

# 在Windows和MAC中測試埠

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[測試埠](#)

[對於Windows](#)

[相關資訊](#)

---

## 簡介

本檔案介紹測試TCP SIP流量連線埠的步驟，以便在出現支援的[Webex通話裝置時進行疑難排解](#)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 瞭解Webex通話環境和架構
- 已閱讀Webex[呼叫的埠參考資訊](#)
- 裝置暫存器問題的基本故障排除。
- 運行CSCAN工具Webex呼叫提供[使用CScan測試Webex呼叫網路品質](#)

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

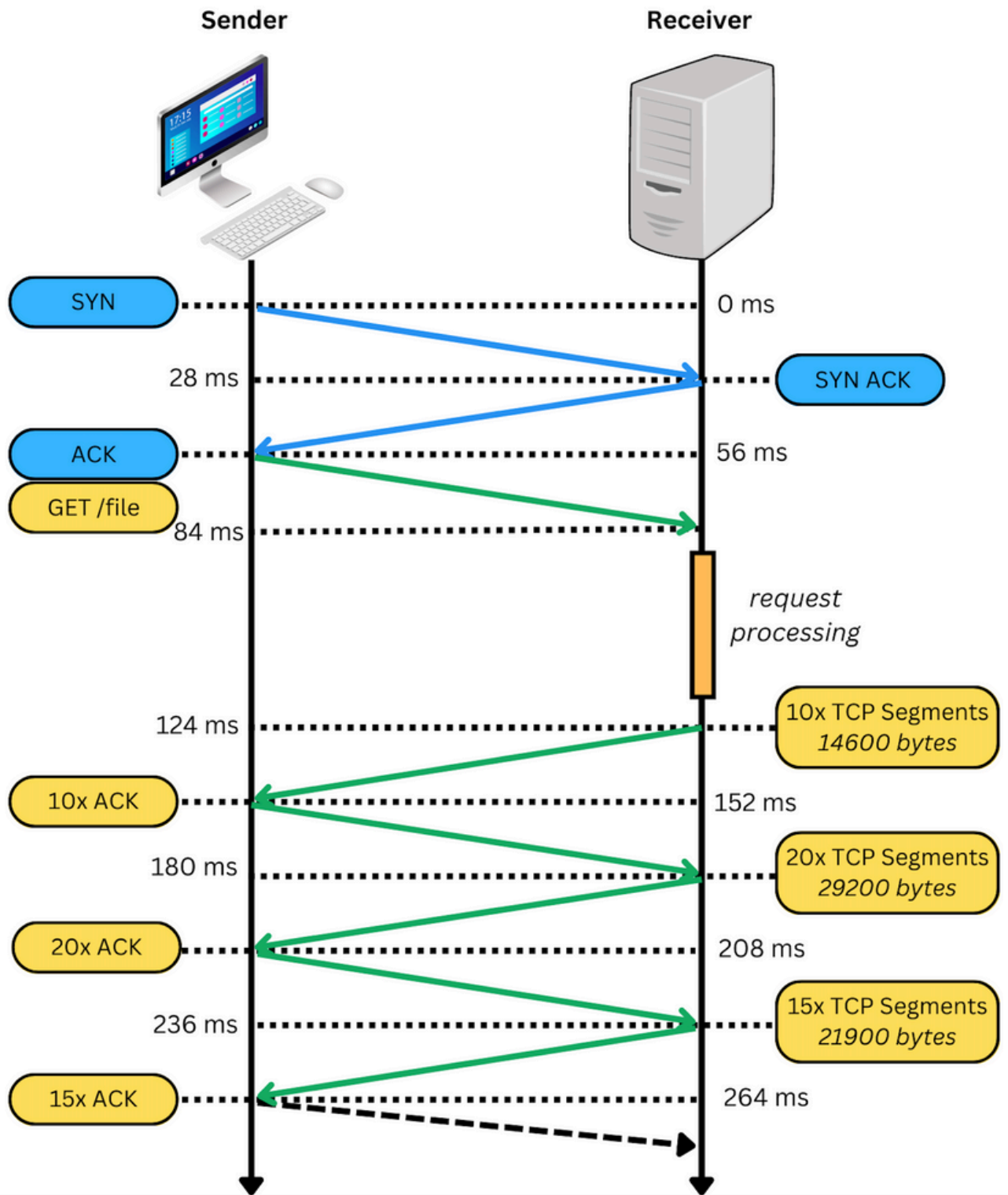
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本檔案介紹排解和測試您是否有權存取Webex通話訊號傳送作業階段啟始通訊協定(SIP)連線埠的基本方法。

