에 충분한 공유 메모리를 할당할 수 없습니다.	시스템에서 다른 어댑터를 제거/비활성화하거나 시스템 메모리를 늘리십시오.

중급 드라이버(가상 어댑터/팀)

표 12에는 중급 드라이버에서 지원하는 이벤트 로깅 메시지가 나열되어 있고 해당 메시지의 원인이 설명되어 있으며, 권장 조치가 제공되어 있습니다.

표 12. 중급 드라이버 이벤트 로깅 메시지

시스템 이벤트 메시지 번호	메시지	원인	수정 조치
1	NDIS에 등록할 수 없습니다.	드라이버가 NDIS 인터페이스에 등록할 수 없습니다.	다른 NDIS 드라이버를 언로드하십시오.
2	관리 인터페이스를 인스턴스화할 수 없습니다.	드라이버에서 장치 인스턴스를 만들 수 없습니다.	운영 체제를 다시 부팅하십시오.
3	관리 인터페이스에 대해 기호 링크를 만들 수 없습니다.	다른 드라이버에서 충돌하는 장치 이름을 만들었습니다.	Bif 라는 이름을 사용하는 충돌 장치 드라이버를 언로드하십시오.
4	Broadcom Advanced Server Program 드라이버가 시작되었습니다.	다른 드라이버에서 충돌하는 장치 이름을 만들었습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
5	Broadcom Advanced Server Program 드라이버가 중지되었습니다.	드라이버가 중지되었습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
6	내부 데이터 구조에 대해 메모리를 할당하지 못했습니다.	드라이버에서 운영 체제의 메모리를 할당할 수 없습니다.	실행 중인 응용 프로그램을 닫아 메모리를 확보하십시오.
7	어댑터에 바인딩할 수 없습니다.	드라이버에서 팀의 물리적 어댑터 중 하나를 열지 못했습니다.	물리적 어댑터 드라이버를 언로드한 다음 다시 로드하거나 업데이트된 물리적 어댑터 드라이버를 설치하거나 물리적 어댑터를 교체하십시오.
8	어댑터에 바인딩했습니다.	드라이버에서 물리적 어댑터를 열었습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
9	네트워크 어댑터의 연결이 끊어졌습니다.	물리적 어댑터가 네트워크에 연결되지 않았습니다(링크가 설정되어 있지 않습니다).	네트워크 케이블이 연결되어 있고 올바른 유형이며, 링크 파트너(예: 스위치 또는 허브)가 제대로 작동 중인지 확인하십시오.

표 12. 중급 드라이버 이벤트 로깅 메시지 (계속)

시스템 이벤트 메시지 번호	메시지	원인	수정 조치
10	네트워크 어댑터가 연결되었습니다.	물리적 어댑터가 네트워크에 연결되었습니다(링크가 설정되어 있습니다).	정보 메시지입니다. 작업이 필요하지 않습니다.
11	Broadcom Advanced Program 기능 드라이버는 이 버전의 운영 체제에서 실행할 수 없습니다.	드라이버가 현재 설치되어 있는 운영 체제를 지원하지 않습니다.	드라이버 릴리스 노트를 확인하고 지원되는 운영 체제에 드라이버를 설치하거나 드라이버를 업데이트하십시오.
12	핫 대기 어댑터를 로드 균형 조정 어댑터가 없는 팀의 기본 어댑터로 선택했습니다.	대기 어댑터가 활성화되었습니다.	오류가 발생한 물리적 어댑터를 교체하십시오.
13	네트워크 어댑터가 고급 장애 조치를 지원하지 않습니다.	물리적 어댑터가 Broadcom NICE(NIC Extension) 를 지원하지 않습니다.	NICE 를 지원하는 어댑터로 교체하십시오.
14	네트워크 어댑터가 관리 인터페이스를 통해 활성화되었습니다.	드라이버에서 관리 인터페이스를 통해 물리적 어댑터를 활성화했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
15	네트워크 어댑터가 관리 인터페이스를 통해 비활성화되었습니다.	드라이버에서 관리 인터페이스를 통해 물리적 어댑터를 비활성화했습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
16	네트워크 어댑터가 활성화되어 네트워크 트래픽에 참여합니다.	물리적 어댑터가 팀에 추가되었거나 팀에서 활성화되었습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.
17	네트워크 어댑터가 비활성화되어 네트워크 트래픽에 더 이상 참여하지 않습니다.	드라이버가 설치된 어댑터를 인식하지 않습니다.	정보 메시지입니다. 작업이 필요하지 않습니다.

4 절: 가상 LAN(VLAN)

- VLAN 개요
- 팀에 VLAN 추가

VLAN 개요

가상 LAN(VLAN)은 물리적인 LAN을 논리 부분으로 분할하여 작업 그룹의 논리 조각을 만들고 각 논리 세그먼트의 보안 정책을 강제 설정할 수 있습니다. 정의된 각 VLAN은 별도의 네트워크로 동작하며 해당 트래픽과 브로드캐스트도 다른 트래픽 및 브로드캐스트와 격리되어 있으므로 각 논리 그룹 내의 대역폭 효율성이 높아집니다. 시스템에서 사용 가능한 메모리 크기에 따라 서버의 각 Broadcom 어댑터에 최대 64개의 VLAN(63개는 태그 지정됨, 1개는 태그 지정되지 않음)을 정의할 수 있습니다.

팀에 VLAN을 추가하여 서로 다른 VLAN ID를 가진 여러 VLAN을 만들 수 있습니다. 추가된 각 VLAN에 가상 어댑터가 하나씩 만들어 집니다.

VLAN은 개별 브로드캐스트 도메인 및/또는 별도의 IP 서브넷을 만드는 데 일반적으로 사용되지만, 때때로 서버에 하나 이상의 VLAN을 동시에 존재하도록 하는데 유용합니다. Broadcom 어댑터는 포트 또는 팀 당 여러 VLAN을 지원하여 매우 유연한 네트워크 구성을 가능하게 합니다.

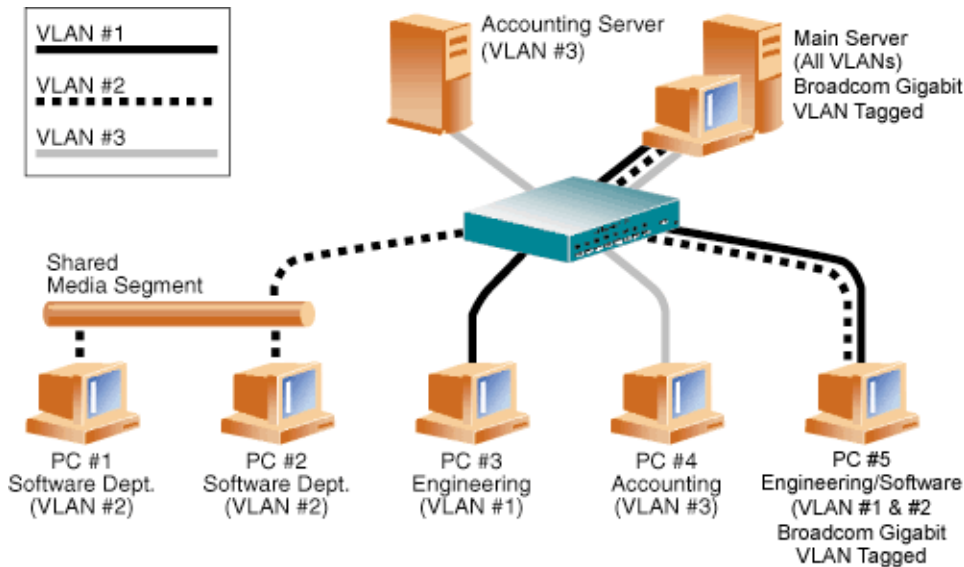


그림 7: 태그 지정 기능이 있는 여러 VLAN을 지원하는 서버의 예

그림 7은 VLAN을 사용하는 네트워크의 예를 보여 줍니다. 이 네트워크 예에서 물리적인 LAN은 스위치, 2개의 서버 및 5개의 클라이언트로 구성되어 있습니다. LAN은 3개의 서로 다른 VLAN으로 논리적으로 구성되어 있으며 각각 다른 IP 서브넷을 나타냅니다. 이 네트워크의 기능은 표 13에 설명되어 있습니다.

표 13. VLAN 네트워크 토폴로지에

구성 요소	설명
VLAN #1	주 서버, PC #3 및 PC #5를 구성하는 IP 서브넷 이 서브넷은 엔지니어링 그룹을 나타냅니다.
VLAN #2	주 서버, 공유된 미디어를 통한 PC #1 및 #2 및 PC #5를 포함합니다. 이 VLAN은 소프트웨어 개발 그룹입니다.
VLAN #3	주 서버, 계정 서버 및 PC #4를 포함합니다. 이 VLAN은 회계 그룹입니다.
기본 이름 서버	모든 VLAN 및 IP 서브넷에서 액세스해야 하는 사용 빈도가 높은 서버입니다. 주 서버에는 Broadcom 어댑터가 설치되어 있습니다. IP 서브넷 세 개가 모두 물리적인 단일 어댑터 인터페이스를 통해 액세스됩니다. 서버는 스위치 포트와 연결되어 있고, VLAN #1, #2 및 #3에 대해 구성되어 있습니다. 어댑터와 연결된 스위치 포트 모두에는 태그가 설정되어 있습니다. 두 장치의 태그 지정 VLAN 기능 덕분에, 서버는 이 네트워크에 있는 3개의 IP 서브넷에서 모두 통신할 수 있으나 이들 간의 브로드캐스트는 별도로 유지합니다.
계정 서버	VLAN #3에만 사용할 수 있습니다. 계정 서버는 VLAN #1 및 #2의 모든 트래픽에서 격리되어 있습니다. 서버에 연결된 스위치 포트는 태그가 해제되어 있습니다.
PC #1 및 #2	공유된 미디어 허브에 연결된 후 스위치에 연결됩니다. PC #1 및 #2는 VLAN #2에만 속해 있고, 주 서버 및 PC #5와 논리적으로 동일한 IP 서브넷에 있습니다. 이 세그먼트와 연결된 스위치 포트는 태그가 해제되어 있습니다.
PC #3	VLAN #1에 속한 PC #3은 주 서버 및 PC #5와만 통신할 수 있습니다. PC #3 스위치 포트는 태그가 해제되어 있습니다.
PC #4	VLAN #3에 속한 PC #4는 서버와만 통신할 수 있습니다. PC #4 스위치 포트에는 태그 지정이 활성화되어 있지 않습니다.
PC #5	VLAN #1 및 #2 모두에 속한 PC #5에는 Broadcom 어댑터가 설치되었으며 스위치 포트 #10에 연결되어 있습니다. 어댑터와 스위치 포트는 모두 VLAN #1 및 #2에 대해 구성되어 있으며 태그가 설정되어 있습니다.



참고: VLAN 태그는 트렁크 링크를 다른 스위치에 만드는 스위치 포트 또는 태그 지원 종점 스테이션(예: Broadcom 어댑터가 있는 서버 또는 워크스테이션)에 연결된 포트에만 설정되어야 합니다.

팀에 VLAN 추가

각 팀에는 최대 64개의 VLAN(63개의 VLAN은 태그가 지정되고 1개의 VLAN은 태그가 지정되지 않음)을 지원합니다. 어댑터에 대한 여러 VLAN과 함께, 단일 어댑터가 있는 서버에는 여러 IP 서브넷에 대한 논리 존재가 있을 수 있습니다. 한 팀에 여러 개의 VLAN이 있을 경우, 서버는 여러 IP 서브넷에 대해 하나의 논리 존재를 두고 로드 균형 조정 및 장애 조치의 이점을 누릴 수 있습니다. Windows 운영 체제에서 팀에 VLAN을 추가하는 지침은 [VLAN 추가](#)를 참조하십시오.



참고: 장애 조치 팀에 속한 어댑터 역시 VLAN을 지원하기 위해 구성될 수 있습니다. 타사 NIC가 장애 조치 팀의 일부인 경우 VLAN은 타사 NIC에 지원되지 않으므로 VLAN은 해당 팀에 대해 구성될 수 없습니다.

5 절: 관리

- CIM
- SNMP

CIM

CIM(Common Information Model)은 DMTF(Distributed Management Task Force)에서 정의한 산업 표준입니다. Microsoft는 Windows Server 2008 등의 Windows 플랫폼에 CIM을 구현합니다. Broadcom은 Windows Server 2008 플랫폼에서 CIM을 지원합니다.

Broadcom 의 CIM 구현은 CIM 클라이언트 응용 프로그램을 통한 다양한 정보 제공 클래스를 제공하게 될 것입니다 . Broadcom CIM 데이터 제공업체는 데이터만 제공하며, 사용자는 Broadcom CIM 제공업체가 제공한 정보를 검색하여 선호하는 CIM 클라이언트 소프트웨어를 선택할 수 있습니다.

Broadcom CIM 제공업체는 BRCM_NetworkAdapter 및 BRCM_ExtraCapacityGroup 클래스를 통해 정보를 제공합니다 . BRCM_NetworkAdapter 클래스는 Broadcom 및 기타 공급업체의 컨트롤러를 모두 포함하는 어댑터 그룹과 관련된 네트워크 어댑터 정보를 제공합니다. BRCM_ExtraCapacityGroup 클래스는 BASP(Broadcom Advanced Server Program)를 위한 팀 구성을 제공합니다. 현재 구현은 팀 정보와 팀의 물리적인 네트워크 어댑터 정보를 제공합니다.

Broadcom Advanced Server Program은 이벤트 로그를 통해 이벤트를 제공합니다. 사용자는 Windows Server 2008에서 제공하는 "이벤트 뷰어"나 CIM을 사용하여 해당 이벤트를 검사 또는 모니터링할 수 있습니다. 또한 Broadcom CIM 제공업체는 CIM 의 일반 이벤트 모델을 통해 이벤트 정보를 제공합니다 . 해당 이벤트는 __InstanceCreationEvent, __InstanceDeletionEvent 및 __InstanceModificationEvent이며 CIM에서 정의됩니다. 이벤트를 올바르게 수신하려면 CIM의 클라이언트 응용 프로그램이 아래 표시된 예와 같은 질의를 사용하여 해당 이벤트를 등록해야 합니다.

```
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_ExtraCapacityGroup"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
```

해당 이벤트에 대한 자세한 내용은 http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf 에서 CIM 설명서를 참조하십시오.

SNMP

BASP Subagent

BASP Subagent인 `baspmgmt.dll`은 Windows Server 2008 SNMP 서비스용으로 제작되었습니다. BASP Subagent를 설치하기 전에 먼저 SNMP 서비스를 설치해야 합니다.

BASP Subagent를 사용하여 SNMP 관리자 소프트웨어는 Broadcom Advanced Server 기능의 구성 및 성능을 능동적으로 모니터링할 수 있습니다. 또한, Subagent는 SNMP 관리자에 경보 트랩을 제공하여 관리자에게 BASP 구성 요소 상태에 대한 모든 변경 사항을 알려줍니다.

BASP Subagent는 BASP 팀에 대한 구성 및 통계, 팀에 참여하는 물리적인 NIC 어댑터 및 팀 구성의 결과로 만들어진 가상 NIC 어댑터를 모니터링할 수 있습니다. 현재 팀 구성이 안된 NIC 어댑터는 모니터링되지 않습니다. BASP 구성 데이터에는 팀 ID, 물리적인/가상/VLAN/팀 어댑터 ID, 물리적인/가상/VLAN/팀 어댑터 설명 및 어댑터의 MAC 주소와 같은 정보가 포함됩니다.

통계에는 물리적인/가상/VLAN/팀 어댑터에 전송 및 수신된 데이터 패킷과 같은 자세한 내용이 포함됩니다.

경보 트랩은 물리적인 어댑터 링크 설정/해제 및 어댑터 설치/제거 이벤트와 같이 팀에 참여하는 물리적인 어댑터 구성에서의 변경 사항에 대한 정보를 전달합니다.

SNMP 관리자는 Broadcom BASP MIB 데이터베이스 파일을 로드해야만 위에서 설명한 정보를 모니터링할 수 있습니다. 아래에 표시된 이러한 파일들은 드라이버 소스 미디어에 포함되어 있습니다.

`baspcfg.mib`

`baspmat.mib`

`basptrap.mib`

BASP 확장형 에이전트

Broadcom NetXtreme Gigabit Ethernet Controller Extended Information SNMP 확장형 에이전트인 `bcmif.dll` 은 Windows Server SNMP 서비스용으로 제작되었습니다.

확장형 에이전트를 통해 SNMP 관리자 소프트웨어에서 Broadcom NetXtreme 어댑터의 구성을 능동적으로 모니터링할 수 있습니다. 이는 표준 SNMP 관리 네트워크 인터페이스 정보에서 이미 제공된 정보를 보완합니다.

확장형 에이전트는 다음과 같은 Broadcom NetXtreme 어댑터에 대해 심층적인 정보를 제공합니다.

- MAC 주소
- 바운드 IP 주소
- IP 서브넷 마스크
- 물리적 링크 상태
- 어댑터 상태
- 회선 속도
- 이중 모드
- 메모리 범위
- 인터럽트 설정
- 버스 번호

- 장치 번호
- 기능 번호

SNMP 관리자는 **Broadcom Extended Information MIB** 파일을 로드하여 위에서 설명한 정보를 모니터링할 수 있습니다 . **bcmif.mib** 파일은 **Broadcom NetXtreme** 어댑터 설치 CD에 포함되어 있습니다.

모니터링되는 워크스테이션에는 **Broadcom Extended Information SNMP** 확장형 에이전트인 **bcmif.dll** 을 설치해야 하며 , **Microsoft Windows Server 2008 SNMP** 서비스를 설치 및 로드해야 합니다.

6 절: 하드웨어 설치

- 안전 주의 사항
- 사전 설치 검사 목록
- 어댑터 설치
- 네트워크 케이블 연결



참고: Broadcom NetXtreme Gigabit Ethernet 어댑터의 애드 인 NIC 모델에만 적용됩니다.

안전 주의 사항



주의! 어댑터가 전압이 흐르는 시스템에 설치되어 있으면 위험할 수 있습니다. 사용자를 보호하고 시스템 구성 요소의 손상을 방지하려면 시스템 커버를 제거하기 전에 다음 주의 사항을 준수하십시오.

- 손과 손목에서 금속 물체나 귀금속을 제거합니다.
- 절연체나 비전도성 도구만 사용하도록 합니다.
- 내부 부품을 만지기 전에 컴퓨터 전원이 꺼져 있고 플러그가 뽑혀 있는지 확인합니다.
- 어댑터를 설치하거나 제거할 때 정전기가 없어야 합니다. 올바르게 접지된 손목 스트랩이나 기타 개인용 정전기 방지 장치 및 정전기 방지 매트를 사용하는 것이 좋습니다.

사전 설치 검사 목록

1. 서버에 최신 BIOS가 사용되고 있는지 확인합니다.
2. 사용자의 시스템이 운영 체제로 부팅된다면 OS 시스템 전원을 제대로 끕니다.
3. 시스템 종료가 완료되면 전원을 끄고 전원 코드를 뽑습니다.
4. 어댑터 카드의 가장자리를 잡고 선적 패키지에서 꺼내어 정전기가 없는 표면에 놓습니다.
5. 특히 어댑터의 카드 가장자리 커넥터에 손상된 흔적이 없는지 검사합니다. 손상된 어댑터를 설치해선 안 됩니다.

어댑터 설치

다음 지침은 대부분의 서버에서 **Broadcom NetXtreme Gigabit Ethernet** 어댑터(애드 인 NIC)를 설치하는 데 적용됩니다. 특정 서버에서 해당 작업 수행에 대한 자세한 내용은 서버와 함께 제공된 설명서를 참조하십시오.

1. **안전 주의 사항** 및 **사전 설치 검사 목록**을 검토합니다 어댑터를 설치하기 전에, 시스템 전원이 꺼져 있고 전원 콘센트에서 플러그가 뽑혀 있으며 전기 접지 절차가 올바르게 수행되고 있는지 확인합니다.
2. 시스템 케이스를 열고 비어 있는 **PCI Express** 슬롯을 선택합니다.
3. 선택한 슬롯에서 빈 커버 플레이트를 제거합니다.
4. 어댑터 커넥터 가장자리를 시스템의 커넥터 슬롯과 맞춥니다.
5. 카드의 양 쪽 모퉁이에 힘을 주어 슬롯이 완전히 장착될 때까지 어댑터 카드를 밀어 넣습니다. 어댑터가 완전히 장착되면 어댑터의 포트 커넥터가 슬롯 개방구에 정렬되고 전면이 시스템 본체에 접하게 됩니다.



주의! 시스템이나 어댑터가 손상될 수 있으므로 카드를 장착할 때 너무 힘을 주지 마십시오. 어댑터가 장착되지 않으면 어댑터를 빼내고 맞춘 후 다시 해보십시오.

6. 어댑터를 어댑터 클립이나 나사로 고정합니다.
7. 시스템 케이스를 완전히 닫고 개인용 정전기 방지 장치를 모두 떼어냅니다.

네트워크 케이블 연결

구리

Broadcom NetXtreme Gigabit Ethernet 어댑터에는 시스템을 Ethernet 구리선 부분에 연결시키는 데 사용되는 1개 이상의 RJ-45 커넥터가 있습니다.



참고: Broadcom NetXtreme Gigabit Ethernet 어댑터는 자동 MDIX(MDI Crossover)를 지원하므로 시스템을 연속해서 연결할 때 케이블을 교차할 필요가 없습니다. 직선 Category 5 케이블을 시스템에 바로 연결하면 통신할 수 있습니다.

1. 적합한 케이블을 선택합니다. 표 14:“10/100/1000BASE-T 케이블 사양”에는 10/100/1000BASE-T 포트 연결에 필요한 구리 케이블 요구 사항이 있습니다.

표 14. 10/100/1000BASE-T 케이블 사양

포트 종류	커넥터	미디어	최대 거리
10BASE-T	RJ-45	Category 3, 4 또는 5 UTP	100m(328ft)
100/1000BASE-T ¹	RJ-45	Category 5 ² UTP	100m(328ft)

¹1000BASE-T 신호를 사용하려면 ISO/IEC 11801:1995와 EIA/TIA-568-A(1995)에 명시되어 있고 TIA/EIA TSB95의 절차에 따라 테스트를 거친 4개의 트위스트 페어 케이블(Category 5)이 필요합니다.

²Category 5는 최소 요구 사항입니다. Category 5e와 Category 6은 완벽하게 지원됩니다.

2. 케이블의 한쪽 끝을 어댑터에 연결합니다.
3. 케이블의 다른 쪽 끝을 RJ-45 Ethernet 네트워크 포트에 연결합니다.



참고: 케이블을 양쪽 끝에 올바르게 꽂으면 어댑터 포트 LED가 작동합니다. 네트워크 링크 및 활동 표시에 대한 자세한 내용은 표 14: 64페이지의 “10/100/1000BASE-T 케이블 사양”을 참조하십시오.

7 절: 드라이버 디스크 작성

드라이버 디스크를 작성하는 지침은 시스템과 함께 제공되는 설명서를 참조하십시오.

8 절: Broadcom Boot Agent 드라이버 소프트웨어

- 개요
- 클라이언트 환경에서 MBA 설정

개요

Broadcom NetXtreme Gigabit Ethernet 어댑터는 PXE(Preboot Execution Environment), RPL(Remote Program Load), iSCSI 부팅 및 BootP(Bootstrap Protocol)를 지원합니다. MBA(Multi-Boot Agent)는 네트워크 시스템이 네트워크의 원격 시스템이 제공하는 이미지로 부팅할 수 있도록 해주는 소프트웨어 모듈입니다. Broadcom MBA 드라이버는 PXE.2.1 사양을 따르며, 단일 및 분할 이진 이미지로 출시됩니다. 이 드라이버는 마더보드에 내장 기본 코드가 있거나 없는 서로 다른 환경의 사용자가 사용할 수 있게 해줍니다.

MBA 모듈은 클라이언트/시스템 환경에서 작동합니다. 네트워크는 네트워크를 통해 여러 시스템에 부팅 이미지를 제공하는 하나 이상의 부팅 시스템으로 이루어집니다. Broadcom MBA 모듈 테스트가 제대로 이루어진 환경은 다음과 같습니다.

- **Linux® Red Hat® PXE 서버.** Broadcom PXE 클라이언트는 네트워크 리소스(NFS 마운트 등)를 원격으로 부팅하고 사용하여 Linux를 설치할 수 있습니다. 원격 부팅의 경우 Linux 범용 드라이버가 Broadcom 범용 네트워크 드라이버 인터페이스(UNDI)와 완벽하게 바인드되므로 Linux 원격 부팅 클라이언트 환경에서 네트워크 인터페이스 기능을 합니다.
- **Intel® APITEST.** Broadcom PXE 드라이버는 모든 API 테스트에서 적합 판정을 받았습니다.
- **WDS(Windows Deployment Service).** Windows Server의 경우 RIS는 Windows Server 2008을 포함한 Windows 운영 체제를 설치하기 위한 Broadcom PXE 클라이언트를 제공하는 WDS로 바뀌었습니다.

클라이언트 환경에서 MBA 설정

애드 인 NIC의 경우 다음 절차를 수행하십시오. LOM의 경우 컴퓨터 시스템 설명서를 참조하십시오.

MBA 클라이언트를 클라이언트 환경에 설정하려면

1. MBA 드라이버를 구성합니다.
2. 부팅 순서에 맞게 BIOS를 설정합니다.

MBA 드라이버 구성

이 섹션은 Broadcom 네트워크 어댑터의 애드 인 NIC 모델에 있는 MBA 드라이버 구성에 관련됩니다. Broadcom 네트워크 어댑터의 LOM 모델에 있는 MBA 드라이버 구성은 해당 시스템 설명서를 참조하십시오.

CCM 사용

1. 시스템을 다시 시작합니다
2. 메시지가 나타나고 4초 이내에 **CTRL+S**를 누릅니다. 어댑터 목록이 표시됩니다.
 - a. 구성할 어댑터를 선택하고 **Enter** 키를 누릅니다. 주 메뉴가 표시됩니다.
 - b. **MBA 구성**을 선택하여 MBA 구성 메뉴를 표시합니다.

```

Comprehensive Configuration Management v7.8.10
Copyright (C) 2000-2013 Broadcom Corporation
All rights reserved.

-----
MBA Configuration Menu
-----

Option ROM           : Enabled
Boot Protocol        : iSCSI
Boot Strap Type      : Auto
Hide Setup Prompt    : Disabled
Setup Key Stroke     : Ctrl-S
Banner Message Timeout : 5 Seconds
Link Speed           : 1Gbps
Pre-boot Wake On LAN : Disabled
VLAN Mode            : Disabled
VLAN ID              : 1
Boot Retry Count     : 0

-----
Enable/Disable Option ROM
[←|→][Enter][Space]:Toggle Value; [↑|↓]:Next Entry; [ESC]:Quit
Current Adapter:Primary, Bus=03 Device=00 Func=00, MAC=00:10:18:A7:19:10
  
```

3. 위쪽 화살표 및 아래쪽 화살표 키를 사용하여 Boot Protocol 메뉴 항목으로 이동합니다. PXE(Preboot Execution Environment) 외에 다른 부팅 프로토콜이 있으면 오른쪽 화살표나 왼쪽 화살표 키를 사용하여 해당 부팅 프로토콜을 선택합니다. 기타 부팅 프로토콜로는 RPL(Remote Program Load)과 BOOTP(Bootstrap Protocol)가 있습니다.



참고: 일부 iSCSI 부트 가능 LOM의 경우 부트 프로토콜은 BIOS를 통해 설정됩니다. 자세한 내용은 해당 시스템 설명서를 참조하십시오.



참고: 시스템에 어댑터가 여러 개이고 구성하고 있는 어댑터가 어느 것인지 모르는 경우 **Ctrl+F6**를 누르면 어댑터의 포트 LED가 깜박이기 시작합니다.

4. 위쪽 화살표, 아래쪽 화살표, 왼쪽 화살표, 오른쪽 화살표 키를 사용하여 다른 메뉴 항목의 값으로 이동하여 변경합니다.
5. **F4** 키를 눌러 설정을 저장합니다.
6. 종료되면 **ESC** 키를 누릅니다.

uEFI 사용

1. 시스템을 다시 시작합니다.
2. 시스템 설정 또는 장치 설정 구성 메뉴로 들어갑니다.
3. MBA 설정을 변경하려는 장치를 선택합니다.
4. **MBA 구성 메뉴**를 선택합니다.
5. PXE(Preboot Execution Environment) 이외의 부팅 프로토콜을 사용 가능할 경우, 드롭다운 메뉴를 사용하여 원하는 부팅 프로토콜을 선택합니다. 사용 가능한 기타 부팅 프로토콜로는 iSCSI와 BOOTP(Bootstrap Protocol)가 있습니다.



참고: iSCSI 부트 가능 LOM의 경우 부트 프로토콜은 BIOS를 통해 설정됩니다. 자세한 내용은 해당 시스템 설명서를 참조하십시오.

6. 위쪽 화살표, 아래쪽 화살표, 왼쪽 화살표, 오른쪽 화살표 키를 사용하여 다른 메뉴 항목의 값으로 이동하여 변경합니다.
7. 주 메뉴로 이동하려면 **뒤로**를 선택합니다.
8. 저장 후 종료하려면 **마침**을 선택합니다.

BIOS 설정

MBA로 네트워크에서 부팅하려면 MBA 활성화 어댑터를 BIOS에서 처음 부팅 가능한 장치로 설정합니다. 이 절차는 시스템 BIOS 종류에 따라 다릅니다. 자세한 내용은 시스템 사용자 설명서를 참조하십시오.

9 절: iSCSI 프로토콜

- [iSCSI 부트](#)
- [iSCSI Crash Dump](#)

iSCSI 부트

Broadcom NetXtreme Gigabit Ethernet 어댑터는 iSCSI 부트를 지원함으로써 디스크가 없는 시스템에서 운영 체제의 네트워크 부팅을 허용합니다. iSCSI 부트는 원격 위치에 있는 iSCSI 대상 시스템에서 표준 IP 네트워크를 통해 Windows 또는 Linux 운영 체제를 부팅할 수 있도록 합니다.

Windows 및 Linux 운영 체제 모두에서 [표 15](#)에 표시되는 일반 매개 변수로 부팅하도록 iSCSI 부트를 구성할 수 있습니다.

iSCSI 부트용으로 지원되는 운영 체제

Broadcom NetXtreme Gigabit Ethernet 어댑터는 다음 운영 체제에서 iSCSI 부트를 지원합니다.

- Windows Server 운영 체제
- Enterprise Linux 배포판

iSCSI 부트 설정

iSCSI 부트 설정은 다음으로 구성됩니다.

이 섹션은 BIOS 모드 iSCSI 부트에 적용됩니다. UEFI iSCSI 부트 설정에 대한 시스템 문서를 참조하십시오. EBDA 메모리 제약 조건으로 인해 로컬 저장소(특히, RAID)가 BIOS 모드에 있는 경우 iSCSI 부트는 지원되지 않습니다.

- [iSCSI 대상 구성](#)
- [iSCSI 부트 매개 변수 구성](#)
- [iSCSI 부트 이미지 준비](#)
- [부팅](#)

iSCSI 대상 구성

iSCSI 대상 구성은 대상 공급업체에 따라 다릅니다. iSCSI 대상 구성에 대한 자세한 내용은 공급업체가 제공한 설명서를 참조하십시오. 일반 단계는 다음과 같습니다.

1. iSCSI 대상을 생성합니다.
2. 가상 디스크를 작성합니다.
3. 1단계에서 생성한 iSCSI 대상에 가상 디스크를 매핑합니다.
4. iSCSI 대상에 iSCSI 초기자를 연결합니다.
5. iSCSI 대상 이름, TCP 포트 번호, iSCSI LUN(Logical Unit Number), 초기자 IQN(Internet Qualified Name) 및 CHAP 인증 세부 정보를 기록합니다.

6. iSCSI 대상을 구성한 후에는 다음 정보를 구합니다.

- 대상 IQN 이름
- 대상 IP 주소
- 대상 TCP 포트 번호
- 대상 LUN
- 초기자 IQN
- CHAP ID 및 비밀

iSCSI 부트 매개 변수 구성

Broadcom iSCSI 부트 소프트웨어를 정적 또는 동적 구성으로 구성합니다. 일반 매개 변수 화면에서 사용 가능한 구성 옵션은 [표 15](#)를 참조하십시오.

[표 15](#)에는 IPv4 및 IPv6 모두의 매개 변수가 나와 있습니다. IPv4 또는 IPv6 전용 매개 변수는 따로 표시되어 있습니다.



참고: IPv6 iSCSI 부팅의 사용 가능 여부는 플랫폼/장치마다 다릅니다.

표 15. 구성 옵션

Option	설명
DHCP를 통한 TCP/IP 매개 변수	이 옵션은 IPv4 전용입니다. iSCSI 부트 호스트 소프트웨어가 DHCP(사용)를 통해 IP 주소 정보를 획득할지 또는 정적 IP 구성(사용 안 함)을 사용할지 여부를 제어합니다.
IP 자동 구성	이 옵션은 IPv6 전용입니다. DHCPv6이 있고 사용되는(사용) 경우 iSCSI 부트 호스트 소프트웨어가 무상태 링크 로컬 주소 및/또는 상태 저장 주소를 구성할지 여부를 제어합니다. Router Solicit 패킷이 4초 간격으로 최대 3회 전송됩니다. 또는 정적 IP 구성을 사용합니다(사용 안 함).
DHCP를 통한 iSCSI 매개 변수	iSCSI 부트 호스트 소프트웨어가 DHCP(사용)를 통해 iSCSI 대상 매개 변수를 획득할지 또는 정적 구성(사용 안 함)을 사용할지 여부를 제어합니다. 정적 정보는 iSCSI 초기자 매개 변수 구성 화면을 통해 입력합니다.
CHAP 인증	iSCSI 부트 호스트 소프트웨어가 iSCSI 대상에 연결할 때 CHAP 인증을 사용할지 여부를 제어합니다. CHAP 인증을 사용할 경우 iSCSI 초기자 매개 변수 구성 화면을 통해 CHAP ID와 CHAP 비밀을 입력합니다.
DHCP 공급업체 ID	iSCSI 부트 호스트 소프트웨어가 DHCP 도중에 공급업체 클래스 ID를 해석하는 방법을 제어합니다. DHCP 오퍼 패킷의 공급업체 클래스 ID 필드가 이 필드의 값과 일치하면 iSCSI 부트 호스트 소프트웨어가 DHCP 옵션 43 필드에서 필요한 iSCSI 부트 확장자를 찾습니다. DHCP를 사용하지 않으면 이 값을 설정할 필요가 없습니다.
링크 연결 지연 시간	Ethernet 링크가 설정된 후 네트워크를 통해 데이터를 전송하기 전에 iSCSI 부트 호스트 소프트웨어가 대기하는 시간(초)을 제어합니다. 유효한 값은 0 ~ 255입니다. 예를 들어 클라이언트 시스템에 대한 스위치 인터페이스에 스페닝 트리와 같은 네트워크 프로토콜을 사용할 경우 이 옵션의 값을 설정해야 할 수 있습니다.
TCP 타임스탬프 사용	TCP 타임스탬프 옵션의 사용 여부를 제어합니다.
대상을 첫 번째 HDD로	iSCSI 대상 드라이브를 시스템의 첫 번째 하드 드라이브로 지정할 수 있습니다.
LUN 사용 중 재시도 횟수	iSCSI 대상 LUN이 사용 중일 때 iSCSI 부트 초기자가 시도할 연결 재시도 횟수를 제어합니다.
IP 버전	이 옵션은 IPv6 전용입니다. IPv4 또는 IPv6 프로토콜 사이를 전환합니다. 한 프로토콜 버전에서 다른 프로토콜 버전으로 전환하면 모든 IP 설정이 손실됩니다.

MBA 부트 프로토콜 구성

부트 프로토콜을 구성하려면

1. 시스템을 다시 시작합니다.
2. PXE 배너에서 **CTRL+S**를 선택합니다. MBA 구성 메뉴가 나타납니다([Broadcom Boot Agent](#) 참조).
3. MBA 구성 메뉴에서 **위쪽 화살표** 또는 **아래쪽 화살표** 키를 사용하여 **Boot Protocol** 옵션으로 이동합니다. **왼쪽 화살표** 또는 **오른쪽 화살표** 키를 사용하여 **Boot Protocol** 옵션을 **iSCSI**로 변경합니다.



참고: BIOS를 통해 부트 프로토콜이 설정된 플랫폼의 경우 자세한 내용은 시스템 설명서를 참조하십시오.

4. 주 메뉴에서 **iSCSI 부트 구성**을 선택합니다.



참고: NetXtreme 네트워크 어댑터에 iSCSI 부트 펌웨어가 프로그래밍되어 있지 않은 경우에는 **iSCSI 부트 구성**을 선택해도 아무런 효과가 없습니다.

iSCSI 부트 구성

- [정적 iSCSI 부트 구성](#)
- [동적 iSCSI 부트 구성](#)

정적 iSCSI 부트 구성

정적 구성에서는 [iSCSI 대상 구성](#)에서 얻은 시스템 IP 주소, 시스템 초기자 IQN 및 대상 매개 변수 데이터를 입력해야 합니다. 구성 옵션에 대한 자세한 내용은 [표 15](#)를 참조하십시오.

정적 구성을 사용하여 **iSCSI 부트 매개 변수**를 구성하려면

1. 일반 매개 변수 메뉴 화면에서 다음을 설정합니다.
 - **DHCP를 통한 TCP/IP 매개 변수:** 사용 안 함 (IPv4용)
 - **IP 자동 구성:** 사용 안 함 (IPv6용)
 - **DHCP를 통한 iSCSI 매개 변수:** 사용 안 함
 - **CHAP 인증:** 사용 안 함
 - **iSCSI 대상으로 부팅:** 사용 안 함
 - **DHCP 공급업체 ID:** BCM ISAN
 - **링크 연결 지연 시간:** 0
 - **TCP 타임스탬프 사용:** 사용(Dell/EMC AX100i와 같은 일부 대상의 경우 **TCP 타임스탬프 사용을 활성화해야 함**)
 - **대상을 첫 번째 HDD로:** 사용 안 함
 - **LUN 사용 중 재시도 횟수:** 0
 - **IP 버전:** IPv6 (IPv6용)
2. **ESC** 키를 선택하여 주 메뉴로 돌아갑니다.
3. 주 메뉴에서 **초기자 매개 변수**를 선택합니다.
4. 초기자 매개 변수 화면에서 다음 값을 입력합니다.
 - IP 주소(지정되지 않은 IPv4 및 IPv6 주소는 각각 "0.0.0.0" 및 "::"이어야 함)
 - 서브넷 마스크 접두사
 - 기본 게이트웨이
 - 주 DNS

- 보조 DNS
- iSCSI 이름(클라이언트 시스템이 사용할 iSCSI 초기자 이름)



참고: IP 주소를 정확하게 입력합니다. 중복되거나 잘못된 세그먼트/네트워크 할당을 찾아내기 위해 IP 주소에서 오류를 확인하는 과정이 없습니다.

5. ESC 키를 선택하여 주 메뉴로 돌아갑니다.
6. 주 메뉴에서 첫 번째 대상 매개 변수를 선택합니다.
7. 첫 번째 대상 매개 변수 화면에서 연결을 활성화하여 iSCSI 대상에 연결합니다. iSCSI 대상을 구성할 때 사용한 값을 사용하여 다음 값을 입력합니다.
 - IP 주소
 - TCP 포트
 - 부팅 LUN
 - iSCSI 이름
8. ESC 키를 선택하여 주 메뉴로 돌아갑니다.
9. ESC 키를 선택하고 구성 저장 후 종료를 선택합니다.
10. F4 키를 눌러 MBA 구성을 저장합니다.

동적 iSCSI 부트 구성

동적 구성에서는 DHCP 서버에서 제공한 시스템 IP 주소와 대상/초기자 정보를 지정하기만 하면 됩니다(DHCP 서버가 iSCSI 부트를 지원하도록 구성에서 IPv4 및 IPv6 구성 참조). IPv4의 경우 초기자 iSCSI 이름을 제외하고 초기자 매개 변수, 첫 번째 대상 매개 변수 또는 두 번째 대상 매개 변수 화면의 모든 설정은 무시되며 지을 필요가 없습니다. IPv6의 경우 CHAP ID 및 비밀을 제외하고 초기자 매개 변수, 첫 번째 대상 매개 변수 또는 두 번째 대상 매개 변수 화면의 모든 설정은 무시되며 지을 필요가 없습니다. 구성 옵션에 대한 자세한 내용은 표 15를 참조하십시오.



