# 네트워크에서 RSPAN(Remote Switch Port Analyzer) 설정 구성

목차

- <u>목표</u>
- <u>적용 가능한 디바이스 | 펌웨어 버전</u>
- <u>소개</u>
- <u>스위치에서 RSPAN VLAN 구성</u>
- <u>시작 스위치에 세션 소스 구성</u>
- <u>시작 스위치에서 세션 대상 구성</u>
- <u>중간 스위치</u>
- <u>최종 스위치에서 세션 소스 구성</u>
- <u>최종 스위치에서 세션 대상 구성</u>
- <u>WireShark에서 캡처된 RSPAN VLAN 패킷 분석</u>

## 목표

이 문서에서는 스위치에서 RSPAN을 구성하는 방법에 대한 지침을 제공합니다.

### 적용 가능한 디바이스 | 펌웨어 버전

- SX350 | 2.2.5.68(<u>최신 다운로드</u>)
- SG350X | 2.2.5.68(<u>최신 다운로드</u>)
- SX550X | 2.2.5.68(<u>최신 다운로드</u>)

### 소개

SPAN(Switch Port Analyzer) 또는 포트 미러링 또는 포트 모니터링이라고도 하는 경우 네트워크 분 석기가 분석할 네트워크 트래픽을 선택합니다.네트워크 분석기는 Cisco SwitchProbe 디바이스 또 는 다른 RMON(Remote Monitoring) 프로브일 수 있습니다.

포트 미러링은 네트워크 디바이스에서 단일 디바이스 포트, 여러 디바이스 포트 또는 전체 VLAN(Virtual Local Area Network)에서 보이는 네트워크 패킷의 사본을 디바이스의 다른 포트에서 네트워크 모니터링 연결에 전송하는 데 사용됩니다.이는 침입 탐지 시스템과 같이 네트워크 트래픽 을 모니터링해야 하는 네트워크 어플라이언스에 일반적으로 사용됩니다.모니터링 포트에 연결된 네트워크 분석기는 진단, 디버깅 및 성능 모니터링을 위해 데이터 패킷을 처리합니다.

RSPAN(Remote Switch Port Analyzer)은 SPAN의 확장입니다.RSPAN은 네트워크 전체에서 여러 스위치를 모니터링하고 원격 스위치에 분석기 포트를 정의함으로써 SPAN을 확장합니다.즉, 네트 워크 캡처 디바이스를 중앙 집중화할 수 있습니다.

RSPAN은 RSPAN 세션의 소스 포트에서 RSPAN 세션 전용 VLAN으로 트래픽을 미러링하는 방식 으로 작동합니다.그런 다음 이 VLAN을 다른 스위치로 트렁킹하여 RSPAN 세션 트래픽을 여러 스 위치에서 전송할 수 있습니다.세션의 대상 포트가 포함된 스위치에서 RSPAN 세션 VLAN의 트래픽 은 단순히 대상 포트에서 미러링됩니다.

#### RSPAN 트래픽 흐름

- 각 RSPAN 세션에 대한 트래픽은 모든 참여 스위치에서 해당 RSPAN 세션을 위한 전용 사용자 지정 RSPAN VLAN을 통해 전달됩니다.
- 시작 디바이스의 소스 인터페이스의 트래픽은 리플렉터 포트를 통해 RSPAN VLAN에 복사됩니다.이 포트는 설정해야 합니다.RSPAN 세션을 구축하는 데만 사용됩니다.
- 이 리플렉터 포트는 RSPAN VLAN에 패킷을 복사하는 메커니즘입니다.RSPAN은 연결된 RSPAN 소스 세션의 트래픽만 전달합니다.어떤 디바이스가 리플렉터 포트로 설정된 포트에 연 결되면, RSPAN 소스 세션이 비활성화될 때까지는 연결되지 않습니다.
- 그런 다음 RSPAN 트래픽은 중간 디바이스의 트렁크 포트를 통해 최종 스위치의 대상 세션으 로 전달됩니다.
- 대상 스위치는 RSPAN VLAN을 모니터링하고 목적지 포트에 복사합니다.

