Catalyst 9000 스위치의 NLB 구축에 대한 IGMP 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[배경 정보](#)
[구성](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 Catalyst 9000 Series 스위치의 IGMP 기능이 Microsoft NLB(Network Load Balancer) 구축 환경에서 어떻게 작동하는지 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft NLB 작동 모드
- IGMP 멀티캐스트

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

NLB는 모든 Windows 2000 Server 및 Windows 2003 Server 제품군 시스템에서 사용할 수 있는 클러스터 기술입니다. 모든 클라이언트에 대한 단일 가상 IP 주소를 전체 클러스터의 대상 IP 주소로 제공합니다.

NLB는 서버 집합 전반에 클라이언트 요청을 배포하는 데 사용할 수 있습니다. NLB는 클라이언트가 적절한 성능 수준을 경험할 수 있도록 클라이언트 로드가 증가함에 따라 스테이트리스 애플리케이션(예: IIS 기반 웹 서버)을 스케일 아웃할 수 있는 서버를 추가할 수 있는 기능을 제공합니다. 또한 서버 오작동으로 인한 다운타임을 줄입니다.

다음 세 가지 모드 중 하나에서 작동하도록 NLB를 구성할 수 있습니다.

- 유니캐스트 모드
- 멀티캐스트 모드
- IGMP(Internet Group Management Protocol) 모드

> 팁: 유니캐스트 모드 및 멀티캐스트 모드 구축은 문서 Catalyst Switches for Microsoft Network Load Balancing Configuration 예시에 설명된 것과 동일한 컨피그레이션 및 검증을 가집니다

이 문서에서는 IGMP(Internet Group Management Protocol) 모드를 중점적으로 다룹니다.

모범 사례

Catalyst 9000 Series 스위치는 스누핑 테이블을 채우기 위해 IGMP 패킷의 레이어 3 헤더를 스누핑합니다. 고정 멀티캐스트 MAC을 사용하여 스위치에서 NLB를 구성해야 하므로 IGMP 스누핑 테이블이 채워지지 않으며 대상 VLAN에 플러딩이 발생합니다. 즉, NLB 서버가 IGMP 모드에 있을 때 (Catalyst 9000의 포워딩은 멀티캐스트 MAC 주소가 아닌 멀티캐스트 IP를 기반으로 함) Catalyst 9000의 IGMP 스누핑에 멀티캐스트 플러드가 자동으로 포함되지 않습니다.

> 참고: Catalyst 9000에서는 NLB의 세 가지 모드에서 모두 플러딩이 발생합니다. 패킷의 목적지가 기본 게이트웨이여야 한다는 점을 감안할 때 사용자 VLAN에서는 플러딩이 발생하지 않습니다. 헤더가 대상 VLAN에 재작성되어야 플러드가 발생합니다.

따라서 성공적인 구축을 위해 다음 모범 사례를 고려하십시오.

- 전용 VLAN을 사용하여 플러딩을 NLB 클러스터로만 제한합니다.
- 고정 MAC 항목을 활용하여 NLB VLAN 내에서 플러드가 발생하는 포트를 제한합니다.

IGMP 모드

이 모드에서는 NLB 클러스터의 가상 MAC이 IANA(Internet Assigned Numbers Authority) 범위에 속하며 0100.5exx.xxxx로 시작합니다. 이 IGMP Snooping 스위치에 구성된 기능은 클러스터의 가상 멀티캐스트 MAC 주소를 MAC 주소 테이블에 프로그래밍하지 않습니다. 이 동적 프로그래밍이 없으므로 스위치에서 NLB 클러스터로부터 수신한 멀티캐스트 트래픽이 동일한 VLAN의 모든 포트 멤버에 플러딩됩니다. Cisco 버그 ID CSCvw18989.

NLB 서버가 사용자와 다른 VLAN에 있는 토폴로지의 경우 클러스터의 가상 IP 주소가 멀티캐스트 MAC 주소를 사용하므로 로컬 서브넷 외부에서 연결할 수 없습니다. 이를 해결하려면 클러스터 VLAN에 레이어 3 인터페이스가 있는 각 디바이스에서 고정 ARP 항목을 구성해야 합니다.