설명:

- DHCP 서버를 사용할 때 DNS 서버 항목을 DHCP 서버에서 제공한 값으로 덮어씁니다. 이 문제는 로컬로 제공된 값이 유효하고 DHCP 서버가 DNS 서버 정보를 제공하지 않는 경우에도 발생합니다. DHCP 서버가 DNS 서버 정보를 제공하지 않으면 주 및 보조 DNS 서버 값이 0.0.0.0으로 설정됩니다. Windows OS가 임무를 수행하게 되면 Microsoft iSCSI 초기자는 iSCSI 초기자 매개 변수를 검색하고 적절한 레지스트리를 정적으로 구성합니다. 이 때 이전에 구성된 내용은 모두 덮어씁니다. DHCP 데몬은 Windows 환경에서 사용자 프로세스로 실행되므로 iSCSI 부트 환경에서 스택이 시작되기 전에 모든 TCP/IP 매개 변수를 정적으로 구성해야 합니다.
- DHCP 옵션 17을 사용할 경우, 대상 정보는 DHCP 서버가 제공하며 초기자 iSCSI 이름은 초기자 매개 변수 화면에서 프로그래밍된 값에서 검색됩니다. 아무 값도 선택하지 않으면 컨트롤러가 다음 이름으로 기본 설정됩니다.

iqn.1995-05.com.broadcom.<11.22.33.44.55.66>.iscsiboot

여기서 문자열 11.22.33.44.55.66은 컨트롤러의 MAC 주소에 해당합니다.

DHCP 옵션 43(IPv4 전용)을 사용할 경우, 초기자 매개 변수, 첫 번째 대상 매개 변수 또는 두 번째 대상 매개 변수 화면의 모든 설정은 무시되며 지을 필요가 없습니다.

동적 구성을 사용하여 iSCSI 부트 매개 변수를 구성하려면

1. 일반 매개 변수 메뉴 화면에서 다음을 설정합니다.
 - DHCP를 통한 TCP/IP 매개 변수: 사용 (IPv4용)
 - IP 자동 구성: 사용 (IPv6용)
 - DHCP를 통한 iSCSI 매개 변수: 사용

- **CHAP 인증:** 사용 안 함
- **iSCSI 대상으로 부팅:** 사용 안 함
- **DHCP 공급업체 ID:** BCM ISAN
- **링크 연결 지연 시간:** 0
- **TCP 타임스탬프 사용:** 사용(Dell/EMC AX100i와 같은 일부 대상의 경우 **TCP 타임스탬프 사용**을 활성화해야 함)
- **대상을 첫 번째 HDD로:** 사용 안 함
- **LUN 사용 중 재시도 횟수:** 0
- **IP 버전:** IPv6 (IPv6용)

2. **ESC** 키를 선택하여 주 메뉴로 돌아갑니다.



참고: 초기자 매개 변수 및 첫 번째 대상 매개 변수 화면의 정보는 무시되며 지을 필요가 없습니다.

3. 구성 저장 후 종료를 선택합니다.

CHAP 인증 활성화

CHAP 인증이 대상에 활성화되어 있는지 확인합니다.

CHAP 인증 사용

1. 일반 매개 변수 화면에서 **CHAP 인증**을 사용으로 설정합니다.
2. 초기자 매개 변수 화면에서 다음 값을 입력합니다.
 - CHAP ID(최대 128바이트)
 - CHAP 비밀(인증이 필요한 경우 길이가 12자 이상이어야 함)
3. ESC 키를 선택하여 주 메뉴로 돌아갑니다.
4. 주 메뉴에서 첫 번째 대상 매개 변수를 선택합니다.
5. 첫 번째 대상 매개 변수 화면에서, iSCSI 대상을 구성할 때 사용한 값을 사용하여 다음 값을 입력합니다.
 - CHAP ID(양방향 CHAP인 경우 옵션)
 - CHAP 비밀(양방향 CHAP인 경우 옵션, 길이가 12자 이상이어야 함)
6. ESC 키를 선택하여 주 메뉴로 돌아갑니다.
7. ESC 키를 선택하고 구성 저장 후 종료를 선택합니다.

DHCP 서버가 iSCSI 부트를 지원하도록 구성

DHCP 서버는 옵션 구성 요소이며 동적 iSCSI 부트 구성 설정을 수행할 경우에만 필요합니다([동적 iSCSI 부트 구성 참조](#)).

DHCP 서버가 iSCSI 부트를 지원하도록 구성하는 방법은 IPv4와 IPv6에서 서로 다릅니다.

- [IPv4를 위한 DHCP iSCSI 부트 구성](#)
- [IPv6을 위한 DHCP iSCSI 부트 구성](#)

IPv4를 위한 DHCP iSCSI 부트 구성

DHCP 프로토콜에는 DHCP 클라이언트에 구성 정보를 제공하는 다양한 옵션이 포함되어 있습니다. iSCSI 부트의 경우, Broadcom 어댑터는 다음과 같은 DHCP 구성을 지원합니다.

- [DHCP 옵션 17, 루트 경로](#)
- [DHCP 옵션 43, 공급업체 정보](#)

DHCP 옵션 17, 루트 경로

옵션 17은 iSCSI 클라이언트에 iSCSI 대상 정보를 전달하는 데 사용됩니다.

IETF RFC 4173에 정의된 루트 경로의 형식은 다음과 같습니다.

```
"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
```

매개 변수는 아래와 같이 정의됩니다.

표 16. DHCP 옵션 17 매개 변수 정의

매개 변수	정의
"iscsi:"	리터럴 문자열
<servername>	iSCSI 대상의 IP 주소 또는 FQDN
":"	구분 기호
<protocol>	iSCSI 대상에 액세스하는 데 사용되는 IP 프로토콜입니다. 현재 TCP만 지원되므로 프로토콜은 6입니다.
<port>	프로토콜과 관련된 포트 번호입니다. iSCSI의 표준 포트 번호는 3260입니다.
<LUN>	iSCSI 대상에서 사용할 논리 단위 번호입니다. LUN 값은 16진법으로 표시되어야 합니다. ID가 64인 LUN은 DHCP 서버의 옵션 17 매개 변수 내에서 40으로 구성되어야 합니다.
<targetname>	IQN 또는 EUI 형식의 대상 이름입니다(IQN 및 EUI 형식에 대한 자세한 내용은 RFC 3720 참조). IQN 이름의 예는 "iqn.1995-05.com.broadcom:iscsi-target"입니다.

DHCP 옵션 43, 공급업체 정보

DHCP 옵션 43(공급업체 정보)은 DHCP 옵션 17보다 많은 구성 옵션을 iSCSI 클라이언트에 제공합니다. 이 구성에서는 부팅에 사용할 수 있는 2개의 iSCSI 대상 IQN과 함께 iSCSI 부트 클라이언트에 초기자 IQN을 할당하는 3개의 하위 옵션이 추가로 제공됩니다. iSCSI 대상 IQN은 DHCP 옵션 17과 형식이 같은 반면 iSCSI 초기자 IQN은 해당 초기자의 IQN에 불과합니다.



참고: DHCP 옵션 43은 IPv4에서만 지원됩니다.

하위 옵션은 아래와 같습니다.

표 17. DHCP 옵션 43 하위 옵션 정의

하위 옵션	정의
201	표준 루트 경로 형식의 첫 번째 iSCSI 대상 정보 "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
202	표준 루트 경로 형식의 두 번째 iSCSI 대상 정보 "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
203	iSCSI 초기자 IQN

DHCP 옵션 43을 사용하려면 DHCP 옵션 17보다 많은 구성이 필요하지만, 이 옵션은 풍부한 환경과 여러 구성 옵션을 제공합니다. 동적 iSCSI 부트 구성을 수행할 때는 DHCP 옵션 43을 사용하는 것이 좋습니다.

DHCP 서버 구성

옵션 17 또는 옵션 43을 지원하도록 DHCP 서버를 구성합니다.



참고: 옵션 43을 사용할 경우 옵션 60도 구성해야 합니다. 옵션 60의 값은 DHCP 공급업체 ID 값과 일치해야 합니다. DHCP 공급업체 ID 값은 BRCM ISAN이며 iSCSI 부트 구성 메뉴의 일반 매개 변수에 표시됩니다.

IPv6을 위한 DHCP iSCSI 부트 구성

DHCPv6 서버는 무상태 또는 상태 저장 IP 구성을 비롯한 다수의 옵션과 정보를 DHCPv6 클라이언트에 제공할 수 있습니다. iSCSI 부트의 경우, Broadcom 어댑터는 다음과 같은 DHCP 구성을 지원합니다.

- DHCPv6 옵션 16, 공급업체 클래스 옵션
- DHCPv6 옵션 17, 공급업체 정보



참고: DHCPv6 표준 루트 경로 옵션은 아직 사용할 수 없습니다. Broadcom은 동적 iSCSI 부트 IPv6 지원에 대해 옵션 16 또는 옵션 17을 사용할 것을 권장합니다.

DHCPv6 옵션 16, 공급업체 클래스 옵션

DHCPv6 옵션 16(공급업체 클래스 옵션)이 있고 구성된 **DHCP 공급업체 ID** 매개 변수와 일치하는 문자열을 포함해야 합니다. **DHCP 공급업체 ID** 값은 BRCM ISAN이며 iSCSI 부트 구성 메뉴의 **일반 매개 변수**에 표시됩니다.

옵션 16의 내용은 <2-byte length> <DHCP Vendor ID>여야 합니다.

DHCPv6 옵션 17, 공급업체 정보

DHCPv6 옵션 17(공급업체 정보)은 보다 많은 구성 옵션을 iSCSI 클라이언트에 제공합니다. 이 구성에서는 부팅에 사용할 수 있는 2개의 iSCSI 대상 IQN과 함께 iSCSI 부트 클라이언트에 초기자 IQN을 할당하는 3개의 하위 옵션이 추가로 제공됩니다.

하위 옵션은 아래와 같습니다.

표 18. DHCP 옵션 17 하위 옵션 정의

하위 옵션	정의
201	표준 루트 경로 형식의 첫 번째 iSCSI 대상 정보 "iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"
202	표준 루트 경로 형식의 두 번째 iSCSI 대상 정보 "iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"
203	iSCSI 초기자 IQN



참고: 표 18에서 대괄호 []는 IPv6 주소에 필요합니다.

옵션 17의 내용은 <2-byte Option Number 201|202|203> <2-byte length> <data>여야 합니다.

DHCP 서버 구성

옵션 16 또는 옵션 17을 지원하도록 DHCP 서버를 구성합니다.



참고: DHCPv6 옵션 16 및 옵션 17의 형식은 RFC 3315에 완전히 정의되어 있습니다.

iSCSI 부트 이미지 준비

- [Windows Server 2008 R2 및 SP2 iSCSI 부트 설정](#)
- [Windows Server 2012 iSCSI 부트 설정](#)
- [Linux iSCSI 부트 설정](#)
- [Broadcom 드라이버를 Windows 이미지 파일로 삽입\(적용\)](#)

Windows Server 2008 R2 및 SP2 iSCSI 부트 설정

Windows Server 2008 R2 및 Windows Server 2008 SP2는 iSCSI 부팅을 지원합니다. 다음 절차에서는 Windows Server 2008 R2가 언급되고 있지만, Windows Server 2008 R2 및 SP2 모두에 공통으로 적용됩니다.

필요한 CD/ISO 이미지:

- Broadcom 드라이버를 삽입한 Windows Server 2008 R2 x64. [Broadcom 드라이버를 Windows 이미지 파일로 삽입\(적용\)](#)을 참조하십시오. 또한 support.microsoft.com에서 Microsoft 기술 자료 항목 KB974072를 참조하십시오.



설명 :

- Microsoft 절차는 NDIS 드라이버만 삽입합니다. 모든 드라이버(VBD, BXND, OIS 및 NetXtreme I NDIS)를 삽입하는 것이 좋습니다.
- 개별 Windows NetXtreme 드라이버를 추출하는 방법에 대한 지침은 특정 드라이버 설치 프로그램의 *silent.txt* 파일을 참조하십시오.

필요한 다른 소프트웨어:

- Bindview.exe(Windows Server 2008 R2만 해당. KB976042 참조)

절차:

1. 부팅할 시스템("원격 시스템")에서 로컬 하드 드라이브를 모두 제거합니다.
2. 최신 Broadcom MBA 및 iSCSI 부트 이미지를 어댑터의 NVRAM에 로드합니다.
3. Broadcom MBA가 첫 번째 부팅 가능 장치로 지정되고 CDRROM이 두 번째 부팅 가능 장치로 지정되도록 원격 시스템의 BIOS를 구성합니다.
4. 원격 장치로부터 연결을 허용하도록 iSCSI 대상을 구성합니다. 대상에서 새로운 O/S 설치를 위한 디스크 공간이 충분한지 확인합니다.
5. 원격 시스템을 부팅합니다. Preboot Execution Environment(PXE) 배너가 표시되면 **Ctrl+S**를 눌러 PXE 메뉴로 들어갑니다.
6. PXE 메뉴에서 **부트 프로토콜을 iSCSI**로 설정합니다.
7. iSCSI 대상 매개 변수를 입력합니다.
8. 일반 매개 변수에서 **대상으로 부팅** 매개 변수를 **1회 사용 안 함**으로 설정합니다.
9. 설정을 저장하고 시스템을 다시 부팅합니다.
원격 시스템이 iSCSI 대상에 연결되고 DVDROM 장치로부터 부팅됩니다.
10. DVD로 부팅하고 설치를 시작합니다.
11. 모든 설치 질문에 적절하게 답변합니다(설치할 운영 체제를 선택하고 라이선스 조건에 동의하는 것 등).
Windows를 설치할 위치를 지정하십시오. 창이 나타나면 대상 드라이브가 표시됩니다. 이것은 iSCSI 부트 프로토콜을 통해 연결된 드라이브이며 원격 iSCSI 대상에 위치합니다.
12. 다음을 선택하여 Windows Server 2008 R2 설치를 진행합니다.

Windows Server 2008 R2 DVD 설치 프로세스가 시작된 후 몇 분이 지나면 시스템이 재부팅됩니다. 재부팅 후, Windows

Server 2008 R2 설치 루틴이 재개되고 설치가 완료됩니다.

13. 시스템이 다시 재부팅되면 원격 시스템이 데스크탑으로 부팅할 수 있는지 확인하십시오.
14. Windows Server 2008 R2가 부팅된 후, 드라이버를 로드하고 Bindview.exe를 실행합니다.
 - a. 모든 서비스를 선택합니다.
 - b. **WFP Lightweight 필터에 AUT에 대한 바인딩 경로**가 표시됩니다. 마우스 오른쪽 단추로 클릭하고 비활성화합니다. 완료되면 응용 프로그램을 종료합니다.
15. OS 및 시스템이 작동하고 원격 시스템 IP 등을 ping하여 트래픽을 전달할 수 있는지 확인합니다.

Windows Server 2012 iSCSI 부트 설정

Windows Server 2012는 iSCSI 부팅 및 설치를 지원합니다. 최신 Broadcom 드라이버가 삽입된 “통합 설치” DVD를 사용해야 합니다. [Broadcom 드라이버를 Windows 이미지 파일로 삽입 \(적용\)](#)을 참조하십시오. 또한 support.microsoft.com에서 Microsoft 기술 자료 항목 KB974072를 참조하십시오.



참고: Microsoft 절차는 NDIS 드라이버만 삽입합니다. 모든 드라이버(VBD, BXND, OIS 및 NetXtreme I NDIS)를 삽입하는 것이 좋습니다.

다음 절차에서는 설치 및 부팅용 이미지를 준비합니다.

1. 부팅할 시스템(“원격 시스템”)에서 로컬 하드 드라이브를 모두 제거합니다.
2. 최신 Broadcom MBA 및 iSCSI 부트 이미지를 어댑터의 NVRAM에 로드합니다.
3. Broadcom MBA가 첫 번째 부팅 가능 장치로 지정되고 CDROM이 두 번째 부팅 가능 장치로 지정되도록 원격 시스템의 BIOS를 구성합니다.
4. 원격 장치로부터 연결을 허용하도록 iSCSI 대상을 구성합니다. 대상에서 새로운 O/S 설치를 위한 디스크 공간이 충분한지 확인합니다.
5. 원격 시스템을 부팅합니다. Preboot Execution Environment(PXE) 배너가 표시되면 **Ctrl+S**를 눌러 PXE 메뉴로 들어갑니다.
6. PXE 메뉴에서 **부트 프로토콜을 iSCSI**로 설정합니다.
7. iSCSI 대상 매개 변수를 입력합니다.
8. 일반 매개 변수에서 **대상으로 부팅** 매개 변수를 **1회 사용 안 함**으로 설정합니다.
9. 설정을 저장하고 시스템을 다시 부팅합니다.
원격 시스템이 iSCSI 대상에 연결되고 DVDROM 장치로부터 부팅됩니다.
10. DVD에서 부팅하고 설치를 시작합니다.
11. 모든 설치 질문에 적절하게 답변합니다(설치할 운영 체제를 선택하고 라이선스 조건에 동의하는 것 등).
Windows를 설치할 위치를 지정하십시오. 창이 나타나면 대상 드라이브가 표시됩니다. 이것은 iSCSI 부트 프로토콜을 통해 연결된 드라이브이며 원격 iSCSI 대상에 위치합니다.
12. 다음을 선택하여 Windows 2012 설치를 계속합니다.
Windows 2012 DVD 설치 프로세스가 시작된 후 몇 분이 지나면 시스템이 재부팅합니다. 재부팅 후, Windows 2012 설치 루틴이 재개되어 설치가 완료됩니다.
13. 시스템이 다시 재부팅되면 원격 시스템이 데스크탑으로 부팅할 수 있는지 확인하십시오.
14. Windows 2012가 OS로 부팅하면, 드라이버 설치 프로그램을 실행하여 Broadcom 드라이버 및 응용 프로그램 설치를 완료하는 것이 좋습니다.

Linux iSCSI 부트 설정

Linux iSCSI 부트는 Red Hat Enterprise Linux 5.5 이상과 SUSE Linux Enterprise Server 11 SP1 이상에서 지원됩니다.

1. 드라이버를 업데이트하려면 최신 **Broadcom Linux** 드라이버 CD가 필요합니다.
2. 네트워크 어댑터에서 대상을 통한 부트 옵션을 비활성화하여 대상에 DVD를 직접 설치하는 iSCSI 부트 매개 변수를 구성합니다.
3. NVRAM 구성에서 HBA 부트 모드를 **사용 안 함**으로 설정하여 비Offload 경로를 통해 설치하도록 구성합니다. (**참고:** 어댑터가 다기능 모드인 경우 이 매개 변수를 변경할 수 없습니다.) RHEL6.2 및 SLES11SP2 이상에서는 Offload 경로를 통한 설치가 지원되지 않습니다. 이 경우 NVRAM 구성에서 HBA 부트 모드를 **사용**으로 설정합니다.
4. 다음과 같이 부트 순서를 변경합니다.
 - a. 네트워크 어댑터에서 부트
 - b. CD/DVD 드라이브에서 부트
5. 시스템을 다시 부팅합니다.
6. 시스템이 iSCSI 대상으로 연결된 후 CD/DVD 드라이브에서 부팅합니다.
7. 해당 OS 지침을 따릅니다.
 - a. RHEL 5.5 - "boot:" 프롬프트에서 "linux dd"를 입력하고 Enter키를 누릅니다.
 - b. SuSE 11.X — 설치를 선택하고 부트 옵션에서 **withiscsi=1 netsetup=1**을 입력합니다. 드라이버를 업데이트하려면 F6 드라이버 옵션에서 **예**를 선택합니다.
8. 드라이버를 업데이트하려면 지침에 따라 드라이버 CD를 로드합니다. 그렇지 않을 경우 이 단계를 건너뛰십시오.
9. "networking device" 프롬프트에서 원하는 네트워크 어댑터 포트를 선택하고 **확인**을 누릅니다.
10. "configure TCP/IP" 프롬프트에서 IP 주소를 획득할 방식을 구성하고 **확인**을 누릅니다.
11. 정적 IP를 선택한 경우 **iscsi** 초기자에 대한 IP 정보를 입력해야 합니다.
12. (RHEL) 미디어 테스트를 "건너뛰려면" 선택합니다.
13. 필요에 따라 설치를 계속합니다. 이때 드라이브를 사용할 수 있습니다. 파일 복사가 완료되면 CD/DVD를 제거하고 시스템을 재부팅합니다.
14. 시스템이 재부팅되면 iSCSI 부트 매개 변수에서 "대상을 통한 부트"를 활성화하고 설치를 계속 진행해 완료합니다.

이 단계에서는 초기 설치 단계가 완료됩니다. 나머지 절차에서는 새 구성 요소 업데이트를 위한 새 사용자 정의 **initrd**를 만듭니다.

15. 원할 경우 **iscsi** 초기자를 업데이트합니다. 먼저 **rpm -e**를 사용하여 기존 초기자를 제거해야 합니다.
16. 네트워크 서비스의 모든 실행 수준이 On인지 확인합니다.
`chkconfig network on`
17. **iscsi** 서비스의 2, 3 및 5 실행 수준이 On인지 확인합니다.
`chkconfig -level 235 iscsi on`
18. Red Hat 6.0의 경우 네트워크 관리자 서비스는 중지되고 비활성화됩니다.
19. 원할 경우 **iscsiuio**를 설치합니다(SuSE 10에는 필요하지 않음).
20. 원할 경우 **linux-nx2** 패키지를 설치합니다.
21. **bibt** 패키지를 설치합니다.
22. **ifcfg-eth***를 제거합니다.
23. 다시 부팅합니다.
24. SUSE 11.1의 경우 아래 그림과 같이 원격 DVD 설치 임시 해결책을 따릅니다.
25. 시스템이 재부팅되면 로그인하여 **/opt/bcm/bibt** 폴더로 변경한 다음, **iscsi_setup.sh** 스크립트를 실행하여 **initrd** 이미지를 만듭니다.

26. initrd 이미지를 /boot 폴더로 복사합니다.
27. 새 initrd 이미지를 가리키도록 grub 메뉴를 변경합니다.
28. CHAP를 활성화하려면 iscsid.conf를 수정해야 합니다(Red Hat에만 해당).
29. 재부팅한 후 필요에 따라 CHAP 매개 변수를 변경합니다.
30. iSCSI 부트 이미지 부팅을 계속 진행하고 생성한 이미지 중 하나를 선택합니다.
31. IPv6의 경우 이제 NVRAM 구성에서 두 초기자 및 대상의 IP 주소를 원하는 IPv6 주소로 변경할 수 있습니다.

SUSE 11.1 원격 DVD 설치 임시 해결책

1. 아래 표시된 내용을 포함하는 boot.open-iscsi라는 새 파일을 생성합니다.
2. 생성한 파일을 /etc/init.d/ 폴더로 복사하여 기존 파일을 덮어씁니다.

새 boot.open-iscsi 파일의 내용:

```
#!/bin/bash
#
# /etc/init.d/iscsi
#
### BEGIN INIT INFO
# Provides:          iscsiboot
# Required-Start:
# Should-Start:      boot.multipath
# Required-Stop:
# Should-Stop:       $null
# Default-Start:     B
# Default-Stop:
# Short-Description: iSCSI initiator daemon root-fs support
# Description:       Starts the iSCSI initiator daemon if the
#                    root-filesystem is on an iSCSI device
#
### END INIT INFO

ISCSIADM=/sbin/iscsiadm
ISCSIUIO=/sbin/iscsiuio
CONFIG_FILE=/etc/iscsid.conf
DAEMON=/sbin/iscsid
ARGS="-c $CONFIG_FILE"

# Source LSB init functions
. /etc/rc.status

#
# This service is run right after booting. So all targets activated
# during mkinitrd run should not be removed when the open-iscsi
# service is stopped.
#
iscsi_load_iscsiuio()
{
    TRANSPORT=`$ISCSIADM -m session 2> /dev/null | grep "bnx2i"`
    if [ "$TRANSPORT" ]; then
        echo -n "Launch iscsiuiio "
        startproc $ISCSIUIO
    fi
}
```



```
iscsi_mark_root_nodes()
{
    $ISCSIADM -m session 2> /dev/null | while read t num i target ; do
        ip=${i%:*}
        STARTUP=`$ISCSIADM -m node -p $ip -T $target 2> /dev/null | grep "node.conn\[0\].startup" | cut
-d' ' -f3`
        if [ "$STARTUP" -a "$STARTUP" != "onboot" ] ; then
            $ISCSIADM -m node -p $ip -T $target -o update -n node.conn[0].startup -v onboot
        fi
    done
}
# Reset status of this service
rc_reset

# We only need to start this for root on iSCSI
if ! grep -q iscsi_tcp /proc/modules ; then
    if ! grep -q bnx2i /proc/modules ; then
        rc_failed 6
        rc_exit
    fi
fi

case "$1" in
    start)
        echo -n "Starting iSCSI initiator for the root device: "
        iscsi_load_iscsiuio
        startproc $DAEMON $ARGS
        rc_status -v
        iscsi_mark_root_nodes
        ;;
    stop|restart|reload)
        rc_failed 0
        ;;
    status)
        echo -n "Checking for iSCSI initiator service: "
        if checkproc $DAEMON ; then
            rc_status -v
        else
            rc_failed 3
            rc_status -v
        fi
        ;;
    *)
        echo "Usage: $0 {start|stop|status|restart|reload}"
        exit 1
        ;;
esac
rc_exit
```

Broadcom 드라이버를 Windows 이미지 파일로 삽입(적용)

Broadcom 드라이버를 Windows 이미지 파일에 삽입하려면, 해당 Windows Server 버전 (2008R2, 2008SP2, 2012 또는 2012R2)에 올바른 Broadcom 드라이버 패키지를 확보해야 합니다. 패키지 이름은 b57nd60a입니다.



참고 : 개별 Windows NetXtreme 드라이버를 추출하는 방법에 대한 지침은 특정 드라이버 설치 프로그램의 *silent.txt* 파일을 참조하십시오.

그런 다음, 드라이버 패키지를 작업 디렉터리에 넣습니다. 예를 들어 드라이버 패키지를 다음 디렉터리로 복사합니다.

- C:\Temp\b57nd60a

마지막으로 이들 드라이버를 Windows 이미지(WIM) 파일에 삽입한 후, 업데이트된 이미지에서 해당 Windows Server 버전을 설치합니다.

세부 단계는 다음과 같습니다.



참고: 이 절차에서 사용된 파일 및 폴더 이름은 예시용입니다. 적용 프로젝트에 따라 파일 및 폴더 이름을 지정할 수 있습니다.

1. Windows Server 2008 R2 및 SP2의 경우 Windows AIK(Automated Installation Kit)를 설치합니다.
-또는-
Windows Server 2012 및 2012 R2의 경우 Windows ADK(Assessment and Deployment Kit)를 설치합니다.
2. 다음 명령을 사용하여 임시 디렉터리를 생성하고 이를 이후의 모든 단계를 위한 현재 디렉터리로 설정합니다.

```
md C:\Temp\x
cd /d C:\Temp\x
```
3. 다음 명령을 사용하여 두 개의 하위 디렉터리를 생성합니다.

```
md src
md mnt
```
4. 다음 명령을 사용하여 원본 DVD를 src 하위 디렉터리로 복사합니다.

```
xcopy N:\ .\src /e /c /i /f /h /k /y /q
```


이 예에서는 설치 DVD가 N: 드라이브에 있습니다.
5. 배포 및 이미징 도구 명령 프롬프트를 관리자 모드에서 엽니다. 그런 다음 c:\Temp\x를 현재 디렉터리로 설정합니다.
이 명령 프롬프트 창은 이후의 모든 단계에서 사용하게 됩니다.
6. 다음 명령을 입력합니다.

```
attrib -r .\src\sources\boot.wim
attrib -r .\src\sources\install.wim
```
7. 다음 명령을 입력하여 boot.wim 이미지를 마운트합니다.

```
dism /mount-wim /wimfile:.\src\sources\boot.wim /index:2 /mountdir:.\mnt
```


인덱스 값은 항상 "2"를 사용해야 합니다.
8. 다음 명령을 입력하여 현재 마운트된 이미지에 다음 드라이버를 추가합니다.

```
dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
```
9. 다음 명령을 입력하여 boot.wim 이미지를 언마운트합니다.

```
dism /unmount-wim /mountdir:.\mnt /commit
```
10. 다음 명령을 입력하여 install.wim 이미지에서 원하는 SKU의 인덱스를 결정합니다.

```
dism /get-wiminfo /wimfile:.\src\sources\install.wim
```


예를 들어, Windows Server 2012에서 인덱스 2는 "Windows Server 2012 SERVERSTANDARD"로 식별됩니다.
11. 다음 명령을 실행하여 install.wim 이미지를 마운트합니다.

```
dism /mount-wim /wimfile:.\src\sources\install.wim /index:X /mountdir:.\mnt
```

X는 10단계에서 구한 인덱스 값의 자리 표시자입니다.

- 다음 명령을 입력하여 현재 마운트된 이미지에 드라이버를 추가합니다.

```
dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
```

- 다음 명령을 실행하여 install.wim 이미지를 언마운트합니다.

```
dism /unmount-wim /mountdir:.\mnt /commit
```

- 다음 명령을 입력하여 .iso 파일을 생성합니다.

```
oscdimg -e -h -m -n -lslipstream -bootdata:2#p0,e,b"c:\Program Files\Windows  
AIK\Tools\PETools\amd64\boot\etfsboot.com"#pEF,e,b"c:\Program Files\Windows  
AIK\Tools\PETools\amd64\boot\efisys.bin" c:\temp\x\src c:\temp\win20xxMOD.iso
```

플랫폼은 설치하려는 운영 체제(예: amd64 또는 x86)의 아키텍처에 대한 자리 표시자입니다. 또한, 파일 이름의 xx는 Windows Server OS 버전(2012, 2008R2, 2008SP2)의 자리 표시자입니다.

- DVD 버닝 응용 프로그램을 사용하여 생성한 .iso 파일을 DVD로 굽습니다.
- 15단계에서 만든 DVD를 사용하여 해당 Windows Server 버전을 설치합니다.

부팅

iSCSI 부트에 대해 시스템을 준비하고 iSCSI 대상에 운영 체제가 있는 경우 마지막 단계는 실제 부팅을 수행하는 것입니다. 시스템은 네트워크를 통해 Windows 또는 Linux로 부팅하며 로컬 디스크 드라이브처럼 작동합니다.

- 서버를 다시 부팅합니다.
- CTRL+S**를 선택합니다.
- 주 메뉴에서 **일반 매개 변수**를 선택하고 **iSCSI 대상으로 부팅 옵션을 사용**으로 구성합니다.

CHAP 인증이 필요한 경우, 성공적으로 부팅했는지 판단한 후 CHAP 인증을 활성화합니다([CHAP 인증 활성화](#) 참조).

기타 iSCSI 부트 고려 사항

iSCSI 부트에 대해 시스템을 구성할 때 고려해야 할 여러 다른 요소가 있습니다.

Windows 환경에서 Speed & Duplex 설정 변경

NDIS 경로를 통한 부팅은 지원됩니다. NDIS 경로를 통해 iSCSI 부트용 BACS 관리 유틸리티를 사용하여 Speed & Duplex 설정을 변경할 수 있습니다.

Locally Administered Address

BACS 구성 탭의 고급 섹션에 있는 Locally Administered Address 속성을 통해 할당된 사용자 정의 MAC 주소는 iSCSI 부트 사용 장치에서 지원되지 않습니다.

가상 LAN(VLAN)

Microsoft iSCSI 소프트웨어 초기자가 포함된 iSCSI 부트에서는 가상 LAN(VLAN) 태그가 지원되지 않습니다.

iSCSI 부트 문제 해결

다음 문제 해결 팁은 iSCSI 부트에 유용합니다.

문제: IPv6 연결을 사용하여 Windows Server 2008을 설치하려 할 경우 iSCSI 대상은 설치 대상으로 인식되지 않습니다.

해결 방법: 이것은 알려진 타사 제품 문제입니다. Microsoft Knowledge Base KB 971443, <http://support.microsoft.com/kb/971443>을 참조하십시오.

문제: iSCSI 구성 유틸리티가 실행되지 않습니다.

해결 방법: NVRAM에 iSCSI 부트 펌웨어가 설치되어 있는지 확인합니다.

문제: iSCSI 부트 LUN을 255로 구성한 후 iSCSI 부트를 수행할 때 파란 시스템 화면이 나타납니다.

해결 방법: Broadcom의 iSCSI 솔루션이 0에서 255 사이의 LUN 범위를 지원하지만 Microsoft 소프트웨어 초기자는 255의 LUN을 지원하지 않습니다. LUN을 0에서 254 사이의 값으로 구성합니다.

문제: 비기본 하드웨어 ID가 있을 경우 기본 드라이버를 업데이트할 수 없습니다.

해결 방법: 설치 미디어에 지원되는 드라이버를 삽입하여 사용자 정의 통합 설치 DVD 이미지를 생성합니다.

iSCSI Crash Dump

Broadcom iSCSI Crash Dump 유틸리티를 사용할 경우 설치 절차에 따라 iSCSI Crash Dump 드라이버를 설치하는 것이 중요합니다. 자세한 내용은 [설치 프로그램 사용](#)을 참조하십시오.

10 절: Linux 드라이버 및 관리 응용 프로그램 설치

- 패키지
- TG3 드라이버 소프트웨어 설치
- 네트워크 설치
- TG3 드라이버 언로드/제거
- 드라이버 메시지
- 채널 본딩을 사용하여 팀 구성
- Linux 관리 응용 프로그램 설치

패키지

Linux TG3 드라이버는 다음과 같은 패키지 형식(파일 이름)으로 릴리스됩니다.

- 소스 RPM(`tg3-version.3dkms.src.rpm`)
- 소스 RPM(`tg3-version.3dkms.noarch.rpm`)
- 보완(`tg3_sup-version.tar.gz`)
- 압축된 tar(`tg3-version.tar.gz`)

RPM 및 TAR 소스 패키지에 드라이버 구축에 필요한 동일한 소스 파일이 들어있습니다. TAR 파일에는 네트워크 설치에 필요한 디스크 이미지와 패치 같은 추가 유틸리티가 있습니다.

TG3 드라이버 소프트웨어 설치

- 소스 RPM 패키지 설치
- 소스 TAR 파일로 드라이버 구축

소스 RPM 패키지 설치

필수 요소:

- Linux 커널 소스
- C 컴파일러

절차:

1. 소스 RPM 패키지를 설치합니다.
`rpm -ivh tg3-version.src.rpm`
2. RPM 경로로 디렉토리를 변경하고 커널의 이진 드라이버를 구축합니다(Linux 배포판이 다를 경우 RPM 경로도 다름).
`cd /usr/src/redhat,OpenLinux,turbo,packages,rpm ...`
`rpm -bb SPECS/tg3.spec or rpmbuild -bb SPECS/tg3.spec`
`rpmbuild -bb SPECS/tg3.spec (for RPM version 4.x.x)`



참고: 소스 RPM 패키지 설치를 시도하는 중에 다음 메시지가 표시될 수 있습니다.

```
error: cannot create %sourcedir /usr/src/redhat/SOURCE
```

가장 일반적인 원인은 rpm-build 패키지가 설치되어 있지 않기 때문입니다. Linux 설치 미디어에서 rpm-build 패키지를 찾은 후 다음 명령을 입력하여 이를 설치합니다.

```
rpm -ivh rpm-build-version.i386.rpm
```

소스 RPM 설치를 완료합니다.

3. 새로 구축한 패키지를 설치합니다(드라이버 및 man 페이지).
`rpm -ivh RPMS/i386/tg3-version.i386.rpm`

커널에 따라 드라이버는 다음 경로에 설치됩니다.

2.6.x 커널 :

```
/lib/modules/kernel_version/kernel/drivers/net/tg3.ko
```

4. 드라이버를 로드합니다.
`modprobe tg3`

네트워크 프로토콜과 주소를 구성하려면 Linux 배포판별 설명서를 참조하십시오.

소스 TAR 파일로 드라이버 구축

1. 디렉터리(*tg3-version*)를 생성하고 해당 디렉터리에 TAR 파일 압축을 풉니다.
`tar xvzf tg3-version.tgz`
2. 드라이버 *tg3.o*를 실행 중인 커널의 로드 가능한 모듈로 구축합니다.
`CD tg3-version`
`make clean`
`make; make install`
3. 드라이버를 로드하고 테스트합니다.
`rmmod tg3`
`modprobe tg3`
 이 명령이 올바르게 실행된 경우 반환되는 메시지가 없습니다.



참고: 설치된 드라이버 위치는 위의 RPM 지침을 참조하십시오.

4. 네트워크 프로토콜과 주소를 구성하려면 해당 운영 체제와 함께 제공된 설명서를 참조합니다.

네트워크 설치

NFS, FTP 또는 HTTP(네트워크 부트 디스크나 PXE 사용)를 통해 네트워크를 설치하는 경우 Linux 운영 체제 배포판의 일부인 *tg3* 드라이버를 사용하십시오.

TG3 드라이버 언로드/제거

- [RPM 설치에서 드라이버 언로드/제거](#)
- [TAR 설치에서 드라이버 제거](#)

RPM 설치에서 드라이버 언로드/제거

드라이버를 언로드하려면 *ifconfig*를 사용하여 드라이버로 열린 모든 *ethX* 인터페이스를 비활성화한 후 다음을 입력합니다.

```
rmmod tg3
```

*rpm*으로 드라이버를 설치한 경우 다음을 수행하여 제거합니다.

```
rpm -e tg3-<version>
```

TAR 설치에서 드라이버 제거

Tar 파일의 *make install*로 드라이버를 설치한 경우 운영 체제에서 드라이버 파일 *tg3.o*를 수동으로 제거해야 합니다. 설치된 드라이버 위치는 [소스 RPM 패키지 설치](#)를 참조하십시오.

tg3 드라이버와 관련된 인터페이스 구성이 있는 경우 **ifconfig ethx down**과 **rmod tg3**를 차례로 입력하여 먼저 인터페이스를 비활성화합니다.

드라이버 메시지

다음은 파일 `/var/log/messages` 파일에 기록되는 가장 일반적인 샘플 메시지입니다. **dmesg -n level**을 사용하면 콘솔에 표시되는 메시지 단계를 조절할 수 있습니다. 대부분의 시스템은 기본적으로 레벨 6으로 설정됩니다.

드라이버 로그인

```
tg3.c:version (date)
```

NIC 감지

```
eth#: Tigon3 [partno (BCM95xxx) rev 4202 PHY (57xx) (PCI Express) 10/100/1000BaseT Ethernet
:00:xx:xx:xx:xx:xx
eth#: RXcsyms [1] LinkChg REG [0] MIirq [0] ASF [0] Split [0] Wirespeed [1]TSOcap [1]
eth#: dma_rwctrl [76180000]
ACPI : PCI interrupt 0000:02:02.0 [A] -> GSI 26 (level,low) -> IRQ 233
```

Flow Control

```
tg3: eth#: Flow control is configured for TX and for RX.
```

링크 연결 및 속도 표시

```
tg3: eth#: Link is up at 1000 Mbps, full duplex.
```

링크 해제 표시

```
tg3: eth#: Link is down.
```

채널 본딩을 사용하여 팀 구성

TG3 드라이버를 설치한 경우 본딩 커널 모듈과 채널 본딩 인터페이스를 사용하여 여러 어댑터를 팀으로 구성할 수 있습니다. Linux 채널 본딩에 대한 자세한 내용은 Linux 설명서를 참조하십시오.

Linux 관리 응용 프로그램 설치

- [개요](#)
- [Linux 서버에 WS-MAN 또는 CIM-XML 설치](#)
- [Linux 클라이언트에 WS-MAN 또는 CIM-XML 설치](#)
- [Broadcom Advanced Control Suite 응용 프로그램 설치](#)

개요

Broadcom Advanced Control Suite 버전 4(BACS4)는 NetXtreme I 어댑터 제품군을 구성하기 위한 관리 응용 프로그램입니다. BACS4 소프트웨어는 Windows 및 Linux 서버/클라이언트 운영 체제에서 작동합니다.

이 챕터에서는 Linux 시스템에 BACS4 관리 응용 프로그램을 설치하는 방법을 설명합니다. Windows 시스템의 경우, BACS4를 포함하여 Windows 드라이버 및 관리 응용 프로그램을 모두 설치하는 설치 프로그램이 제공됩니다(지침은 [Windows 드라이버 및 관리 응용 프로그램 설치](#) 참조).