#### RSPAN 포트 멤버십 규칙

- 모든 스위치에서 RSPAN VLAN의 멤버십은 태그만 가능합니다.
- 스위치 시작
- SPAN 소스 인터페이스는 RSPAN VLAN의 멤버일 수 없습니다.
- 리플렉터 포트는 이 VLAN의 멤버일 수 없습니다.
- 원격 VLAN에 멤버십이 없는 것이 좋습니다.
  - 중간 스위치

- 미러링된 트래픽을 전달하는 데 사용되지 않는 모든 포트에서 RSPAN 멤버십을 제거하는 것이 좋 습니다.

- 일반적으로 RSPAN 원격 VLAN에는 2개의 포트가 포함됩니다.
  - 최종 스위치
- 미러링된 트래픽의 경우 소스 포트는 RSPAN VLAN의 멤버여야 합니다.
- 대상 인터페이스를 포함하여 다른 모든 포트에서 RSPAN 멤버십을 제거하는 것이 좋습니다.

## 네트워크에서 RSPAN 구성

#### 스위치에서 RSPAN VLAN 구성

RSPAN VLAN은 RSPAN 소스와 대상 세션 간에 SPAN 트래픽을 전달합니다.여기에는 다음과 같은 특수 특징이 있습니다.

- RSPAN VLAN의 모든 트래픽은 항상 플러딩됩니다.
- RSPAN VLAN에서 MAC(Media Access Control) 주소 학습이 발생하지 않습니다.
- RSPAN VLAN 트래픽은 트렁크 포트에서만 이동합니다.
- STP는 RSPAN VLAN 트렁크에서 실행할 수 있지만 SPAN 대상 포트에서는 실행할 수 없습니 다.
- remote-span VLAN 컨피그레이션 모드 명령을 사용하여 VLAN 컨피그레이션 모드의 시작 및 최종 스위치 모두에 RSPAN VLAN을 구성하거나 아래 지침을 따라야 합니다.

1단계. Start Switch의 웹 기반 유틸리티에 로그인하고 Display Mode 드롭다운 목록에서 Advanced를 선택합니다.



2단계. VLAN Management(VLAN 관리) > VLAN Settings(VLAN 설정)를 선택합니다.

-	VLAN Managemen	t)
	VLAN Settings	
	Interface Settings	
	Port to VLAN	
	Port VLAN Membe	ership
	Private VLAN Sett	tings
	GVRP Settings	
	VLAN Groups	
	Voice VLAN	

- Access Port Multicast TV VLA
- Customer Port Multicast TV V

3단계. **추가**를 클릭합니다.

١	VLAN Settings						
	VLA	N Table					
		VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps	
		1		Default	Enabled	Enabled	
		10	VLAN 10	Static	Enabled	Enabled	
		Add	Edit	Delete			

4단계. VLAN *ID* 필드에 VLAN ID를 입력합니다.

VLAN ID: 20 (Range: 2 - 4094)

참고:이 예에서는 VLAN 20이 VLAN ID로 사용됩니다.

5단계. (선택 사항) VLAN Name 필드에 VLAN Name을 입력합니다.

VLAN ID:	20	(Range: 2 - 4094)
VLAN Name	: RSPAN VLAN	(10/32 characters used)

참고:이 예에서는 RSPAN VLAN이 VLAN 이름으로 사용됩니다.

6단계. (선택 사항) VLAN Interface State(VLAN 인터페이스 상태) 확인란을 선택하여 VLAN을 활성 화합니다.VLAN이 종료되면 VLAN은 더 높은 레벨에서 메시지를 전송하거나 수신하지 않습니다.예 를 들어 IP 인터페이스가 구성된 VLAN을 종료하면 VLAN에 브리징은 계속되지만 스위치에서 VLAN의 IP 트래픽을 전송하고 수신할 수 없습니다.이 기능은 기본적으로 활성화되어 있습니다.

7단계. (선택 사항) SNMP(Simple Network Management Protocol) 트랩의 링크 상태 생성을 활성화 하려면 Link Status SNMP Traps 확인란을 선택합니다.이 기능은 기본적으로 활성화되어 있습니다.

