ネットワークでのリモートスイッチポートアナ ライザ(RSPAN)の設定

目次

- <u>目的</u>
- 該当するデバイス |ファームウェアのバージョン
- <u>概要</u>
- <u>スイッチでのRSPAN VLANの設定</u>
- 開始スイッチでのセッションソースの設定
- 開始スイッチでのセッション宛先の設定
- <u>中間スイッチ</u>
- 最終スイッチでのセッションソースの設定
- 最終スイッチでのセッション宛先の設定
- WireSharkでキャプチャされたRSPAN VLANパケットを分析する

目的

この記事では、スイッチでRSPANを設定する方法について説明します。

該当するデバイス |ファームウェアのバージョン

- Sx350 | 2.2.5.68 (最新のダ<u>ウンロード</u>)
- SG350X | 2.2.5.68 (最新のダ<u>ウンロード</u>)
- Sx550X | 2.2.5.68 (最新のダ<u>ウンロード</u>)

概要

スイッチポートアナライザ(SPAN)、またはポートミラーリングまたはポートモニタリングとも呼 ばれる場合、ネットワークアナライザによる分析のためにネットワークトラフィックを選択しま す。ネットワーク アナライザは、Cisco SwitchProbe デバイスのこともあれば、その他の Remote Monitoring (RMON; リモート モニタリング) プローブのこともあります。

ネットワークデバイス上でポートミラーリングを使用して、1つのデバイスポート、複数のデバイ スポート、またはVirtual Local Area Network(VLAN)全体で確認されたネットワークパケットのコ ピーを、デバイス上の別のポートのネットワークモニタリング接続に送信します。これは、侵入 検知システムなどのネットワークトラフィックの監視を必要とするネットワークアプライアンス でよく使用されます。モニタリングポートに接続されたネットワークアナライザは、データパケ ットを処理して診断、デバッグ、およびパフォーマンスモニタリングを行います。

リモートスイッチポートアナライザ(RSPAN)は、SPANの拡張機能です。RSPANは、ネットワー ク全体で複数のスイッチのモニタリングを有効にし、アナライザポートをリモートスイッチで定 義できるようにすることで、SPANを拡張します。つまり、ネットワークキャプチャデバイスを 一元化できます。

RSPANは、RSPANセッションの送信元ポートからのトラフィックを、RSPANセッション専用の VLANにミラーリングすることで動作します。その後、このVLANは他のスイッチにトランキング され、RSPANセッショントラフィックを複数のスイッチ間で転送できるようになります。セッシ ョンの宛先ポートを含むスイッチでは、RSPANセッションVLANからのトラフィックが宛先ポー トにミラーリングされます。

RSPANトラフィックフロー

- 各 RSPAN セッションのトラフィックは、すべての参加スイッチの当該 RSPAN セッション 専用であるユーザ指定の RSPAN VLAN で伝送されます。
- 開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLANにコピーされます。これは、設定する必要がある物理ポートです。RSPANセ ッションの構築にのみ使用されます。
- このリフレクタポートは、パケットをRSPAN VLANにコピーするメカニズムです。 RSPANは、所属するRSPANソースセッションからのトラフィックのみを転送します。 RSPAN ソース セッションがディセーブルになるまで、リフレクタ ポートとして設定されて いるポートに接続されているどのデバイスでも接続が失われます。
- その後、RSPANトラフィックは、中間デバイスのトランクポートを介して最終スイッチの宛 先セッションに転送されます。
- 宛先スイッチはRSPAN VLANをモニタし、宛先ポートにコピーします。

RSPANポートメンバーシップ規則

- すべてのスイッチで:RSPAN VLANのメンバーシップはタグ付けのみ可能です。
- スイッチの開始

- SPAN送信元インターフェイスをRSPAN VLANのメンバにすることはできません。

- リフレクタポートをこのVLANのメンバにすることはできません。
- リモートVLANにメンバーシップがないことをお勧めします。

•中間スイッチ

– ミラーリングされたトラフィックの通過に使用されないすべてのポートからRSPANメンバーシ ップを削除することを推奨します。

- 通常、RSPANリモートVLANには2つのポートがあります。

• 最終スイッチ

- ミラートラフィックの場合、送信元ポートはRSPAN VLANのメンバである必要があります。

– 宛先インターフェイスを含む他のすべてのポートからRSPANメンバーシップを削除することを 推奨します。

ネットワークでのRSPANの設定

スイッチでのRSPAN VLANの設定

RSPAN VLANは、RSPAN送信元セッションと宛先セッションの間でSPANトラフィックを伝送し ます。これには次の特性があります。

- RSPAN VLAN内のすべてのトラフィックは常にフラッディングされます。
- RSPAN VLANでは、メディアアクセスコントロール(MAC)アドレスの学習は行われません。
- RSPAN VLANトラフィックは、トランクポートでのみ流れます。