BACS4 유틸리티는 공급자 구성 요소와 클라이언트 소프트웨어라는 두 가지 주요 부분으로 이루어져 있습니다. 공급자는 하나 이상의 NIC가 포함된 서버, 즉 "관리 호스트"에 설치됩니다. 공급자는 NIC에 대한 정보를 수집하고 클라이언트 소프트웨어가 설치되어 있는 관리 PC에서 해당 정보를 검색할 수 있게 합니다. 클라이언트 소프트웨어를 사용하면 공급자로부터 제공되는 정보를 볼 수 있고 NIC를 구성할 수 있습니다. BACS 클라이언트 소프트웨어에는 GUI(그래픽 사용자 인터페이스)와 CLI(명령줄 인터페이스)가 포함되어 있습니다.

통신 프로토콜

공급자와 클라이언트 소프트웨어 사이에 통신이 이루어지기 위해서는 통신 프로토콜이 있어야 합니다. 이러한 통신 프로토콜은 DMTF(Distributed Management Task Force) 의 WBEM(Web-Based Enterprise Management) 및 CIM(Common Information Model) 표준을 독점 또는 오픈 소스로 구현한 것입니다. 네트워크 관리자는 네트워크에서 사용되는 표준에 따라 최상의 옵션을 선택할 수 있습니다.

다음 표에는 관리 호스트 및 클라이언트에 설치된 운영 체제를 기준으로 사용 가능한 옵션이 나와 있습니다.

<i>클라이언트 운영 체제:</i>	<i>관리 호스트 운영 체제:</i>	<i>BACS가 사용 가능한 통신 프로토콜:</i>
Windows	Windows	WMI WS-MAN(WinRM)
Windows	Linux	CIM-XML(OpenPegasus) WS-MAN(OpenPegasus)
Linux	Windows	WS-MAN(WinRM)
Linux	Linux	CIM-XML(OpenPegasus) WS-MAN(OpenPegasus)

- WMI = Windows Management Instrumentation.
- WS-MAN = Web Service-Management. WinRM은 Windows 기반 구현이고, OpenPegasus는 Linux에서 작동하는 오픈 소스 구현입니다.
- CIM-XML = OpenPegasus의 XML 기반 버전.

네트워크에 Windows 및 Linux 서버에 액세스하는 Windows 및 Linux 클라이언트가 혼합되어 있는 경우에는 WS-MAN이 적합한 선택입니다. Linux가 서버에 설치된 유일한 OS일 경우 CIM-XML이 한 옵션입니다. 네트워크가 Windows 서버 및 클라이언트로만 구성된 경우 WMI가 한 옵션입니다. WMI는 매우 간단히 구성할 수 있지만 Windows OS에서만 지원됩니다. (Windows 프로토콜 설치 및 구성에 대한 지침은 [Windows 드라이버 및 관리 응용 프로그램 설치](#)를 참조하십시오.)

BACS 설치에는 관리 스테이션의 관리 호스트 및 클라이언트 소프트웨어에 공급자 구성 요소를 설치하는 작업이 포함됩니다. 설치 프로세스는 클라이언트 및 관리 호스트에 설치된 운영 체제의 조합과 선택된 통신 프로토콜에 따라 달라집니다.

Linux 서버에 WS-MAN 또는 CIM-XML 설치

1단계: OpenPegasus 설치

Red Hat Linux OS에서는 다음의 두 가지 설치 옵션을 사용할 수 있습니다.

- [Inbox RPM](#)으로부터(Red Hat만 해당)
- [소스로부터](#)(Red Hat 및 SuSE)

SUSE Linux Enterprise Server 11(SLES11) OS의 경우, 소스 RPM을 사용해야 합니다.



참고 : Inbox RPM은 WS-MAN 통신 프로토콜을 지원하지 않습니다. WS-MAN을 사용하려면 소스로부터 OpenPegasus를 설치해야 합니다.

[Inbox RPM](#)으로부터(Red Hat만 해당)

Red Hat Linux에서 Inbox OpenPegasus RPM은 `tog-pegasus-<version>.<arch>.rpm`으로 제공됩니다.

1. 다음 명령을 사용하여 `tog-pegasus`를 설치합니다.
`rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. 다음 명령을 사용하여 `Pegasus`를 시작합니다.
`/etc/init.d/tog-pegasus start`



참고: SuSE Linux에서는 Inbox OpenPegasus RPM을 사용할 수 없습니다. OpenPegasus는 다음 절차에서 설명된 대로 소스로부터 설치해야 합니다.

Inbox Pegasus에서 HTTP는 기본적으로 비활성화되어 있습니다. Inbox OpenPegasus를 설치한 후 더 이상 구성이 필요하지 않으면 [4단계: Broadcom CMPI 공급자 설치](#)의 지침을 따릅니다. HTTP를 활성화하려면 [HTTP 활성화](#)를 참조하십시오.

[소스로부터](#)(Red Hat 및 SuSE)

OpenPegasus 소스는 www.openpegasus.org에서 다운로드할 수 있습니다.



참고 : 설치되지 않은 경우 `openssl` 및 `libopenssl-devel rpm`을 다운로드하여 설치합니다. 이 단계는 옵션이며 HTTPS를 사용하여 클라이언트를 관리 호스트로 연결하려는 경우에만 필요합니다.

환경 변수 설정

OpenPegasus 구축을 위한 환경 변수를 다음과 같이 설정합니다.

환경 변수	설명
PEGASUS_ROOT	Pegasus 소스 트리의 위치
PEGASUS_HOME	구축된 실행 파일, 리포지토리의 위치. 예 : \$PEGASUS_HOME/bin, PEGASUS_HOME/lib, \$PEGASUS_HOME/repository 및 \$PEGASUS_HOME/mof 하위 디렉터리.
PATH	\$PATH:\$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Linux 32 비트 시스템 : "LINUX_IX86_GNU" Linux 64 비트 시스템 : "LINUX_X86_64_GNU"
PEGASUS_HAS_SSL	옵션. HTTPS 지원을 "true" 로 설정합니다.
PEGASUS_ENABLE_PROTOCOL_WSMAN	옵션. WSMAN 프로토콜 지원을 "true" 로 설정합니다.

추가 설정

\$PEGASUS_HOME 변수는 셸 환경에서 설정해야 하고, \$PEGASUS_HOME/bin은 \$PATH 환경에 추가해야 합니다.

예

- export PEGASUS_PLATFORM="LINUX_X86_64_GNU"
- export PEGASUS_CIM_SCHEMA="CIM222"
- export PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER=true
- export PEGASUS_ROOT="/share/pegasus-2.10-src"
- export PEGASUS_HOME="/pegasus"
- export PATH=\$PATH:\$PEGASUS_HOME/bin

SSL 지원의 경우, 다음의 환경 변수를 추가합니다.

- export PEGASUS_HAS_SSL=true

WS-MAN 지원의 경우, 다음의 환경 변수를 추가합니다.

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

OpenPegasus의 CIM-XML 및 WSMAN은 HTTP 또는 HTTPS에 동일한 포트를 사용합니다. HTTP 및 HTTPS용 기본 포트 번호는 각각 5989와 5989입니다.



참고: 이러한 내보내기를 `.bash_profile`의 끝에 추가할 수 있습니다. 이 파일은 `/root` 디렉터리에 있습니다.

- 사용자가 PuTTY를 사용하여 로그인하면 환경 변수가 설정됩니다.
- Linux 시스템 자체에서, 환경 변수가 설정되지 않은 각 단말에 대해 다음 명령을 실행합니다.
`source /root/.bash_profile`
- 로그아웃하고 다시 로그인하면 환경 변수가 설정됩니다.

OpenPegasus 구축 및 설치

`$PEGASUS_ROOT`(Pegasus 소스 루트 디렉터리의 위치)에서 다음 명령을 실행합니다.

```
make clean
make
make repository
```



참고: OpenPegasus가 소스로부터 구축될 때마다 모든 구성이 기본값으로 재설정됩니다. OpenPegasus를 재구축하는 경우, **3단계: 서버에서 OpenPegasus 구성**에서 언급된 대로 구성을 다시 실행해야 합니다.

2단계: 서버에서 CIM 서버 시작

`cimserver` 명령을 사용하여 CIM 서버를 시작합니다. CIM 서버를 중지하려면 `cimserver -s` 명령을 사용합니다.

OpenPegasus가 제대로 설치되었는지 확인하려면 다음 명령을 입력합니다.

```
cimcli ei -n root/PG_Interop PG_ProviderModule
```



참고: OpenPegasus가 소스로부터 컴파일된 경우, CIM 서버를 시작할 때 `PEGASUS_HOME`을 정의해야 합니다. 그렇지 않을 경우 CIM 서버가 리포지토리를 올바르게 로드하지 않습니다. `“.bash_profile”` 파일에서 `PEGASUS_HOME` 설정을 고려하십시오.

3단계: 서버에서 OpenPegasus 구성

`cimconfig` 명령을 사용하여 다음 표에 표시된 대로 OpenPegasus를 구성합니다.

명령	설명
<code>cimconfig -l</code>	유효한 속성 이름을 모두 나열합니다.
<code>cimconfig -l -c</code>	유효한 속성 이름 및 해당 값을 모두 나열합니다.
<code>cimconfig -g <property name></code>	특정 속성을 조회합니다.
<code>cimconfig -s <property name>=<value> -p</code>	특정 속성을 설정합니다.
<code>cimconfig --help</code>	명령에 대한 자세한 정보를 봅니다.

CIM 서버는 `cimconfig`를 실행하기 전에 시작해야 하며, 구성 변경을 적용하려면 다시 시작해야 합니다.

인증 활성화

다음의 OpenPegasus 속성이 이 단원에서 설명된 대로 설정되어야 합니다. 그렇지 않을 경우 Broadcom CIM 공급자가 올바르게 작동하지 않습니다. BACS를 시작하고 공급자에 연결하기 전에 다음이 설정되었는지 확인합니다.

아직 시작되지 않은 경우 CIM 서버를 시작합니다. 그리고 다음을 설정합니다.

- `cimconfig -s enableAuthentication=true -p`
- `cimconfig -s enableNamespaceAuthorization=false -p`
- `cimconfig -s httpAuthType=Basic -p`
- `cimconfig -s passwordFilePath=cimserver.passwd -p`
- `cimconfig -s forceProviderProcesses=false -p`

루트 사용자가 원격으로 연결하기를 원할 경우:

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

권한이 있는 사용자 구성: Linux 시스템 사용자를 사용하여 OpenPegasus를 인증합니다. BACS를 통해 연결하려면 `cimuser`를 사용하여 OpenPegasus에 시스템 사용자를 추가해야 합니다.

- `cimuser -a -u <username> -w <password>`

예: `cimuser -a -u root -w linux1`

HTTP 활성화

1. CIM 서버가 시작되지 않았으면 시작합니다.
2. 다음 명령을 사용하여 HTTP 포트를 설정합니다(옵션).
`cimconfig -s httpPort=5988 -p`
이 속성은 Inbox OpenPegasus에 사용할 수 없습니다.
3. 다음 명령을 사용하여 HTTP 연결을 활성화합니다.
`cimconfig -s enableHttpConnection=true -p`
4. 새 구성을 적용하려면 각각 `cimserver -s` 및 `cimserver` 명령을 사용하여 CIM 서버를 중지했다 다시 시작합니다.

HTTPS 활성화

1. CIM 서버가 시작되지 않았으면 시작합니다.
2. 다음 명령을 사용하여 HTTPS 포트를 설정합니다(옵션).
`cimconfig -s httpsPort=5989 -p`
이 속성은 Inbox OpenPegasus에 사용할 수 없습니다.
3. 다음 명령을 사용하여 HTTPS 연결을 활성화합니다.
`cimconfig -s enableHttpsConnection=true -p`
4. 새 구성을 적용하려면 각각 `cimserver -s` 및 `cimserver` 명령을 사용하여 CIM 서버를 중지했다 다시 시작합니다.

4단계: Broadcom CMPI 공급자 설치

CMPI 공급자를 설치하기 전에 OpenPegasus가 설치되어 있는지 확인합니다.

설치

다음 명령을 입력하여 Broadcom CMPI 공급자를 설치합니다.

```
% rpm -i BRCM_CMPIProvider-{version}.{arch}.rpm
```

설치 제거

다음 명령을 입력하여 Broadcom CMPI 공급자를 설치 제거합니다.

```
% rpm -e BRCM_CMPIProvider
```

5단계: 필요 시 Linux 방화벽 구성 수행

다음 절차를 따라 방화벽에서 해당 포트를 엽니다.

Red Hat

1. 시스템을 클릭하고 **관리**를 선택한 후 **방화벽**을 선택합니다.
2. 기타 포트를 선택합니다.
3. 포트 및 프로토콜 대화 상자에서 **사용자 정의**를 선택합니다.
4. **포트/포트 범위** 필드에서 포트 번호를 추가합니다.
5. **프로토콜** 필드에서 TCP 또는 UDP 등으로 프로토콜을 추가합니다.
6. 방화벽 규칙을 적용하려면 **적용**을 클릭합니다.

예:

- HTTP를 통한 CIM-XML의 경우, 포트 번호가 5988이고 프로토콜이 TCP입니다.
- HTTPS를 통한 CIM-XML의 경우, 포트 번호가 5989이고 프로토콜이 TCP입니다.

SuSE

1. **계산**을 클릭한 다음 **YaST**를 클릭합니다.
2. 왼쪽 창에서 **보안 및 사용자**를 선택합니다.
3. 오른쪽 창에서 **방화벽**을 두 번 클릭합니다.
4. 왼쪽 창에서 **사용자 정의 규칙**을 선택합니다.
5. 오른쪽 창에서 **추가**를 클릭합니다.
6. 다음 값을 입력합니다.
 - **소스 네트워크**: 0/0(모두를 의미)
 - **프로토콜**: TCP(또는 해당 프로토콜)
 - **대상 포트**: <포트 번호> 또는 <포트 번호 범위>
 - **소스 포트**: 빈 상태로 둡니다.
7. 방화벽 규칙을 적용하려면 **다음**을 클릭한 다음 **마침**을 클릭합니다.

예:

CIM-XML의 경우, 다음 값을 사용합니다.

- 소스 네트워크: 0/0(모두를 의미)
- 프로토콜: TCP
- 대상 포트: 5988:5989
- 소스 포트: 빈 상태로 둡니다.

6단계: **BACS** 및 관련 관리 응용 프로그램 설치

[Broadcom Advanced Control Suite 응용 프로그램 설치](#)를 참조하십시오.

Linux 클라이언트에 WS-MAN 또는 CIM-XML 설치

HTTP를 사용하려면, BACS 관리 응용 프로그램을 설치하는 것 이외에 Linux 클라이언트 시스템에 특별한 소프트웨어 구성 요소가 필요하지 않습니다. 단, WS-MAN 설치의 경우 HTTPS 프로토콜을 BACS에서 사용하도록 구성할 수 있습니다(옵션).

Linux 클라이언트에서 HTTPS 구성

HTTP 대신 HTTPS를 사용하려면 다음 단계를 따릅니다(WS-MAN만 해당).

Windows/Linux 서버용 자체 서명된 인증서 생성

Linux 또는 Windows에서 Openssl을 사용하여 다음과 같이 자체 서명된 인증서를 생성할 수 있습니다.



참고 : 다음 링크에서 openssl 을 다운로드하여 설치할 수 있습니다 . <http://gnuwin32.sourceforge.net/packages/openssl.htm>.

1. 다음 명령을 입력하여 개인 키를 생성합니다.
`openssl genrsa -des3 -out server.key 1024`

2. 암호 문구를 입력하라는 메시지가 나타납니다. 이 암호 문구를 기억하고 있어야 합니다.

3. 다음 단계에 따라 CSR(인증서 서명 요청)을 생성합니다.

CSR 을 생성하는 과정에서 여러 가지 정보를 입력해야 합니다 . " 일반 이름 " 을 입력하라는 메시지가 나타나면 Windows Server 호스트 이름 또는 IP 주소를 입력합니다 .

다음 명령을 입력합니다 (여기에는 응답 샘플이 함께 나와 있습니다).

```
openssl req -new -key server.key -out server.csr
```

명령이 작동하지 않을 경우 다음을 시도합니다 .

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

openssl.cnf 파일은 openssl 이 있는 동일한 디렉터리에 저장해야 합니다 . Openssl.cnf 는 C:\Program Files(x86)\GnuWin32\share 에 있습니다 .

다음과 같은 정보가 필요합니다 .

- 국가 이름 (두 자로 된 코드) []: **US**
- 구 / 군 / 시 또는 시 / 도 이름 (전체 이름) []: **California**
- 지역 이름 (예 : 시) []: **Irvine**
- 조직 이름 (예 : 회사) []: **Broadcom Corporation**
- 조직 구성 단위 이름 (예 : 부서) []: **Engineering**
- 일반 이름 (예 : 사용자 이름) []: Windows 서버의 호스트 이름 또는 IP 주소를 입력합니다 . IPv6 의 경우 대괄호 [] 를 포함하여 [xyxy:xxx:...:xxx] 의 형식으로 공통 이름을 입력합니다 .
- (선택 사항) 이메일 주소 []:

인증서 요청과 함께 전송할 다음과 같은 추가 특성을 입력합니다 .

- 챌린지 암호 []: **linux1**
- 회사 이름 (옵션) []:

4. 키에서 암호 문구를 제거합니다.

다음 명령을 입력합니다 .

```
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
```


5. 자체 서명된 인증서 생성:

365 일 사용할 수 있는 자체 서명된 인증서를 생성하려면 다음 명령을 입력합니다 .

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

다음과 같은 출력이 표시됩니다 .

```
Signature ok
subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-LAB3/
emailAddress=
Getting Private key
```

6. 다음 명령을 입력하여 자체 서명된 인증서가 제대로 생성되었는지 확인합니다.

```
openssl verify server.crt
```

다음과 같은 출력이 표시됩니다 .

```
server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
LAB3/emailAddress=
error 18 at 0 depth lookup:self signed certificate
OK
```

"error 18 at 0 depth lookup:self signed certificate" 오류 메시지는 무시해도 됩니다 . 이 오류는 인증서가 자체 서명된 것임을 의미합니다 .

7. 다음과 같이 인증서를 "crt"에서 "pkcs12" 형식으로 변환합니다.

Windows 서버의 경우 인증서는 pkcs12 형식이어야 합니다 . 다음 명령을 입력합니다 .

```
openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
```

다음과 같은 정보를 입력하라는 메시지가 나타납니다 .

```
Enter Export Password:
Verifying - Enter Export Password:
```

암호를 입력합니다 . 입력한 암호는 반드시 기억하고 있어야 합니다 . Windows 서버와 클라이언트에서 인증서를 가져올 때 암호가 필요합니다 .

8. 인증서 파일 server.crt의 복사본을 만든 다음, BACS를 설치할 서버로 인증서 파일을 가져올 수 있도록 해당 서버에 복사본을 배치해 둡니다. BACS가 실행되는 서버에 연결하는 데 Windows 또는 Linux 클라이언트를 사용할 계획이라면 클라이언트 시스템에도 인증서를 전송(복사하여 붙여 넣기)해야 합니다.

Linux 에서 인증서 확장자는 ".pem" 이어야 합니다 . ".crt" 및 ".pem" 확장자는 동일하므로 .crt 를 .pem 으로 변환하기 위해 openssl 명령을 사용할 필요가 없습니다 . 파일을 그대로 복사할 수 있습니다 .



참고: IPv4 주소, IPv6 주소 및 호스트 이름에 각각 별개의 인증서를 생성해야 합니다.

Linux 클라이언트에서 자체 서명된 인증서 가져오기

Linux 배포판에서 다음의 인증서 디렉터리를 메모합니다.

- 모든 SuSE 버전에서 인증서 디렉터리는 /etc/ssl/certs입니다.
- Red Hat에서는 인증서 디렉터리가 각 버전마다 다를 수 있습니다. 일부 버전은 /etc/ssl/certs 또는 /etc/pki/tls/certs입니다. 다른 버전은 인증서 디렉터리를 찾으십시오.

Windows/Linux 서버용 자체 서명된 인증서 생성에서 생성한 hostname.pem을 Linux 클라이언트의 인증서 디렉터리로 복사합니다. 예를 들어, 인증서 디렉터리가 /etc/ssl/certs일 경우 hostname.pem을 /etc/ssl/certs로 복사합니다.

1. 디렉터리를 /etc/ssl/certs로 변경합니다.
2. 다음 명령을 실행하여 해시 값을 생성합니다.


```
openssl x509 -noout -hash -in hostname.pem
```

다음과 같은 값이 반환됩니다.

```
100940db
```

3. 다음 명령을 실행하여 해시 값에 대한 기호 링크를 생성합니다.

```
ln -s hostname.pem 100940db.0
```

Linux 클라이언트에서 HTTPS/SSL 연결 테스트

다음 명령을 사용하여 인증서가 Linux에 올바르게 설치되었는지 테스트합니다.

```
# curl -v --capath /etc/ssl/certs https://Hostname or IPAddress:5986/wsman
```

이 테스트에 실패할 경우, 인증서가 올바르게 설치되지 않으며 수정 조치를 취하라는 오류 메시지가 나타납니다.

Broadcom Advanced Control Suite 응용 프로그램 설치

Broadcom Advanced Control Suite(BACS) 소프트웨어는 Linux RPM 패키지를 사용하여 Linux 시스템에 설치할 수 있습니다. 이 설치에는 BACS GUI와 CLI 클라이언트가 포함됩니다.

시작하기 전에:

- Broadcom 네트워크 어댑터가 올바르게 설치되어 있고 이 유틸리티로 관리할 시스템에 NIC의 장치 드라이버가 설치되어 있는지 확인합니다.
- 이 유틸리티로 관리할 시스템에 CIM 공급자가 올바르게 설치되어 있는지 확인합니다.
- Linux 호스트에서 iSCSI를 관리하기 위해, open-iscsi 및 sg 유틸리티가 Linux 호스트에 설치되어 있는지 확인합니다.

BACS 설치

1. 최신 BACS 관리 응용 프로그램 RPM 패키지를 다운로드합니다.
2. 다음 명령을 사용하여 RPM 패키지를 설치합니다.


```
% rpm -i BACS-{version}.{arch}.rpm
```

BACS 사용

- XWindow 에서 GUI 를 사용하려면 , BACS4 데스크탑 아이콘을 두 번 클릭하거나 시스템 도구 아래 작업 표시줄에서 BACS 프로그램에 액세스합니다.
- BACS CLI를 사용하려면, 릴리스 파일과 함께 제공된 BACSCLI_Readme.txt 파일을 참조하십시오.

BACS 제거

RPM 패키지를 설치 제거하려면 다음 명령을 사용합니다.

```
% rpm -e BACS
```

11 절: VMware 드라이버 소프트웨어

- 패키지
- 드라이버

패키지

VMware 드라이버는 다음 패키지 형식으로 릴리스됩니다.

표 19. VMware 드라이버 패키지

형식	드라이버
VMware VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

드라이버

드라이버 다운로드, 설치 및 업데이트

NetXtreme I GbE 네트워크 어댑터용 VMware ESX/ESXi 드라이버를 다운로드, 설치 또는 업데이트하려면 <http://www.vmware.com/support>를 참조하십시오.

드라이버 매개 변수

NetQueue

옵션 매개 변수 **force_netq**를 사용하여 수신 및 전송 네트워크 대기열의 수를 설정할 수 있습니다. NetQueue를 지원하는 BCM57XX 장치는 BCM5718, BCM5719, BCM5720, BCM5721, BCM5722입니다.

기본적으로 드라이버는 최적의 NetQueue 개수를 사용합니다. 대기열의 수를 명시적으로 강제 설정하려면, 다음 명령을 통해 포트당 NetQueue 개수를 설정합니다.

```
esxcfg-module -s force_netq=x,x,x... tg3
```

x에 허용된 값은 -1부터 15까지입니다.

- 1-15는 지정된 NIC에 대해 NetQueue 개수를 강제 설정합니다.
- 0은 NetQueue를 비활성화합니다.
- -1은 드라이버 NetQueue 기본값을 사용하도록 지정합니다.

“x” 항목의 수는 32까지 올라갈 수 있습니다. 즉, 지원되는 최대 NIC = 32입니다.

용례:

- ```
esxcfg-module -s force_netq=-1,0,1,2 tg3]
```
- tg3 NIC 0: NetQueue의 기본 수를 사용합니다.
  - tg3 NIC 1: NetQueue 기능을 비활성화합니다.
  - tg3 NIC 2: 1 NetQueue를 사용합니다.
  - tg3 NIC 3: 2 NetQueue를 사용합니다.

위의 NIC #은 vmnic<#>와 일치하지 않습니다. NIC 번호는 시스템 vmnic 검색 순서 번호입니다. NetQueue 개수가 시스템에 탑재된 CPU의 수와 일치하는 것이 가장 좋습니다.

## 드라이버 매개 변수

일부 옵션 매개 변수를 vmkload\_mod 명령의 명령행 인수로 제공할 수 있습니다. 이러한 매개 변수는 esxcfg-module 명령을 통해서도 설정할 수 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

## 드라이버 기본값

표 20. VMware 드라이버 기본값

| 매개 변수           | 기본값                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------|
| Speed           | 보급된 모든 속도 자동 협상                                                                                      |
| Flow Control    | 보급된 수신 및 전송 자동 협상                                                                                    |
| MTU             | 1500(범위: 46 ~ 9000)                                                                                  |
| 수신 링 크기         | 200(범위: 0-511). 일부 칩은 64로 고정되어 있습니다.                                                                 |
| 수신 대용량 링 크기     | 100(범위: 0-255). 모든 칩이 대용량 링을 지원하는 것은 아니며, 대용량 프레임 지원 하는 일부 칩은 대용량 링을 사용하지 않습니다.                      |
| 전송 링 크기         | 511(범위(MAX_SKB_FRAGS+1): -511). MAX_SKB_FRAGS는 커널 및 아키텍처별로 다릅니다. x86용 2.6 커널에서 MAX_SKB_FRAGS는 18입니다. |
| 합체 수신 마이크로초     | 20(범위: 0-1023)                                                                                       |
| 합체 수신 마이크로초 IRQ | 20(범위: 0-255)                                                                                        |
| 합체 수신 프레임       | 5(범위: 0-1023)                                                                                        |
| 합체 수신 프레임 IRQ   | 5(범위: 0-255)                                                                                         |
| 합체 전송 마이크로초     | 72(범위: 0-1023)                                                                                       |
| 합체 전송 마이크로초 IRQ | 20(범위: 0-255)                                                                                        |
| 합체 전송 프레임       | 53(범위: 0-1023)                                                                                       |
| 합체 전송 프레임 IRQ   | 5(범위: 0-255)                                                                                         |
| 합체 통계 마이크로초     | 1000000(약 1초). 일부 합체 매개 변수가 사용되지 않거나, 일부 칩에서 다른 기본값을 가집니다.                                           |
| MSI             | 사용(칩에서 지원하고 인터럽트 테스트를 통과한 경우).                                                                       |
| WoL             | 사용 안 함.                                                                                              |

## 드라이버 메시지

다음은 파일 `/var/log/messages`에 기록되는 가장 일반적인 샘플 메시지입니다. `dmesg -n <level>`을 사용하면 콘솔에 표시되는 메시지 단계를 조절할 수 있습니다. 대부분의 시스템은 기본적으로 레벨 6으로 설정됩니다. 모든 메시지를 보려면 수준을 보다 높게 설정하십시오.

### 드라이버 로그인

```
tg3.c:v3.118g (Jan 4, 2012)
```

### NIC 감지

```
vmnic0#: Tigon3 [partno (BCM95xxx) rev 4202 PHY (57xx) (PCI Express) 10/100/1000BaseT Ethernet
:00:xx:xx:xx:xx:xx
vmnic0#: RXcsums [1] LinkChg REG [0] MIirq [0] ASF [0] Split [0] Wirespeed [1]TSOcap [1]
vmnic0#: dma_rwctrl [76180000]
ACPI : PCI interrupt 0000:02:02.0 [A] -> GSI 26 (level,low) -> IRQ 233
```

### 링크 연결 및 속도 표시

```
tg3: vmnic0: Link is up at 1000 Mbps, full duplex.
tg3: vmnic0: Flow control is on for TX and on for RX.
```

### 링크 해제 표시

```
tg3: vmnic0: Link is down.
```

---

## 12 절: Windows 드라이버 및 관리 응용 프로그램 설치

- 드라이버 소프트웨어 설치
- 드라이버 소프트웨어 수정
- 드라이버 소프트웨어 복구 또는 다시 설치
- 장치 드라이버 제거
- 어댑터의 속성 확인 또는 변경
- 전원 관리 옵션 설정
- BACS4와 함께 사용할 통신 프로토콜 구성

## 드라이버 소프트웨어 설치



**참고:** 이 지침은 Broadcom NetXtreme 어댑터가 출고 시 설치되지 않은 경우를 전제로 한 것입니다. 출고 시 컨트롤러가 설치된 경우 드라이버 소프트웨어도 설치되어 있습니다.

새 하드웨어 장치(예: Broadcom NetXtreme 어댑터)를 설치하거나 기존 장치 드라이버를 제거한 후 Windows를 처음 시작하는 경우, 운영 체제가 새 하드웨어를 자동 감지하고 해당 장치의 드라이버 소프트웨어를 설치하라는 메시지를 표시합니다.

그래픽 대화형 설치 모드([설치 프로그램 사용 참조](#)) 및 명령행 자동 설치 모드([자동 설치 사용 참조](#))를 모두 사용할 수 있습니다.



### 설명:

- 드라이버 소프트웨어를 설치하기 전에, Windows 운영 체제가 최신 서비스 팩이 적용된 최신 버전으로 업그레이드되었는지 확인합니다.
- Windows 운영 체제와 함께 Broadcom NetXtreme Gigabit Ethernet 어댑터를 사용하려면 네트워크 장치 드라이버를 설치해야 합니다. 드라이버는 설치 CD에 있습니다.
- Microsoft Windows Server 2008 R2의 Server Core 설치 옵션에서는 BACS이 지원되지 않습니다.

## 설치 프로그램 사용

설치 프로그램을 사용하면 Broadcom 장치 드라이버는 물론 관리 응용 프로그램까지 설치됩니다. 설치 프로그램을 실행하는 동안 설치되는 항목은 다음과 같습니다.

- **Broadcom 장치 드라이버.** Broadcom 장치 드라이버를 설치합니다.
- **Control Suite.** Broadcom Advanced Control Suite(BACS)
- **BASP.** Broadcom Advanced Server Program을 설치합니다.
- **SNMP.** Simple Network Management Protocol subagent를 설치합니다.
- **CIM 공급자.** Common Information Model 공급자를 설치합니다.
- **iSCSI Crash Dump 드라이버.** iSCSI Crash Dump 유틸리티에 필요한 드라이버를 설치합니다.



**참고 :** BACS 소프트웨어 및 관련된 관리 응용 프로그램의 설치는 옵션이지만 설치 프로그램을 사용할 때는 Broadcom 장치 드라이버를 반드시 설치해야 합니다.



**참고:** BASP는 Windows Small Business Server(SBS) 2008에서 사용할 수 없습니다.

**iSCSI Crash Dump에 대한 Microsoft iSCSI 소프트웨어 초기자를 설치하려면**

지원되는 경우 Broadcom iSCSI Crash Dump 유틸리티를 사용하려면 다음 설치 순서를 따르는 것이 중요합니다.

- 설치 프로그램 실행
- 패치(MS KB939875)와 함께 Microsoft iSCSI 소프트웨어 초기자 설치



**참고:** 설치 프로그램을 통해 장치 드라이버를 업그레이드하는 경우 BACS 구성 탭의 고급 섹션에서 **iSCSI Crash Dump**를 다시 활성화하십시오.

설치 프로그램을 실행한 후에 이 절차를 수행하여 장치 드라이버 및 관리 응용 프로그램을 설치합니다.

1. Microsoft iSCSI 소프트웨어 초기자(버전 2.06 이상)가 OS에 포함되어 있지 않은 경우 이를 설치합니다. Microsoft iSCSI 소프트웨어 초기자를 설치해야 하는지 확인하려면 표 21을 참조하십시오. Microsoft에서 iSCSI 소프트웨어 초기자를 다운로드하려면 다음 사이트로 이동하십시오 . <http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986>.
2. <http://support.microsoft.com/kb/939875>에서 iSCSI Crash Dump 파일 생성용 Microsoft 패치(Microsoft KB939875)를 설치합니다. Microsoft 패치를 설치해야 하는지 확인하려면 표 21을 참조하십시오.

**표 21. Windows 운영 체제 및 iSCSI Crash Dump**

| 운영 체제                  | MS iSCSI 소프트웨어 초기자 필요 | Microsoft 패치(MS KB939875) 필요 |
|------------------------|-----------------------|------------------------------|
| <b>NDIS</b>            |                       |                              |
| Windows Server 2008    | 예(OS에 들어 있음)          | 아니오                          |
| Windows Server 2008 R2 | 예(OS에 들어 있음)          | 아니오                          |
| Windows Server 2012    | 예(OS에 들어 있음)          | 아니오                          |
| <b>OIS</b>             |                       |                              |
| Windows Server 2008    | 아니오                   | 아니오                          |
| Windows Server 2008 R2 | 아니오                   | 아니오                          |
| Windows Server 2012    | 아니오                   | 아니오                          |

**자동 설치 사용**



**설명:**

- 모든 명령은 대소문자를 구분합니다.
- 자동 설치에 대한 자세한 내용은 Driver\_Management\_Apps\_Installer 폴더의 Silent.txt 파일을 참조하십시오.

명령줄 지침은 설치 폴더에 있는 readme.txt 파일을 참조하십시오.



**참고:** REINSTALL 스위치는 동일한 설치 프로그램이 이미 시스템에 설치된 경우에만 사용해야 합니다. 이전 버전의 설치 프로그램을 업그레이드하는 경우 위에 나열된 `setup /s /v/qn`을 사용합니다.



---

## 드라이버 소프트웨어 수정

드라이버 소프트웨어를 수정하려면

1. 제어판에서 **프로그램 추가 또는 제거**를 두 번 클릭합니다.
2. **Broadcom Driver and Management Applications(Broadcom 드라이버 및 관리 응용 프로그램)**를 클릭하고 **변경**을 클릭합니다.
3. 계속하려면 **다음**을 클릭합니다.
4. **수정, 추가 또는 제거**를 클릭하여 프로그램 기능을 변경합니다. 새 어댑터의 드라이버를 설치하는 경우에는 이 옵션을 사용할 수 없습니다. 새 어댑터 설치에 대한 자세한 내용은 [드라이버 소프트웨어 복구 또는 다시 설치](#)를 참조하십시오.
5. 계속하려면 **다음**을 클릭합니다.
6. 아이콘을 클릭하여 기능 설치 방법을 변경합니다.
7. **다음**을 클릭합니다.
8. **설치**를 클릭합니다.
9. 설치 프로그램을 닫으려면 **마침**을 클릭합니다.
10. 설치 프로그램에서 시스템을 다시 시작할 필요가 있는지 확인합니다. 화면 지침을 따릅니다.

## 드라이버 소프트웨어 복구 또는 다시 설치

드라이버 소프트웨어를 복구하거나 다시 설치하려면

1. 제어판에서 **프로그램 추가 또는 제거**를 두 번 클릭합니다.
2. **Broadcom Driver and Management Applications(Broadcom 드라이버 및 관리 응용 프로그램)**를 클릭하고 **변경**을 클릭합니다.
3. 계속하려면 **다음**을 클릭합니다.
4. **복구 또는 다시 설치**를 클릭하여 오류를 수정하거나 새 어댑터의 드라이버를 설치합니다.
5. 계속하려면 **다음**을 클릭합니다.
6. **설치**를 클릭합니다.
7. 설치 프로그램을 닫으려면 **마침**을 클릭합니다.
8. 설치 프로그램에서 시스템을 다시 시작할 필요가 있는지 확인합니다. 화면 지침을 따릅니다.

## 장치 드라이버 제거

장치 드라이버를 제거하면 설치된 관리 응용 프로그램도 제거됩니다.



**참고:** Windows Server 2008과 Windows Server 2008 R2는 장치 드라이버를 이전에 설치된 드라이버로 교체하기 위한 장치 드라이버 롤백 기능을 제공합니다. 그러나 롤백 기능을 개별 구성 요소 중 하나에서 사용할 경우 NetXtreme 장치의 복잡한 소프트웨어 아키텍처로 인해 문제가 발생할 수 있습니다. 따라서 드라이버 설치 프로그램 사용을 통해서만 드라이버 버전을 변경하는 것이 좋습니다.

장치 드라이버를 제거하려면

1. 제어판에서 **프로그램 추가 또는 제거**를 두 번 클릭합니다.
2. **Broadcom Driver and Management Applications(Broadcom 드라이버 및 관리 응용 프로그램)**를 클릭하고 **제거**를 클릭합니다. 화면에 표시되는 지침을 따릅니다.
3. 시스템을 다시 부팅하여 드라이버를 완전히 제거합니다. 시스템을 다시 부팅하지 않으면 드라이버를 성공적으로 설치할 수 없습니다.

---

## 어댑터의 속성 확인 또는 변경

Broadcom 네트워크 어댑터의 속성을 보거나 변경하려면

1. 제어판에서 **Broadcom Control Suite 4**를 클릭합니다.
2. 구성 탭의 고급 섹션을 클릭합니다.

---

## 전원 관리 옵션 설정

전원 관리 옵션을 설정하여 운영 체제가 컨트롤러를 꺼서 절전하도록 하거나 컨트롤러가 컴퓨터의 절전 모드를 해제하도록 할 수 있습니다. 장치가 다른 작업(예: 호출 서비스)을 수행하고 있다면 운영 체제는 해당 장치를 종료하지 않습니다. 운영 체제는 시스템이 최대 절전 모드를 시도할 경우에만 가능한 모든 장치를 종료하려 합니다. 어댑터가 항상 전원이 켜져 있게 하려면 **전원을 절약하기 위해 컴퓨터가 이 장치를 끌 수 있음** 확인란을 클릭하지 마십시오.



**참고:** 블레이드 서버에서는 전원 관리 옵션을 사용할 수 없습니다.



**설명:**

- 전원 관리 탭은 전원 관리를 지원하는 서버에만 사용할 수 있습니다.
- 컴퓨터가 대기 상태일 때 WOL(Wake on LAN)을 활성화하려면 **이 장치로 컴퓨터를 대기 상태에서 빠져 나오게 함** 확인란을 선택합니다.
- 관리 스테이션에서만 대기 모드 상태의 컴퓨터를 해제시킬 수 있음을 선택한 경우 컴퓨터는 *Magic Packet*을 통해서만 대기 상태에서 빠져나올 수 있습니다.



**주의!** 팀의 멤버인 어댑터의 경우 **전원을 절약하기 위해 컴퓨터가 이 장치를 끌 수 있음**을 선택하지 마십시오.

## BACS4와 함께 사용할 통신 프로토콜 구성

BACS4 관리 응용 프로그램은 공급자 구성 요소와 클라이언트 소프트웨어라는 두 가지 주요 부분으로 이루어져 있습니다. 공급자는 하나 이상의 NIC가 포함된 서버, 즉 "관리 호스트"에 설치됩니다. 공급자는 NIC에 대한 정보를 수집하고 클라이언트 소프트웨어가 설치되어 있는 관리 PC에서 해당 정보를 검색할 수 있게 합니다. 클라이언트 소프트웨어를 사용하면 공급자로부터 제공되는 정보를 볼 수 있고 NIC를 구성할 수 있습니다. BACS 클라이언트 소프트웨어에는 GUI(그래픽 사용자 인터페이스)와 CLI(명령줄 인터페이스)가 포함되어 있습니다.

공급자와 클라이언트 소프트웨어 사이에 통신이 이루어지기 위해서는 통신 프로토콜이 있어야 합니다. 네트워크의 클라이언트와 관리 호스트에서 사용되는 운영 체제 혼합(Linux, Windows 또는 모두)에 따라 사용할 적절한 통신 프로토콜을 선택할 수 있습니다. 각 네트워크 구성에서 사용 가능한 통신 프로토콜에 대한 설명은 [Linux 관리 응용 프로그램 설치](#)를 참조하십시오.