8단계. Apply(적용)를 클릭한 다음 Close(닫기)를 클릭합니다.

VLAN						
VLAN ID:	20	(Range: 2 - 4094)				
VLAN Name:	RSPAN VLAN	(10/32 characters used)				
VLAN Interface	VLAN Interface State: 🕑 Enable					
Link Status SN	IMP Traps: 🕑 Enable					
Range						
✤ VLAN Range:		•				
Apply	Close					

**참고:**스위치에서 VLAN 관리에 대한 자세한 내용을 보려면 <u>여기</u>를 클릭하십시오.

9단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

/	IP 4	48-Por	t Gigabit I	PoE Sta	okable Mana	ء، ged Swite	sco ch
,	VLAN Settings						
	VLA	N Table					
		VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps	
		1		Default	Enabled	Enabled	
		10	VLAN 10	Static	Enabled	Enabled	
		20	RSPAN VLAN	Static	Enabled	Enabled	
		Add	Edit	Delete	)		

10단계. Status and Statistics(상태 및 통계) > SPAN & RSPAN > RSPAN VLAN을 선택합니다.

Status and Statistics
System Summary
CPU Utilization
Interface
Etherlike
Port Utilization
GVRP
802.1x EAP
ACL
TCAM Utilization
Health
▼ SPAN & RSPAN
RSPAN VLAN
Session Destinations
Session Sources
<ul> <li>Diagnostics</li> </ul>
► RMON
▶ sFlow
▶ View Log
Administration

11단계. RSPAN VLAN 드롭다운 목록에서 VLAN ID를 선택합니다.이 VLAN은 RSPAN에만 사용해 야 합니다.



**참고:**이 예에서는 VLAN 20이 선택됩니다.

12단계. 적용을 **누릅니다**.



13단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

🚫 Sav

# MP 48-Port Gigabit PoE Stackable Managed Switch

### **RSPAN VLAN**

Success. To permanently save the configuration, go to the File Operations page

A VLAN must be added to the VLAN Database using the VLAN Settings screen before it can be co



14단계. 최종 스위치에서 1~13단계를 반복하여 RSPAN VLAN을 구성합니다.

이제 시작 및 최종 스위치 모두에서 RSPAN 세션 전용 VLAN을 구성해야 합니다.

#### 시작 스위치에 세션 소스 구성

1단계. Status **and Statistics(상태 및 통계) > SPAN & RSPAN > Session Sources(세션 소스)를 선** 택합니다.

cisco

<ul> <li>Status and Statistics</li> </ul>
System Summary
CPU Utilization
Interface
Etherlike
Port Utilization
GVRP
802.1x EAP
ACL
TCAM Utilization
Health
SPAN & RSPAN
RSPAN VLAN
Session Destinations
Session Sources
Diagnostics
RMON
▶ sFlow
View Log
Administration

2단계. **추가**를 클릭합니다.

Session Sources							
Ses	Session Source Table						
Filte	er: 📄 Sessi	ion ID equals to	0 🔽 G0	Clear Filter			
	Session ID	Destination	Source Interface	Monitor Type			
0 results found.							
С	Add Edit Delete						

3단계. 세션 ID 드롭다운 목록에서 세션 번호를 선택합니다.세션 ID는 RSPAN 세션당 일관적이어 야 합니다.



참고:이 예에서는 세션 1이 선택됩니다.

4단계. 원하는 소스 인터페이스 유형에 대한 라디오 버튼을 클릭하고 드롭다운 목록 또는 목록에서 인터페이스를 선택합니다.

중요:소스 인터페이스는 대상 포트와 같을 수 없습니다.

Source Interface: 

Unit
Port
GE2
VLAN
Remote VLAN (VLAN 20)

옵션은 다음과 같습니다.