- STPはRSPAN VLANトランクでは実行できますが、SPAN宛先ポートでは実行できません。
- RSPAN VLANは、VLANコンフィギュレーションモードでremote-span VLANコンフィギュレ ーションモードコマンドを使用して、開始スイッチと最終スイッチの両方で設定する必要が あり、次の手順に従います。

ステップ1:スタートスイッチのWebベースのユーティリティにログインし、[Display Mode]ドロ ップダウンリストで[**Advanced**]を選択します。



ステップ2:[VLAN Management] > [VLAN Settings]を選択します。



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

ステップ3:[Add]をクリ**ックします**。

١	VLAN Settings								
	VLA	VLAN 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					

ステップ4:[VLAN ID]フィールドにVLAN IDを入力します。

VLAN ID: 20 (Range: 2 - 4094)

注:この例では、VLAN IDとしてVLAN 20が使用されています。

ステップ5:(オプション)[VLAN Name]フィールドにVLAN名を入力します。

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

注:この例では、VLAN名としてRSPAN VLANが使用されています。

ステップ6:(オプション)[VLAN Interface State]チェックボックスをオンにして、VLANを有効に します。VLANがシャットダウンされている場合、VLANはメッセージを送受信しません。たとえ ば、IPインターフェイスが設定されているVLANをシャットダウンすると、VLANへのブリッジン グは続行されますが、スイッチはVLAN上でIPトラフィックを送受信できません。この機能はデフ ォルトで有効になっています。

ステップ7:(オプション)[Link Status SNMP Traps]チェックボックスをオンにして、簡易ネット ワーク管理プロトコル(SNMP)トラップのリンクステータス生成を有効にします。この機能はデフ ォルトで有効になっています。

ステップ8:[Apply]をクリックし、[Close]をクリックします。

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

注:スイッチでのVLANの管理の詳細については、ここをクリックして<u>ください</u>。

ステップ9:(オプション)[Save]をクリックして実行構成ファイルを更新します。

🚫 Save

cisco

IP 48-Port Gigabit PoE Stackable Managed Switch

VLAN Settings

VLA	VLAN 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)					

ステップ10:[Status and Statistics] > [SPAN & RSPAN] > [RSPAN VLAN]を選択します。

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
Diagnostics
RMON
▶ sFlow
▶ View Log
 Administration

ステップ11:[RSPAN VLAN]ドロップダウンリストからVLAN IDを選択します。このVLANは、 RSPAN専用に使用する必要があります。

RSPAN VLAN

A VLAN must be added to the VLAN Database using the VLAN Settings screen

注:この例では、VLAN 20が選択されています。

ステップ12:[Apply]をクリ**ックします**。

RSPAN VLAN				
A VLAN must be added to the VLAN Database using the VLAN Settings screen				
RSPAN VLAN: 20 V				
Apply				
Apply Cancer				

ステップ13:(オプション)[**Save**]をクリック**し**、実行コンフィギュレーションファイルを更新します。

MP 48-Port Gigabit PoE Stackable Man	aged Sv	vitch
RSPAN VLAN		
Success. To permanently save the configuration, go t	o the File Ope	rations page
A VLAN must be added to the VLAN Database using the VLAN Settin	igs screen befo	re it can be co
RSPAN VLAN: 20 T		
Apply Cancel		

ステップ14:最終スイッチで、ステップ1 ~ 13を繰り返してRSPAN VLANを設定します。

これで、開始スイッチと最終スイッチの両方で、RSPANセッション専用のVLANを設定できまし た。

開始スイッチでのセッションソースの設定

ステップ1:[Status and Statistics] > [SPAN & RSPAN] > [Session Sources]を選択します。

 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
Diagnostics
RMON
▶ sFlow
View Log
Administration

ステップ2:[Add]をクリ**ックします**。

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 re	0 results found.								
C	Add Edit Delete								

ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。セッションIDは 、RSPANセッションごとに一貫している必要があります。



注:この例では、Session 1が選択されています。

ステップ4:目的の送信元インターフェイスタイプのオプションボタンをクリックし、ドロップダ ウンリストからインターフェイスを選択します(複数可)。

重要:送信元インターフェイスを宛先ポートと同じにすることはできません。

Source Interface:
Unit 1
Port GE2
VLAN 1
Remote VLAN (VLAN 20)

次のオプションがあります。

- [Unit and Port]:[Unit]ドロップダウンリストから必要なオプションを選択し、[Port]ドロップダウンリストから送信元ポートとして設定するポートを選択できます。
- VLAN:モニタするVLANを[VLAN]ドロップダウンリストから選択できます。VLANは、ホストのグループが、場所に関係なく、同じ物理ネットワーク上にあるかのように通信するのに役立ちます。このオプションを選択すると、編集できませんでした。
- リモートVLAN:定義されたRSPAN VLANが表示されます。このオプションを選択すると、 編集できませんでした。

注:この例では、ユニット1のポートGE2が選択されています。これは、モニタされるリモートイ ンターフェイスです。

ステップ5:(オプション)ステップ4で[Unit and Port]をクリックした場合は、モニタするトラフィックのタイプに応じて、目的の[Monitor Type]オプションボタンをクリックします。



次のオプションがあります。

- RxおよびTx:このオプションは、着信パケットと発信パケットのポートミラーリングを許可します。このオプションはデフォルトで選択されています。
- Rx:着信パケットのポートミラーリングを許可します。
- •Tx:このオプションは、発信パケットのポートミラーリングを許可します。

注:この例では、Rxが選択されています。

ステップ6:[Apply]をクリックし、[Close]をクリックします。

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

ステップ7:(オプション)[Save]をクリックして実行構成ファイルを更新します。

ЛF	IP 48-Port Gigabit PoE Stackable Managed Switch								
Se	Session Sources								
S	ies	sion Source 1	Table						
F	ilte	r: 📃 Sessi	ion ID equals to	• Go Cle	ar Filter				
C	Session ID Destination Source Interface Monitor Type								
		1	No Destination	GE1/2	Rx				
	,	Add	Edit	Delete					

これで、Start Switchでセッションソースを設定できました。

開始スイッチでのセッション宛先の設定

ステップ1:[Status and Statistics] > [SPAN & RSPAN] > [Session Destinations]を選択します。

 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
 Diagnostics
► RMON
▶ sFlow
View Log
Administration

ステップ2:[Add]をクリ**ックします**。

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

ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。これは、設定さ れたセッションソースから選択されたIDと同じである必要があります。

Session ID:	1 🔻
Destination Type:	1
	3
Port:	4
Network Traffic:	6
	7

注:この例では、Session 1が選択されています。

ステップ4:[Destination Type]領域から[**Remote VLAN**]オプションボタンをクリックします。 Wiresharkを実行しているコンピュータなどのネットワークアナライザがこのポートに接続されて います。

重要:宛先インターフェイスを送信元ポートと同じにすることはできません。

Destination Type: Local Interface Remote VLAN (VLAN 20)

注:[リモートVLAN]を選択すると、ネットワークトラフィックが自動的に有効になります。

ステップ5:[Reflector Port]領域で、[Unit]ドロップダウンリストから必要なオプションを選択します。[Port]ドロップダウンリストから、送信元ポートとして設定するポートを選択します。

Reflector Port:	Unit	1 🔻	Port	GE20 🔻
Network Traffic:	✓ E	nable		

注:この例では、ユニット1のポートGE20が選択されています。

ステップ6:[Apply]をクリックし、[Close]をクリ**ックします**。

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

			🚫 Save	ci
/IP 48-Port	Gigabit Pol	E Stackable N	lanaged S	Switch
Session Dest	inations			
Session Destinat	ion Table			
Session ID	Destination Type	Destination	Network Traffic	
□ 1	Remote	VLAN 20 via GE1/20	Enabled	
Add	Edit)elete		

ステップ7:(オプション)[Save]をクリックして実行構成ファイルを更新します。

これで、Start Switchでセッションの宛先を設定できました。

中間スイッチ

RSPANの送信元セッションと宛先セッションを分離する中間スイッチも存在できます。これらの スイッチはRSPANを実行できる必要はありませんが、RSPAN VLANの要件に対応する必要があ ります。