이 챕터의 지침은 Windows 관리 호스트가 Windows 클라이언트와 통신하는 시나리오에 대해서만 설명합니다. 이러한 시나리오에서는 WMI 또는 WS-MAN(WinRM) 통신 프로토콜을 사용할 수 있습니다. 본 챕터에서 설명하는 드라이버 설치 관리자를 사용하여 드라이버와 관리 응용 프로그램을 설치하면 WMI 및 WS-MAN에 필요한 공급자가 관리 호스트에 설치됩니다. 또한, BACS4 유틸리티가 클라이언트에 설치됩니다. 다음 섹션에서는 통신 프로토콜별로 수행해야 할 추가 구성 단계를 설명합니다.

Linux 설치의 경우, 드라이버는 관리 응용 프로그램과 별도로 설치됩니다.

## WS-MAN 사용

WS-MAN 통신 프로토콜을 사용하려면 다음 절의 지침을 따릅니다.

- [WS-MAN Windows Server 구성](#)
- [WS-MAN Windows 클라이언트 설치](#)

### WS-MAN Windows Server 구성

1단계: 서버에 WinRM 소프트웨어 구성 요소 설치

WinRM 2.0은 다음 운영 체제에 사전 설치되어 있습니다.

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows 2012 R2

Windows Server 2008 의 경우 다음 링크에서 WinRM 2.0 과 Windows Powershell 2.0 이 포함된 Windows Management Framework Core를 설치합니다.

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11829>

## 2단계: 서버에서 기본 구성 수행

WinRM이 제대로 작동하려면 Windows 방화벽을 활성화해야 합니다. 방화벽 구성에 대한 자세한 내용은 **7단계: 추가 서버 구성**을 참조하십시오. 방화벽을 구성했으면 명령 프롬프트를 열고 다음 명령을 실행하여 Windows 서버에 대한 원격 관리 기능을 활성화합니다.

```
winrm quickconfig
```

다음 명령을 사용하여 서비스에 대한 구성 정보를 볼 수 있습니다.

```
winrm get winrm/config
```

## 3단계: 서버에서 사용자 구성 수행

WinRM 에 연결하려면 로컬 또는 원격 컴퓨터의 로컬 관리자 그룹에 속한 구성원 계정을 사용해야 합니다. `get winrm/config` 명령을 실행하면 다음과 같은 결과가 출력됩니다.

```
RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
```

BA는 BUILTIN\Administrators를 의미합니다.

WinRM의 연결 허용 목록에 다른 사용자 그룹을 추가하려면 새 사용자 그룹을 포함하도록 RootSDDL을 수정하면 됩니다. 이를 위해서는 새 그룹에 대한 SDDL ID가 있어야 합니다. 예를 들어, 다음 명령을 실행하면 SDDL ID가 S-1-5-21-1866529496-2433358402-1775838904-1021인 새 사용자 그룹이 추가됩니다.

```
winrm set winrm/config/Service @{RootSDDL="O:NSG:BAD:P(A;GA;;;BA)(A;GA;;;S-1-5-21-1866529496-2433358402-1775838904-1021)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)"}
```

## 4단계: 서버에서 HTTP 구성 수행

BACS GUI를 사용하려면 다음과 같이 HTTP 프로토콜을 구성해야 합니다.



**참고:** WinRM 2.0의 기본 HTTP 포트는 5985입니다.

1. 시작을 클릭하고(또는 Windows 로고 키를 누름) **실행**을 선택합니다.
2. `gpedit.msc`를 입력하여 로컬 그룹 정책 편집기를 엽니다.
3. 컴퓨터 구성 아래 있는 **관리 템플릿** 폴더를 연 다음 **Windows 구성 요소** 폴더를 엽니다.
4. **WinRM(Windows Remote Management)**을 선택합니다.
5. **WinRM(Windows Remote Management)** 아래에서 **WinRm 클라이언트**를 선택합니다.
6. **WinRM 클라이언트** 아래 있는 **신뢰할 수 있는 호스트**를 두 번 클릭합니다.
7. **TrustedHostsList**에 클라이언트의 호스트 이름을 입력합니다. 모든 클라이언트를 신뢰할 수 있으면 별표(\*)만 입력합니다.
8. **WinRM 서비스**를 선택합니다.
9. **기본 인증 허용**을 활성화합니다.
10. **암호화되지 않은 트래픽 허용**을 활성화합니다.

11. 그룹 정책 창을 닫습니다.
12. 명령 프롬프트에서 다음 명령을 실행하여 기본 설정으로 WinRM을 구성합니다.  
winrm qc or winrm quickconfig
13. "Make these changes[y/n]?"라는 도구 메시지가 나타나면 "y"를 입력합니다.
14. 다음 명령 중 하나를 입력하여 HTTP 수신기가 생성되었는지 확인합니다.  
winrm enumerate winrm/config/listener  
  
또는  
winrm e winrm/config/Listener
15. 명령 프롬프트에 다음 명령을 입력하여 로컬로 테스트를 수행합니다.  
winrm id

### 5단계: 서버에서 HTTPS 구성 수행(HTTP 대신 HTTPS 사용)

이 단계는 인증서가 없는 경우 자체 서명된 인증서를 생성하고 이를 Windows 서버로 가져오는 두 가지 개별 과정으로 진행됩니다. 인증서가 없는 경우에는 Windows 서버에 자체 서명된 인증서를 구성해야만 Windows 클라이언트에서 BACS GUI로 HTTPS/SSL 통신을 수행할 수 있습니다. 자체 서명된 인증서를 사용하여 Windows 클라이언트도 구성해야 합니다. [HTTPS 구성 수행\(HTTPS를 사용하려는 경우\)](#)을 참조하십시오.



**참고:** 자체 서명된 인증서는 어떤 Windows 서버에서든 생성할 수 있습니다. 서버에 BACS가 설치되어 있지 않아도 됩니다. 임의의 Windows 서버에서 자체 서명된 인증서를 생성했다면 해당 인증서를 클라이언트의 로컬 드라이브에 복사해야 합니다.

1. 시작을 클릭하고(또는 Windows 로고 키를 누름) 실행을 선택합니다.
2. `gpedit.msc`를 입력하여 로컬 그룹 정책 편집기를 엽니다.
3. 컴퓨터 구성 아래 있는 관리 템플릿 폴더를 연 다음 Windows 구성 요소 폴더를 엽니다.
4. WinRM(Windows Remote Management)을 선택합니다.
5. WinRM(Windows Remote Management) 아래에서 WinRm 클라이언트를 선택합니다.
6. WinRM 클라이언트 아래 있는 신뢰할 수 있는 호스트를 두 번 클릭합니다.
7. TrustedHostsList에 클라이언트의 호스트 이름을 입력합니다. 모든 클라이언트를 신뢰할 수 있으면 별표(\*)만 입력합니다.
8. WinRM 서비스를 선택합니다.
9. 기본 인증 허용을 활성화합니다.

### Windows Server에 필요한 자체 서명된 인증서 생성:

Windows에서 Openssl을 사용하여 다음과 같이 자체 서명된 인증서를 생성할 수 있습니다.

1. 다음 명령을 입력하여 개인 키를 생성합니다.  
openssl genrsa -des3 -out server.key 1024
2. 암호 문구를 입력하라는 메시지가 나타납니다. 이 암호 문구를 기억하고 있어야 합니다.
3. 다음 단계에 따라 CSR(인증서 서명 요청)을 생성합니다.  
  
CSR을 생성하는 과정에서 여러 가지 정보를 입력해야 합니다. "일반 이름"을 입력하라는 메시지가 나타나면 Windows Server 호스트 이름 또는 IP 주소를 입력합니다.  
  
다음 명령을 입력합니다(여기에는 응답 샘플이 함께 나와 있습니다).  
openssl req -new -key server.key -out server.csr  
  
명령이 작동하지 않을 경우 다음을 시도합니다.

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

openssl.cnf 파일은 openssl 이 있는 동일한 디렉터리에 저장해야 합니다. Openssl.cnf 는 C:\Program Files(x86)\GnuWin32\share에 있습니다.

다음과 같은 정보가 필요합니다.

- 국가 이름(두 자로 된 코드) []: **US**
- 구/군/시 또는 시/도 이름(전체 이름) []: **California**
- 지역 이름(예: 시) []: **Irvine**
- 조직 이름(예: 회사) []: **Broadcom Corporation**
- 조직 구성 단위 이름(예: 부서) []: **Engineering**
- 일반 이름(예: 사용자 이름) []: Windows 서버의 호스트 이름 또는 IP 주소를 입력합니다. IPv6의 경우 대괄호 []를 포함하여 [xyxy:xxx:.....:xxx]의 형식으로 공통 이름을 입력합니다.
- (선택 사항) 이메일 주소 []:

인증서 요청과 함께 전송할 다음과 같은 추가 특성을 입력합니다.

- 챌린지 암호 []: **password1**
- 회사 이름(옵션) []:

#### 4. 키에서 암호 문구를 제거합니다.

다음 명령을 입력합니다.

```
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
```

#### 5. 자체 서명된 인증서 생성:

365일 사용할 수 있는 자체 서명된 인증서를 생성하려면 다음 명령을 입력합니다.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

다음과 같은 출력이 표시됩니다.

```
Signature ok
subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-LAB3/
emailAddress=
Getting Private key
```

#### 6. 다음 명령을 입력하여 자체 서명된 인증서가 제대로 생성되었는지 확인합니다.

```
openssl verify server.crt
```

다음과 같은 출력이 표시됩니다.

```
server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
LAB3/emailAddress=
error 18 at 0 depth lookup:self signed certificate
OK
```

"error 18 at 0 depth lookup:self signed certificate" 오류 메시지는 무시해도 됩니다. 이 오류는 인증서가 자체 서명된 것임을 의미합니다.

#### 7. 다음과 같이 인증서를 "crt"에서 "pkcs12" 형식으로 변환합니다.

Windows 서버의 경우 인증서는 pkcs12 형식이어야 합니다. 다음 명령을 입력합니다.

```
openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
```

다음과 같은 정보를 입력하라는 메시지가 나타납니다.

```
Enter Export Password:
Verifying - Enter Export Password:
```

암호를 입력합니다. 입력한 암호는 반드시 기억하고 있어야 합니다. Windows 서버와 클라이언트에서 인증서를 가져올 때 암호가 필요합니다.

8. 인증서 파일 `server.crt`의 복사본을 만든 다음, BACS를 설치할 서버로 인증서 파일을 가져올 수 있도록 해당 서버에 복사본을 배치해 둡니다. BACS가 실행되는 서버에 연결하는 데 Windows 클라이언트를 사용할 계획이라면 클라이언트 시스템에도 인증서를 전송(복사하여 붙여 넣기)해야 합니다.



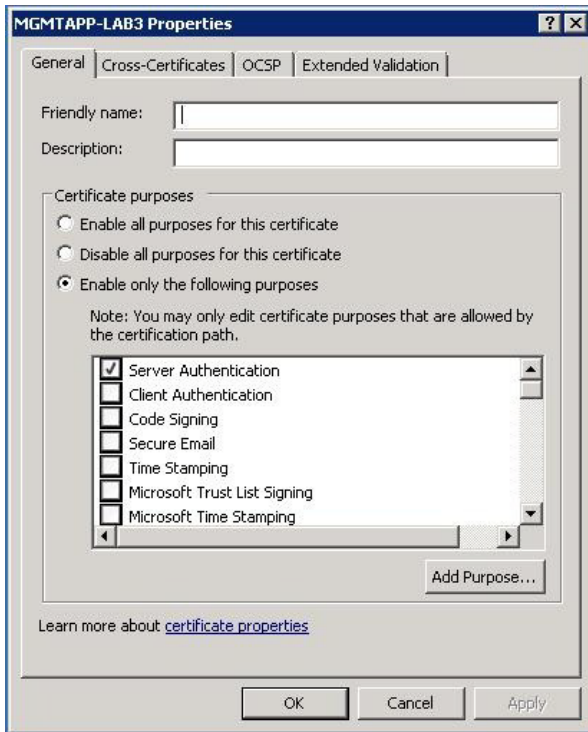
**참고:** IPv4 주소, IPv6 주소 및 호스트 이름에 각각 별개의 인증서를 생성해야 합니다.

#### Windows 서버에 자체 서명된 인증서 설치:

인증서를 설치하려면 앞서 생성한 `hostname.pfx` 파일을 Windows 서버로 먼저 전송해야 합니다.

1. 시작을 클릭하고(또는 Windows 로고 키를 누름) 실행을 선택합니다.
2. MMC를 입력하고 확인을 클릭합니다.
3. 파일 > 스냅인 추가/제거를 클릭합니다.
4. 추가를 클릭합니다.
5. 인증서를 선택하고 추가를 클릭합니다.
6. 컴퓨터 계정을 선택합니다.
7. 다음을 클릭하고 마침을 클릭합니다.
8. 달기를 클릭하고 확인을 클릭합니다.
9. 인증서(로컬 컴퓨터) 폴더를 연 다음 개인 폴더를 엽니다.
10. 인증서를 마우스 오른쪽 단추로 클릭하고 모든 작업을 선택한 다음 가져오기를 클릭합니다.
11. 다음을 클릭하여 인증서 가져오기 마법사를 시작합니다.
12. `hostname.pfx`를 찾아 선택합니다.
13. 개인 키의 암호를 입력하라는 메시지가 나타나면 Windows Server에 필요한 자체 서명된 인증서 생성:에서 만든 암호를 그대로 입력합니다.
14. 지침에 따라 기본값을 선택하고 작업을 계속 진행합니다.  
인증서가 설치되었다는 표시가 창 오른쪽에 나타납니다. 인증서의 이름은 자체 서명된 인증서를 생성할 때 지정한 이름과 같습니다.
15. 인증서를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.  
다음과 같은 대화 상자가 나타납니다.





16. 그림에 나와 있는 것과 같이 서버 인증만 활성화되어 있어야 합니다.

17. 신뢰할 수 있는 루트 인증 기관을 열고 인증서를 엽니다.

18. 11.단계부터 17.단계까지의 지침을 따릅니다.



**참고:** 자체 서명된 인증서를 클라이언트로 가져오는 방법에 대한 자세한 내용은 [HTTPS 구성 수행\(HTTPS를 사용하려는 경우\)](#)을 참조하십시오.

## 6단계: 서버에서 WinRM HTTPS/SSL 구성

1. 다음과 같이 WinRM 수신기를 생성합니다.

- a. 시작을 클릭하고(또는 Windows 로고 키를 누름) 실행을 선택합니다.
- b. MMC를 입력하고 확인을 클릭합니다.
- c. 개인 저장소에서 자체 서명된 인증서를 선택합니다.  
예를 들어 , 호스트 이름을 사용하여 인증서를 생성했으면 호스트 이름이 표시됩니다 .
- d. 인증서를 두 번 클릭하여 엽니다.
- e. 자세히 탭을 클릭합니다.
- f. 화면을 아래로 스크롤하여 지문 필드를 선택합니다.
- g. 자세히 창에서 지문을 선택하여 복사합니다. 이렇게 복사한 내용을 다음 단계에서 삽입할 것입니다.
- h. 명령 프롬프트로 돌아갑니다.
- i. 다음 명령을 입력합니다.
 

```
winrm create winrm/config/Listener?Address=*+Transport=
HTTPS @{Hostname="<HostName or IPAddress>";
CertificateThumbprint="<paste from the previous step and remove the spaces>"}
```

**설명:**

- 인증서를 생성하는 데 호스트 이름을 사용했으면 호스트 이름을 입력합니다. 인증서를 생성하는 데 IP 주소를 사용했으면 IP 주소를 입력합니다. IPv6 주소의 경우 대괄호 [ ] 안에 주소를 포함합니다.
- 시스템에 HTTPS가 구성된 경우 새 HTTPS 수신기를 만들기 전에 수신기를 삭제해야 합니다. 다음 명령을 사용합니다.

```
winrm delete winrm/config/Listener?Address=*&Transport=HTTPS
```

- 위 명령을 실행하면 SelfSSL로 생성한 인증서 및 서버의 모든/임의 네트워크 주소를 사용하여 HTTPS 포트(5986)에 대한 수신기가 생성됩니다.
  - winrm 명령을 사용하여 HTTPS 수신기를 수정하거나 설정할 수 있습니다. 사용자가 정의한 임의의 포트에서 WinRM 수신기를 구성할 수 있기 때문입니다.
  - 명령 프롬프트에서 다음 명령을 실행하여 수신기가 올바르게 구성되었는지 확인합니다.
 

```
winrm e winrm/config/listener
```
- 서버에서 HTTPS/SSL 연결을 테스트합니다.
    - 서버의 명령 프롬프트에서 다음 명령을 입력합니다.
 

```
winrs -r:https://yourserver:5986 -u:username -p:password hostname
```
    - 설정이 올바르게 된 뒤 명령을 실행했을 때 서버 호스트 이름이 출력됩니다.
    - WinRM 서비스 구성을 확인하려면 다음 명령을 실행합니다.
 

```
winrm get winrm/config/service
```

**7단계: 추가 서버 구성**

필요하면 다음과 같이 방화벽 규칙을 수정합니다.

**Windows Server 2008 R2**

- 관리 도구 메뉴에서 고급 보안이 설정된 **Windows 방화벽**을 엽니다.
- 인바운드 규칙을 마우스 오른쪽 단추로 클릭하고 새 규칙을 선택합니다.  
새 규칙 마법사가 열립니다.
- 포트를 선택하고 다음을 클릭합니다.
- 프로토콜 및 포트 화면에서 TCP를 선택하고 포트 번호를 입력합니다. 예를 들어, HTTP에 대해서는 5985를, HTTPS에 대해서는 5986을 입력할 수 있습니다.
- 다음을 클릭합니다.
- 작업 화면에서 연결 허용을 선택하고 다음을 클릭합니다.
- 서버가 작업 그룹에 속해 있으면 프로필에 대해 세 가지 프로필을 모두 선택할 수 있습니다.
- 규칙의 이름을 지정하고 마침을 클릭합니다.
- 새 규칙이 활성화되었는지 확인합니다(녹색 확인란이 선택되어 있어야 합니다).

**Windows XP**

- 시작 > 제어판을 클릭하고 **Windows 방화벽**을 두 번 클릭합니다.
- 예외 탭을 클릭합니다.
- 포트 추가를 클릭합니다.
- 의미 있는 이름(예: "WinRM rule")과 포트 번호(예: HTTP의 경우 5985, HTTPS의 경우 5986)를 입력합니다.
- 확인을 클릭합니다.

## 유용한 WinRM 명령

| 명령                                                                                               | 설명                                                            |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <code>winrm quickconfig</code> or <code>winrm qc</code>                                          | 기본 설정을 사용하여 WinRM을 구성합니다.                                     |
| <code>winrm enumerate winrm/config/Listener</code> or <code>winrm e winrm/config/Listener</code> | 어느 서비스 수신기가 활성화되어 있는지, 수신에 어느 포트와 IP 주소를 사용하고 있는지 확인할 수 있습니다. |
| <code>winrm get winrm/config/Service</code>                                                      | WinRM 서비스 구성을 확인합니다.                                          |
| <code>winrm delete winrm/config/Listener?Address=*&amp;Transport=HTTPS</code>                    | 수신기를 삭제합니다(이 경우에는 HTTPS 수신기를 삭제합니다).                          |

## 유용한 WinRM 웹 사이트

- <http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx>
- <http://technet.microsoft.com/en-us/library/cc782312%28WS.10%29.aspx>
- <http://msdn.microsoft.com/en-us/library/aa384295%28v=VS.85%29.aspx>
- 다음은 <http://support.microsoft.com>에서 제공하는 자료:
  - “Configuring WINRM for HTTPS”
  - “Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0, and BITS 4.0)”

## WS-MAN Windows 클라이언트 설치

Windows 클라이언트에서 다음과 같은 구성 단계를 수행합니다.

## 1. HTTP 구성 수행(HTTP를 사용하려는 경우)

- 시작을 클릭하고(또는 Windows 로고 키를 누름) **실행**을 선택합니다.
- `gpedit.msc`를 입력하여 로컬 그룹 정책 편집기를 엽니다.
- 컴퓨터 구성 아래 있는 관리 템플릿 폴더를 연 다음 **Windows 구성 요소** 폴더를 엽니다.
- WinRM(Windows Remote Management)**을 선택합니다.
- WinRM(Windows Remote Management)** 아래에서 **WinRm 클라이언트**를 선택합니다.
- WinRM 클라이언트** 아래 있는 **신뢰할 수 있는 호스트**를 두 번 클릭합니다.
- TrustedHostsList**에 클라이언트의 호스트 이름을 입력하고 **확인**을 클릭합니다. 모든 클라이언트를 신뢰할 수 있으면 "\*"만 입력합니다.
- WinRM 서비스**를 선택합니다.
- 기본 **인증 허용**을 활성화하고 **확인**을 클릭합니다.
- 명령 프롬프트에서 다음 명령을 실행하여 연결을 테스트합니다.  
`winrm id -remote:<remote machine Hostname or IP Address>`

## 2. HTTPS 구성 수행(HTTPS를 사용하려는 경우)

Windows Server에 필요한 자체 서명된 인증서 생성:에서 설명하는 대로 자체 서명된 인증서를 생성했다면 서버와 클라이언트 사이의 연결을 위해 클라이언트로 인증서를 가져올 수 있습니다. 다음 단계의 작업을 진행하려면 먼저 **Windows Server에 필요한 자체 서명된 인증서 생성:** 섹션에 나와 있는 모든 단계를 완료해야 합니다. 여기에는 클라이언트를 통해 액세스할 수 있는 위치에 `hostname.pfx`를 복사하는 작업도 포함됩니다.

- 시작을 클릭하고(또는 Windows 로고 키를 누름) **실행**을 선택합니다.
- MMC**를 입력하고 **확인**을 클릭합니다.
- 파일**을 클릭하고 **스냅인 추가/제거**를 선택합니다.
- 추가**를 클릭합니다.
- 인증서**를 선택하고 **추가**를 클릭합니다.
- 컴퓨터 계정**을 선택하고 **다음**을 클릭합니다.

- g. 마침을 클릭합니다.
- h. 닫기를 클릭한 후 확인을 클릭합니다.
- i. 인증서(로컬 컴퓨터) 아래에서 신뢰할 수 있는 루트 인증 기관을 마우스 오른쪽 단추로 클릭하고 모든 작업을 선택한 다음 가져오기를 선택합니다.
- j. 다음을 클릭하여 인증서 가져오기 마법사를 시작합니다.
- k. Windows Server에 필요한 자체 서명된 인증서 생성:에서 생성한 .pfx 파일을 찾아 선택합니다. 파일 형식 목록의 선택 항목을 개인 정보 교환(\*.pfxas, \*.p12)으로 변경하고 hostname.pfx 파일을 선택한 다음 열기를 클릭합니다.
- l. 개인 키에 지정했던 암호를 입력하고 다음을 클릭합니다.

### 3. WinRM HTTPS/SSL 구성

클라이언트에서 winrm을 실행하면 WinRM HTTPS 연결을 사용하여 서버로부터 정보를 검색하여 가져올 수 있습니다. 클라이언트에서 WinRM HTTPS/SSL 연결을 테스트하려면 다음 단계를 수행합니다.

- a. 서버 운영 체제 정보를 검색하여 가져오려면 다음 명령을 입력합니다.
 

```
winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername -u:username -p:password -skipCAcheck
```
- b. 서버 WinRM ID 정보를 검색하여 가져오려면 다음 명령을 입력합니다.
 

```
winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
```
- c. 서버의 Windows 서비스를 열거하려면 다음 명령을 입력합니다.
 

```
winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -skipCAcheck
```



**참고:** winrm 명령행 테스트에 -skipCAcheck 스위치를 사용하는 것이 중요합니다. 인증서가 자체 생성된 것이고, 클라이언트로 가져오는 것이 아니기 때문입니다. 이 스위치를 사용하지 않으면 WSMANFault 오류 메시지가 나타납니다.

## WMI 사용

Windows 클라이언트에서 WMI를 사용하는 데는 별도의 구성이 필요하지 않습니다. Windows 서버에서 WMI 구성하려면 다음 섹션에서 설명하는 단계를 수행합니다.

### 1단계: WMI 컨트롤을 사용하여 네임스페이스 보안 설정

WMI 컨트롤에서 제공하는 한 가지 방법을 사용하여 네임스페이스 보안을 관리할 수 있습니다. WMI 컨트롤을 시작하려면 명령 프롬프트에서 다음 명령을 실행합니다.

```
wmingmt
```

WMI가 설치되어 있는 Windows 9x 또는 Windows NT4 컴퓨터에서는 다음 명령을 대신 사용해도 됩니다.

```
wbemcnt1.exe
```

또는 다음과 같은 방법으로 WMI 컨트롤을 열고 보안 탭에 액세스할 수도 있습니다.

1. 내 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **관리**를 클릭합니다.
2. **서비스 및 응용 프로그램**을 두 번 클릭한 다음 **WMI 컨트롤**을 두 번 클릭합니다.
3. **WMI 컨트롤**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
4. WMI 컨트롤 속성 창에서 **보안** 탭을 클릭합니다.
5. Root라는 폴더가 있고, 그 옆에 + 기호가 표시됩니다. 필요에 따라 이 트리를 확장한 후 권한을 설정할 네임스페이스를 찾습니다.
6. **보안**을 클릭합니다.

사용자 및 사용 권한의 목록이 표시됩니다. 사용자가 목록에 있으면 해당 권한을 적절히 수정합니다. 사용자가 목록에 없으면 **추가**를 클릭한 후 계정이 있는 위치(로컬 컴퓨터, 도메인 등)로부터 사용자를 추가합니다.



**참고:** 이러한 내보내기를 `.bash_profile`의 끝에 추가할 수 있습니다. 이 파일은 `/root` 디렉터리에 있습니다.

- 네임스페이스 보안을 보고 설정하려면 사용자에게 "보안 읽기" 및 "보안 편집" 권한이 있어야 합니다. **Administrators** 사용자는 기본적으로 이러한 권한을 가지며, 필요에 따라 다른 사용자 계정에 권한을 할당할 수도 있습니다.
- 네임스페이스에 원격으로 액세스해야 하는 사용자라면 "원격으로부터 사용 가능" 권한을 선택해야 합니다.
- 네임스페이스에 대해 설정된 사용자 권한은 기본적으로 해당 네임스페이스에만 적용됩니다. 사용자가 트리 구조의 특정 네임스페이스 및 그 하위 네임스페이스 전체에 대한 액세스 권한을 갖게 하거나 하위 네임스페이스에서만 권한을 갖도록 지정하려면 **고급**을 클릭합니다. **편집**을 클릭한 후 대화 상자가 열리면 액세스 범위를 지정합니다.

### 2단계: DCOM 원격 실행 및 활성화 사용 권한 부여

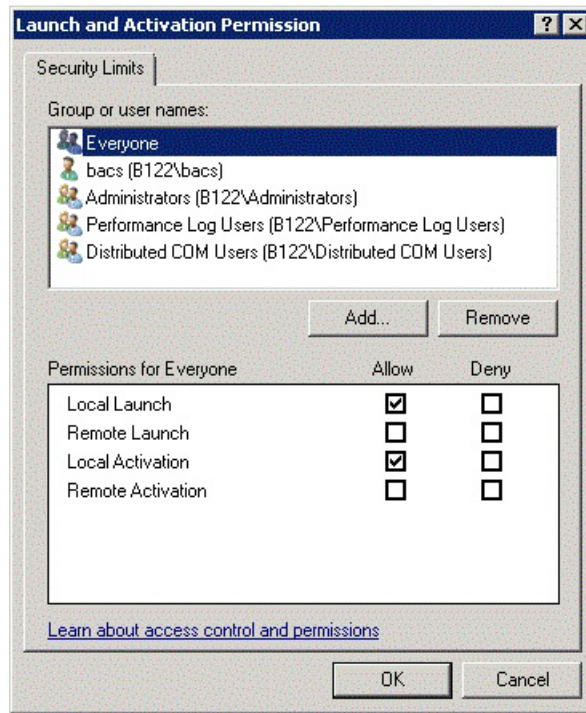
Windows 도메인 환경에서는 BACS 관리를 위해 WMI 구성 요소에 액세스하는 데 필요한 수준의 권한이 도메인 관리자 계정에 부여되어 있으므로 별도의 구성 작업이 필요하지 않습니다. 그러나 규모가 큰 엔터프라이즈 환경에서는 BACS4 클라이언트 GUI를 사용하여 로컬 또는 원격 호스트에 액세스하려는 사용자에게 도메인 관리자 계정 권한이 없을 수도 있습니다. 사용자가 BACS4 클라이언트 GUI를 사용하여 원격 호스트에 연결할 수 있게 하려면 원격 호스트에 대한 WMI 보안 액세스를 구성해야 합니다.

다음 절차를 따르면 이와 같은 액세스를 쉽게 구성할 수 있습니다. WMI 액세스를 위한 보안을 구성하는 데 필요한 권한이 없으면 네트워크 관리자에게 문의하십시오.

1. **시작 > 실행**을 클릭하고 **DCOMCFG**를 입력한 다음 **확인**을 클릭합니다.

2. 구성 요소 서비스 대화 상자가 나타납니다.
3. 구성 요소 서비스를 연 다음 컴퓨터를 엽니다.
4. 내 컴퓨터를 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다.
5. 내 컴퓨터 속성에서 COM 보안 탭을 클릭합니다.
6. 실행 및 활성화 사용 권한 아래에서 제한 편집을 클릭합니다.
7. 사용자 이름 또는 그룹이 그룹 또는 사용자 이름 목록에 없으면 다음 단계를 따릅니다.
  - a. 실행 사용 권한 대화 상자에서 추가를 클릭합니다.
  - b. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 선택할 개체 이름을 입력하십시오. 입력란에 사용자 이름 및 그룹을 추가한 다음 확인을 클릭합니다.
  - c. 실행 사용 권한 대화 상자의 그룹 또는 사용자 이름 목록에서 사용자 이름 및 그룹을 선택합니다.
  - d. 사용자의 권한 영역에서 원격 시작 및 원격 활성화에 대해 허용을 선택한 다음 확인을 클릭합니다.

그림 8: 실행 및 활성화 사용 권한



자세한 내용은 Microsoft Developer Network 사이트에 있는 [Securing a Remote WMI Connection](#)(원격 WMI 연결 보호)을 참조하십시오.

### 각기 다른 시스템의 WMI를 위한 특수 구성

Windows Vista 및 Windows 7의 경우 관리자 그룹의 모든 사용자가 WMI 네임스페이스를 사용하여 연결할 수 있게 하려면 필요에 따라 사용자가 LocalAccountTokenFilterPolicy를 변경해야 할 수도 있습니다.

# 13 절: Broadcom Advanced Control Suite 4 사용

- [Broadcom Advanced Control Suite 개요](#)
- [Broadcom Advanced Control Suite 시작](#)
- [BACS 인터페이스](#)
- [Windows에서 기본 설정 구성](#)
- [호스트에 연결](#)
- [호스트 관리](#)
- [네트워크 어댑터 관리](#)
- [통계 보기](#)
- [팀 구성](#)
- [명령줄 인터페이스 유틸리티를 사용하여 구성](#)
- [BACS 문제 해결](#)

## Broadcom Advanced Control Suite 개요

Broadcom Advanced Control Suite(BACS)는 시스템에 설치된 각 네트워크 어댑터에 대한 유용한 정보를 제공하는 통합 유틸리티입니다. BACS를 사용하면 각 어댑터의 속성 값을 확인 및 수정하고 트래픽 통계를 확인하는 것 외에 네트워크 객체에 대한 상세 테스트, 진단 및 분석을 수행할 수 있습니다. BACS는 Windows 및 Linux 운영 체제에서 작동합니다.

Broadcom Advanced Control Suite에서 실행하는 Broadcom Advanced Server Program(BASP)은 로드 균형 조정, 결합 허용 및 VLAN(Virtual Local Area Networks)에 대한 팀 구성에 사용됩니다. BASP 기능은 하나 이상의 Broadcom 네트워크 어댑터를 사용하는 시스템에만 사용할 수 있습니다. BASP는 Windows 운영 체제에서만 작동합니다.



**참고:** 일부 BACS 기능은 특정 어댑터와만 관련이 있습니다. BACS의 단일 인스턴스를 사용하여 여러 호스트 및 어댑터 유형과 통신할 수 있으므로 이 문서는 모든 BACS 기능에 대해 설명합니다.

BACS 응용 프로그램에 그래픽 사용자 인터페이스와 명령행 인터페이스(BACSCLI)가 포함됩니다. BACS GUI 및 BACS CLI는 다음 운영 체제 제품군에서 작동할 수 있습니다.

- Windows
- Windows Server
- Linux Server

지원되는 최신 OS 버전에 대한 자세한 내용은 소프트웨어 배포 시 함께 제공된 릴리스 문서를 참조하십시오.

---

## Broadcom Advanced Control Suite 시작

제어판에서 **Broadcom Control Suite 4**를 클릭하거나 Windows 또는 Windows Server 바탕화면 아래에 있는 작업 표시줄에서 **BACS** 아이콘을 클릭합니다.

Linux 시스템에서, **BACS4** 데스크탑 아이콘을 두 번 클릭하거나 **시스템 도구** 아래 작업 표시줄에서 **BACS** 프로그램에 액세스합니다. (Linux 시스템에서 **BACS**를 시작할 수 없는 경우, [BACS 문제 해결](#)에서 관련 항목을 참조하십시오.)

---

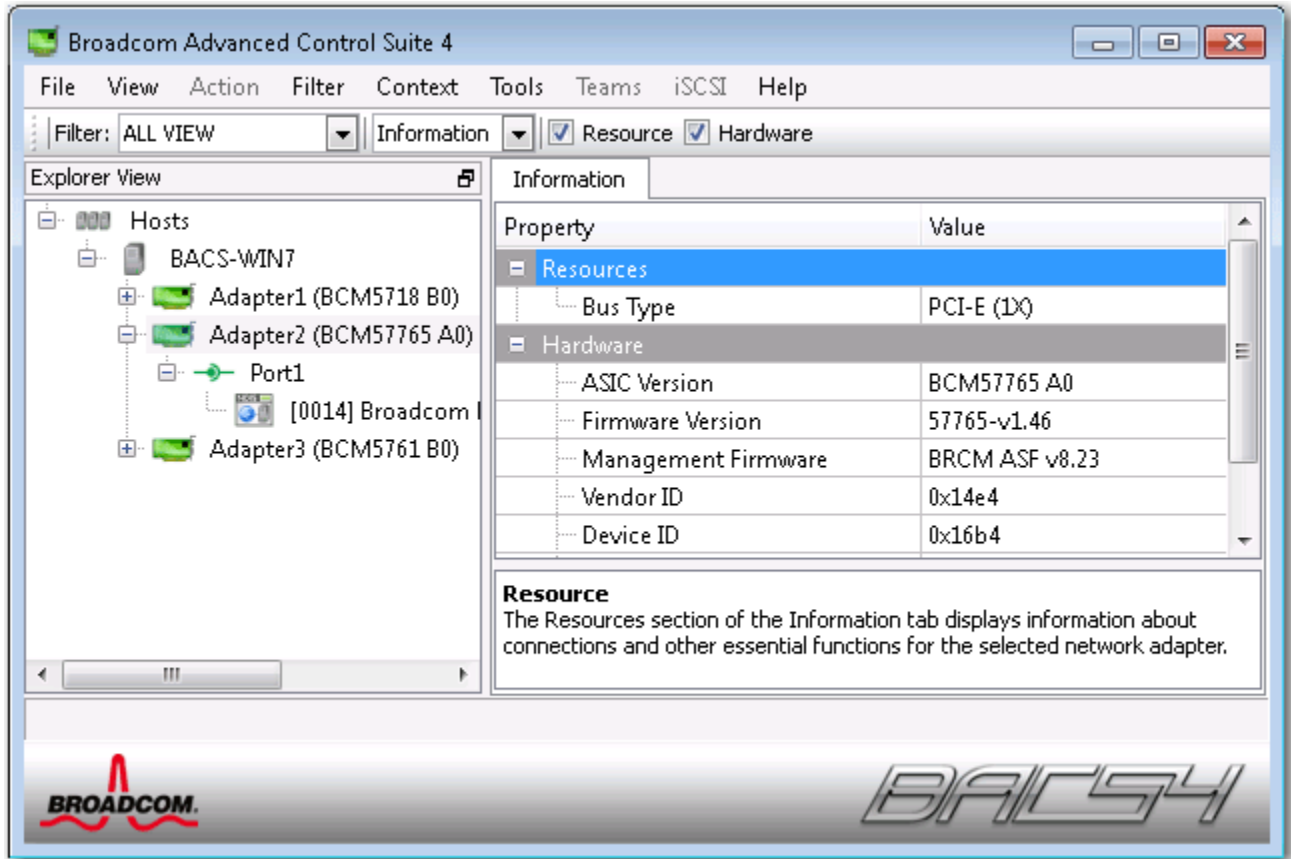
## BACS 인터페이스

BACS 인터페이스는 다음 영역으로 구성됩니다.

- 탐색기 보기 창
- 컨텍스트 보기 선택기
- 컨텍스트 보기 창
- 메뉴 모음
- 설명 창

기본적으로, 탐색기 보기 창은 기본 창 왼쪽에, 컨텍스트 보기 창은 오른쪽에, 컨텍스트 보기 선택기는 메뉴 모음 아래에, 설명 창은 컨텍스트 보기 창 아래에 도킹 및 고정되어 있습니다. 두 창간에 구분선을 끌어서 창 크기를 변경할 수 있습니다.





## 탐색기 보기 창

탐색기 보기 창을 기본 창 왼쪽, 오른쪽, 위 또는 아래에 도킹 및 고정시킬 수 있습니다.

탐색기 보기 창에는 BACS에서 확인, 분석, 테스트 또는 구성할 수 있는 개체가 나열됩니다. 탐색기 보기 창에서 항목을 선택하면 해당 항목에 사용 가능한 정보와 옵션을 표시하는 탭이 컨텍스트 보기 창에 나타납니다.

이 패널은 관리 가능한 개체를 드라이버와 해당 하위 구성 요소로 동일한 계층 방식으로 나타내도록 구성되어 있습니다. 이 방식은 다양한 C-NIC(Converged Network Interface Controller) 요소의 관리를 간소화합니다. 계층의 최상위는 호스트 컨테이너로, BACS에서 관리하는 모든 호스트가 나열됩니다. 호스트 아래에는 설치된 네트워크 어댑터가 나타나고, 각 어댑터 아래에는 물리적 포트, NDIS 및 iSCSI 등의 관리 가능한 요소가 함께 나타납니다.

탐색기 보기 창에서 각 장치 옆의 아이콘은 해당 장치의 상태를 보여 줍니다. 장치 이름 옆의 아이콘이 정상으로 나타나면 해당 장치가 연결되어 작동하고 있는 것입니다.

- **X.** 장치 아이콘에 빨강 "X" 표시가 나타나면 해당 장치가 현재 네트워크에 연결되어 있지 않은 것입니다.
- **회색으로 나타남.** 장치 아이콘이 회색으로 나타나면 해당 장치가 현재 사용되고 있지 않은 것입니다.

## 컨텍스트 보기 선택기

메뉴 모음 아래에 필터와 탭 범주가 포함된 컨텍스트 보기 선택기가 나타납니다. 컨텍스트 보기 창의 탭에 나타나는 범주를 확장 및 축소할 수 있지만, 범주 이름 옆에 있는 상자를 선택하여 범주를 표시할 수도 있습니다.

### 필터 보기

여러 C-NIC를 사용하는 다중 호스트 환경에서는 어댑터별로 관리 가능한 요소가 매우 많아서 모든 요소를 확인, 구성 및 관리하기가 어렵고 복잡할 수 있습니다. 필터를 사용하여 특정 장치 기능을 선택하십시오. 가능한 필터 보기는 다음과 같습니다.

- 모두
- 팀 보기
- NDIS 보기
- iSCSI 보기
- iSCSI 대상 보기

## 컨텍스트 보기 창

컨텍스트 보기 창은 탐색기 보기 창에서 선택한 개체에 대해 확인할 수 있는 모든 매개 변수를 표시합니다. 매개 변수는 매개 변수 유형에 따라 탭 및 범주별로 그룹화됩니다. 제공되는 탭은 정보, 구성, 진단 및 통계 탭입니다. BACS 인터페이스는 상황에 맞는 인터페이스이기 때문에 선택한 개체에 적용되는 매개 변수만 컨텍스트 보기 창에서 확인 및 구성할 수 있습니다.

## 메뉴 모음

메뉴 모음에 다음 항목이 나타나지만, 메뉴 모음은 상황에 따라 변하므로 모든 항목이 동시에 나타나지는 않습니다.