- Unit and Port(유닛 및 포트) Unit(유닛) 드롭다운 목록에서 원하는 옵션을 선택하고 Port(포트) 드롭다운 목록에서 소스 포트로 설정할 포트를 선택할 수 있습니다.
- VLAN VLAN 드롭다운 목록에서 모니터링할 원하는 VLAN을 선택할 수 있습니다.VLAN을 사용하면 호스트 그룹이 위치에 관계없이 동일한 물리적 네트워크에 있는 것처럼 통신할 수 있 습니다.이 옵션을 선택하면 편집할 수 없습니다.
- 원격 VLAN 정의된 RSPAN VLAN이 표시됩니다.이 옵션을 선택하면 편집할 수 없습니다.

**참고:**이 예에서는 유닛 1의 포트 GE2가 선택됩니다.모니터링될 원격 인터페이스입니다.

5단계. (선택 사항) 4단계에서 장치 및 포트를 클릭한 경우 모니터링할 트래픽 유형에 대해 원하는 모니터 유형 라디오 버튼을 클릭합니다.



옵션은 다음과 같습니다.

- Rx 및 Tx 이 옵션은 수신 및 발신 패킷의 포트 미러링을 허용합니다.이 옵션은 기본적으로 선택되어 있습니다.
- Rx 이 옵션은 수신 패킷의 포트 미러링을 허용합니다.
- Tx 이 옵션은 발신 패킷의 포트 미러링을 허용합니다.

참고:이 예에서는 Rx가 선택됩니다.

6단계. Apply(적용)를 클릭한 다음 Close(닫기)를 클릭합니다.

Session ID:	1 •
Source Interface:	: ● Unit 1 ▼ Port GE2 ▼ ○ VLAN 1 ▼ ○ Remote VLAN (VLAN 20)
Monitor Type:	<ul> <li>Rx and Tx</li> <li>Rx</li> <li>Tx</li> </ul>
Apply	Close

7단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

NP 48-Port Gigabit PoE Stackable Managed Switch							
Session Sources							
Se	ssion Source	Table					
Filt	er: 📃 Sess	ion ID equals to	• Go Cle	ar Filter			
	Session ID	Destination	Source Interface	Monitor Type			
	1	No Destination	GE1/2	Rx			
	Add Edit Delete						

이제 시작 스위치에 세션 소스를 구성해야 합니다.

### 시작 스위치에서 세션 대상 구성

1단계. Status **and Statistics(상태 및 통계) > SPAN & RSPAN > Session Destinations(세션 대상)를** 선택합니다.

<b>-</b> 5	Status and Statistics
	System Summary
	CPU Utilization
	Interface
	Etherlike
	Port Utilization
	GVRP
	802.1x EAP
	ACL
	TCAM Utilization
	Health
Ŧ	SPAN & RSPAN
	RSPAN VLAN
	Session Destinations
	Session Sources
►	Diagnostics
►	RMON
►	sFlow
►	View Log
► A	dministration

2단계. **추가**를 클릭합니다.

Session Destinations							
Ses	Session Destination Table						
Session ID Destination Type Destination Network Traffic							
0 results found.							
C	Add Edit Delete						

3단계. 세션 ID 드롭다운 목록에서 세션 번호를 선택합니다.구성된 세션 소스에서 선택한 ID와 동일 해야 합니다.



참고:이 예에서는 세션 1이 선택됩니다.

4단계. Destination Type(대상 유형) 영역에서 **Remote VLAN(원격 VLAN**) 라디오 버튼을 클릭합니 다.Wireshark를 실행하는 컴퓨터와 같은 네트워크 분석기가 이 포트에 연결되어 있습니다.

중요:대상 인터페이스는 소스 포트와 같을 수 없습니다.

Destination Type: Local Interface Remote VLAN (VLAN 20)

참고:Remote VLAN을 선택하면 네트워크 트래픽이 자동으로 활성화됩니다.

5단계. Reflector Port(리플렉터 포트) 영역의 Unit(유닛) 드롭다운 목록에서 원하는 옵션을 선택합니 다.Port 드롭다운 목록에서 소스 포트로 설정할 포트를 선택합니다.