VLAN 1 ~ 1005がVLAN Trunking Protocol(VTP)で認識されている場合、VLAN IDとそれに関連す るRSPAN特性はVTPによって伝搬されます。拡張VLAN範囲(1006 ~ 4094)でRSPAN VLAN IDを 割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

インターフェイスVLANを中間スイッチのトランクポートとして割り当てる方法については、こ こをクリ<u>ックし</u>てください。

ネットワーク全体のRSPANセッションを定義する各RSPAN VLANと同時に、複数のRSPAN VLANをネットワークに持つことは正常です。つまり、ネットワーク内の任意の場所で複数の RSPAN送信元セッションがパケットをRSPANセッションに送信できます。また、ネットワーク 全体で複数のRSPAN宛先セッションを持ち、同じRSPAN VLANを監視し、ユーザにトラフィッ クを提示することもできます。RSPAN VLAN IDはセッションを分離します。

最終スイッチでのセッションソースの設定

ステップ1:[Status and Statistics] > [SPAN & RSPAN] > [Session Sources]を選択します。

 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	6
Session Sources	
Diagnostics	
RMON	
▶ sFlow	
▶ View Log	
 Administration 	

ステップ2:[Add]をクリ**ックします**。

Session So	urces			
Session Source	e Table			
Filter: 📃 Se	ssion ID equals t	o 🔻 Go	Clear Filter	
Session II	Destination	Source Interface	Monitor Type	
0 results found				
Add	Edit	Delete		

ステップ3:(オプション)[Session ID]ドロップダウンリストからセッション番号を選択します。 セッションIDは、セッションごとに一貫している必要があります。



注:この例では、Session 1が選択されています。

ステップ4:[Source Interface]領域から[Remote VLAN]オプションボタンをクリックします。

Session ID:	1 •
Source Interface:	: 🔘 Unit 🛯 🔻 Port 🛛 🗉 🖉 🔍 VLAN 📋 💌 💽 Remote VLAN (VLAN 20)
Monitor Type:	 Rx and Tx Rx Tx
Apply	Close

注:リモートVLANのモニタタイプが自動的に設定されます。

ステップ5:[Apply]をクリックし、[**Close**]をクリ**ックします**。

ステップ6:(オプション)[Save]をクリックして実行構成ファイルを更新します。

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

これで、最終スイッチのセッションソースが設定されているはずです。

最終スイッチでのセッション宛先の設定

ステップ1:[Status and Statistics] > [SPAN & RSPAN] > [Session Destinations]を選択します。

• \$	itatus 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

ステップ2:[Add]をクリ**ックします**。

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

ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。これは、設定されたセッションソースから選択されたIDと同じである必要があります。

Session ID:	1 🔻	
Destination Type:	1	
	3	
Port:	4	
Network Traffic:	5 6	
	7	

注:この例では、Session 1が選択されています。

ステップ4:[Destination Type]領域から[Local Interface]オプションボタンをクリックします。

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

ステップ5:[Port(ポート)]領域で、[Unit(ユニット)]ドロップダウンリストから必要なオプショ ンを選択します。[Port]ドロップダウンリストから、送信元ポートとして設定するポートを選択し ます。

Port: Unit 1

Port GE20

Network Traffic: 📃 Enable

注:この例では、ユニット1のポートGE20が選択されています。

ステップ6:(オプション)ネットワークトラフィックを有効にするには、[**ネットワークトラフィ ックを有効**にする]チェックボックスをオンにします。

Port:	Unit 1	 Port 	GE20 V
Network Traffic:	🗹 Ena	ble	

ステップ7:[Apply]をクリックし、[Close]をクリ**ックします**。

ステップ8:(オプション)[Save]をクリックして実行構成ファイルを更新します。

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

これで、最終スイッチでセッションの宛先を設定できました。

WireSharkでキャプチャされたRSPAN VLANパケットを分析する

このシナリオでは、ユニット1(GE1/2)の送信元インターフェイスのホストGE2(GE1/2)のIPアドレ スは192.168.1.100で、ユニット1(GE1/20を介したVLAN 20)のホストのIPアドレスは 192.168.1.127ですポート。

フィルタip.addr == 192.168.1.100を使用して、Wiresharkはリモートソースインターフェイスか らキャプチャされたパケットを表示します。