### 파일 메뉴

- 다른 이름으로 팀 저장: 현재 팀 구성을 파일로 저장합니다.
- 팀 복원: 저장된 팀 구성을 파일에서 복원합니다.

### 동작 메뉴

- 호스트 제거: 선택한 호스트를 제거합니다.
- 호스트 새로 고침: 선택한 호스트를 새로 고칩니다.

### 보기 메뉴

- 탐색기 보기: 탐색기 보기 창을 표시하거나 숨깁니다.
- 도구 모음: 도구 모음을 표시하거나 숨깁니다.
- 상태 표시줄: 상태 표시줄을 표시하거나 숨깁니다.
- Broadcom 로고: BACS의 Broadcom 로고를 표시하거나 숨깁니다. 이때 최대 표시 공간을 최적화할 수 있습니다.

### 도구 메뉴

- 옵션: BACS 기본 설정 구성에 사용됩니다.

### 팀(Windows만 해당)

- 팀 생성: 팀 구성 마법사 또는 고급 모드를 사용하여 새 팀을 생성합니다.
- 팀 관리: 팀 구성 마법사 또는 고급 모드를 사용하여 기존 팀을 관리합니다.

## 설명 창

설명 창은 컨텍스트 보기 창에서 선택한 매개 변수에 대한 정보, 구성 지침 및 옵션을 제공합니다.

## Windows에서 기본 설정 구성

Windows에서 BACS 트레이 아이콘을 사용하거나 사용하지 않으려면 다음을 수행합니다.

Windows 시스템에서 프로그램을 설치하면 Windows 작업 표시줄에 BACS의 아이콘이 배치됩니다. 옵션 창을 사용하여 이 아이콘을 설정하거나 해제할 수 있습니다.

1. 도구 메뉴에서 **옵션**을 선택합니다.
2. **BACSTray** 아이콘 사용(이 옵션은 기본적으로 사용됨)을 선택하거나 선택을 취소합니다.
3. **확인**을 클릭합니다.

### Windows에서 팀 구성 모드 설정

1. 도구 메뉴에서 **옵션**을 선택합니다.
2. 팀을 생성할 때 팀 구성 마법사의 지원이 필요하지 않으면 **전문가 모드**를 선택하고, 그렇지 않으면 **마법사 모드**를 선택합니다.
3. **확인**을 클릭합니다.

### Windows에서 탐색기 보기 새로 고침 시간 설정

1. 도구 메뉴에서 **옵션**을 선택합니다.
2. 탐색기 보기 새로 고침 시간을 5초로 설정하려면 **자동**을 선택합니다. 그렇지 않으면 사용자 정의를 선택하고 원하는 시간(초 단위)을 선택합니다.
3. **확인**을 클릭합니다.

---

## 호스트에 연결

여러 Windows 또는 Linux 호스트를 추가하여 BACS에서 관리할 수 있습니다.

### 로컬 호스트를 추가하려면

1. 동작 메뉴에서 **호스트 추가**를 클릭합니다.
2. 두 Windows 및 Linux 호스트에 대해 기본 설정을 변경하지 마십시오. 로컬 호스트에 연결하는 동안 **사용자 이름**과 **암호**는 필요하지 않습니다.
3. BACS에서 이 호스트에 대한 정보를 저장하기를 원하면 **보존**을 선택합니다.
4. **확인**을 클릭합니다. BACS를 사용하여 해당 호스트를 확인 및 관리할 수 있습니다.

### 원격 호스트를 추가하려면

1. 동작 메뉴에서 **호스트 추가**를 클릭합니다.
2. **호스트** 상자에 원격 호스트 이름 또는 IP 주소를 입력합니다.
3. **프로토콜** 목록에서 프로토콜을 선택합니다. Windows용 프로토콜 옵션은 **WMI**, **WSMan** 또는 **모두 시도**입니다. Linux용 프로토콜 옵션은 **CimXML**, **WSMan** 또는 **모두 시도**입니다. **모두 시도** 옵션은 GUI 클라이언트에 모든 옵션을 시도하도록 합니다.
4. 보안을 강화하려면 **HTTP** 체계 또는 **HTTPS** 체계를 선택합니다.
5. 호스트를 구성할 때 사용한 **포트 번호** 값을 입력합니다(기본값 **5985**와 다른 경우).
6. **사용자 이름**과 **암호**를 입력합니다.
7. BACS에서 이 호스트에 대한 정보를 저장하기를 원하면 **보존**을 선택합니다. BACS를 다시 열 때마다 탐색기 창에 호스트가 나타나며, 호스트에 연결할 때 호스트 IP 주소나 호스트 이름을 입력하지 않아도 됩니다. 보안상의 이유로 **사용자 이름**과 **암호**는 매번 입력해야 합니다.
8. **확인**을 클릭합니다.

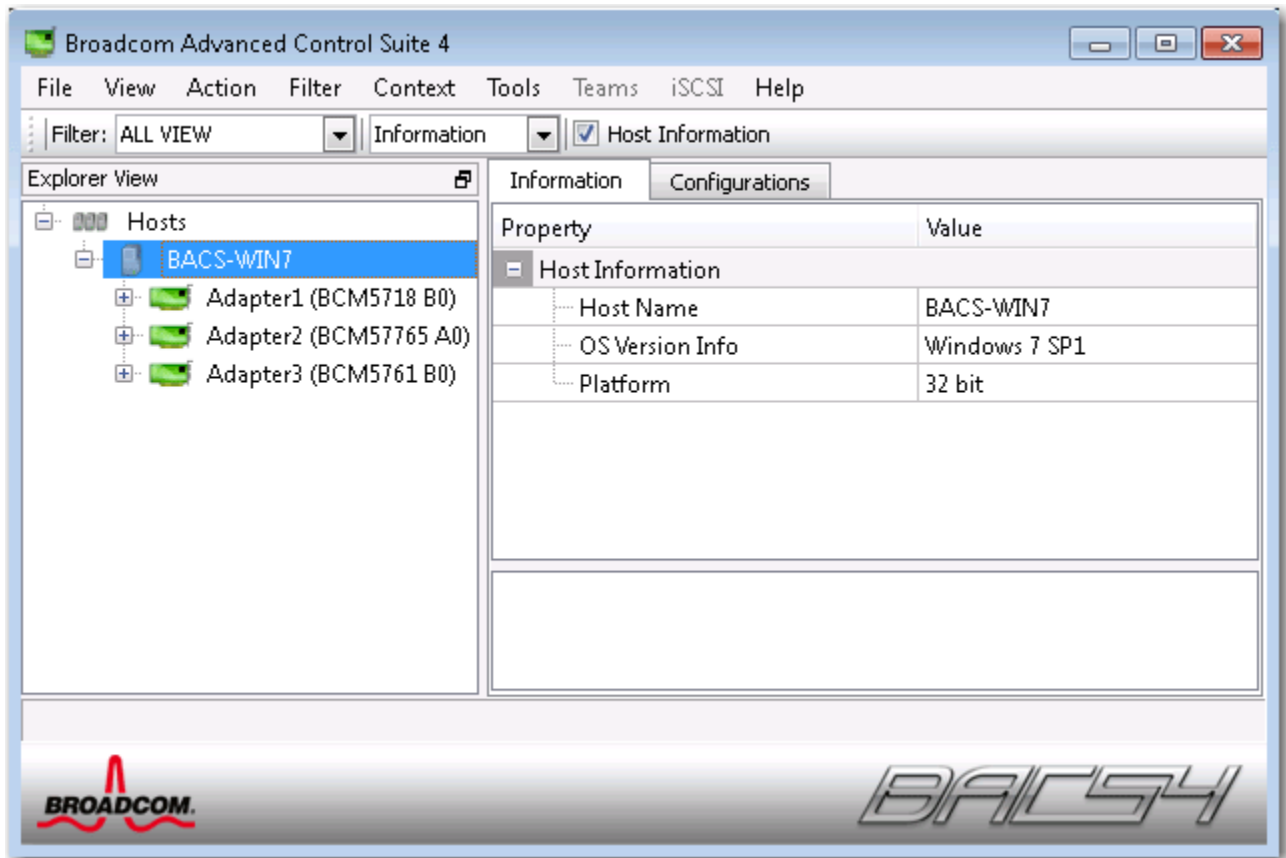
## 호스트 관리

호스트 수준에서, 다음 탭에서 호스트 정보를 확인하고 매개 변수를 구성할 수 있습니다.

- 정보
- 구성

호스트 정보를 확인하려면

탐색기 보기 창에서 호스트를 선택한 다음 호스트 수준 정보를 보려면 **정보** 탭을 선택합니다.



### 정보 탭: 호스트 정보

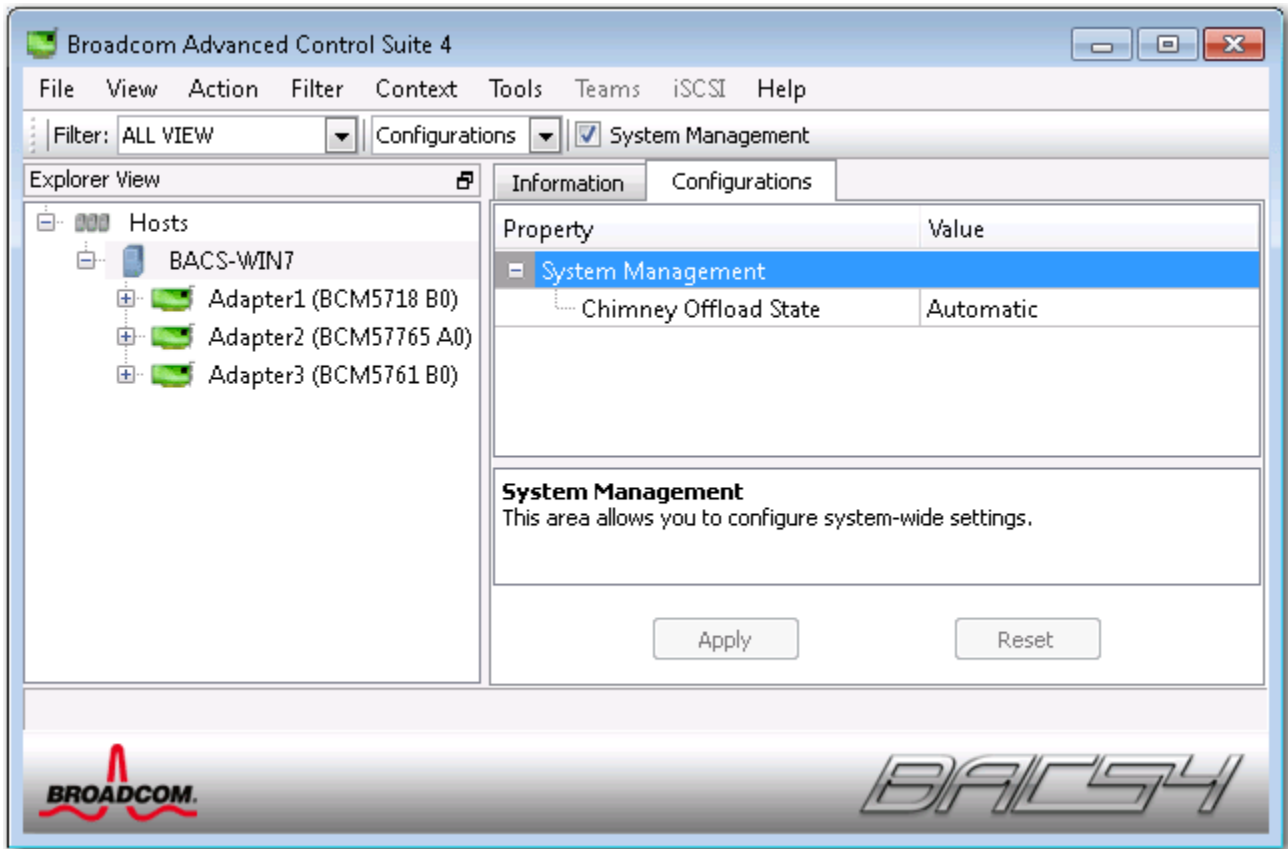
**호스트 이름** . 호스트의 이름을 표시합니다.

**OS 버전 정보** . 운영 체제와 버전을 표시합니다.

**플랫폼** . 하드웨어 아키텍처 플랫폼을 표시합니다(예: 32비트 또는 64비트).

호스트를 구성하려면

탐색기 보기 창에서 호스트를 선택한 다음 호스트 수준 매개 변수를 구성하려면 구성 탭을 선택합니다.



## 네트워크 어댑터 관리

설치된 네트워크 어댑터가 탐색기 보기 창의 계층 트리에 호스트 아래 수준에 나타납니다. 어댑터 수준에서, 다음 탭에서 정보를 확인하고 매개 변수를 구성할 수 있습니다.

- 정보
- 구성

### 어댑터 정보 확인

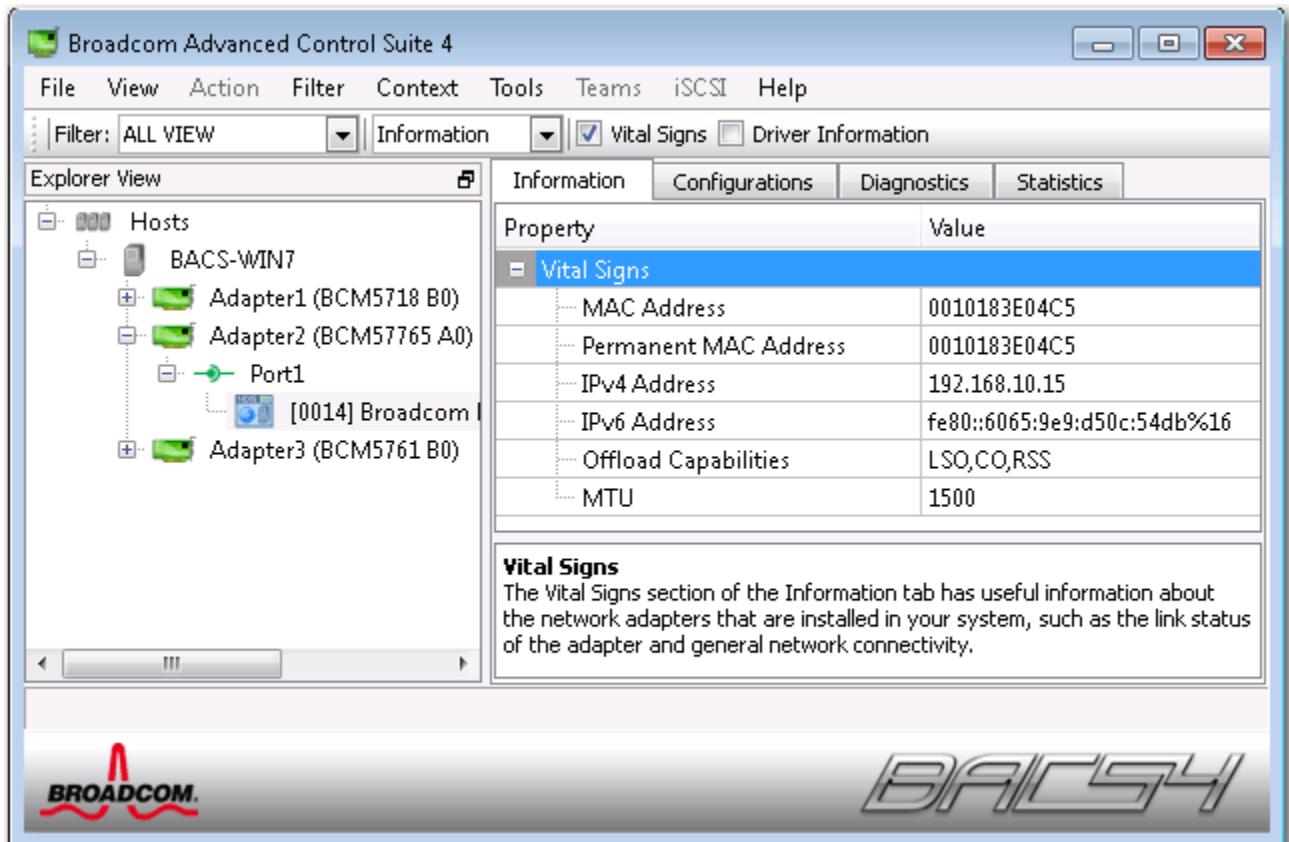
정보 탭의 주요 징후 섹션에는 어댑터 링크 상태 및 일반 네트워크 연결 같이 사용 중인 시스템에 설치된 네트워크 어댑터에 대한 유용한 정보가 있습니다.

탐색기 보기 창에서 네트워크 어댑터를 선택한 다음 어댑터 수준 정보를 보려면 **정보** 탭을 선택합니다.



설명 :

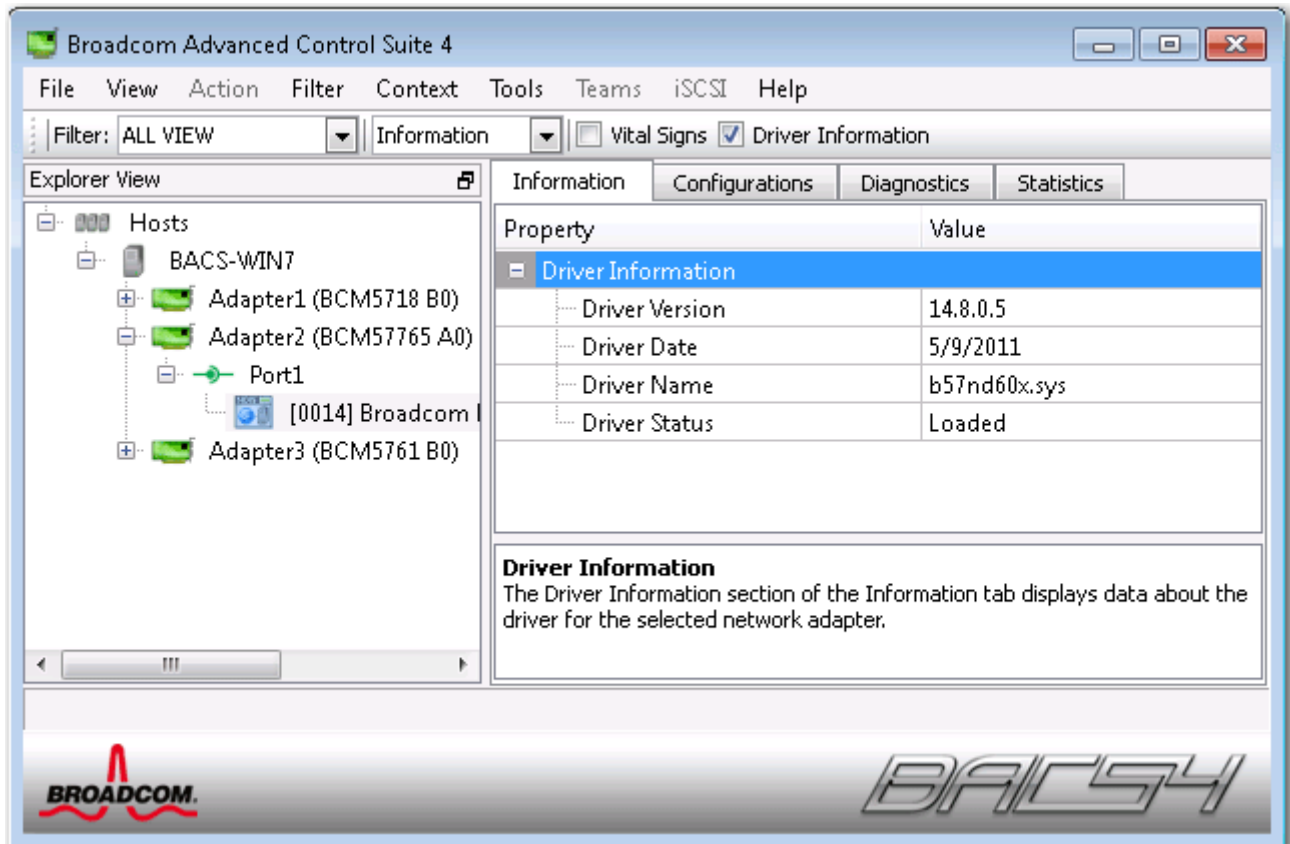
- Broadcom 네트워크에 대한 정보가 타사 네트워크 어댑터에 대한 정보보다 더욱 포괄적일 수 있습니다.
- 일부 정보는 모든 Broadcom 네트워크 어댑터에 대해 표시되지 않습니다.



## 드라이버 정보 보기

정보 탭의 드라이버 정보 섹션에는 선택한 네트워크 어댑터의 드라이버 데이터가 표시됩니다.

설치된 네트워크 어댑터에 대한 드라이버 정보를 확인하려면 탐색기 보기 창에 나열된 어댑터 이름을 클릭하고 정보 탭을 클릭합니다.



**드라이버 상태** . 어댑터 드라이버의 상태입니다.

- **로드됨** . 정상 작동 모드입니다. 어댑터 드라이버가 Windows에서 로드되어 작동되고 있습니다.
- **로드되지 않음** . 어댑터와 연결된 드라이버가 Windows에서 로드되지 않았습니다.
- **정보를 사용할 수 없음** . 어댑터와 연결된 드라이버에서 값을 가져올 수 없습니다.

**드라이버 이름** . 어댑터 드라이버의 파일 이름입니다.

**드라이버 버전** . 어댑터 드라이버의 현재 버전입니다.

**드라이버 날짜** . 어댑터 드라이버를 생성한 날짜입니다.



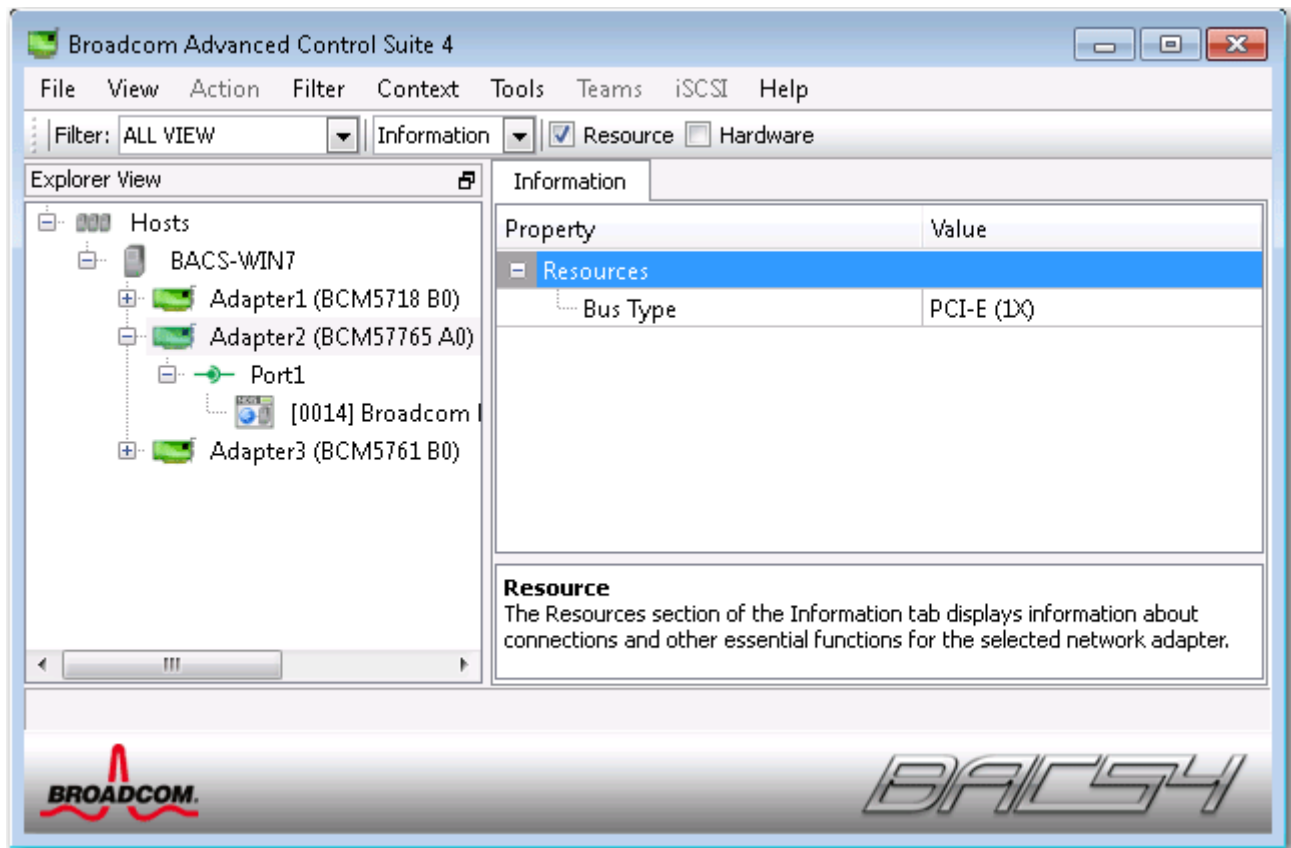
## 리소스 정보 보기

정보 탭의 리소스 섹션에는 선택한 네트워크 어댑터에 대한 연결 및 기타 필수 기능 정보가 표시됩니다.

설치된 네트워크 어댑터에 대한 리소스를 확인하려면 탐색기 보기 창에 나열된 어댑터 이름을 클릭하고 정보 탭을 클릭합니다.



**참고:** 일부 정보는 모든 Broadcom 네트워크 어댑터에 대해 표시되지 않습니다.



**버스 유형** . 어댑터에 사용된 입출력(I/O) 상호 연결 유형입니다.

**슬롯 번호** . 어댑터에 상주하는 시스템 보드의 슬롯 번호입니다. PCI Express 유형 어댑터에는 이 항목이 표시되지 않습니다.

**버스 속도 (MHz)** . 어댑터에 사용된 버스 클럭 신호 주파수입니다. PCI Express 유형 어댑터에는 이 항목이 표시되지 않습니다.

**버스 너비 (비트)** . 버스가 한 번에 어댑터와 송수신 가능한 비트 수입니다. PCI Express 유형 어댑터에는 이 항목이 표시되지 않습니다.

**버스 번호** . 어댑터가 설치된 버스 번호를 나타냅니다.

**장치 번호** . 운영 체제에서 어댑터에 할당된 번호입니다.

**기능 번호** . 어댑터의 포트 번호입니다. 포트가 한 개 달린 어댑터의 기능 번호는 0입니다. 2개의 포트 어댑터에서 첫 번째 포트의 기능 번호는 0이고, 두 번째 포트의 기능 번호는 1입니다.

**인터럽트 요청** . 어댑터와 연결된 인터럽트 회선 번호입니다. 유효한 번호는 2 ~ 25입니다.

**메모리 주소** . 어댑터에 할당된 메모리 매핑 주소입니다. 0 이외 값을 지정해야 합니다.

## 하드웨어 정보 보기

정보 탭의 하드웨어 섹션에는 선택한 네트워크 어댑터에 대한 하드웨어 설정 정보가 표시됩니다.

설치된 네트워크 어댑터에 대한 하드웨어를 확인하려면 탐색기 보기 창에 나열된 어댑터 이름을 클릭하고 정보 탭을 클릭합니다.



**참고:** 일부 정보는 모든 Broadcom 네트워크 어댑터에 대해 표시되지 않습니다.

The screenshot shows the Broadcom Advanced Control Suite 4 application window. The 'Information' tab is active, and the 'Hardware' section is expanded. The left pane shows a tree view with 'Hosts' > 'BACS-WIN7' > 'Adapter1 (BCM5718 B0)'. The right pane displays a table of hardware properties and their values.

| Property             | Value          |
|----------------------|----------------|
| <b>Hardware</b>      |                |
| ASIC Version         | BCM57765 A0    |
| Firmware Version     | 57765-v1.46    |
| Management Firmware  | BRCM ASF v8.23 |
| Vendor ID            | 0x14e4         |
| Device ID            | 0x16b4         |
| Sub-System Vendor ID | 0x14e4         |
| Sub System ID        | 0x16b4         |

Below the table, there is a 'Hardware' section with the following text: "The Hardware section of the Information tab displays information about the hardware settings for the selected network adapter."

**ASIC 버전** . Broadcom 어댑터의 칩 버전입니다. 이 정보는 타사가 제조한 어댑터에서는 표시되지 않습니다.

**펌웨어 버전** . Broadcom 어댑터의 펌웨어 버전입니다. 이 정보는 타사가 제조한 어댑터에 대해서는 표시되지 않습니다. 이 정보는 Broadcom NetXtreme 어댑터에 대해서만 표시됩니다.

**공급업체 ID**. 공급업체 ID입니다.

**장치 ID**. 어댑터 ID입니다.

**하위 시스템 공급업체 ID**. 하위 시스템 공급업체 ID입니다.

**하위 시스템 ID**. 하위 시스템 ID입니다.

## 네트워크 테스트

진단 탭의 **네트워크 테스트** 옵션을 사용하여 IP 네트워크 연결을 확인할 수 있습니다. 이 테스트에서는 드라이버가 올바르게 설치되어 있는지 확인하고 동일한 서브넷에 있는 게이트웨이 또는 지정된 다른 IP 주소로의 연결을 테스트합니다. 네트워크 테스트에서는 TCP/IP를 사용하여 ICMP 패킷을 원격 시스템에 보낸 다음 응답을 기다립니다.



**참고:** 한 팀으로 그룹화된 어댑터에 대해서는 네트워크 테스트 옵션을 사용할 수 없습니다([팀 구성](#) 참조).

### 네트워크 테스트를 실행하려면

1. 탐색기 보기 창에서 테스트할 어댑터 이름을 클릭합니다.
2. **실행할 테스트 선택** 목록에서 **네트워크 테스트**를 선택합니다. **네트워크 테스트** 옵션을 사용할 수 없으면 창 오른쪽의 **컨텍스트 보기** 탭에서 **진단**을 선택하고 **네트워크 테스트**를 선택합니다.
3. 대상 IP 주소를 변경하려면 **Ping을 실행할 IP 주소**를 선택합니다. 네트워크 테스트 창에 대상 IP 주소를 입력하고 **확인**을 클릭합니다.
4. **테스트**를 클릭합니다.

**상태** 필드에 네트워크 테스트 결과가 표시됩니다.

## 진단 테스트 실행

진단 탭의 **진단 테스트** 옵션을 사용하여 Broadcom 네트워크 어댑터에 있는 물리적 구성 요소의 상태를 확인할 수 있습니다. 테스트를 수동으로 실행할 수도 있고 BACS 3에서 계속해서 수행하도록 선택할 수도 있습니다. 테스트가 계속해서 수행되는 경우에는 테스트를 수행할 때마다 각 테스트의 **결과** 필드에 있는 통과 및 실패 횟수가 증가합니다. 예를 들어, 테스트가 4번 수행되고 실패가 없는 경우 해당 테스트에 대한 **결과** 필드의 값은 4/0입니다. 그러나, 통과가 3번이고 실패가 1번인 경우 **결과** 필드의 값은 3/1입니다.



### 설명 :

- 진단 테스트를 실행하려면 관리자 권한이 있어야 합니다.
- 이러한 테스트가 실행되는 동안 네트워크 연결은 일시적으로 중단됩니다.
- 각 테스트를 지원하지 않는 Broadcom 어댑터도 있습니다.

### 진단 테스트를 한 번만 실행하려면

1. 탐색기 보기 창에서 테스트할 어댑터 이름을 클릭하고 진단 탭을 선택합니다.
2. **실행할 테스트 선택** 목록에서 **진단 테스트**를 선택합니다.
3. 실행할 진단 테스트를 선택합니다. **모두 선택**을 클릭하여 모든 테스트를 선택하거나 **모두 지우기**를 클릭하여 모든 테스트의 선택을 취소합니다.
4. **루프 수**에서 테스트를 실행할 횟수를 선택합니다.
5. **테스트 실행**을 클릭합니다.
6. 네트워크 연결이 일시적으로 중단된다고 경고하는 오류 메시지 창에서 **예**를 클릭합니다. 각 테스트의 **결과** 필드에 결과가 표시됩니다.

**제어 레지스터** . 이 테스트에서는 레지스터에 여러 값을 쓰고 결과를 확인하여 네트워크 어댑터 레지스터의 읽기 및 쓰기 기능을 검사합니다. 어댑터 드라이버는 이 레지스터를 사용하여 정보 전송 및 수신과 같은 네트워크 기능을 수행합니다. 테스트에 실패한 경우, 장치가 올바르게 작동하지 않는 것입니다.

**MII 레지스터** . 이 테스트에서는 물리적 계층(PHY)의 레지스터에 대한 읽기 및 쓰기 기능을 검사합니다. 물리 계층은 회선의 전기 신호를 제어하고 1000Mbit/s 정도의 네트워크 속도를 구성하는 데 사용됩니다.

**EEPROM** . 이 테스트에서는 EEPROM의 일부를 읽고 **Checksum**을 계산하여 전자적으로 지울 수 있는 프로그래밍 가능 읽기 전용 메모리(EEPROM)의 내용을 확인합니다. 계산된 **Checksum**이 EEPROM에 저장된 **Checksum**과 다르면 테스트가 실패합니다. EEPROM 이미지를 업그레이드하는 경우 이 테스트에 대한 코드를 변경할 필요가 없습니다.

**내부 메모리** . 이 테스트에서는 어댑터의 내부 메모리가 올바르게 작동하는지 검사하며, 메모리에 패턴 값을 쓰고 결과를 한 번 더 읽습니다. 오류 값을 한 번 더 읽으면 테스트가 실패합니다. 내부 메모리가 올바르게 작동하지 않으면 장치가 작동할 수 없습니다.

**칩 내장 CPU** . 이 테스트에서는 어댑터에서 내부 CPU의 작동을 검사합니다.

**일시 중지** . 이 테스트에서는 네트워크 장치 드라이버 인터페이스 사양(NDIS) 드라이버가 어댑터에서 인터럽트를 수신할 수 있는지 검사합니다.

**루프백 MAC** . NDIS 드라이버가 어댑터로 패킷을 전송하고 어댑터로부터 패킷을 수신할 수 있는지 확인하는 테스트입니다.

**루프백 PHY** . NDIS 드라이버가 어댑터로 패킷을 전송하고 어댑터로부터 패킷을 수신할 수 있는지 확인하는 테스트입니다.

**LED 테스트** . 모든 포트 LED가 5번 깜박이도록 하여 어댑터를 확인합니다.

## 케이블 분석

진단 탭의 **케이블 분석 옵션**을 사용하여 Ethernet 네트워크의 Ethernet 카테고리 5 케이블 연결에서 각 쌍 회로의 상태를 모니터링할 수 있습니다. 분석은 케이블 품질을 측정하고 IEEE 802.3ab에 대해 사양을 비교합니다.



### 설명 :

- 케이블 분석 테스트를 실행하려면 관리자 권한이 있어야 합니다.
- 네트워크 연결은 분석 동안 일시적으로 중단됩니다.
- **Broadcom NetXtreme** 어댑터의 경우 연결이 없을 때 **Gigabit** 연결 속도 연결에 대해 케이블 분석 테스트만 실행할 수 있습니다.
- 일부 **Broadcom** 네트워크 어댑터에 대해서는 이 옵션을 사용할 수 없습니다.

### 케이블 분석을 실행하려면

1. 포트가 **자동**으로 설정되어 있고 **Speed & Duplex** 드라이버 설정도 **자동**으로 설정되어 있는 스위치의 포트에 케이블을 연결하십시오.
2. 탐색기 보기 창에서 테스트할 어댑터 이름을 클릭합니다.
3. **실행할 테스트 선택** 목록에서 **케이블 분석**을 선택합니다. **케이블 분석** 옵션을 사용할 수 없으면 창 오른쪽의 **컨텍스트 보기** 탭에서 **진단**을 선택하고 **케이블 분석**을 선택합니다.
4. **실행**을 클릭합니다.
5. 네트워크 연결이 일시적으로 중단된다고 경고하는 오류 메시지 창에서 **예**를 클릭합니다.

**거리** . 유효한 케이블 거리(미터)입니다(**Noise** 결과가 반환되는 경우는 제외).

**상태** . 이 케이블 쌍의 링크 유형을 나타냅니다.

- **Good**. 케이블/PCB 신호 경로 상태 양호, Gigabit 링크 없음.
- **Crossed**. 둘 이상의 케이블/PCB 신호 경로에서 핀 샷 또는 혼선 발생.
- **Open**. 트위스트 페어에서 하나 또는 두 개의 핀이 열려 있음.
- **Short**. 동일한 트위스트 페어의 두 개 핀 샷.
- **Noise**. 영구적 소음 있음(강제 10/100으로 인한 가장 일반적인 원인).
- **GB Link**. Gigabit 링크 가동 및 실행 중.
- **N/A**. 알고리즘에서 결과를 내지 못 함

**연결됨** . 링크 연결 속도 및 이중 모드입니다.

**상태** . 테스트 실행 후의 상태(완료됨 또는 실패)입니다.

테스트 결과에 영향을 미칠 수 있는 다음의 여러 가지 요인이 있습니다.

- **링크 파트너**. 다양한 스위치 및 허브 제조업체에서 다른 PHY를 구현함. 일부 PHY는 IEEE와 호환되지 않습니다.
- **케이블 품질**. Category 3, 4, 5 및 6이 테스트 결과에 영향을 미칠 수 있음
- **전기적 간섭**. 테스트 환경이 테스트 결과에 영향을 미칠 수 있음

## 어댑터 속성 설정

구성 탭의 **고급**을 사용하여 선택한 어댑터의 사용 가능한 속성 값을 확인하고 변경할 수 있습니다. 잠재적으로 사용 가능한 속성 및 해당 설정은 다음과 같습니다.



### 설명 :

- 속성 값을 변경하려면 관리자 권한이 있어야 합니다.
- 특정 어댑터의 사용 가능한 속성 목록이 다를 수 있습니다.
- Broadcom 네트워크 어댑터의 종류에 따라 일부 속성이 표시되지 않을 수 있습니다.

### 어댑터 속성을 설정하려면

1. 탐색기 보기 창에서 어댑터 이름을 클릭하고 **구성** 탭을 클릭합니다.
2. **고급** 섹션에서 설정할 속성을 선택합니다.
3. 속성의 값을 변경하려면 속성 목록에서 항목을 선택하거나 적합한 새 값을 입력합니다(선택 옵션은 속성에 따라 다름).
4. 모든 속성의 변경 사항을 확인하려면 **적용**을 클릭합니다. 속성을 원래 값으로 되돌리려면 **다시 설정**을 클릭합니다.

**802.1p QoS.** 서비스 품질을 활성화합니다. 서비스 품질은 트래픽 유형에 따라 필요한 수준 또는 신뢰성 및 지연을 보장하기 위해 다른 네트워크 트래픽 유형을 다르게 처리하는 IEEE 사양입니다. 이 속성은 기본적으로 **Disable**입니다. 네트워크 인프라가 QoS를 지원하지 않는 경우 이 속성을 활성화해서는 안 됩니다. 활성화하면 문제가 발생할 수 있습니다.

**Flow Control.** PAUSE 프레임의 수신 또는 전송을 활성화 또는 비활성화합니다. PAUSE 프레임을 사용하면 네트워크 어댑터와 스위치로 전송 속도를 제어할 수 있습니다. PAUSE 프레임을 수신하는 쪽에서 일시적으로 전송을 중지합니다.

- **Auto**(기본값). PAUSE 프레임 수신 및 전송이 최적화됩니다.
- **Disable.** PAUSE 프레임 수신 및 전송이 비활성화됩니다.
- **Rx PAUSE.** PAUSE 프레임 수신이 활성화됩니다.
- **Rx/Tx PAUSE.** PAUSE 프레임 수신 및 전송이 활성화됩니다.
- **Tx PAUSE.** PAUSE 프레임 전송이 활성화됩니다.

**Speed & Duplex.** Speed & Duplex 속성은 연결 속도 및 모드를 네트워크의 연결 속도 및 모드로 설정합니다. Full-Duplex 모드에서는 어댑터가 네트워크 데이터를 전송하면서 동시에 수신할 수 있습니다.

- **10Mb Full.** 속도를 10Mbit/s로 설정하고 모드를 Full-Duplex로 설정합니다.
- **10Mb Half.** 속도를 10Mbit/s로 설정하고 모드를 Half-Duplex로 설정합니다.
- **100Mb Full.** 속도를 100Mbit/s로 설정하고 모드를 Full-Duplex로 설정합니다.
- **100Mb Half.** 속도를 100Mbit/s로 설정하고 모드를 Half-Duplex로 설정합니다.
- **Auto**(기본값). 최적의 네트워크 연결이 가능하도록 속도 및 모드를 설정합니다(권장).