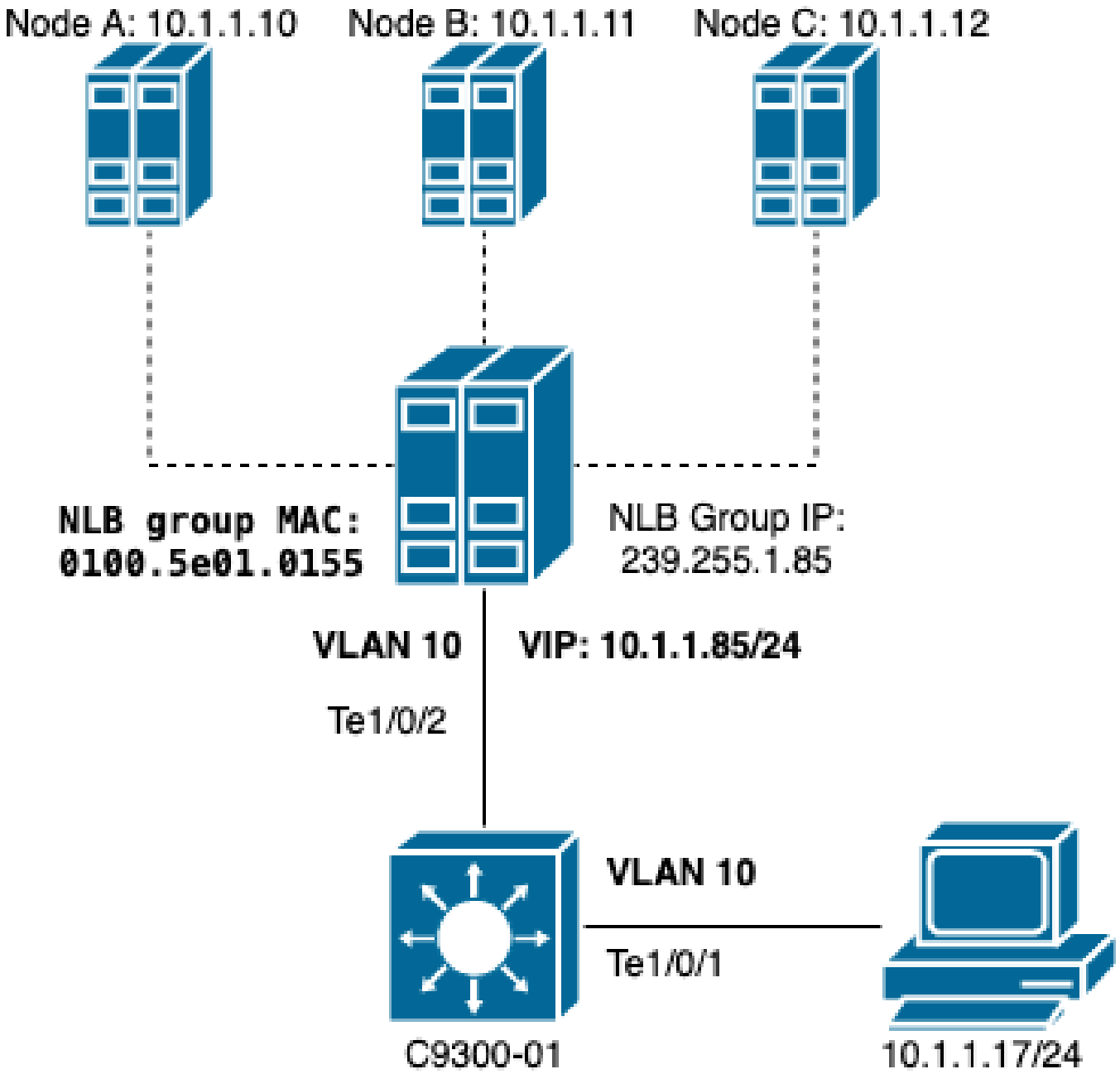
Catalyst 9000 Series 스위치의 IGMP 스누핑 기능은 포워딩을 위해 멀티캐스트 MAC 주소를 사용하지 않습니다. 멀티캐스트 IP 주소를 사용하므로 다른 레거시 플랫폼(예: Catalyst 6000 Series)처럼 MAC 테이블에서 멀티캐스트 MAC 주소를 자동으로 프로그래밍할 수 없습니다. 모든 신규 플랫폼에서는 레거시 스위치에서 발견되는 주소 중복 문제를 방지하기 위해 멀티캐스트 IP 주소 포워딩 방식을 사용합니다.