Intel(R) 82579LM Gigabit Network Connection: Local Area Connection																		
File	e Edit	View	Go	Сар	ture	Ar	nalyz	e	Statis	tics	Tel	lepho	ny	Wir	eless	Тоо	ls	Help
		•	010	×	G	9	¢	⇒	€2	Ŷ	₽ [I		Ð,	Q	Q. I		
Ē	ip.addr =	= 192.16	8.1.10	00														
No		imo		Cour	~~~	_				Dev	ational	tion				Drot	ocol	Longth
INO.	211 1	0 0833.	70	102	160	1 1	127			10	501141 2 1 4	0011 00 1	100			TCM		Lengui 74
	312 1	0 08270	72 D/I	102	168	1 1	100			10	2.10	50.1. 58 1	127			TCM	D	74
	313 2	0 9829	12	192	168	1 1	127			19	2.10	58 1	100			TCM	D	74
	314 2	0.9834	aa	192	168	1 1	100			19	2.10	58 1	127			TCM	P	74
	316.2	1.9829	34	192	168	1 1	127			19	2.16	58.1	100			TCM	P	74
	317 2	1.9834	14	192	.168	.1.1	100			19	2.16	58.1	.127			TCM	P	74
	322.2	2.9899	20	192	.168	.1.1	127			19	2.16	58.1.	100			TCM	P	74
	323 2	2.9903	86	192	.168	.1.1	100			19	2.16	58.1.	.127			ICM	P	74
	337 2	5.0968	24	192	.168	.1.1	100			23	9.25	55.25	55.2	50		SSD	P	214
	339 2	6.0978	23	192	.168	.1.1	100			23	9.25	55.25	55.2	50		SSD	P	214
	343 2	7.1094	45	192	.168	.1.1	100			23	9.25	55.25	55.2	50		SSD	Р	214
	372 2	8.1188	96	192	.168	.1.1	100			23	9.25	55.25	55.2	50		SSD	Р	214
	736 5	6.7451	36	192	.168	.1.1	100			19	2.16	58.1.	255			BRO	WSE	R 258
	852 6	5.4426	12	192	.168	.1.1	100			19	2.16	58.1.	255			NBN	S	92
	853 6	5.4426	96	192	.168	.1.1	127			19	2.16	58.1.	. 100			NBN	S	104
	854 6	5.44334	40	192	.168	.1.1	100			19	2.16	58.1.	.127			BRO	WSE	R 232
	856 6	5.63624	40	192	.168	.1.1	100			19	2.10	58.1.	.127			UDP)	1268
	857 6	5.6759	35	192	.168	.1.1	127			19	2.10	58.1.	. 100			TCP)	66
	858 6	5.6764	65	192	.168	.1.1	100			19	2.10	58.1.	.127			TCP)	66
	859 6	5.6765	10	192	.168	.1.1	127			19	2.16	58.1.	.100			TCP		54
	860 6	5.6766	38	192	.168	.1.1	127			19	2.10	58.1.	. 100			TCP)	275
	861 6	5.67674	49	192	.168	.1.1	127			19	2.16	58.1.	. 100			HTT	P/X.	787
	862 6	5.6771	81	192	.168	.1.1	100			19	2.16	58.1.	.127			TCP		60
	863 6	5.6792	96	192	.168	.1.1	100			19	2.16	58.1.	.127			TCP)	1514
	864 6	5.6792	07	192	.168	.1.1	100			19	2.16	58.1.	.127			HTT	Р/Х.	964
	865 6	5.67924	44	192	.168	.1.1	127			19	2.16	58.1.	. 100			TCP		54
	866 6	5.67929	99	192	.168	.1.1	127			19	2.16	58.1.	.100			TCP		54
	867 6	5.6796	67	192	.168	.1.1	100			19	2.16	58.1.	.127			TCP		60
	869 6	5.80042	24	192	.168	.1.1	100			19	2.16	58.1.	.127			UDP		1268
	871 6	6.1345	37	192	.168	.1.1	100			19	2.16	58.1.	.127			UDP		1268
	873 6	6.58599	97	192	.168	.1.1	100			19	2.16	58.1.	.127			UDP		1268
	882 6	7.9111	23	192	.168	.1.1	100			19	2.16	58.1.	.127			LLM	NR	106

この記事に関連するビデオを表示…

<u>シスコのその他のテクニカルトークを表示するには、ここをクリックしてください</u>