**설명 :**

- **Auto**를 선택하는 것이 좋습니다. 이를 선택하면 네트워크 어댑터가 네트워크의 회선 속도를 동적으로 검색할 수 있습니다. 네트워크 성능이 변경될 때마다 네트워크 어댑터가 자동으로 감지하고 새 회선 속도와 이중 모드를 조정합니다. 속도가 지원되면 **Auto**를 선택하여 **1Gbit/s** 속도가 사용됩니다.
- **1Gb Full Auto**는 1Gb 연결을 지원하는 링크 파트너에 연결해야 합니다. 연결은 1Gb 연결로만 제한되므로 **Ethernet@Wirespeed** 기능은 비활성화됩니다. 링크 파트너가 1Gb 연결만 지원할 경우 **Wake on LAN** 기능이 작동하지 않을 수 있습니다. 또한 운영 체제 부재 시의 관리 트래픽에도 영향을 줄 수 있습니다.
- **10Mb Half** 및 **100Mb Half** 설정은 네트워크 어댑터를 **Half-Duplex** 모드 상태로 네트워크에 강제 연결합니다. 네트워크가 같은 모드에서 작동하도록 구성되지 않으면 네트워크 어댑터가 작동되지 않을 수 있습니다.
- **10Mb Full** 및 **100Mb Full** 설정은 네트워크 어댑터를 **Full-Duplex** 모드 상태로 네트워크에 강제 연결합니다. 네트워크가 같은 모드에서 작동하도록 구성되지 않으면 네트워크 어댑터가 작동되지 않을 수 있습니다.

**Wake Up Capabilities.** 네트워크 어댑터에서 네트워크 절전 모드 해제 프레임 수신한 경우 저전력 모드에서 해제되도록 할 수 있습니다. 두 가지 유형의 절전 모드 해제 프레임, **Magic Packet** 및 **Wake Up Frame**이 가능합니다.

이 속성은 Broadcom NetXtreme 어댑터에 대해서만 사용할 수 있습니다.

- **Both**(기본값). 절전 모드 해제 프레임으로 **Magic Packet** 및 **Wake Up Frame**을 모두 선택합니다.
- **Magic Packet**. 절전 모드 해제 프레임으로 **Magic Packet**을 선택합니다.
- **None**. 절전 모드 해제 프레임을 선택하지 않습니다.
- **Wake-up Frame**. 절전 모드 해제 프레임으로 **Wake Up Frame**을 선택하고 네트워크 어댑터가 **Ping** 또는 **ARP**(주소 분해 프로토콜) 요청과 같은 이벤트를 수신한 경우 컴퓨터의 절전 모드를 해제할 수 있습니다. 이 옵션은 운영 체제의 절전 모드와 함께 사용되며 **Power Save**(절전) 설정에서 **WOL**이 활성화되지 않으면 작동하지 않습니다.

**우선 순위 & VLAN.** 네트워크 트래픽 및 VLAN 태그의 우선 순위를 모두 지정할 수 있습니다. VLAN ID 설정이 0(영)이 아닌 값으로 구성된 경우 VLAN 태그만이 발생합니다.

- **우선 순위 & VLAN 활성화(기본값).** 패킷 우선 순위 지정 및 VLAN 태그 허용
- **우선 순위 & VLAN 비활성화.** 패킷 우선 순위 지정 및 VLAN 태그 허용 안 함
- **우선 순위 활성화.** 패킷 우선 순위 지정만 허용
- **VLAN 활성화.** VLAN 태그만 허용



**참고:** 중급 드라이버가 VLAN 태그용 네트워크 어댑터를 관리하는 경우 **우선 순위 & VLAN 비활성화** 및 **우선 순위 활성화** 설정을 사용할 수 없습니다. **우선 순위 & VLAN 활성화** 설정을 사용하여 **VLAN ID**를 0(영)으로 변경합니다.

**VLAN ID.** 우선 순위 & VLAN 활성화가 우선 순위 & VLAN 설정으로 선택되면 VLAN 태그를 활성화하고 VLAN ID를 구성합니다. VLAN ID의 범위는 1부터 4094까지이며 연결된 스위치의 VLAN 태그 값과 일치해야 합니다. 이 필드의 0값(기본값)은 VLAN 태그를 활성화합니다.

#### NDIS 미니포트 드라이버를 통한 VLAN 태그의 위험 평가

Broadcom의 NDIS 6.0 미니포트 드라이버는 Broadcom 어댑터가 포함된 시스템이 태그가 지정된 VLAN에 연결되도록 합니다. 그러나 **BASP**와는 달리 VLAN 참여에 대한 NDIS 6 드라이버는 단일 VLAN ID만을 지원합니다.

또한 **BASP**와는 달리 NDIS 6.0 드라이버는 아웃바운드 패킷의 VLAN 태그만을 제공하나 VLAN ID 멤버십에 근거하여 들어오는 패킷의 필터링은 지원하지 않습니다. 이는 모든 미니포트 드라이버의 기본 동작입니다. VLAN 멤버십 기반 필터링 패킷의 부족이 보안 문제를 야기할 수 있는 반면 다음은 IPv4 네트워크에 대하여 이 드라이버 한계에 근거한 위험 평가를 제공합니다.

여러 VLAN이 있는 올바르게 구성된 네트워크는 각 VLAN별로 분리된 IP 세그먼트가 있어야 합니다. 이는 아웃바운드 트래픽이 라우팅 테이블에 의존하여 트래픽을 전달할 어댑터(가상의 또는 물리적)를 확인하며 VLAN 멤버십 기반의 어댑터를 결정하지 않으므로 꼭 필요합니다.

Broadcom의 NDIS 6.0 드라이버 상의 VLAN 태그 지원이 전송(Tx) 트래픽에만 한정되므로 운영 체제로 전달되는 다른 VLAN으로부터 들어오는 트래픽(Rx)에 위험이 있습니다. 그러나 위의 올바르게 구성된 네트워크에 근거하여 IP 조

각 및/또는 스위치 VLAN 구성은 위험을 제한하는 추가적인 필터링을 제공할 수 있습니다.

지속적인 연결 시나리오에서 동일한 IP 세그먼트 상에 있는 두 대의 컴퓨터는 VLAN 멤버십 필터링이 발생하지 않으므로 VLAN 구성에 관계 없이 통신할 수 있습니다. 그러나 이러한 연결 유형은 VLAN 환경에서 일반적인 것이 아니므로 이 시나리오는 보안이 이미 파괴되었을 수 있음을 가정합니다.

위의 위험이 바람직하지 않거나 VLAN ID 멤버십을 필터링해야 하는 경우 중급 드라이버로 지원해야 합니다.

## 통계 보기

통계 탭에 제공된 정보를 사용하여 Broadcom 네트워크 어댑터와 타사 네트워크 어댑터 모두의 트래픽 통계를 확인할 수 있습니다. 통계 정보와 그 범위는 Broadcom 어댑터가 더 포괄적입니다.

설치된 네트워크 어댑터에 대한 통계 정보를 확인하려면 탐색기 보기 창에 나열된 어댑터 이름을 클릭하고 통계 탭을 클릭합니다.

각 통계의 최신 값을 가져오려면 **새로 고침**을 클릭합니다. 모든 값을 0으로 변경하려면 **다시 설정**을 클릭합니다.



### 설명 :

- 팀 통계는 비활성화된 경우 Broadcom 네트워크 어댑터에 대해 컴파일되지 않습니다.
- Broadcom 네트워크 어댑터의 종류에 따라 일부 통계가 표시되지 않을 수 있습니다.

## 일반 통계

일반 통계는 어댑터로(부터) 전송되고 수신된 통계를 나타냅니다.

**성공적으로 전송된 프레임** . 성공적으로 전송된 프레임 수입니다. 이 숫자는 전송 상태가 성공적으로 전송으로 보고될 때 증가합니다.

**성공적으로 수신된 프레임** . 성공적으로 수신된 프레임 수입니다. 이 숫자에는 내부 MAC 하위 계층 오류로 인해 너무 긴 프레임, 프레임 검사 순서(FCS), 길이, 정렬 오류 또는 프레임 손실로 수신된 프레임은 포함되지 않습니다. 이 숫자는 수신 상태가 성공적으로 수신으로 보고될 때 증가합니다.

**전송된 직접 프레임** . 성공적으로 전송된 직접 데이터 프레임 수입니다.

**전송된 멀티캐스트 프레임** . 브로드캐스트 주소가 아닌 그룹 대상 주소로 성공적으로 전송된 프레임 수입니다(상태 값이 성공적으로 전송으로 표시됨).

**전송된 브로드캐스트 프레임** . 브로드캐스트 주소로 성공적으로 전송된 프레임 수입니다(전송 상태가 성공적으로 전송으로 표시됨). 멀티캐스트 주소로 전송된 프레임은 브로드캐스트 프레임이 아니며 제외됩니다.

**수신된 직접 프레임** . 성공적으로 수신된 직접 데이터 프레임 수입니다.

**수신된 멀티캐스트 프레임** . 성공적으로 수신했으며 브로드캐스트가 아닌 활성 그룹 주소로 전송되는 프레임 수입니다. 이 숫자에는 내부 MAC 하위 계층 오류로 인해 너무 긴 프레임, FCS, 길이, 정렬 오류 또는 프레임 손실로 수신된 프레임은 포함되지 않습니다. 이 숫자는 성공적으로 수신 상태로 표시될 때 증가합니다.



수신된 브로드캐스트 프레임 . 성공적으로 수신했으며 브로드캐스트 그룹 주소로 전송되는 프레임 수입입니다. 이 숫자에는 내부 MAC 하위 계층 오류로 인해 너무 긴 프레임, FCS, 길이, 정렬 오류 또는 프레임 손실로 수신된 프레임은 포함되지 않습니다. 이 숫자는 성공적으로 수신 상태로 표시될 때 증가합니다.

**CRC 오류와 함께 수신된 프레임** . 잘못된 CRC가 있는 프레임 수입입니다.

## 팀 구성

팀 구성 기능으로 네트워크 장치를 팀으로 작동하도록 함께 그룹화할 수 있으며 가상 NIC(단일 어댑터로 작동하는 여러 어댑터의 그룹)를 생성할 수 있습니다. 또한, 로드 균형 조정 및 장애 조치를 활성화할 수 있습니다. 팀을 구성하려면 **Broadcom Advanced Server Program(BASP)** 소프트웨어를 사용해야 합니다. 팀 구성 소프트웨어의 기술 및 구현 고려 사항에 대한 포괄적인 설명은 **Broadcom** 네트워크 어댑터 사용 설명서의 "**Broadcom Gigabit Ethernet** 팀 구성 서비스"를 참조하십시오.

팀 구성은 다음 방법 중 하나를 통해 완료됩니다.

- [Broadcom 팀 구성 마법사 사용](#)
- [전문가 모드 사용](#)



### 설명 :

- 팀 구성 프로토콜에 관한 자세한 내용은 **Broadcom** 네트워크 어댑터 사용 설명서의 "팀 구성"을 참조하십시오.
- 팀 구성 시 **LiveLink™**를 활성화하지 않는 경우 스위치에서 스페닝 트리 프로토콜(STP)을 비활성화하는 것이 좋습니다. 그러면 장애 조치 시 스페닝 트리 루프 결정으로 인한 시스템 종료 시간이 최소화됩니다. **LiveLink**는 이러한 문제를 완화합니다.
- **BASP**는 시스템에 하나 이상의 **Broadcom** 네트워크 어댑터가 설치되었을 경우에만 사용 가능합니다.
- 모든 멤버가 해당 기능을 지원하고 이를 위해 구성된 경우에만 **LSO(Large Send Offload)** 및 **Checksum Offload** 속성을 팀을 위해 사용할 수 있습니다.
- 팀을 생성 또는 수정하려면 관리자 권한이 있어야 합니다.
- 멤버가 다른 속도로 연결된 팀 환경에서 로드 균형 알고리즘은 임계값이 충족될 때까지 느린 속도 링크(100Mbps 또는 10Mbps)와 연결된 멤버보다 **Gigabit Ethernet** 링크와 연결된 멤버를 선호합니다. 이것은 제대로 작동함을 의미합니다.
- **WOL(Wake on LAN)**은 **Ethernet** 인터페이스를 통해 특정 패킷이 도착하면 시스템이 절전 모드에서 해제되도록 하는 기능입니다. 가상 어댑터는 소프트웨어 전용 장치로 구현되므로 **WOL** 기능을 구현할 수 있는 하드웨어 기능이 없기 때문에, 가상 어댑터를 통해 시스템을 절전 상태에서 해제할 수 없습니다. 그러나 물리적 어댑터는 어댑터가 팀의 일부인 경우에도 이 속성을 지원합니다.

## 팀 유형

다음과 같은 네 가지 유형의 로드 균형 조정 팀을 생성할 수 있습니다.

- **Smart Load Balancing** 및 장애 조치
- 링크 집계(802.3ad)
- 일반 트렁킹(FEC/GEC)/802.3ad-Draft Static
- **SLB(Auto-Fallback Disable)** - **Auto-Fallback Disable** 기능은 팀 구성 마법사에서 **Smart Load Balancing** 및 장애 조치 유형 팀에 대해 구성됩니다.

이러한 유형에 대한 설명은 **Broadcom® NetXtreme® BCM57XX 사용 설명서**에 있는 "로드 균형 조정 및 결함 허용"을 참조하십시오.

## Broadcom 팀 구성 마법사 사용

Broadcom 팀 구성 마법사를 사용하여 팀을 새로 만들거나 이미 팀을 만든 경우 기존 팀을 구성하거나 VLAN을 만들 수 있습니다.

**1.** 다음과 같이 팀을 생성하거나 편집합니다.

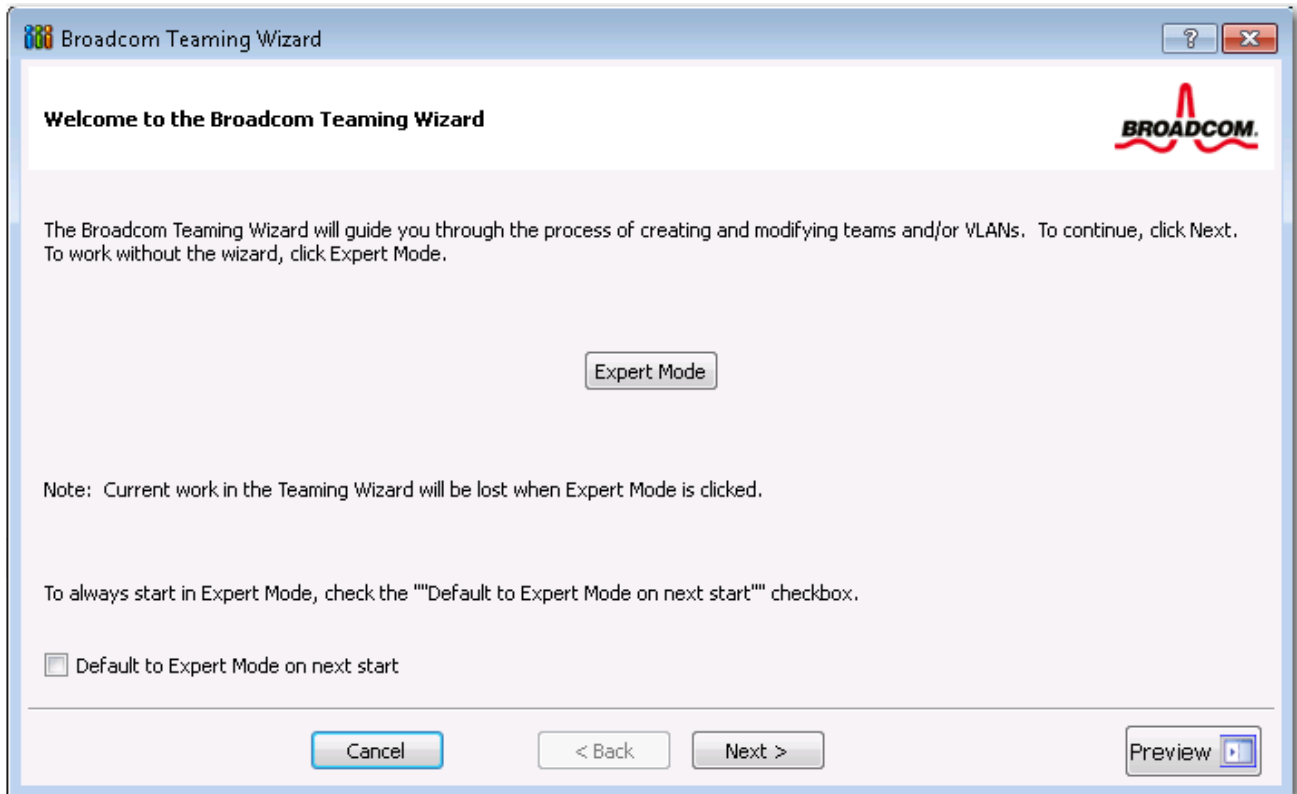
새 팀을 생성하려면 팀 메뉴에서 **팀 생성**을 선택하거나 "할당되지 않은 어댑터" 섹션에서 장치 중 하나를 마우스 오른쪽 단추로 클릭하고 **팀 생성**을 선택합니다. 할당되지 않은 어댑터 섹션에 나열된 장치가 없는 경우, 즉 모든 어댑터가 이미 팀에 할당된 경우에는 이 옵션을 사용할 수 없습니다.

기존 팀을 구성하려면 팀 목록에서 하나를 마우스 오른쪽 단추로 클릭하고 **팀 편집**을 선택합니다. 이 옵션은 팀이 이미 생성되어 팀 관리 창에 나열된 경우에만 사용할 수 있습니다.



**참고:** 마법사 없이 작업하려는 경우 **전문가 모드**를 클릭합니다. 팀을 생성할 때 항상 전문가 모드를 사용하려는 경우 **다음에 시작할 때 전문가 모드를 기본값으로 설정**을 선택합니다. [전문가 모드 사용](#)을 참조하십시오.

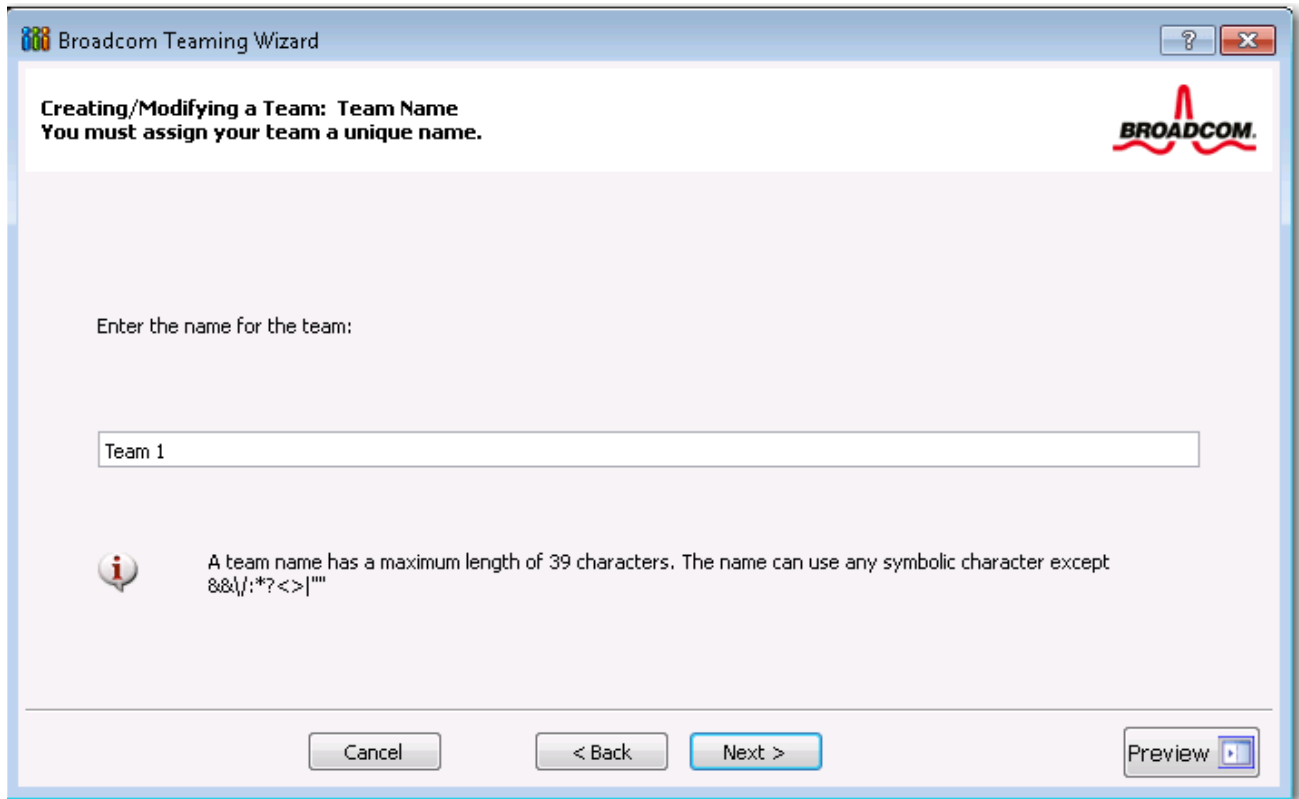
**2.** 마법사를 계속해서 사용하려면 **다음**을 클릭합니다.



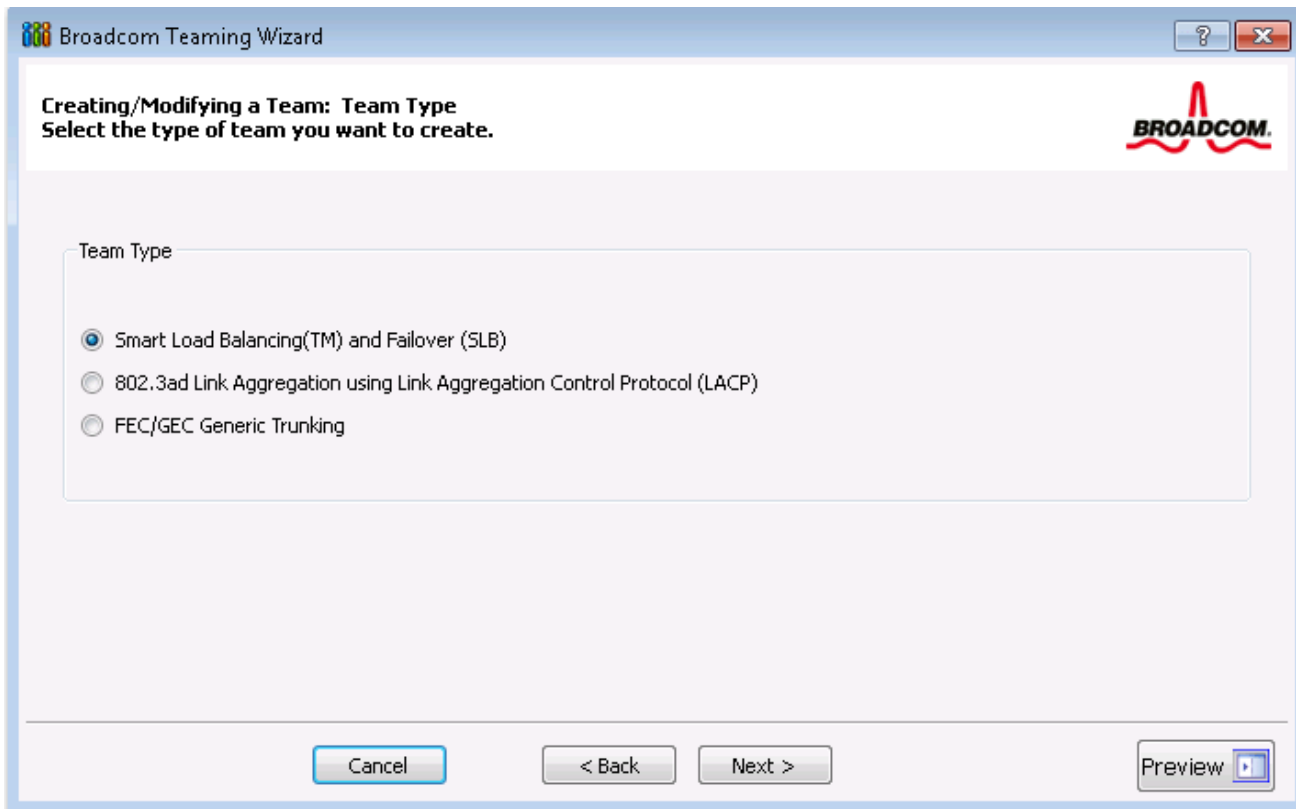
**3.** 팀 이름을 입력한 후 **다음**을 클릭합니다. 설정을 검토하거나 변경하려는 경우 **뒤로**를 클릭합니다. **취소**를 클릭하여 설정을 취소하고 마법사를 종료합니다.



**참고:** 팀 이름은 39자 미만이어야 하며 공백으로 시작할 수 없고 다음 문자가 포함될 수 없습니다. & \ / : \* ? < > |



4. 생성하려는 팀 유형을 선택합니다. 팀 유형이 SLB 유형의 팀이면 **다음**을 클릭합니다. 팀 유형이 SLB 유형의 팀이 아니면 대화 상자가 나타납니다. 팀 멤버에게 연결된 네트워크 스위치가 팀 유형에 맞게 올바르게 구성되어 있는지 확인한 다음 계속하려면 **확인**을 클릭합니다.



5. 사용 가능한 어댑터 목록에서 팀에 추가할 어댑터를 클릭한 다음 **추가**를 클릭합니다. 팀 멤버를 제거하려면 **팀 멤버** 목록에서 어댑터를 클릭한 다음 **제거**를 클릭합니다. **다음**을 클릭합니다.

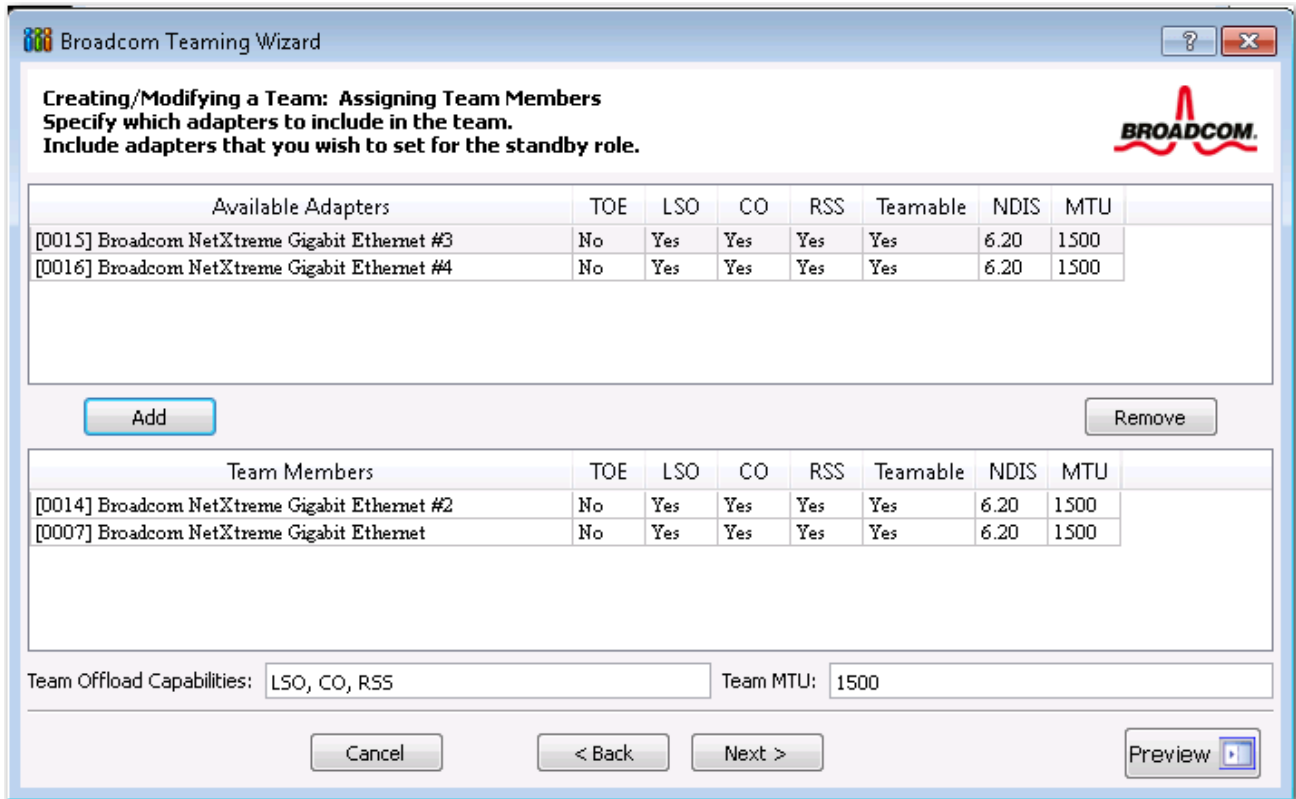


**참고:** 팀에는 Broadcom 네트워크 어댑터가 하나 이상 할당되어야 합니다.

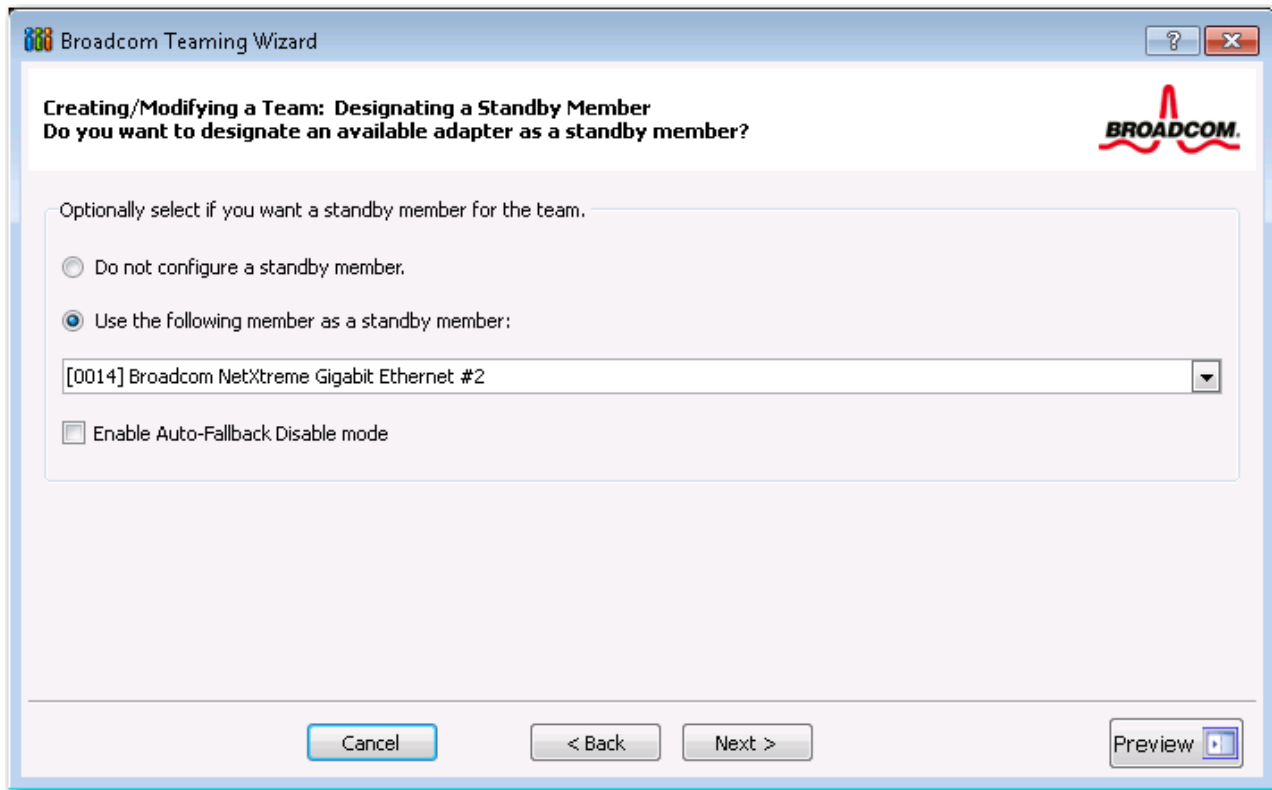
LSO(Large Send Offload)와 CO(Checksum Offload) 열은 어댑터에서 LSO 및/또는 CO 속성이 지원되는지 여부를 나타냅니다. 모든 멤버가 해당 기능을 지원하고 이를 위해 구성된 경우에만 팀을 위해 LSO 및 CO 속성을 사용할 수 있습니다. 이 경우 팀 Offload 기능은 화면 맨 아래에 나타납니다.



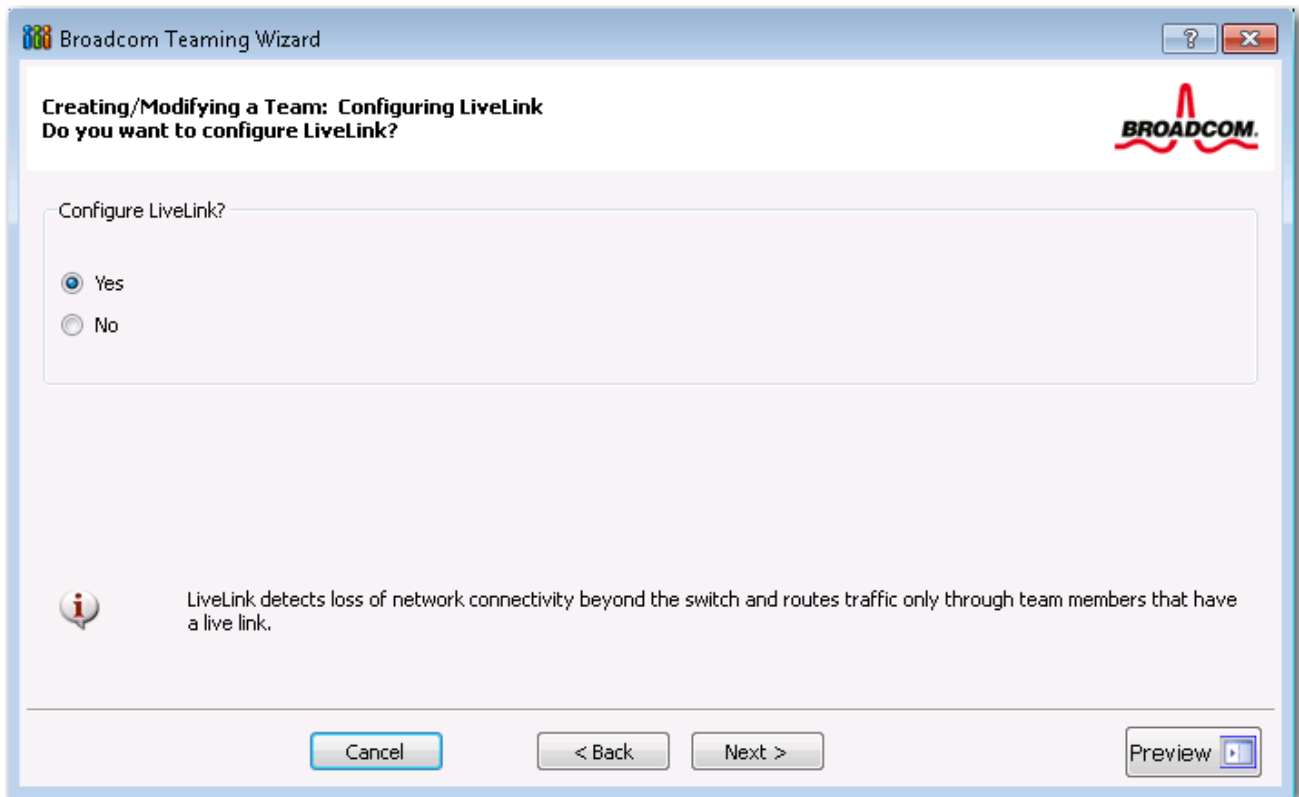
**참고:** 드라이버가 사용되지 않는 팀에 네트워크 어댑터를 추가하면 팀의 Offload 기능에 부정적인 영향을 끼칠 수 있습니다. 이는 팀의 성능에 영향을 끼칠 수 있습니다. 따라서 드라이버를 사용할 수 있는 네트워크 어댑터만을 팀 멤버로 추가하는 것이 좋습니다.



6. 어댑터 중 하나를 대기 멤버로 지정하려면(옵션) **다음 멤버를 대기 멤버로 사용하십시오.**를 선택하고 어댑터 목록에서 대기 멤버를 선택합니다.
7. **Auto-Fallback Disable** 모드 기능을 사용하여 기본 멤버가 복원되면 팀은 기본 멤버로 다시 스위칭하지 않고 대기 멤버를 사용하여 계속 진행할 수 있습니다. 이 기능을 활성화하려면 **Auto-Fallback Disable 모드 활성화**를 선택합니다. 다음을 클릭합니다.



8. LiveLink를 구성하려면 예를, 그렇지 않으면 아니오를 선택하고 다음을 클릭합니다.



9. 검색 간격(검색 대상에 대한 링크 패킷의 재전송 시간 간격(초)) 및 검색 재시도 최대 횟수(장애 조치 실행 전 검색 대상으로부터 연속으로 손실된 응답 수)를 선택합니다.

10. Probe VLAN ID를 태그가 지정된 VLAN에 있는 검색 대상과 연결할 수 있도록 설정합니다. 번호 설정은 검색 대상의 VLAN ID뿐만 아니라 팀이 연결된 스위치의 포트도 일치해야 합니다.



**참고:** LiveLink가 활성화된 각 팀은 단일 VLAN의 검색 대상과만 통신할 수 있습니다. VLAN ID 0은 태그가 지정되지 않은 네트워크와 동일합니다. Probe VLAN ID가 0 이외의 값으로 설정된 경우에는 동일한 VLAN 태그 값(16.단계 참조)으로 VLAN을 생성해야 합니다.

11. 목록 상단의 검색 대상을 클릭하고, 대상 IP 주소 편집을 클릭한 다음 IP 주소 상자에 하나 또는 모든 검색 대상의 대상 IP 주소를 입력한 후 확인을 클릭합니다. 다음을 클릭합니다.



**참고:** 첫 번째 검색 대상만 필요합니다. IP 주소를 다른 검색 대상에 할당함으로써 최대 세 개까지 검색 대상을 지정하여 백업으로 사용할 수 있습니다.

12. 목록에서 팀 멤버를 선택하고 멤버 IP 주소 편집을 클릭한 다음 IP 주소 상자에 멤버 IP 주소를 입력합니다. 목록의 팀 멤버 모두에 대해 이 단계를 반복하고 확인을 클릭합니다. 다음을 클릭합니다.