> 참고: 이더넷 멀티캐스트 MAC 주소가 중복됩니다. 동일한 MAC 주소가 32개의 서로 다른 멀티캐스트 그룹에 할당됩니다. 이더넷 세그먼트의 한 사용자가 멀티캐스트 그룹 225.1.1.1에 가입하고 다른 사용자가 230.1.1.1에 가입하면 두 사용자 모두 두 멀티캐스트 스트림을 수신합니다(MAC 주소는 01-00-5e-01-01-01 동일). LAN 세그먼트에서 멀티캐스트 네트워크를 엔지니어링하는 경우 이러한 중복에 대해 특별히 주시하고 문제를 방지하기 위해 설계해야 합니다.

구성

동일한 VLAN의 소스 및 대상

네트워크 다이어그램



이 섹션에서는 클러스터와 사용자가 동일한 VLAN에 있을 때 NLB를 구성하는 방법에 대해 설명합니다.

1. NLB VLAN이 생성되었는지 확인합니다. 홍수로 인해 NLB 트래픽에 전용 VLAN을 두는 것이 좋습니다.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   NLB                              active    Te1/0/1, Te1/0/2, Te1/0/3
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

2. 다이 NLB 트래픽을 가져와야 하는 포트의 고정 MAC 주소 항목을 구성합니다. 이 명령은 NLB VLAN의 NLB 클러스터 경로에 있는 모든 트렁크 포트 또는 액세스 포트를 포함해야 합니다. 다이어그램에서 Tengig1/0/2를 통해 NLB로 향하는 경로는 하나뿐입니다.

<#root>

C9300-01(config)#

mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet 1/0/2

C9300-01#

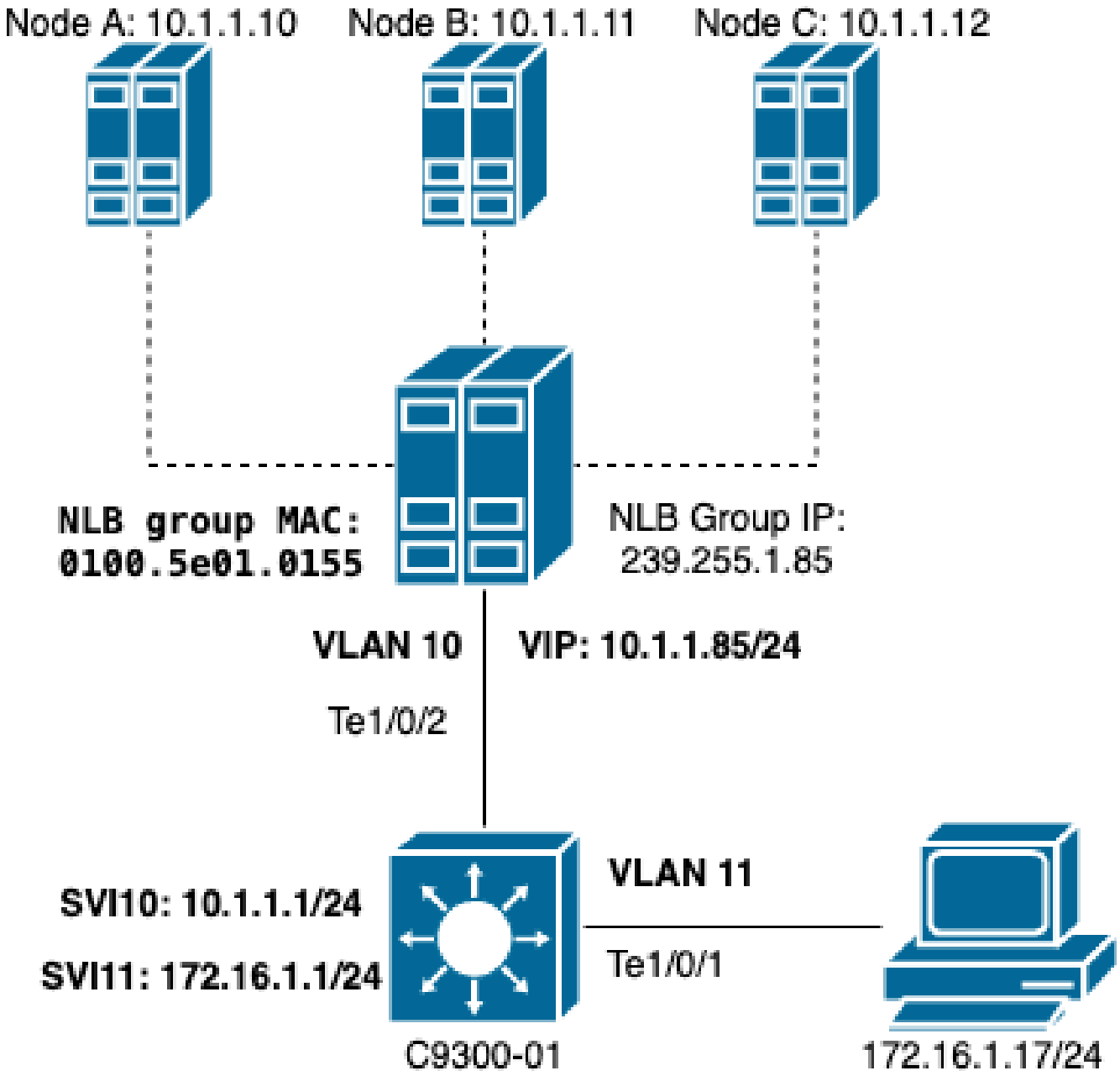
show run | in mac

```
mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet1/0/2
```

