WindowsおよびMACでのポートのテスト

内容

<u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>テストポート</u> <u>Windows の場合</u>

<u>関連情報</u>

はじめに

このドキュメントでは、<u>Webexコールでサポートされているデバイス</u>が存在する場合のトラブル シューティングのために、TCP SIPトラフィックポートをテストする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Webex通話環境とアーキテクチャの理解
- ・ <u>Webexコ</u>ーリングの<u>ポート参照情報を</u>読んだ<u>こと</u>
- デバイスレジスタの問題に関する基本的なトラブルシューティング
- ・ Webex通話オファーのCSCANツール「<u>Use CScan to Test Webex Calling Network Quality</u>

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

このドキュメントでは、Webex Calling Signaling Session Initiation Protocol(SIP)ポートにアクセ スできるかどうかをトラブルシューティングしてテストする基本的な方法について説明します。 場合によっては、デバイスが登録に失敗し、Control Hubでofflineまたはissuesステータスが表示 されます。

デバイスが登録する必要のあるSIPフローかどうかを調査できるように、パケットキャプチャが 必要です。



パケットキャプチャが成功すると、次の図のようになります。

	No Time	< Snime	Destination	Pentocol	lida
	310 2023-03-08 17:46:43.063779	10.21.144.144	199.59.66.120		56959 - 8934 [SYN] Seque Win+65535 Lenve M55=1358 W5+64 T5va1+2164988443 T5ecr+0 SACK_PERH+1
	312 2023-03-08 17:46:43.203038	199.59.66.120	10.21.144.144	TCP	8934 - 56959 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1260 SACK_PERM=1 TSval=3981094889 TSecr=2164980443 MS=4
1	313 2023-03-08 17:46:43.203115	10.21.144.144	199.59.66.120	TCP	56959 - 8934 [ACK] Seg=1 Ack=1 Win=132288 Len=0 TSval=2164980583 TSecr=3981894889
1	314 2023-03-08 17:46:43.205513	10.21.144.144	199.59.66.120	TLSv1.2	Client Hello
1	316 2023-03-08 17:46:43.329379	199.59.66.120	10.21.144.144	TCP	8934 - 56959 [ACK] Seq=1 Ack=518 Win=30832 Len=0 TSval=3981094950 TSecr=2164900585
I	318 2023-03-08 17:46:43.331761	199.59.66.120	10.21.144.144	TLSv1.2	Server Hello