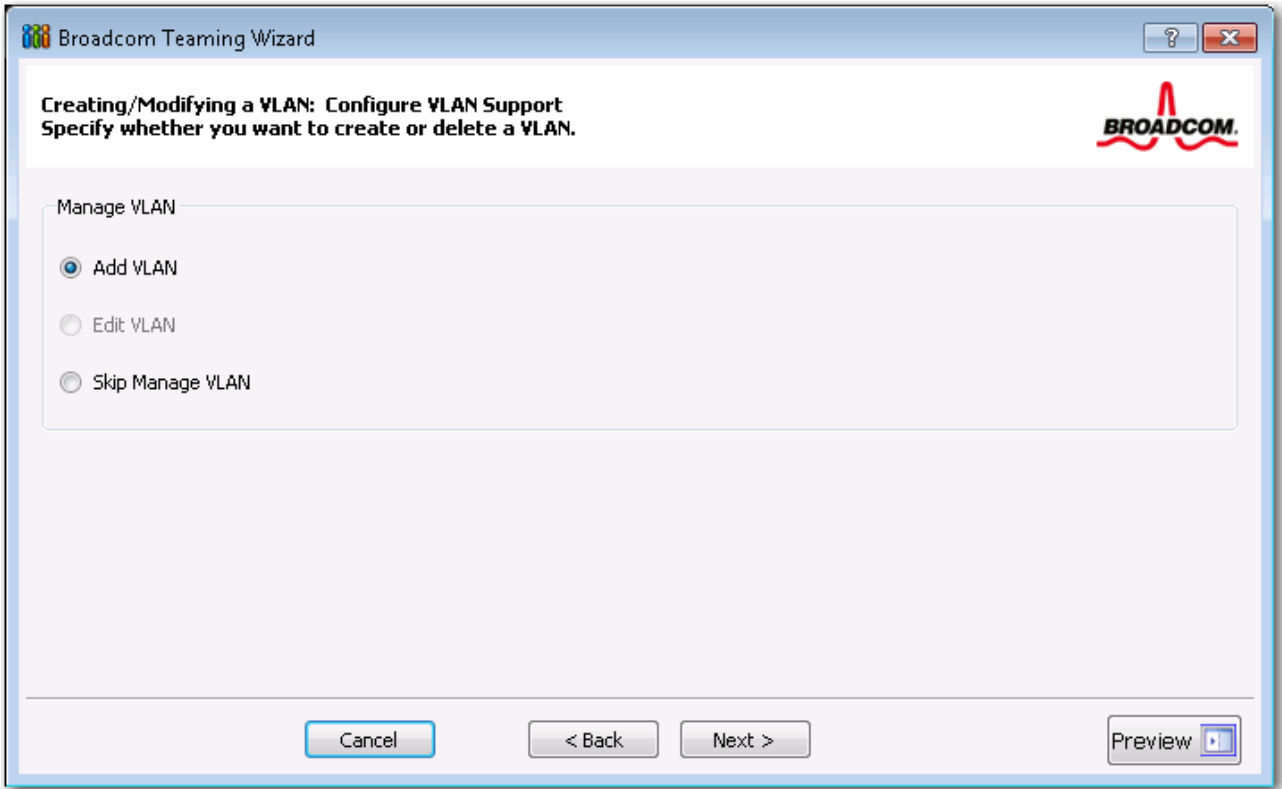
**참고:** 모든 멤버 IP 주소는 검색 대상과 동일한 서브넷에 있어야 합니다.

13. 팀에 VLAN을 생성하려면 VLAN 추가를, 기존 VLAN의 설정을 변경하려면 VLAN 편집을 선택하고 다음을 클릭합니다. VLAN을 생성하거나 편집하지 않으려면 VLAN 관리 건너뛰기를 선택하고 다음을 클릭한 다음 마침 화면에서 마법사를 계속합니다(이 절차의 18.단계 참조).

VLAN을 통해 다른 서브넷에 있는 여러 가상 어댑터를 추가할 수 있으며, 시스템의 한 네트워크 어댑터를 통해 여러 서브넷에 속할 수 있습니다.



**참고:** VLAN은 모든 팀 멤버가 Broadcom 어댑터일 경우에만 생성될 수 있습니다.

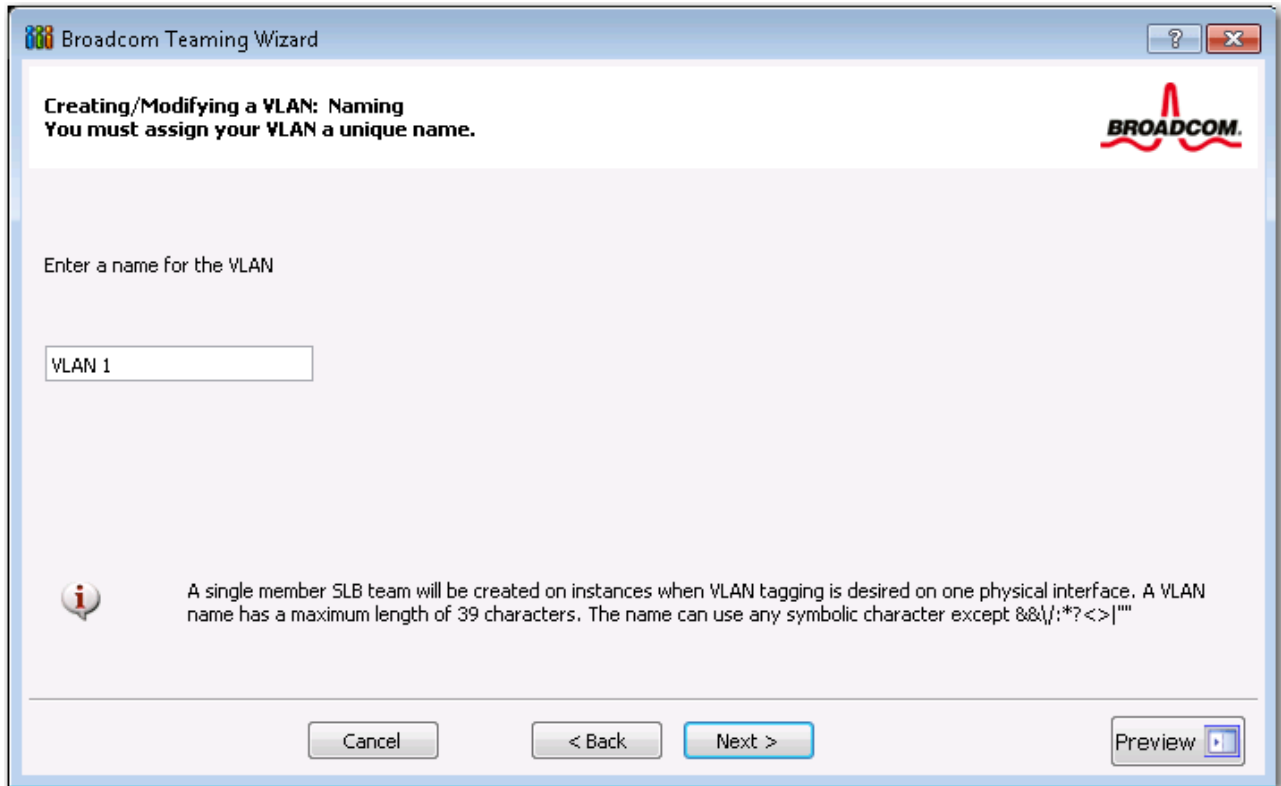


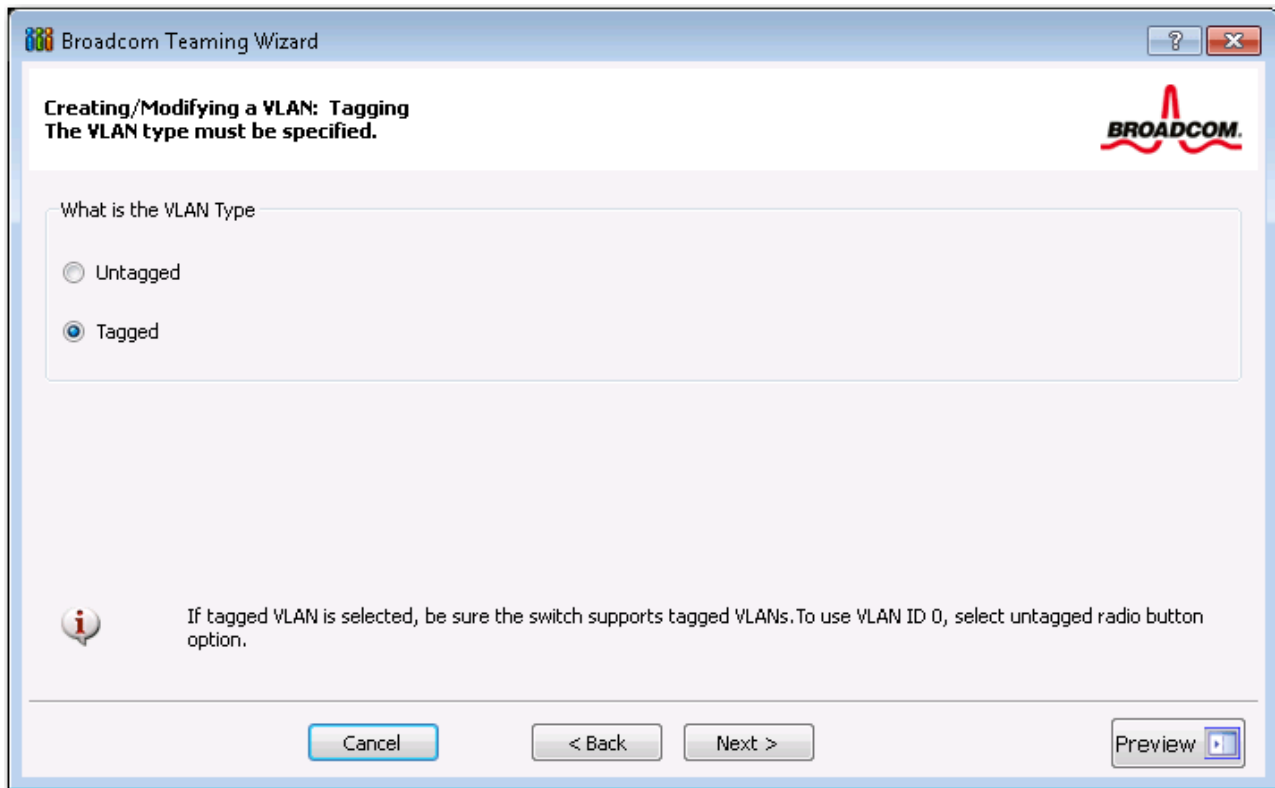
14. VLAN 이름을 입력한 후 다음을 클릭합니다.



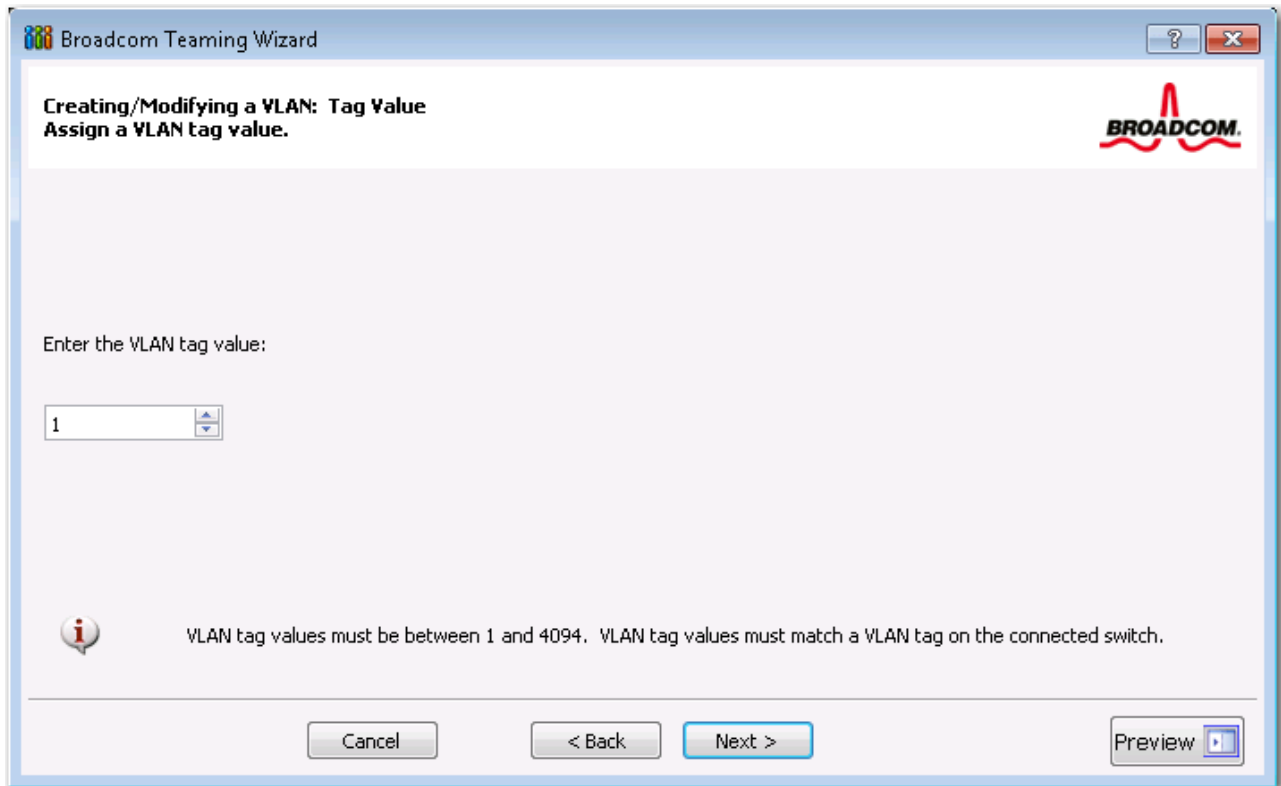
**참고:** 팀 이름은 39자 미만이어야 하며 공백으로 시작할 수 없고 다음 문자가 포함될 수 없습니다. & \ / : \* ? < > |







16. VLAN 태그 값을 입력하고 다음을 클릭합니다. 1과 4,094 사이의 값을 입력해야 합니다.

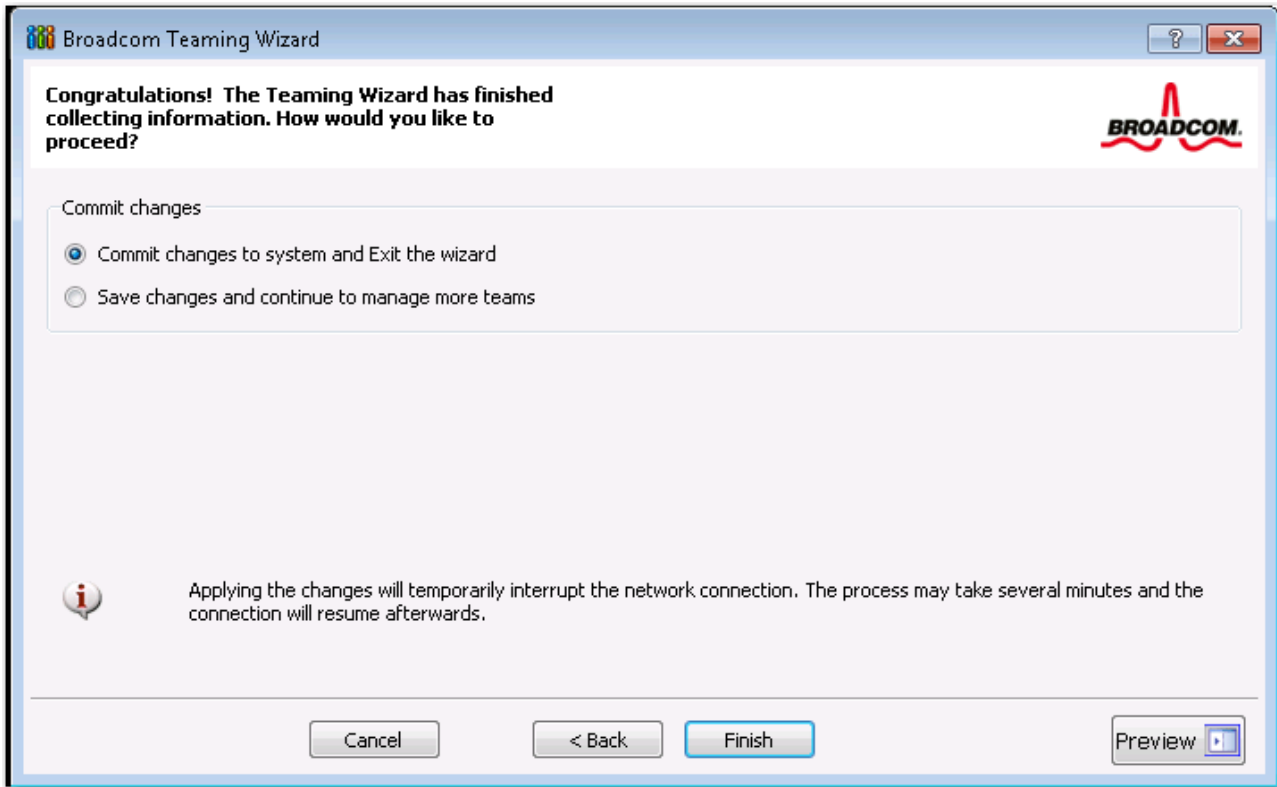


17. 다른 VLAN을 추가하거나 관리하려면 **예**를 선택하고 **다음**을 클릭합니다. 원하는 VLAN을 모두 추가하거나 관리할 때까지 이 단계를 반복합니다.

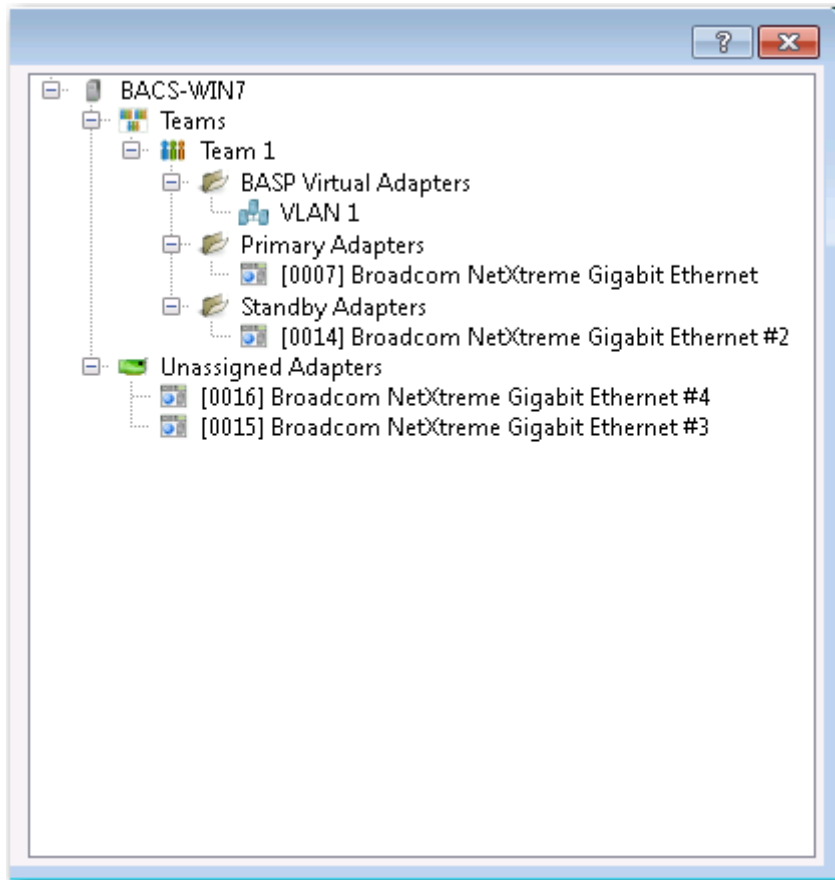


**참고:** 팀당 최대 64개의 VLAN을 정의할 수 있습니다(VLAN 63개에는 태그가 지정되고 VLAN 1개에는 태그가 지정되지 않음). VLAN마다 메모리 및 프로세서를 사용하기 때문에 VLAN을 여러 개 추가하면 Windows 인터페이스의 반응 시간이 느려질 수 있습니다. Windows 성능이 저하되는 정도는 시스템 구성에 따라 다릅니다.

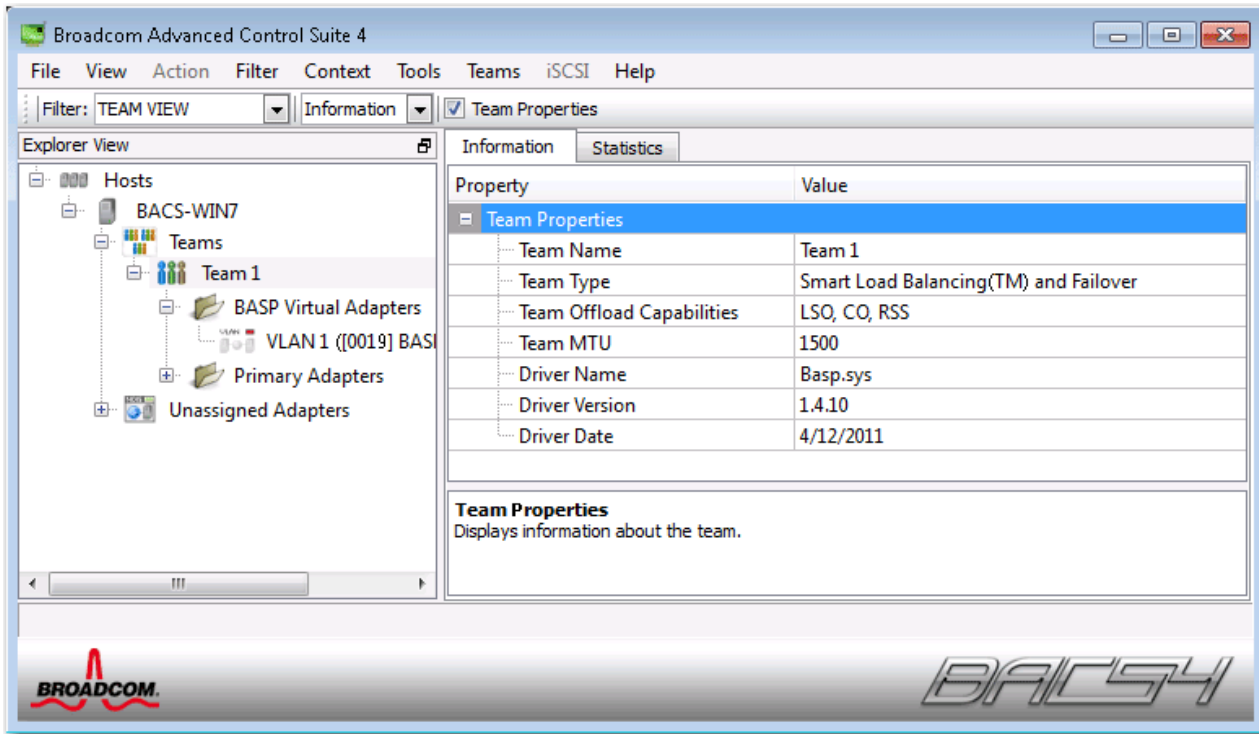
18. 팀의 변경 사항을 적용 및 커밋하려면 **시스템의 변경 사항을 커밋하고 마법사를 종료합니다.**를 선택합니다. 변경 사항을 적용하지만 계속해서 마법사를 사용하려면 **변경 사항을 저장하고 계속해서 추가 팀을 관리합니다.**를 선택합니다. **마침**을 클릭합니다.



**참고:** Broadcom 팀 구성 마법사 절차가 진행되는 동안 언제든지 **미리 보기**를 클릭하여 변경 사항이 커밋되기 전의 팀 모양을 미리 볼 수 있습니다.



19. 팀 관리 창에서 팀 이름을 클릭하여 **정보** 탭에서 해당 팀의 속성을 확인하고, **통계** 탭에서 데이터를 송수신할 수 있습니다.



## 전문가 모드 사용

전문가 모드를 사용하여 팀을 생성 및 수정하고 VLAN을 추가하며 Smart Load Balancing 및 장애 조치와 SLB(Auto-Fallback Disable) 팀에 대한 LiveLink를 구성할 수 있습니다. 마법사를 사용하여 팀을 생성하려면 [Broadcom 팀 구성 마법사 사용](#)을 참조하십시오.

기본 팀 구성 모드를 설정하려면 도구 모음에서 옵션을 선택한 다음 전문가 모드 또는 마법사 모드를 선택합니다(기본값: 마법사 모드).

## 팀 생성



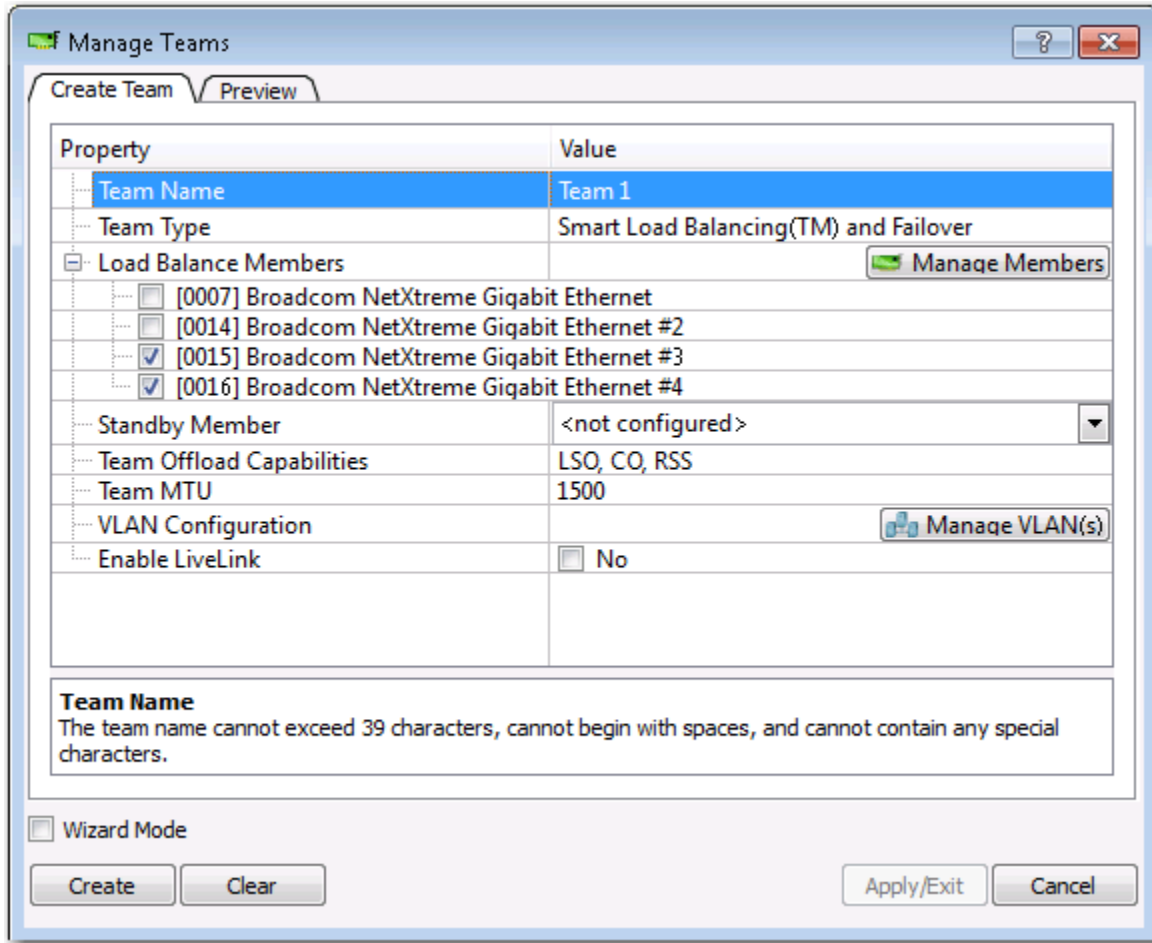
**참고:** SLB 팀 유형의 멤버에는 DHCP(동적 호스트 구성 프로토콜)를 활성화하지 않는 것이 좋습니다.


1. 팀 메뉴에서 팀 생성을 선택하거나 "할당되지 않은 어댑터" 섹션에서 장치 중 하나를 마우스 오른쪽 단추로 클릭하고 팀 생성을 선택합니다. 할당되지 않은 어댑터 섹션에 나열된 장치가 없는 경우, 즉 모든 어댑터가 이미 팀에 할당된 경우에는 이 옵션을 사용할 수 없습니다.
2. 전문가 모드를 클릭합니다.




**참고:** 팀을 생성할 때 항상 전문가 모드를 사용하려는 경우 다음에 시작할 때 전문가 모드를 기본값으로 설정을 클릭합니다.

3. 팀 생성 탭을 클릭합니다.




 **참고:** 팀 생성 탭은 팀 구성이 가능한 어댑터를 사용할 수 있는 경우에만 나타납니다.

4. 팀 이름 필드를 클릭하여 팀 이름을 입력합니다.
5. 팀 유형 필드를 클릭하여 팀 유형을 선택합니다.
6. 로드 균형 조정 멤버 목록에서 어댑터를 선택하여 사용 가능한 어댑터를 팀에 할당합니다. 로드 균형 조정 멤버 목록에는 선택된 어댑터가 하나 이상 있어야 합니다.
7. 다른 사용 가능한 어댑터를 대기 멤버 목록에서 선택하여 대기 멤버가 되도록 할당할 수 있습니다.

 **참고:** 팀에는 Broadcom 네트워크 어댑터가 하나 이상 할당되어야 합니다.

LSO(Large Send Offload), CO(Checksum Offload) 및 RSS는 LSO, CO 및/또는 RSS 속성이 팀을 위해 지원되는지 나타냅니다. 모든 멤버가 지원하고 모든 멤버가 해당 기능을 구성했을 때 LSO, CO, 및 RSS 속성은 팀만을 위해 사용됩니다.

 **참고:** 드라이버가 사용되지 않는 팀에 네트워크 어댑터를 추가하면 팀의 Offload 기능에 부정적인 영향을 끼칠 수 있습니다. 이는 팀의 성능에 영향을 끼칠 수 있습니다. 따라서 드라이버를 사용할 수 있는 네트워크 어댑터만을 팀 멤버로 추가하는 것이 좋습니다.

8. Team MTU의 값을 입력합니다.

9. 팀 정보를 저장하려면 **생성**을 클릭합니다.
10. 필요한 팀을 모두 정의할 때까지 4.~9. 단계를 반복합니다. 팀이 정의되면 팀 목록에서 선택할 수 있지만 아직 생성된 것은 아닙니다. 변경 사항을 적용하기 전에 팀 구조를 확인하려면 **미리 보기** 탭을 클릭합니다.
11. 정의한 팀을 모두 생성하고 팀 관리 창을 종료하려면 **적용/종료**를 클릭합니다.
12. 네트워크 연결이 일시적으로 중단된다는 메시지가 나타나면 **예**를 클릭합니다.

**설명 :**

- 팀 이름은 39자 미만이어야 하며 공백으로 시작할 수 없고 다음 문자가 포함될 수 없습니다. & \ / : \* ? < > |
- 팀 이름은 고유해야 합니다. 팀 이름을 한 번 이상 사용하려고 시도하면 이름이 이미 있음을 나타내는 오류 메시지가 표시됩니다.
- 팀 멤버의 최대 수는 8입니다.
- 팀 구성이 올바르게 수행되면 구성된 각 팀에 대해 가상 팀 어댑터 드라이버가 만들어집니다.
- 가상 팀을 비활성화하고 나중에 다시 활성화하려면 가상 팀을 다시 활성화하기 전에 먼저 모든 팀 멤버를 비활성화한 후에 다시 활성화해야 합니다.
- 일반 트렁킹 및 링크 집계 팀을 만들면 대기 멤버를 지정할 수 없습니다. 대기 멤버는 **Smart Load Balancing** 및 장애 조치, **SLB(Auto-Fallback Disable)** 등, 두 팀 유형에서만 작동합니다.
- **SLB(Auto-Fallback Disable)** 팀인 경우, 대기 멤버에서 로드 균형 조정 멤버에 트래픽을 복원하려면 팀 속성 탭의 **Fallback** 단추를 클릭합니다.
- **SLB** 팀을 구성할 때, 허브에 팀 멤버를 연결하는 것이 테스트를 위해 지원되는 경우에도 스위치에 팀 멤버를 연결하는 것이 좋습니다.
- 타사가 제조한 일부 네트워크 장치가 지원되거나 팀 구성용으로 완전 인증되었습니다.

13. 팀 IP 주소를 구성합니다.
  - a. 제어판에서 **네트워크 연결**을 두 번 클릭합니다.
  - b. 구성할 팀의 이름을 마우스 오른쪽 단추로 클릭한 후 **속성**을 클릭합니다.
  - c. 일반 탭에서 **인터넷 프로토콜(TCP/IP)**을 클릭한 후 **속성**을 클릭합니다.
  - d. IP 주소 및 팀 구성에 필요한 모든 기타 **TCP/IP**를 구성한 후 완료되면 **확인**을 클릭합니다.

## 팀 수정

팀을 만든 후에는 다음과 같은 방법으로 팀을 수정할 수 있습니다.

- 팀 유형 변경
- 팀에 할당된 멤버 변경
- VLAN 추가
- VLAN 수정(전문가 모드 사용)
- 팀 또는 VLAN 제거(전문가 모드 사용)

### 팀을 수정하려면

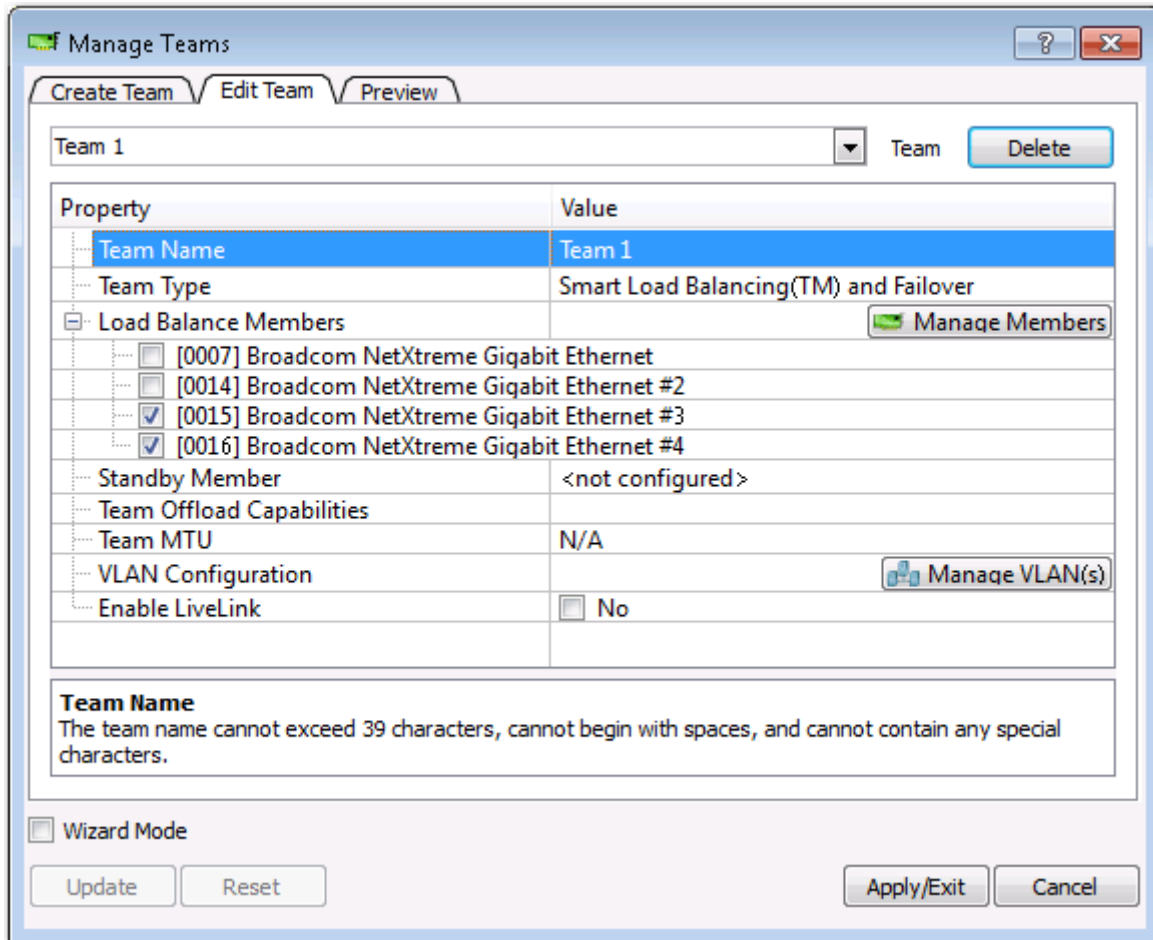
1. 팀 메뉴에서 **팀 편집**을 클릭하거나 목록에서 팀 중 하나를 마우스 오른쪽 단추로 클릭하고 **팀 편집**을 선택합니다. 이 옵션은 팀이 이미 생성되어 팀 관리 창에 나열된 경우에만 사용할 수 있습니다.
2. 마법사 시작 화면이 나타납니다. **다음**을 클릭하여 마법사로 팀을 수정하거나 **전문가 모드**를 클릭하여 전문가 모드에서 작업합니다.



**참고:** 전문가 모드의 **팀 편집** 탭은 시스템에 구성된 팀이 있는 경우에만 나타납니다.



## 3. 팀 편집 탭을 클릭합니다.



4. 원하는 사항을 변경한 후 **업데이트**를 클릭합니다. 아직 변경 사항이 적용되지 않았습니다. 변경 사항을 적용하기 전에 업데이트된 팀 구조를 확인하려면 **미리 보기** 탭을 클릭합니다.
5. 업데이트를 적용하고 팀 관리 창을 종료하려면 **적용/종료**를 클릭합니다.
6. 네트워크 연결이 일시적으로 중단된다는 메시지가 나타나면 **예**를 클릭합니다.

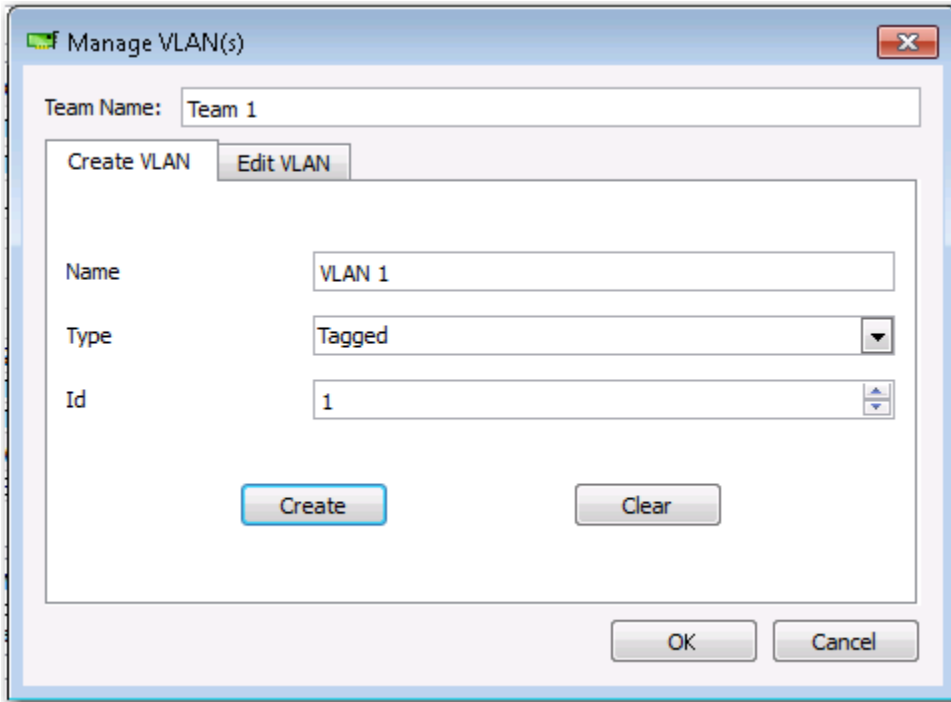
## VLAN 추가

팀에 가상 LAN(VLAN)을 추가할 수 있습니다. 이 작업으로 다른 서브넷에 있는 여러 가상 어댑터를 추가할 수 있으며, 시스템의 한 네트워크 어댑터를 통해 여러 서브넷에 속할 수 있습니다. VLAN을 사용하여 로드 균형 멤버의 로드 균형 조정 기능을 연결할 수 있으며, 장애 조치 어댑터를 채용할 수도 있습니다.

팀당 최대 64 개의 VLAN을 정의할 수 있습니다(VLAN 63개에는 태그가 지정되고 VLAN 1개에는 태그가 지정되지 않음). VLAN은 모든 팀 멤버가 Broadcom 어댑터일 경우에만 생성될 수 있습니다. 타사 어댑터로 VLAN을 생성하려는 경우 오류 메시지가 나타납니다.

**VLAN과 함께 팀을 구성하려면**

1. 팀 메뉴에서 **VLAN 추가**를 선택합니다.
2. 시작 화면이 나타납니다.
3. **전문가 모드**를 클릭합니다.
4. 팀 관리 창의 **팀 생성** 탭에서 **VLAN 관리**를 클릭합니다.
5. VLAN 이름을 입력하고 유형과 ID를 선택합니다.
6. VLAN 정보를 저장하려면 **생성**을 클릭합니다. VLAN이 정의되면 팀 이름 목록에서 선택할 수 있지만 아직 생성된 것은 아닙니다.
7. 이 과정을 계속하다가 모든 VLAN이 정의되면 **확인**을 클릭하여 생성합니다.



8. 네트워크 연결이 일시적으로 중단된다는 메시지가 나타나면 **예**를 클릭합니다.



