

在Windows和MAC中测试端口

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[测试端口](#)

[对于Windows](#)

[相关信息](#)

简介

本文档介绍测试TCP SIP流量端口的步骤，以便在支持[Webex Calling](#)的设备出现时进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解您的Webex呼叫环境和架构
- 已阅读Webex[呼叫的端口参考信息](#)
- 对设备寄存器问题进行基本故障排除。
- 运行CSCAN工具Webex calling offers [Use CScan to Test Webex Calling Network Quality](#)

使用的组件

本文档不限于特定的软件和硬件版本。

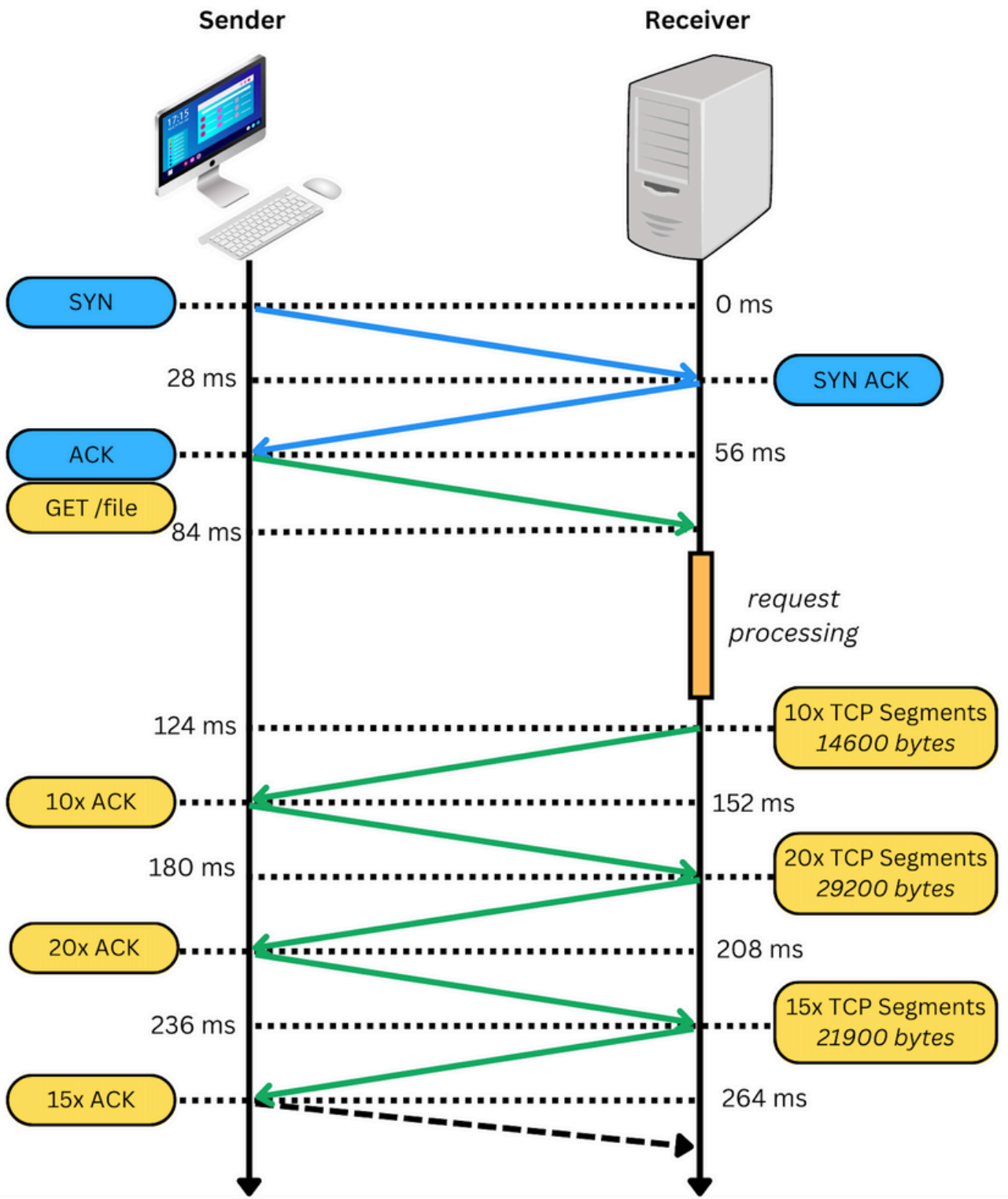
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍一种故障排除和测试您是否有权访问Webex呼叫信令会话发起协议(SIP)端口的基本方法。