赤いボックスは、TCP接続が確立されたことを示します。

次の図に、TCP接続が確立されない場合の例を示します。

				extended/ogaina.acsa
🔳 🔬 🎯 🖿 🛍 🔯 🔍	🗢 🔿 🕋 😽 🤅	🖞 📃 🔲 લ્લ્લ 📰		Mail Password Required Description
cp.port==8934				Elettre Accounts
Time	Source	Destination	Protocol	jada 🖉
165 2023-03-07 16:58:22.783274	10.63.247.223	199.59.66.120	TCP	33253 - 8934 (SYN) Seq+0 Win+29200 Len+0 MSS+1460 SACK_PERM+1 TSval+554863878 TSecr+0 WS+128
284 2823-83-87 16:58:23.813725	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 33253 - 8934 [SYN] Seque Win-29280 Lenve MSS-1460 SACK_PERM-1 TSval-554864136 TSecr-
518 2023-03-07 16:58:25.829736	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Min=29280 Len=0 MSS=1460 SACK_PERM=1 TSval=554864640 TSecr=
697 2023-03-07 16:50:29.925727	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 33253 - 8934 [SYN] Seque Win-29280 Lenve HSS-1460 SACK_PERM-1 TSval-554865664 TSecr-
869 2023-03-07 16:58:38.117740	10.63.247.223	199.59.66.120		(TCP Retransmission) (TCP Port numbers reused) 33253 - 8934 (51N) Seq=0 Win=29280 Len=0 MSS=1468 SACK_PERM=1 TSval=554867712 TSecr=
874 2023-03-07 16:58:42.149311	10.63.247.223	199.59.66.120	TCP	35421 - 8934 [SYN] Seq=0 WIn=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=554868719 TSecr=0 WS=128
922 2023-03-07 16:58:43.173771	10.63.247.223	199.59.66.120		(TCP Retransmission) (TCP Port numbers reused) 35421 → 8934 (SYN) Seq=0 Min=29280 Len=0 MSS=1468 SACK_PERM=1 TSval=554868976 TSecr=
976 2823-83-87 16:58:45.189784	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 35421 - 8934 [SYN] Seque Win-29280 Lenve HSS-1460 SACK_PERM+1 TSval-554869480 TSecr-
1131 2023-03-07 16:58:49.381716	10.63.247.223	199.59.66.120		(TCP Retransmission) (TCP Port numbers reused) 35421 → 8934 (51N) Seq=0 Win=29280 Len=0 MSS=1468 SACK_PERM=1 TSval=554870528 TSecr=
1322 2023-03-07 16:50:54.245731	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 33253 - 8934 [SYN] Seque Win-29280 Lenve HSS=1460 SACK_PERM=1 TSval=554871744 TSecre
1352 2023-03-07 16:50:57.573740	10.63.247.223	199.59.66.120		(TCP Retransmission) (TCP Port numbers reused) 35421 → 8934 (51N) Seq=0 Win=29280 Len=0 MSS=1468 SACK_PERM=1 TSval=554872576 TSecr=
1414 2023-03-07 16:59:02.140200	10.63.247.223	199.59.66.120	TCP	46199 - 8934 [SYN] Seq+8 WIn+29288 Len+8 MSS=1468 SACK_PERM=1 TSval=554873719 TSecr+8 WS=128
1487 2023-03-07 16:59:03.173731	10.63.247.223	199.59.66.120		(TCP Retransmission) (TCP Port numbers reused) 46199 → 8934 (SYN) Seq=8 Min=29288 Len=8 MSS=1468 SACK_PERM=1 TSval=554873976 TSecr=
1531 2023-03-07 16:59:05.109733	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 46199 ~ 8934 [SYN] Seque Win=29280 Lenve HSS=1468 SACK_PERM=1 TSval=554874480 TSecr-
1632 2823-83-87 16:59:89.349728	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 46199 - 8934 [SYN] Seque Win-29280 Lenve MSS-1468 SACK_PERM-1 TSval-S54875528 TSecr-
1777 2023-03-07 16:59:13.701733	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 35421 - 8934 [SYN] Seque Win-29280 Lenve MSS=1468 SACK_PERM=1 TSval=554876688 TSecre
1830 2023-03-07 16:59:17.541733	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 46199 + 8934 [SYN] Seq+8 Win=29288 Len+8 MSS=1468 SACK_PERM=1 TSval=554877568 TSecr=
1835 2023-03-07 16:59:22.630363	10.63.247.223	199.59.65.120	TCP	-36213 - 8934 [S1N] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva1=554878840 TSecr=0 MS=128
2899 2823-83-87 16:59:23.653727	10.63.247.223	199.59.65.120	TCP	(TCP Retransmission) (TCP Port numbers reused) 36213 → 8934 (SYN) Seq=8 Min=29288 Len=8 MSS=1468 SACK_PERM=1 TSval=554879896 TSecr=
2994 2823-83-87 16:59:25.669778	10.63.247.223	199.59.65.120		[TCP Retransmission] [TCP Port numbers reused] 36213 - 8934 [S1N] Seque Win-29280 Lenve MSS=1468 SACK_PERM=1 TSval=554879680 TSecre
3016 2023-03-07 16:59:27.269726	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 33253 - 8934 [STN] Seq=8 Win=29288 Len=8 MSS=1468 SACK_PERM=1 TSval=554888888 TSecre
3119 2023-03-07 16:59:29.029718	10.63.247.223	199.59.65.120		[TCP Retransmission] [TCP Port numbers reused] 36213 - 8934 [STN] Seque Win-29280 Lenve MSS=1468 SACK_PERM=1 TSval=554888648 TSecre
3212 2023-03-07 16:59:33.669739	10.63.247.223	199.59.66.120		[TCP Retransmission] [TCP Port numbers reused] 46199 - 8934 [STN] Seq=8 Win=29288 Len=8 MSS=1468 SACK_PERM=1 TSval=554881648 TSecre
Frame 165: 74 bytes on wire (592 bits), 74 b Ithernet II. Src: Cisco Sbile:ff (4ciet:76:8	ytes captured (592 b hillerff), Detri TETF-	115) VERP-VETD by (00:00:5e:00:01:bs)		

ここでは、キャプチャにTCP SYNのみが表示されているため、デバイスはTCP接続を開くことが できません。

◆ 注:この種の問題が発生した場合は、これがブロックされた理由を調査する必要があります 。場合によっては、ファイアウォール側でブロックされますが、さらに調査を行う必要があ ります。

Windows/MACからのTCP接続を検証するために実行できる手順がいくつかあります。

テストポート

Windows の場合

パワーシェルを開き、次のコマンドを使用します。

tnc 10.119.57.136 -p 8934 tnc 10.119.56.136 -p 8934

さらに、 ipconfig 送信元を確認するには、次の手順を実行します。

```
Windows PowerShell
windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\-''---''> tnc 85.119.57.136 -p 8934
ComputerName : 85.119.57.136
RemoteAddress : 85.119.57.136
RemotePort : 8034
RemotePort
                    : 8934
                  : Wi-Fi
: 10.152.200.59
InterfaceAlias
SourceAddress
TcpTestSucceeded : True
PS C:\Users\
                       N tnc 85.119.56.136 -p 8934
LomputerName : 85.119.56.136
RemoteAddress : 85.119.56.136
RemotePort : 8034
                   : 8934
                  : Wi-Fi
: 10.152.200.59
InterfaceAlias
SourceAddress
TcpTestSucceeded : True
```

💊 注:ここに示すIPアドレスは、Webex Calling Session Border Controller(SBC)です。

ターミナルに移動し、次のコマンドを使用します。

nmap -sV -p 8934 10.119.57.136 nmap -sV -p 8934 10.119.56.136

さらに、 ipconfig 送信元を確認するには、次の手順を実行します。

O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O
 O

18

関連情報

- ・ <u>CScanを使用したWebex通話ネットワーク品質のテスト</u>
- シスコテクニカルサポートおよびダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。