**참고:** 어댑터 성능을 최적 상태로 유지하려면 각 어댑터에 생성된 VLAN 8개 각각의 시스템 메모리가 64MB여야 합니다.

**VLAN 속성 및 통계 보기 및 VLAN 테스트 실행**

**VLAN 속성 및 통계를 보고 VLAN 테스트를 실행하려면**

1. 나열된 VLAN 중 하나를 선택합니다.
2. VLAN 어댑터의 속성을 보려면 **정보** 탭을 클릭합니다.
3. VLAN 어댑터의 통계를 보려면 **통계** 탭을 클릭합니다.
4. VLAN 어댑터에서 네트워크 테스트를 실행하려면 **진단** 탭을 클릭합니다.

## VLAN 삭제

아래 절차는 전문가 모드 상태인 경우 적용됩니다.

### VLAN을 삭제하려면

1. 삭제할 VLAN을 선택합니다.
2. 팀 메뉴에서 **VLAN 제거**를 선택합니다.
3. **적용**을 클릭합니다.
4. 네트워크 연결이 일시적으로 중단된다는 메시지가 나타나면 **예**를 클릭합니다.



**참고:** 팀을 삭제하면 해당 팀에 구성된 VLAN도 모두 삭제됩니다.

## Smart Load Balancing 및 장애 조치와 SLB(Auto-Fallback Disable) 팀에 대한 LiveLink 구성

LiveLink는 SLB(Smart Load Balancing) 및 SLB(Auto-Fallback Disable) 유형의 팀 구성에 대해서만 사용할 수 있는 BASP 기능입니다. LiveLink는 해당 스위치 이외의 링크 손실을 감지하고 라이브 링크가 있는 팀 멤버를 통해서만 트래픽을 돌아가게 합니다.

LiveLink를 구성하기 전에 다음 참고 사항을 읽어 보십시오.



### 설명 :

- LiveLink™ 구성을 시작하기 전에 LiveLink 설명을 살펴보십시오. 지정할 각 검색 대상이 사용 가능하고 작동되는지도 확인하십시오. 검색 대상의 IP 주소가 변경될 경우 LiveLink를 다시 구성해야 합니다. 검색 대상의 MAC 주소가 변경될 경우 팀을 다시 시작해야 합니다("문제 해결" 참조).
- 검색 대상이 팀과 동일한 서브넷에 있어야 하며 브로드캐스트, 멀티캐스트 또는 유니캐스트가 아닌 정적으로 지정된 유효한 IP 주소가 있어야 하며 항상 사용 가능해야 합니다.
- 검색 대상에 대한 네트워크 연결성을 확인하려면 팀에서 검색 대상을 Ping합니다.
- 최대 네 개까지 검색 대상을 지정할 수 있습니다.
- 검색 대상 또는 팀 멤버에 할당된 IP 주소는 처음 또는 마지막 8진수 값이 영(0)이 될 수 없습니다.

### LiveLink를 구성하려면

1. 팀 메뉴에서 **팀 편집**을 선택합니다.
2. 전문가 모드를 클릭합니다(팀 구성 마법사를 통해 LiveLink를 구성하려면 **Broadcom 팀 구성 마법사 사용** 참조).
3. 멤버 관리 창에서 **팀 편집** 탭을 클릭합니다.
4. **LiveLink 활성화**를 선택합니다. 아래에 LiveLink 구성 옵션이 나타납니다.
5. **검색 간격**(검색 대상에 대한 링크 패킷의 각 재전송 간 초) 및 **검색 재시도 최대 횟수**(장애 조치 실행 전 검색 대상으로부터 연속으로 손실된 응답 수)에 대한 기본값을 사용하는 것이 좋습니다. 다른 값을 지정하려면 **간격 검색(초)** 목록에서 원하는 검색 간격을 클릭하고 **검색 최대 재시도 횟수**에서 원하는 검색 재시도 횟수를 클릭합니다.
6. 검색 대상이 있는 VLAN과 일치하도록 **Probe VLAN ID**를 설정합니다. 이렇게 하면 연결된 스위치 포트의 공유 구성에 따라 적절한 VLAN 태그가 링크 패킷에 적용됩니다.



**참고:** LiveLink가 활성화된 각 팀은 단일 VLAN의 검색 대상과만 통신할 수 있습니다. VLAN ID 0은 태그가 지정되지 않은 네트워크와 동일합니다.

7. **검색 대상 1**을 선택하고 한 검색 대상이나 모든 검색 대상의 대상 IP 주소를 입력합니다.



**참고:** 첫 번째 검색 대상만 필요합니다. IP 주소를 다른 검색 대상에 할당함으로써 최대 세 개까지 검색 대상을 지정하여 백업으로 사용할 수 있습니다.

8. 나열된 팀 멤버 중 하나를 선택하고 멤버 IP 주소를 입력합니다.



**참고:** 모든 멤버 IP 주소는 검색 대상과 동일한 서브넷에 있어야 합니다.

9. **업데이트**를 클릭합니다. 목록의 기타 각 팀 멤버에 대해 이러한 단계를 반복합니다.

10. **적용/종료**를 클릭합니다.

## 구성 저장 및 복원

### 구성을 저장하려면

1. 파일 메뉴에서 **다른 이름으로 팀 저장**을 선택합니다.
2. 새 구성 파일의 경로 및 파일 이름을 입력한 후 **저장**을 클릭합니다(.bcg 확장자가 추가됨).  
구성 파일의 형식은 텍스트 파일이므로 모든 텍스트 편집기에서 열어 볼 수 있습니다. 파일에는 어댑터와 팀 구성에 대한 정보가 모두 들어 있습니다.

### 구성을 복원하려면

1. 파일 메뉴에서 **팀 복원**을 선택합니다.
2. 복원할 파일의 이름을 클릭한 후 **열기**를 클릭합니다.



**참고:** 필요한 경우 파일이 있는 폴더로 이동합니다.

3. **적용**을 클릭합니다.
4. 네트워크 연결이 일시적으로 중단된다는 메시지가 나타나면 **예**를 클릭합니다.
5. 구성이 이미 로드된 경우 현재 구성을 저장할 지 여부를 묻는 메시지가 나타납니다. 현재 구성을 저장하려면 **예**를 클릭합니다. 저장하지 않으면 현재 로드된 구성 데이터는 손실됩니다.



**참고:** 팀이 많은 VLAN과 정적 IP 주소로 구성된 경우 팀을 복원하는 데 시간이 오래 걸릴 수 있습니다.

## BASP 통계 보기

통계 섹션에는 팀에 속한 네트워크 어댑터에 대한 성능 정보가 표시됩니다.

팀 멤버 어댑터나 팀 전체에 대한 **BASP** 통계 정보를 확인하려면 팀 관리 창에 나열된 어댑터나 팀의 이름을 클릭하고 **통계** 탭을 클릭합니다.

각 통계의 최신 값을 가져오려면 **새로 고침**을 클릭합니다. 모든 값을 0으로 변경하려면 **다시 설정**을 클릭합니다.

**최대 . 패킷** . 전송된 패킷 수입입니다.

**최대 . 수신 패킷** . 취소된 패킷 수입입니다.

**최대 . 전송 패킷** . 대기열 상의 패킷 수입입니다.

**최대 패킷** . 수신한 패킷 수입입니다.

**최대 수신 패킷** . 취소된 패킷 수입입니다.

**검색 재시도 횟수** . 장애 조치 실행 전 검색 대상으로부터 연속으로 손실된 응답 수입입니다.

---

## 명령줄 인터페이스 유틸리티를 사용하여 구성

Broadcom 네트워크 어댑터를 구성할 때 BACS 대신 BACSCLI를 사용할 수도 있습니다. BACSCLI는 비대화형 명령줄 인터페이스(CLI) 모드 또는 대화형 모드에서 콘솔을 사용하여 정보를 보고 네트워크 어댑터를 구성할 수 있게 해주는 Broadcom 유틸리티입니다. BACS와 마찬가지로 BACSCLI는 각 네트워크 어댑터에 대한 정보를 제공하며 자세한 테스트를 수행하고, 진단을 실행하고, 통계를 보고, 속성 값을 수정할 수 있게 해줍니다. BACSCLI에서는 로드 균형 조정 및 장애 조치를 위해 네트워크 어댑터를 팀으로 묶을 수도 있습니다.

사용 가능한 명령 및 예제의 전체 목록은 Dell에서 제공한 CD에 있는 BACSCLI ReadMe 텍스트 파일을 참조하십시오.

Broadcom NetXtreme I 및 NetXtreme II 네트워크 어댑터가 있는 시스템에서 BACSCLI는 BACS가 설치 프로그램으로 설치될 때 설치됩니다.

---

## BACS 문제 해결

**문제:** Linux 시스템에서 BACS를 열려 할 때 다음 오류 메시지가 표시됩니다.

“이 시스템에서 BACS 클라이언트의 다른 인스턴스가 실행 중입니다. 한 번에 하나의 BACS 클라이언트 인스턴스만 실행될 수 있습니다. 실행 중인 다른 BACS 클라이언트가 없는 것이 확실하다면 이전 인스턴스가 예기치 않게 종료된 것일 수 있습니다.”

**해결 방법:** 이 메시지는 사용자가 두 번째 BACS 인스턴스를 실행하려 하면 표시됩니다. 이 메시지가 표시되지만 현재 실행 중인 BACS 인스턴스가 없다면 이전의 BACS 인스턴스가 예기치 않게 종료된 것일 수 있습니다. 이전 인스턴스를 제거하려면 `“/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}”` 파일을 제거합니다.

## 14 절: 사양

- 10/100/1000BASE-T 케이블 사양
- 성능 사양

### 10/100/1000BASE-T 케이블 사양

표 22. 10/100/1000BASE-T 케이블 사양

| 포트 종류                       | 커넥터   | 미디어                                    | 최대 거리       |
|-----------------------------|-------|----------------------------------------|-------------|
| 10BASE-T                    | RJ-45 | Category 3, 4 또는 5 비차폐 단일 트위스트 페어(UTP) | 100m(328피트) |
| 100/1000BASE-T <sup>1</sup> | RJ-45 | Category 5 <sup>2</sup> UTP            | 100m(328피트) |

<sup>1</sup>1000BASE-T 신호를 사용하려면 ISO/IEC 11801:1995와 ANSI/EIA/TIA-568-A(1995)에 명시되어 있고 TIA/EIA TSB95의 절차에 따라 추가 성능 테스트를 거친 4개의 트위스트 페어 케이블(Category 5)이 필요합니다.

<sup>2</sup>Category 5는 최소 요구 사항입니다. Category 5e와 Category 6은 완벽하게 지원됩니다.

### 성능 사양

표 23. 성능 사양

| 기능                                         | 사양                    |
|--------------------------------------------|-----------------------|
| <b>PCI Express™ 유형 컨트롤러 (BCM57XX 컨트롤러)</b> |                       |
| PCI Express 인터페이스                          | x1, x2, x4 링크 너비      |
| PCI Express 집적 대역폭(전송 및 수신)                | 2.5Gbps 또는 5.0Gbps    |
| 10/100/1000BASE-T                          | 10/100/1000Mbps(전 이중) |



## 15 절: 규정

- FCC Class B 표시
- VCCI Class B 표시
- CE 표시
- 캐나다 규정 정보(캐나다만 해당)
- MIC 표시(대한민국만 해당)
- BSMI

### FCC Class B 표시

Broadcom NetXtreme Gigabit Ethernet Controller  
BCM95721A211  
BCM95722A2202

이 장치는 FCC 규정 15부를 준수하며 작동 시 다음 두 조건이 적용됩니다. 1) 장치는 유해한 간섭을 유발하지 않습니다. 2) 이 장치는 원하지 않는 작동을 유발할 수 있는 간섭을 포함하여 수신된 모든 간섭을 수용해야 합니다.

테스트 결과 이 장치는 FCC 규정 15부에 의거하여 Class B 디지털 장치의 제한 사항을 준수합니다. 이러한 제한 사항은 거주지 설치 시 유해한 간섭으로부터 보호하기 위한 것입니다. 장치가 무선 주파수 에너지를 생성, 사용 및 방사할 수 있으므로 지침에 따라 설치하여 사용하지 않는 경우 무선 통신에 유해한 간섭을 일으킬 수 있습니다. 그러나 특정 설치 시에 간섭이 발생하지 않는다고 보증하지는 않습니다. 라디오나 TV 수신 시 유해한 간섭을 일으키는 경우(장치를 껐다가 다시 켜보면 간섭을 일으키는 지 알 수 있음), 다음 조치 중 하나 이상을 수행하여 간섭을 해결하도록 합니다.

- 수신 안테나의 방향을 조정합니다.
- 장치를 수신기에서 멀리 떨어진 곳에 놓습니다.
- 수신기가 연결되지 않은 다른 회로의 콘센트에 연결하십시오.
- 도움이 필요하면 대리점이나 숙련된 라디오/TV 기술자에게 문의합니다.

장치를 기계 또는 전기적으로 변경하지 마십시오.



**참고:** Broadcom의 허가 없이 어댑터를 변경하거나 개조하면 장비 작동 권한이 무효가 될 수 있습니다.

Broadcom Corporation  
190 Mathilda Place  
Sunnyvale, California 94086 USA

---

## VCCI Class B 표시

장치는 Information Technology Equipment의 VCCI(Voluntary Control Council Interference) 표준을 따르는 Class B 제품입니다. 집안의 라디오나 TV 수신기 옆에서 사용하면 무선 간섭을 일으킬 수 있습니다. 설명서 지침에 따라 장치를 설치하고 사용하십시오.



**주의!** 주파수 범위가 59-66MHz인 전도성 무선 주파수 에너지가 있는 곳에서는 이 장비가 손상될 우려가 있습니다. RF 에너지를 제거해야 정상적으로 작동됩니다.

## VCCI Class B 규정 ( 일본 )

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

---

## CE 표시

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| БЪЛГАРСКИ<br>Bulgarian | <p>Този продукт отговаря на 2006/95/EC (Нисковолтова директива), 2004/108/EC (Директива за електромагнитна съвместимост) и измененията на Европейския съюз.</p> <p><b>Европейски съюз, Клас B</b></p> <p>Това устройство на Broadcom е класифицирано за използване в типичната за Клас B жилищна среда.</p> <p>Изготвена е "Декларация за съответствие" според горепосочените директиви и стандарти, която се съхранява в Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                    |
| ČESKY<br>Czech         | <p>Bylo ustanoveno, že tento produkt splňuje směrnici 2006/95/EC (nízkonapěťová směrnice), směrnici 2004/108/EC (směrnice EMC) a dodatky Evropské unie.</p> <p><b>Evropská unie, třída B</b></p> <p>Toto zařízení společnosti Broadcom je klasifikováno pro použití v obvyklém prostředí domácnosti (třída B).</p> <p>„Prohlášení o shodě“ v souladu s výše uvedenými směrnici a normami bylo zpracováno a je uloženo v archivu společnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                  |
| Danish                 | <p>Denne produkt er fundet i overensstemmelse med 2006/95/EC (Lavvoltage-direktivet), 2004/108/EC (EMC-direktivet) og den Europæiske Unions ændringer.</p> <p><b>Den Europæiske Union, Klasse B</b></p> <p>Denne Broadcom-enhed er klassificeret til anvendelse i et typisk Klasse B-hjemligt miljø.</p> <p>En "Overensstemmelseserklæring", som er i henhold til foregående direktiver og standarder, er udført og arkiveret hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                            |
| NEDERLANDS<br>Dutch    | <p>Dit product is in overeenstemming bevonden met 2006/95/EC (Laagspanningsrichtlijn), 2004/108/EC (EMC-richtlijn) en amendementen van de Europese Unie.</p> <p><b>Europese Unie/Klasse B</b></p> <p>Dit Broadcom-apparaat is geclassificeerd voor gebruik in een typische klasse B woonomgeving.</p> <p>Een "Verklaring van conformiteit" in overeenstemming met de voorgenoemde richtlijnen en standaarden is beschikbaar bij Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                              |
| English                | <p>This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive), and amendments of the European Union.</p> <p><b>European Union, Class B</b></p> <p>This Broadcom device is classified for use in a typical Class B domestic environment.</p> <p>A "Declaration of Conformity" in accordance with the preceding directives and standards has been made and is on file at Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                        |
| EESTLANE<br>Estonian   | <p>Antud toode vastab direktiividele 2006/95/EU (Madalpinge direktiiv), 2004/108/EU (EMC direktiiv) ja ELi parandustele.</p> <p><b>Euroopa Liit, Klass B</b></p> <p>Antud Broadcom toode on klassifitseeritud kasutamiseks tüüpilises B-klassi koduses keskkonnas.</p> <p>Vastavalt ülaltoodud direktiividele ja standarditele on koostatud „Vastavusdeklaratsioon“, mis on arvel ettevõttes Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                                                 |
| Finnish                | <p>Tämä tuote täyttää Euroopan unionin direktiivin 2006/95/EY (pääjännittdirektiivi) ja direktiivin 2004/108/EY (sähkömagneettisesta yhteensopivuudesta annettu direktiivi), sellaisina kuin ne ovat muutettuina, vaatimukset.</p> <p><b>Euroopan unioni, luokka B</b></p> <p>Tämä Broadcom-laite on luokiteltu käytettäväksi tyypillisessä huonon B kotiympäristössä.</p> <p>Yllä mainittujen direktiivien ja standardien mukainen vaatimustenmukaisuusvakuutus on tehty, ja sitä säilyttää Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p> |
| FRANÇAIS<br>French     | <p>Ce produit a été déclaré conforme aux directives 2006/95/EC (Directive sur la faible tension), 2004/108/EC (Directive EMC) et aux amendements de l'Union européenne.</p> <p><b>Union européenne, classe B</b></p> <p>Cet appareil Broadcom est classé pour une utilisation dans un environnement résidentiel classique (classe B).</p> <p>Une « Déclaration de Conformité » relative aux normes et directives précédentes a été rédigée et est enregistrée auprès de Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                      |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DEUTSCH<br/>German</p>                   | <p>Es ist befunden worden, dass dieses Produkt in Übereinstimmung mit 2006/95/EC (Niederspannungs-Richtlinie), 2004/108/EC (EMV-Richtlinie) und Ergänzungen der Europäischen Union steht.</p> <p><b>Europäische Union, Klasse B</b><br/>Dieses Gerät von Broadcom ist für die Verwendung in einer typisch häuslichen Umgebung der Klasse B vorgesehen.</p> <p>Eine Konformitätserklärung in Übereinstimmung mit den oben angeführten Normen ist abgegeben worden und kann bei Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>     |
| <p>ΕΛΛΗΝΙΚΟΣ<br/>Greek</p>                  | <p>Το προϊόν αυτό συμμορφώνεται με τις οδηγίες 2006/95/ΕΕ (Οδηγία περί χαμηλής τάσης), 2004/108/ΕΕ (Οδηγία περί ηλεκτρομαγνητικής συμβατότητας), και τροποποιήσεις τους από την Ευρωπαϊκή Ένωση.</p> <p><b>Ευρωπαϊκή Ένωση, Κατηγορία Β</b><br/>Αυτή η συσκευή Broadcom είναι κατάλληλη για χρήση σε ένα σύνθετες οικιακό περιβάλλον κατηγορίας Β.</p> <p>Μία «Δήλωση Συμμόρφωσης» σύμφωνα με τις προηγούμενες οδηγίες και πρότυπα υπάρχει και είναι αρχειοθετημένη στο Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>           |
| <p>MAGYAR<br/>Hungarian</p>                 | <p>A termék megfelel a 2006/95/EGK (alacsony feszültségű eszközökre vonatkozó irányelv), a 2004/108/EGK (EMC irányelv) és az Európai Unió ajánlásainak.</p> <p><b>Európai Unió, „B” osztály</b><br/>Ez a Broadcom eszköz „B” osztályú besorolást kapott, tipikus lakossági környezetben való használatra alkalmas.</p> <p>Az előbbiekben ismertetett irányelvek és szabványok szellemében „Megfeleléségi nyilatkozat” készült, amely az irországi Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                 |
| <p>PORTUGUES<br/>Iberian<br/>Portuguese</p> | <p>Este produto está em conformidade com 2006/95/EC (Directiva de baixa tensão), com 2004/108/EC (Directiva de compatibilidade electromagnética) e com as alterações da União Europeia.</p> <p><b>União Europeia, Classe B</b><br/>Este dispositivo Broadcom está classificado para utilização num ambiente doméstico típico Classe B.</p> <p>Foi elaborada uma “declaração de conformidade” de acordo com as normas e directivas anteriores, encontrando-se arquivada na Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>         |
| <p>ITALIANO<br/>Italian</p>                 | <p>Il presente prodotto è stato determinato essere conforme alla 2006/95/CE (Direttiva Bassa Tensione), alla 2004/108/CE (Direttiva CEM) e a rettifiche da parte dell'Unione Europea.</p> <p><b>Unione Europea, Classe B</b><br/>Il presente dispositivo Broadcom è classificato per l'uso nel tipico ambiente domestico di Classe B.</p> <p>Una "Dichiarazione di conformità" secondo gli standard e le direttive precedenti è stata emessa e registrata presso Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                  |
| <p>LATVISKS<br/>Latvian</p>                 | <p>Sis izstrādājums atbilst direktīvām 2006/95/EK (Direktīva par zemsprieguma iekārtām), 2004/108/EK (Direktīva par elektromagnētisko saderību) un to labojumiem Eiropas Savienības ietvaros.</p> <p><b>Eiropas Savienība, klase B</b><br/>Šī firmas Broadcom ražotā ierīce ir atzīta par derīgu darbam B klasei atbilstošos mājas apstākļos.</p> <p>“Atbilstības deklarācija”, kas ir saskaņā ar iepriekšminētajām direktīvām un standartiem, ir sastādīta un tiek glabāta firmā Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p> |
| <p>Lithuanian</p>                           | <p>Buvo nustatyta, kad šis produktas atitinka direktyvą 73/23/EEB (žemos įtampos direktyva), 89/336/EEB (elektromagnetinio suderinamumo direktyva) ir Europos Sąjungos pataisas.</p> <p><b>Europos Sąjunga, B klasė</b><br/>Šis „Broadcom“ prietaisas yra klasifikuotas naudoti įprastose B klasės gyvenamosiose aplinkose.</p> <p>Atitikties deklaracija pagal visas galiojančias direktyvas ir standartus yra sudaryta ir saugoma įrašyta failė Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                 |



|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maltese                | <p>Gie stabbilit li dan il-prodott hu konformi ma' 2006/95/KE (Direttiva dwar il-Vultaġġ Baxx), 2004/108/KE (Direttiva EMC), u emendi ta' l-Unjoni Ewropea.</p> <p><b>Unjoni Ewropea, Klassi B</b></p> <p>Dan it-tagħmir Broadcom hu kklassifikat għall-użu f' ambjent residenzjali tipiku ta' Klassi B. Saret "Dikjarazzjoni ta' Konformità" b'konformità mad-direttivi u ma' l-istandards imsemmijin qabel, u din tinsab iffajljata għand Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                                            |
| POLSKI<br>Polish       | <p>Niniejszy produkt został określony jako zgodny z dyrektywą niskonapięciową 2006/95/WE i dyrektywą zgodności elektromagnetycznej 2004/108/WE oraz poprawkami do nich.</p> <p><b>Unia Europejska, klasa B</b></p> <p>Niniejsze urządzenie firmy Broadcom zostało zakwalifikowane do klasy B, do użytku w typowych środowiskach domowych.</p> <p>Zgodnie ze stosownymi dyrektywami i normami została sporządzona „Deklaracja zgodności”, która jest dostępna w aktach firmy Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                            |
| ROMAN<br>Romanian      | <p>S-a stabilit că acest produs respectă cerințele Directivei 2006/95/CE privind echipamentele de joasă tensiune, ale Directivei 2004/108/CE (Directiva EMC) privind compatibilitatea electromagnetică și ale amendamentelor Uniunii Europene.</p> <p><b>Uniunea Europeană, Clasa B</b></p> <p>Acest echipament Broadcom este clasificat pentru utilizare într-un mediu casnic tipic de Clasă B. Conform directivelor și standardelor de mai sus, a fost emisă o „Declarație de Conformitate”, arhivată la sediul Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                      |
| SLOVENSKY<br>Slovakian | <p>Tento výrobok vyhovuje požiadavkám smernice 2006/95/EC (smernica o nízkom napätí), 2004/108/EC (smernica o elektromagnetickej kompatibilite) a neskorším zmenám a doplnkom Európskej.</p> <p><b>Európska únia, Trieda B</b></p> <p>Toto zariadenie Broadcom triedy B je určené pre domáce prostredie.</p> <p>„Vyhlásenie o zhode“ vydané v súlade s predchádzajúcimi smernicami a štandardmi sa nachádza v spoločnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                                                              |
| Slovenian              | <p>Ta izdelek je v skladu z 2006/95/ES (Direktiva o nizki napetosti), 2004/108/ES (Direktiva o elektromagnetni združljivosti) in dopolnili Evropske unije.</p> <p><b>Evropska unija, razred B</b></p> <p>Ta Broadcomova naprava je razvrščena za uporabo v značilnem bivalnem okolju razreda B.</p> <p>«Izjava o skladnosti» je bila sprejeta v skladu s predhodnimi direktivami in standardi in je shranjena na naslovu Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                                                               |
| ESPAÑOL<br>Spanish     | <p>Este producto se ha fabricado de conformidad con la Directiva para bajo voltaje 2006/95/EC (Low Voltage Directive), la Directiva para compatibilidad electromagnética 2004/108/EC (EMC Directive) y las enmiendas de la Unión Europea.</p> <p><b>Unión Europea, Clase B</b></p> <p>Este dispositivo Broadcom está clasificado para ser utilizado en un entorno doméstico convencional de Clase B.</p> <p>Se ha realizado una "Declaración de conformidad" de acuerdo con las directivas y estándares anteriores y está archivada en Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p> |
| SVENSK<br>Swedish      | <p>Denna produkt överensstämmer med EU-direktivet 2006/95/EC (lågspänningsdirektivet), 2004/108/EC (EMC direktivet), och andra ändringar enligt den Europeiska unionen.</p> <p><b>Europeiska unionen, klass B</b></p> <p>Den här Broadcom-enheten är klassificerad för användning i vanlig klass B-bostadsmiljö.</p> <p>En "Försäkran om överensstämmelse" i enlighet med de föregående direktiven och standarderna har framställts och finns registrerad hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                          |
| TURK<br>Turkish        | <p>Bu ürünün 2006/95/EC (Düşük Voltaj Direktifi), 2004/108/EC (EMC Direktifi), ve Avrupa Birliği'nin ilavelerine uygun olduğu belirlenmiştir.</p> <p><b>Avrupa Birliği, B Sınıfı</b></p> <p>Bu Broadcom cihazı, tipik bir B sınıfı, ev içi ortamda kullanılmak üzere sınıflandırılmıştır.</p> <p>Yukarıda belirtilen direktifler ve standartlara uygun olarak, bir "Uygunluk Beyanı" hazırlanmıştır, ve Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.</p>                                                                                                                                |

---

## 캐나다 규정 정보(캐나다만 해당)

### Industry Canada, Class B

This Class B digital apparatus complies with Canadian ICES-003.

**Notice:** The Industry Canada regulations provide that changes or modifications not expressly approved by Broadcom could void your authority to operate this equipment.

### Industry Canada, classe B

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

**Avis :** Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Broadcom y sont apportés.

# MIC 표시 ( 대한민국만 해당 )

## CLASS B 장치

Broadcom NetXtreme Gigabit Ethernet Controller  
 BCM95721A211  
 BCM95722A2202

| 기종별            | 사용자안내문                                                     |
|----------------|------------------------------------------------------------|
| B급 기기<br>(가정용) | 이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다. |



1. 기기의 명칭(모델명) : BCM95721A211
2. 인증번호 : E-G021-04-2613(B)
3. 인증받은 자의 상호 : Broadcom
4. 제조년월일: 5/12/2004
5. 제조자/제조국가 : Foxconn/China



1. 기기의 명칭(모델명) : BCM95722A2202G
2. 인증번호 : BCM-BCM95722A2202G (B)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일: 04/30/2007
5. 제조자/제조국가 : Foxconn/China

이 장치는 업무 이외의 목적으로 승인되었으며 거주지를 포함하여 모든 환경에서 사용할 수 있습니다.

---

## BSMI

### BSMI 通告 (僅限於台灣)

大多數的 Dell 電腦系統被 BSMI (經濟部標準檢驗局) 劃分為乙類數位裝置。但是, 使用某些選件會使有些組態的等級變成甲類。若要確定您的電腦系統適用等級, 請檢查所有位於電腦底部或背面板、擴充卡安裝托架, 以及擴充卡上的 BSMI 註冊標籤。如果其中有一甲類標籤, 即表示您的系統為甲類數位裝置。如果只有 BSMI 的檢磁號碼標籤, 則表示您的系統為乙類數位裝置。

一旦確定了系統的 BSMI 等級, 請閱讀相關的 BSMI 通告。請注意, BSMI 通告規定凡是未經 Dell Inc. 明確批准的擅自變更或修改, 將導致您失去此設備的使用權。

此裝置符合 BSMI (經濟部標準檢驗局) 的規定, 使用時須符合以下兩項條件:

- 此裝置不會產生有害干擾。
- 此裝置必須能接受所接收到的干擾, 包括可能導致無法正常作業的干擾。

### 乙類

此設備經測試證明符合 BSMI (經濟部標準檢驗局) 之乙類數位裝置的限制規定。這些限制的目的是為了在住宅區安裝時, 能防止有害的干擾, 提供合理的保護。此設備會產生、使用並散發射頻能量; 如果未遵照製造廠商的指導手冊來安裝和使用, 可能會干擾無線電通訊。但是, 這並不保證在個別的安裝中不會產生干擾。您可以透過關閉和開啓此設備來判斷它是否會對廣播和電視收訊造成干擾; 如果確實如此, 我們建議您嘗試以下列一種或多種方法來排除干擾:

- 重新調整天線的接收方向或重新放置接收天線。
- 增加設備與接收器的距離。
- 將設備連接至不同的插座, 使設備與接收器連接在不同的電路上。
- 請向經銷商或有經驗的無線電 / 電視技術人員查詢, 以獲得幫助。



## 16 절: 문제 해결 단계

- 하드웨어 진단
- 문제 해결 검사 목록
- 네트워크 링크 및 활동 상태 검사
- 최신 드라이버가 로드되었는지 검사
- 케이블 길이 테스트 실행
- 네트워크 연결 테스트
- Broadcom Boot Agent
- BASP(Broadcom Advanced Server Program)
- 이더넷을 통한 커널 디버깅
- 기타

### 하드웨어 진단

어댑터 하드웨어를 테스트할 때 루프백 진단 테스트를 사용할 수 있습니다. 이 테스트를 통해 실제 링크 상에서 패킷 정보가 전송되는 경우, 어댑터의 내부/외부 진단에 액세스할 수 있습니다. [진단 테스트 실행](#) 참조).

### BACS 진단 테스트 실패

BACS의 [진단 테스트 실행](#) 탭에서 진단 테스트를 실행하는 중 실패가 발생하면 이는 시스템에 설치된 NIC 또는 LOM 하드웨어에 문제가 있다는 의미일 수 있습니다.

- 제어 레지스터.
- MII 레지스터
- EEPROM
- 내부 메모리.
- 칩 내장 CPU
- 일시 중지
- 루프백 - MAC
- 루프백 - PHY
- LED 테스트

다음 문제 해결 단계를 통해 오류를 해결할 수도 있습니다.

1. 오류가 발생한 장치를 제거하여 슬롯에 옮기고 카드 앞뒤가 올바른 상태에서 슬롯에 완전히 장착되었는지 확인합니다.
2. 테스트를 다시 실행합니다.
3. 카드에 계속 오류가 나면 모델이 같은 다른 카드로 바꾼 후 테스트를 실행합니다. 알려진 좋은 품질의 카드에서 테스트가 통과되면 하드웨어 공급업체에 문의하여 오류가 발생한 장치에 대해 도움을 받으십시오.
4. 시스템 전원을 꺼 AC 전원을 제거한 후 시스템을 다시 부팅합니다.
5. 진단 소프트웨어를 제거하고 다시 설치합니다.
6. 하드웨어 공급업체에 문의하십시오.

## BACS 네트워크 테스트 실패

일반적으로 BACS [네트워크 테스트](#) 오류는 네트워크나 IP 주소 구성에 문제가 있기 때문에 발생합니다. 다음은 네트워크 문제 해결 시 수행해야 할 일반적인 단계입니다.

1. 케이블이 연결되었으며 링크가 올바른지 확인합니다.
2. 드라이버가 로드되고 활성화되었는지 확인합니다.
3. NIC/LOM에 연결된 케이블을 교체합니다.
4. "ipconfig" 명령을 사용하거나 OS IP 할당 도구를 선택하여 IP 주소를 제대로 할당했는지 확인합니다.
5. 어댑터가 연결된 네트워크의 IP 주소가 올바른지 확인합니다.

---

## 문제 해결 검사 목록



**주의!** 컴퓨터 케이스를 열기 전에 [안전 주의 사항](#)을 검토하십시오.

다음 검사 목록은 **Broadcom NetXtreme Gigabit Ethernet** 어댑터를 설치하거나 시스템에서 실행할 때 발생할 수 있는 문제를 해결하기 위해 수행하도록 권장되는 조치들입니다.

- 케이블과 연결 부분을 모두 검사합니다. 네트워크 어댑터의 케이블과 스위치가 올바르게 연결되었는지 확인합니다. 케이블 길이와 등급이 [네트워크 케이블 연결](#)에 나열된 요구 사항을 준수하는지 확인합니다.
- [하드웨어 설치](#)를 검토하여 어댑터 설치를 확인합니다. 어댑터가 슬롯에 올바르게 위치해 있는지 확인합니다. 보드 구성 요소 또는 PCI 에지 커넥터의 확인한 손상과 같은 특정 하드웨어 문제를 검사합니다.
- 구성 설정을 확인하고 다른 장치와 충돌하면 변경합니다.
- 시스템에 최신 **BIOS**가 사용되고 있는지 확인합니다.
- 어댑터를 다른 슬롯에 삽입해 봅니다. 새 위치에서 작동하는 경우 시스템의 원래 슬롯에 결함이 있을 수 있습니다.
- 결함이 있는 어댑터를 올바르게 작동하는 어댑터로 교체합니다. 첫 번째 어댑터가 작동하지 않는 슬롯에 두 번째 어댑터가 작동하는 경우 원래 어댑터에 결함이 있을 수 있습니다.
- 제대로 작동이 되는 다른 시스템에 어댑터를 설치한 후 테스트를 다시 실행합니다. 어댑터가 새 시스템에서 테스트를 통과한 경우 원래 시스템에 결함이 있을 수 있습니다.
- 시스템에서 다른 어댑터를 모두 제거한 후 테스트를 다시 실행합니다. 어댑터가 테스트를 통과한 경우 다른 어댑터에 충돌이 발생했을 수 있습니다.

---

## 네트워크 링크 및 활동 상태 검사

포트 LED로 알 수 있는 네트워크 링크 및 활동 상태를 확인하려면 [네트워크 연결 테스트](#) 및 [어댑터 정보 확인](#)을 참조하십시오.

---

## 최신 드라이버가 로드되었는지 검사

### Windows

어댑터, 해당 링크 상태 및 네트워크 연결에 대한 유용한 정보를 보려면 [어댑터 정보 확인](#)을 참조하십시오.

### Linux

TG3 Linux 드라이버가 올바르게 로드되었는지 확인하려면 다음을 실행합니다.

```
lsmod | grep tg3
```

드라이버가 로드된 경우 다음과 같은 행이 표시됩니다(*size*는 드라이버 크기(바이트), *n*은 구성된 어댑터 수).

표 24. Linux 드라이버

| 모듈  | size | 사용자 |
|-----|------|-----|
| TG3 | size | n   |

---

## 케이블 길이 테스트 실행

Windows 환경에서는 케이블 길이 테스트를 실행할 수 있습니다. 케이블 길이 테스트에 대한 자세한 내용은 [케이블 분석](#)을 참조하십시오.

## 네트워크 연결 테스트



**참고:** 강제 링크 속도를 사용하는 경우 어댑터와 스위치가 모두 동일한 속도로 강제 설정되었거나 양쪽 모두 자동 협상을 위해 구성되었는지 확인합니다.

## Windows

네트워크 연결이 작동하는지 확인하려면 ping 명령을 사용합니다.



**참고:** 네트워크 연결은 Broadcom Advanced Control Suite 2의 [네트워크 테스트](#) 기능을 사용하여 테스트할 수도 있습니다.

1. 드라이버가 로드되고 활성화되었는지 확인합니다.
2. 케이블이 연결되었으며 링크가 올바른지 확인합니다.
3. 시작을 클릭한 후 실행을 클릭합니다.
4. 열기 상자에 cmd를 입력한 후 확인을 클릭합니다.
5. 테스트할 네트워크 연결을 보려면 ipconfig /all을 입력합니다.
6. 어댑터가 연결된 네트워크의 IP 주소가 올바른지 확인합니다.
7. Ping IP 주소를 입력한 후 Enter 키를 누릅니다.

표시된 Ping 통계는 네트워크 연결이 작동하는지 여부를 나타냅니다.

## Linux

Ethernet 인터페이스가 가동되어 실행 중인지 확인하려면 ifconfig를 실행하여 Ethernet 인터페이스의 상태를 확인합니다. netstat -i를 사용하여 Ethernet 인터페이스의 통계를 확인할 수 있습니다. ifconfig 및 netstat에 대한 정보는 [Linux 드라이버 소프트웨어](#)를 참조하십시오.

연결이 설정되었는지 확인하려면 네트워크에 IP 호스트를 Ping합니다.

명령행에서 Ping IP 주소를 입력한 후 Enter 키를 누릅니다.

표시된 Ping 통계는 네트워크 연결이 작동하는지 여부를 나타냅니다.

## Broadcom Boot Agent

**문제:** PXE를 사용하는 DHCP를 통해 네트워크 설정을 가져올 수 없습니다.

**해결 방법:** 올바른 작동을 위해 PXE 클라이언트가 연결된 포트에 STP(스패닝 트리 프로토콜)가 비활성화되었거나, portfast 모드(Cisco)가 활성화되었는지 확인하십시오. 예를 들어, spantree portfast 4/12를 활성화하도록 설정합니다.

---

## BASP(Broadcom Advanced Server Program)

**문제:** 팀의 일부인 NIC를 물리적으로 제거하고 다시 부팅할 경우 팀이 예상한 대로 수행되지 않습니다.

**해결 방법:** 시스템에서 팀 구성 NIC를 물리적으로 제거하려면 먼저 팀에서 NIC를 삭제해야 합니다. 시스템을 종료하기 전에 이 작업을 수행하지 않을 경우 다음 부팅 시 팀이 분해되어 예상치 못한 팀 동작이 발생할 수 있습니다.

**문제:** INETCFG를 사용하여 내 팀을 수정한 경우 내가 변경한 팀 구성 변경 사항이 적용되지 않았습니다.

**해결 방법:** INETCFG를 사용하여 팀을 수정한 경우 다시 초기화한 후 다시 부팅해야 변경 사항이 적용됩니다.

---

## 이더넷을 통한 커널 디버깅

**문제:** Windows 8.0 또는 Windows Server 2012 시스템에서 이더넷 네트워크를 통해 커널 디버깅을 수행하려고 할 때 시스템이 부팅되지 않습니다. 이 문제는 Windows 8.0 또는 Windows Server 2012 OS가 UEFI 모드에 대해 구성된 시스템의 일부 어댑터에서 발생할 수 있습니다. UEFI 사전 부팅 환경 중에 마스크 불가능 인터럽트 예외 발생을 알리는 펌웨어 오류가 화면에 표시될 수 있습니다.

**해결 방법:** Microsoft 기술 자료 항목 번호 2920163, "[이더넷을 통한 커널 디버깅에 대해 구성된 시스템에서 부팅 중 마스크 불가능 인터럽트 오류 발생](#)"을 참조하십시오.

---

## 기타

**문제:** Large Send Offload(LSO) 및 Checksum Offload는 일부 팀에서만 작동합니다.

**해결 방법:** 팀의 어댑터 중 하나가 LSO를 지원하지 않는 경우 LSO가 팀에 맞게 작동되지 않습니다. 팀의 LSO를 지원하지 않는 어댑터를 제거하거나 LSO를 지원하는 어댑터로 교체하십시오. 이는 Checksum Offload에서도 동일하게 적용됩니다.