在某些情况下，设备无法注册，并且在控制中心上显示offline 或issues 状态。

您需要捕获数据包，以便可以调查设备是否注册了预期的SIP流：



在数据包捕获中，如果成功，则类似于下一个映像：

No.	Time	Source	Destination	Protocol	Info
310	2023-03-08 17:46:43.863779	10.21.144.144	199.59.66.120	TCP	56959 → 8934 [SYN] Seq=0 Win=65535 Len=0 MSS=2308 Win=0 TSval=2164988443 TSecr=0 SACK_Flags=0
312	2023-03-08 17:46:43.283838	199.59.66.120	10.21.144.144	TCP	8934 → 56959 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=2308 SACK_Flags=1 TSval=3981894589 TSecr=2164988443 Win=4
313	2023-03-08 17:46:43.283115	10.21.144.144	199.59.66.120	TCP	56959 → 8934 [ACK] Seq=1 Ack=1 Win=32768 Len=0
314	2023-03-08 17:46:43.280513	10.21.144.144	199.59.66.120	TLSv1.2	Client Hello
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=38832 Len=0 TSval=3981894590 TSecr=2164988443
318	2023-03-08 17:46:43.331761	199.59.66.120	10.21.144.144	TLSv1.2	Server Hello

红色方框表示TCP连接已建立。

在下一张图中，是未建立TCP连接的示例：

No.	Time	Source	Destination	Protocol	Info
165	2023-03-07 16:58:22.783274	10.63.247.223	199.59.66.128	TCP	33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54863878 TSecr=0 WS=128
204	2023-03-07 16:58:23.813725	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54864648 TSecr=0
318	2023-03-07 16:58:25.829726	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54865684 TSecr=0
697	2023-03-07 16:58:29.925727	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54867712 TSecr=0
869	2023-03-07 16:58:38.117748	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54869740 TSecr=0
174	2023-03-07 16:58:42.945113	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54871768 TSecr=0
922	2023-03-07 16:58:43.173771	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54873796 TSecr=0
976	2023-03-07 16:58:45.189784	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54875824 TSecr=0
1135	2023-03-07 16:58:49.191716	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54877852 TSecr=0
1322	2023-03-07 16:58:54.245731	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54879880 TSecr=0
1352	2023-03-07 16:58:57.573768	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54881908 TSecr=0
1454	2023-03-07 16:59:02.945113	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54883936 TSecr=0
1487	2023-03-07 16:59:03.173771	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54885964 TSecr=0
1519	2023-03-07 16:59:05.189784	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54887992 TSecr=0
1632	2023-03-07 16:59:09.149708	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54890020 TSecr=0
1777	2023-03-07 16:59:13.793733	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54892048 TSecr=0
1838	2023-03-07 16:59:17.543733	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54894076 TSecr=0
1935	2023-03-07 16:59:22.635113	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54896104 TSecr=0
2099	2023-03-07 16:59:23.653727	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54898132 TSecr=0
2094	2023-03-07 16:59:25.609778	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54899660 TSecr=0
3014	2023-03-07 16:59:27.269708	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54901688 TSecr=0
3119	2023-03-07 16:59:29.829718	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54903716 TSecr=0
3212	2023-03-07 16:59:33.689739	10.63.247.223	199.59.66.128	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSval=54905744 TSecr=0

在这里，捕获中只看到TCP SYN，因此设备无法打开TCP连接。

注意：遇到此类问题时，您需要调查阻止此问题的原因。在某些情况下，防火墙端会阻止该数据包，但需要进一步调查。

您可以执行一些步骤来验证来自Windows/MAC的TCP连接。

测试端口

对于Windows

打开电源外壳，然后使用以下命令：

```
tnc 10.119.57.136 -p 8934
tnc 10.119.56.136 -p 8934
```

此外，使用 `ipconfig` 要检查源，请执行以下操作：

```
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        : 8934
InterfaceAlias    : Wi-Fi
SourceAddress     : 10.152.200.59
TcpTestSucceeded : True

PS C:\Users\...> tnc 85.119.56.136 -p 8934

ComputerName      : 85.119.56.136
RemoteAddress     : 85.119.56.136
RemotePort        : 8934
InterfaceAlias    : Wi-Fi
SourceAddress     : 10.152.200.59
TcpTestSucceeded : True
```

 注意：此处显示的IP地址是Webex呼叫会话边界控制器(SBC)。

转至Terminal并使用以下命令：

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

此外，使用 `ipconfig` 要检查源，请执行以下操作：

```
apple -- -bash -- 141x42
[LCURENO-M-5HQZ:~] $ nmap -sV -p 8934 85.119.57.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-20 14:13 CST
Nmap scan report for 85.119.57.136
Host is up (0.094s latency).

PORT      STATE      SERVICE VERSION
8934/tcp  filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
[LCURENO-M-5HQZ:~] $
[LCURENO-M-5HQZ:~] $
[LCURENO-M-5HQZ:~] $ nmap -sV -p 8934 85.119.56.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-20 14:14 CST
Nmap scan report for 85.119.56.136
Host is up (0.089s latency).

PORT      STATE      SERVICE VERSION
8934/tcp  filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
[LCURENO-M-5HQZ:~] $
```

相关信息

- [使用CScan测试Webex呼叫网络质量](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。