Reflector Port:	Unit	1 🔻	Port	GE20 🔻	<u>·</u> ]
Network Traffic:	1	Enable			_

참고:이 예에서는 유닛 1의 포트 GE20이 선택됩니다.

6단계. Apply(적용)를 클릭한 다음 Close(닫기)를 클릭합니다.

Session ID: 1 T
Destination Type:  Local Interface Remote VLAN (VLAN 20)
Reflector Port: Unit 1   Port GE20
Network Traffic: 🕑 Enable
Apply Close

7단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

Л	NP 48-Port Gigabit PoE Stackable Managed Switch					
5	Session Destinations					
	Ses	sion Destinat	tion Table			
		Session ID	Destination Type	Destination	Network Traffic	
		1	Remote	VLAN 20 via GE1/20	Enabled	
		Add	Edit	Delete		

이제 시작 스위치에 세션 대상을 구성해야 합니다.

#### 중간 스위치

또한 RSPAN 소스 및 대상 세션을 구분하는 중간 스위치가 있을 수 있습니다.이러한 스위치는 RSPAN을 실행할 수는 없지만 RSPAN VLAN의 요구 사항에 대응해야 합니다.

VTP(VLAN Trunking Protocol)에 표시되는 VLAN 1~1005의 경우 VLAN ID 및 관련 RSPAN 특성이 VTP에 의해 전파됩니다.확장 VLAN 범위(1006~4094)에서 RSPAN VLAN ID를 할당하는 경우 모든 중간 스위치를 수동으로 구성해야 합니다.

인터페이스 VLAN을 중간 스위치의 트렁크 포트로 할당하는 방법을 알아보려면 <u>여기</u>를 클릭하십시 오.

네트워크 전체의 RSPAN 세션을 정의하는 각 RSPAN VLAN과 함께 네트워크에 여러 RSPAN VLAN을 동시에 갖는 것은 정상입니다.즉, 네트워크의 모든 위치에서 여러 RSPAN 소스 세션이 패 킷을 RSPAN 세션에 제공할 수 있습니다.또한 네트워크 전반에 걸쳐 여러 RSPAN 대상 세션이 있 을 수 있으며, 동일한 RSPAN VLAN을 모니터링하고 사용자에게 트래픽을 제공할 수 있습니다 .RSPAN VLAN ID는 세션을 분리합니다.

#### 최종 스위치에서 세션 소스 구성

1단계. Status **and Statistics(상태 및 통계) > SPAN & RSPAN > Session Sources(세션 소스)를 선 택합니다**.

<ul> <li>Status and Statistics</li> </ul>
System Summary
CPU Utilization
Interface
Etherlike
Port Utilization
GVRP
802.1x EAP
ACL
TCAM Utilization
Health
▼ SPAN & RSPAN
RSPAN VLAN
Session Destinations
Session Sources
<ul> <li>Diagnostics</li> </ul>
► RMON
▶ sFlow
▶ View Log
Administration

2단계. 추가를 클릭합니다.

Session Sources						
Ses	Session Source Table					
Filte	Filter: Session ID equals to Go Clear Filter					
	Session ID	Destination	Source Interface	Monitor Type		
0 results found.						
	Add	Edit	Delete			

3단계. (선택 사항) Session ID 드롭다운 목록에서 세션 번호를 선택합니다.세션 ID는 세션당 일관 되어야 합니다.

Session ID:	1 🔻	
Source Interface: Monitor Type:	1 2 3	iit   :an
	4 5 6 7	_

참고:이 예에서는 세션 1이 선택됩니다.

4단계. Source Interface(소스 인터페이스) 영역에서 Remote VLAN(**원격 VLAN**) 라디오 버튼을 클 릭합니다.

Session ID:	1 •
Source Interface:	○ Unit 1 ▼ Port GE1 ▼ ○ VLAN 1 ▼ ● Remote VLAN (VLAN 20)
Monitor Type:	<ul> <li>Rx and Tx</li> <li>Rx</li> <li>Tx</li> </ul>
Apply	Close

**참고:**원격 VLAN의 모니터 유형이 자동으로 구성됩니다.

5단계. **적용**을 클릭한 다음 **닫기를 클릭합니다**.