참고: 고정 MAC 주소 항목에는 필요한 만큼 매핑된 포트를 포함할 수 있습니다. 이러한 포트 맵은 NLB의 VLAN 내에서 예상되는 플러드를 줄입니다. 이 예에서 고정 MAC 항목은 NLB 클러스터로 향하는 트래픽이 Te1/0/3에서 플러딩되는 것을 방지할 수 있습니다.

다른 VLAN의 소스 및 대상

네트워크 다이어그램



이 섹션에서는 클러스터와 사용자가 서로 다른 VLAN에 있을 때 NLB를 구성하는 방법에 대해 설명합니다.

1. NLB VLAN 및 IP 주소를 NLB 클러스터의 기본 게이트웨이로 구성합니다.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   NLB                              active    Te1/0/2, Te1/0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

```
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

C9300-01#
```

show run interface vlan 10

```
Building configuration...

Current configuration : 59 bytes
!
interface Vlan10
 ip address 10.1.1.1 255.255.255.0
end
```

2. NLB 클러스터 서버의 가상 IP 주소에 대한 고정 ARP 항목을 구성합니다. 정적 ARP는 클러스터 VLAN에 SVI(Switch Virtual Interface)가 있는 모든 레이어 3 디바이스에 구성해야 합니다. 고정 ARP의 목적은 라우티드 패킷을 NLB VLAN으로 전송하는 데 필요한 재작성 정보를 스위치에 제공하는 것입니다.

<#root>

C9300-01(config)#

arp 10.1.1.85 0100.5e01.0155 arpa

3. 액세스 레이어와 기본 게이트웨이에서 생성된 사용자 VLAN을 확인합니다. 양쪽 모두에서 기본 게이트웨이를 구성하는 것이 중요합니다. (NLB 클러스터 및 사용자)

<#root>

C9300-01#

show vlan id 11

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
11   Users2                           active    Te1/0/1, Te1/0/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
11   enet  100011     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

```
Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------

C9300-01#

show run interface vlan 11

Building configuration...

Current configuration : 59 bytes
!
interface Vlan11
 ip address 172.16.1.1 255.255.255.0
end
```

참고: 대상 MAC가 이그레스 SVI에서 학습되지 않은 MAC 헤더 재작성 이후에 라우팅된 패킷은 해당 VLAN에서 플러딩됩니다. 플러드를 완화하려면 NLB 서버에 대해서만 게이트웨이와 별도의 VLAN을 생성해야 합니다. NLB 트래픽에 대한 전용 VLAN을 구성하지 않으려면 NLB 트래픽을 수신해야 하는 포트에 대해 고정 MAC 주소 항목, 즉 mac address-table static 0100.5exx.xxxx vlan # interface interface_name을 구성할 수 있습니다

문제 해결

1. 고정 MAC 주소가 트래픽을 NLB로 전달해야 하는 모든 대상 포트에 구성되었는지 확인합니다.