在某些情況下，裝置註冊失敗，並在控制中心顯示offline 或issues 狀態。

您需要捕獲資料包，以便可以調查該裝置是否具有需要註冊的SIP流：



在封包擷取中，如果成功，它看起來與下一個映像類似：

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=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=28950 Len=0 MSS=1208 SACK_Flags=1 TSval=3981894589 TSecr=2164988443 WS=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=132788 Len=0 TSV=2164988583 TSecr=3981894589
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=2164988585
318	2023-03-08 17:46:43.331761	199.59.66.120	10.21.144.144	TLSv1.2	Server Hello

紅色方框表示TCP連線已建立。

下一張圖是未建立TCP連線的範例：

No.	Time	Source	Destination	Protocol	Info
165	2023-03-07 16:58:22.783274	10.63.247.223	199.59.66.120	TCP	33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54863878 TSecr=0 WS=128
284	2023-03-07 16:58:23.813725	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54864648 TSecr=0 WS=128
318	2023-03-07 16:58:25.829726	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54865684 TSecr=0 WS=128
697	2023-03-07 16:58:29.925727	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54867112 TSecr=0 WS=128
869	2023-03-07 16:58:38.117748	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54868540 TSecr=0 WS=128
174	2023-03-07 16:58:42.945113	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54870000 TSecr=0 WS=128
922	2023-03-07 16:58:43.173771	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54868976 TSecr=0 WS=128
976	2023-03-07 16:58:45.189784	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54869840 TSecr=0 WS=128
1135	2023-03-07 16:58:49.191716	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54870208 TSecr=0 WS=128
1322	2023-03-07 16:58:54.245731	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54871744 TSecr=0 WS=128
1352	2023-03-07 16:58:57.577748	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54873776 TSecr=0 WS=128
1454	2023-03-07 16:58:58.945003	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54875712 TSecr=0 WS=128
1487	2023-03-07 16:59:03.173731	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54873976 TSecr=0 WS=128
1519	2023-03-07 16:59:05.189783	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54874840 TSecr=0 WS=128
1632	2023-03-07 16:59:09.149708	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54875520 TSecr=0 WS=128
1777	2023-03-07 16:59:13.791733	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54876688 TSecr=0 WS=128
1838	2023-03-07 16:59:17.541733	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54877560 TSecr=0 WS=128
1935	2023-03-07 16:59:22.635113	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54879000 TSecr=0 WS=128
2099	2023-03-07 16:59:23.653727	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54879960 TSecr=0 WS=128
2194	2023-03-07 16:59:25.609778	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54879680 TSecr=0 WS=128
3014	2023-03-07 16:59:27.269708	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54880800 TSecr=0 WS=128
3119	2023-03-07 16:59:29.829718	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 36213 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54880840 TSecr=0 WS=128
3212	2023-03-07 16:59:33.689739	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=0 Win=29208 Len=0 MSS=1468 SACK_PERM=1 TSval=54881680 TSecr=0 WS=128

在這裡，捕獲中只看到TCP SYN，因此裝置無法開啟TCP連線。

注意：遇到此類問題時，您需要調查阻止此問題的原因。在某些情況下，防火牆端會封鎖此封包，但需要進一步調查。

您可以執行一些步驟來驗證來自Windows/MAC的TCP連線。

## 測試埠

對於Windows

開啟電源外殼，然後使用以下命令：

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

此外，使用 ipconfig 要檢查源，請執行以下操作：

```
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：此處顯示的IP地址是Webex呼叫會話邊界控制器(SBC)。

前往終端機並使用以下命令：

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

此外，使用 `ipconfig` 要檢查源，請執行以下操作：

```
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:~] $
```

## 相關資訊

- [使用CScan測試Webex呼叫網路品質](#)
- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。