6단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

#### 🗙 Save cisco IP 48-Port Gigabit PoE Stackable Managed Switch Session Sources Session Source Table 1 (GE1/1) 🔻 Filter: Session ID equals to Clear Filter Go Session ID Destination Source Interface Monitor Type VLAN 20 Rx 1 Add... Edit... Delete

이제 최종 스위치에 세션 소스를 구성해야 합니다.

## 최종 스위치에서 세션 대상 구성

1단계. Status **and Statistics(상태 및 통계) > SPAN & RSPAN > Session Destinations(세션 대상)를** 선택합니다.

<ul> <li>Status and Statistics</li> </ul>
System Summary
CPU Utilization
Interface
Etherlike
Port Utilization
GVRP
802.1× EAP
ACL
TCAM Utilization
Health
SPAN & RSPAN
RSPAN VLAN
Session Destinations
Session Sources
<ul> <li>Diagnostics</li> </ul>
► RMON
▶ sFlow
View Log
<ul> <li>Administration</li> </ul>

2단계. **추가**를 클릭합니다.

Session Destinations						
Ses	Session Destination Table					
	Session ID	Destination Type	Destination Type Destination Network Traffic			
0 re	0 results found.					
	Add Edit Delete					

3단계. 세션 ID 드롭다운 목록에서 세션 번호를 선택합니다.구성된 세션 소스에서 선택한 ID와 동일 해야 합니다.

Session ID:	1 🔻	
Destination Type:	1	
	3	
Port:	4	
	5	
Network Traffic:	0 7	

참고:이 예에서는 세션 1이 선택됩니다.

4단계. Destination Type(대상 유형) 영역에서 Local Interface(로컬 인터페이스) 라디오 버튼을 클릭 합니다.

Destination Type: 
Contemposities
Destination Type: 
Contemposities
Destination Type: 
Contemposities
Destination Type: 
Destin

5단계. Port(포트) 영역의 Unit(유닛) 드롭다운 목록에서 원하는 옵션을 선택합니다.Port 드롭다운 목록에서 소스 포트로 설정할 포트를 선택합니다.

Port:	Unit 1 🔻 Port GE20 🔻
Network Traffic:	Enable

**참고:**이 예에서는 유닛 1의 포트 GE20이 선택됩니다.

6단계. (선택 사항) 네트워크 트래픽 활성화 확인란을 선택하여 네트워크 트래픽을 활성화합니다.



7단계. Apply(적용)를 **클릭한** 다음 Close(닫기)를 클릭합니다.

8단계. (선택 사항) Save를 클릭하여 실행 중인 컨피그레이션 파일을 업데이트합니다.

l	NP 48-Port Gigabit PoE Stackable Managed Switch					
	Session Destinations					
	Ses	sion Destinat	ion Table			
		Session ID	Destination Type	Destination	Network Traffic	
		1	Remote	VLAN 20 via GE1/20	Enabled	
		Add	Edit	)elete		

이제 최종 스위치에 세션 대상을 구성해야 합니다.

#### WireShark에서 캡처된 RSPAN VLAN 패킷 분석

이 시나리오에서는 구성된 소스 인터페이스의 호스트, 유닛 1(GE1/2)에 있는 GE2의 IP 주소는 192.168.1.100입니다. 구성된 대상 인터페이스의 호스트, 유닛 1의 GE20(GE1/20을 통한 VLAN 20)의 IP 주소는 192.168.1.127입니다. Wireshark는 이 포트에 연결된 호스트에서 실행 중입니다.

Wireshark는 ip.addr == 192.168.1.100 필터를 사용하여 원격 소스 인터페이스에서 캡처된 패킷을 표시합니다.