<#root>

```
C9300-01#

show mac address multicast

Vlan Mac Address Type Ports
---- ----------- ---- -----
10 0100.5e01.0155 USER Te1/0/2
```

2. NLB 클러스터가 클라이언트와 다른 서브넷에 있는 구축의 경우 NLB 서버의 가상 IP를 멀티캐스트 MAC 주소와 매핑하는 고정 ARP 항목이 있는지 확인합니다.

<#root>

```
C9300-01#

show run | in arp

arp 10.1.1.85 0100.5e01.0155 ARPA

C9300-01#

show ip arp

Protocol Address Age (min) Hardware Addr Type Interface
```

```
Internet 10.1.1.1 - c4c6.0309.cf46 ARPA Vlan10
Internet 10.1.1.85 - 0100.5e01.0155 ARPA
Internet 172.16.1.1 - c4c6.0309.cf54 ARPA Vlan11
```

3. 자주 사용하지 않는 크기의 NLB 서버 IP에 대해 ping을 수행합니다. 포트의 컨트롤러를 지우고 이 명령의 여러 번 반복해서 어떤 크기가 그렇게 많이 사용되지 않았는지 확인합니다.

<#root>

C9300-01#

show controllers ethernet-controller Te1/0/2 | in 1024

0 1024 to 1518 byte frames 0 1024 to 1518 byte frames

C9300-01#

clear controllers ethernet-controller Te1/0/2

HOST#

ping 10.1.1.85 time 0 rep 1000 size 1024

```
Type escape sequence to abort.
Sending 1000, 1024-byte ICMP Echos to 10.1.1.85, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

4. 대상 포트에서 ping이 제대로 전달되었는지, 동일한 ping 테스트가 다른 포트에 플러딩되었는지 확인합니다. 서로 다른 인터페이스에서 동일한 컨트롤러 카운터 명령을 사용하여 이를 확인합니다.

<#root>

C9300-01#

show controllers ethernet-controller Te1/0/1 | in 1024

```
 <-- Ingress Host port
0 1024 to 1518 byte frames 1000 1024 to 1518 byte frames
```

C9300-01#

show controllers ethernet-controller Te1/0/2 | in 1024

```
 <-- Egress port to NLB
1000 1024 to 1518 byte frames 0 1024 to 1518 byte frames
```

5. EPC가 있는 인그레스 포트와 SPAN이 있는 이그레스 포트에서 패킷 캡처를 수행하고 스위치가 데이터를 전달하는지 확인합니다.

<#root>

C9300-01#

monitor capture tac buffer size 10 match any interface Te1/0/1 in

C9300-01#

monitor capture tac start

C9300-01#

monitor capture tac stop

C9300-01#

monitor capture tac export location flash:DataTraffic.pcap

> 팁: EPC(Embedded Packet Capture) 기능은 패킷이 레이어 2 인그레스 또는 이그레스 방향으로 전달될 때 신뢰할 수 있습니다. 그러나 트래픽이 스위치에 의해 라우팅된 다음 이그레스 포트로 전달되는 경우 EPC를 신뢰할 수 없습니다. 레이어 3 라우팅이 발생한 후 이그레스(egress)에서 패킷을 캡처하려면 SPAN(Switch Port Analyzer) 기능을 사용합니다.

<#root>

C9300-01(config)#

monitor session 1 source interface Te1/0/2 tx

C9300-01(config)#

monitor session 1 destination interface Te1/0/3 encapsulation replicate

C9300-01#

show monitor session all

```
Session 1
---------
Type : Local Session
Source Ports :
TX Only : Te1/0/2
Destination Ports : Te1/0/3
Encapsulation : Replicate
Ingress : Disabled
```

관련 정보

- Microsoft 네트워크 부하 분산 구성용 Catalyst 스위치 예
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.