*Intel(R) 82579LM Gigabit Network Connection: Local Area Connection																		
File	e Edit	View	Go	Сар	ture	Ar	nalyz	e	Statis	tics	Tele	phony	y V	Virele	ss	Tools	Help	
		0	010	$\mathbf{x}$	G	Q	æ		Ð	Ŷ	J.	I		Ð, G	. (	1		
	in addr -	- 102.16	0 1 10	20		-				<u> </u>	× (=			-	-			
닏	ip.addr =	= 192.10	0.1.10	50														
No.	Т	Time			Source					Destination						Protoco	l Lengt	h
	311 1	9.9822	72	192	.168	.1.1	127			192	2.168	3.1.1	00			ICMP		74
	312 1	9.9827	94	192	.168	.1.1	100			192	2.168	3.1.1	27			ICMP		74
	313 2	0.9829	12	192	.168	.1.1	127			192	2.168	3.1.1	00			ICMP		74
	314 2	0.9834	00	192	.168	.1.1	100			192	2.168	3.1.1	27			ICMP		74
	316 2	1.9829	34	192	.168	.1.1	127			192	2.168	3.1.1	00			ICMP		74
	317 2	1.9834	14	192	.168	.1.1	100			192	2.168	3.1.1	27			ICMP		74
	322 2	2.9899	00	192	.168	.1.1	127			192	2.168	3.1.1	00			ICMP		74
	323 2	2.9903	86	192	.168	.1.1	100			192	2.168	3.1.1	27			ICMP		74
	337 2	5.0968	24	192	.168	.1.1	100			239	9.255	5.255	.250	9		SSDP	2	14
	339 2	6.0978	23	192	.168	.1.1	100			239	9.255	5.255	.250	3		SSDP	2	14
	343 2	7.1094	45	192	.168	.1.1	100			239	9.255	5.255	.250	3		SSDP	2	14
	372 2	8.1188	96	192	.168	.1.1	100			239	9.255	5.255	.250	9		SSDP	2	14
	736 5	6.7451	36	192	.168	.1.1	100			192	2.168	3.1.2	55			BROWS	ER 2	58
	852 6	5.4426	12	192	.168	.1.1	100			192	2.168	3.1.2	55			NBNS		92
	853 6	5.4426	96	192	.168	.1.1	127			192	2.168	3.1.1	00			NBNS	1	.04
	854 6	5.4433	40	192	.168	.1.1	100			192	2.168	3.1.1	27			BROWS	ER 2	32
	856 6	5.6362	40	192	.168	.1.1	100			192	2.168	3.1.1	27			UDP	12	68
	857 6	5.6759	35	192	.168	.1.1	127			192	2.168	3.1.1	00			TCP		66
	858 6	5.6764	65	192	.168	.1.1	100			192	2.168	3.1.1	27			TCP		66
	859 6	5.6765	10	192	.168	.1.1	127			192	2.168	3.1.1	00			TCP		54
	860 6	5.6766	38	192	.168	.1.1	127			192	2.168	3.1.1	00			тср	2	75
	861 6	5.6767	49	192	.168	.1.1	127			192	2.168	3.1.1	00			HTTP/	X 7	87
	862 6	5.6771	81	192	.168	.1.1	100			192	2.168	3.1.1	27			TCP		60
	863 6	5.6792	06	192	.168	.1.1	100			192	2.168	3.1.1	27			тср	15	14
	864 6	5.6792	07	192	.168	.1.1	100			192	2.168	3.1.1	27			HTTP/	X 9	64
	865 6	5.6792	44	192	.168	.1.1	127			192	2.168	3.1.1	00			TCP		54
	866 6	5.6792	99	192	.168	.1.1	127			192	2.168	3.1.1	00			TCP		54
	867 6	5.6796	67	192	.168	.1.1	100			192	2.168	3.1.1	27			TCP		60
	869 6	5.8004	24	192	.168	.1.1	100			192	2.168	3.1.1	27			UDP	12	68
	871 6	6.1345	37	192	.168	.1.1	100			192	2.168	3.1.1	27			UDP	12	68
	873 6	6.5859	97	192	.168	.1.1	100			192	2.168	3.1.1	27			UDP	12	68
	882 6	7.9111	23	192	.168	.1.1	100			192	2.168	3.1.1	27			LLMNR	1	06

## 이 문서와 관련된 비디오 보기...

<u>여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.</u>