

Porte di prova in Windows e MAC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Porte di test](#)

[Per Windows](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come testare le porte del traffico TCP SIP per risolvere i problemi relativi alla presenza di [dispositivi supportati per Webex Calling](#).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comprensione dell'ambiente e dell'architettura Webex Calling
- Aver letto le [informazioni di riferimento sulla porta per Webex Calling](#)
- Risoluzione dei problemi di base relativi al registro dispositivi.
- Esecuzione dello strumento CSCAN Webex Calling offre [Utilizzo di CScan per verificare la qualità della rete Webex Calling](#)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

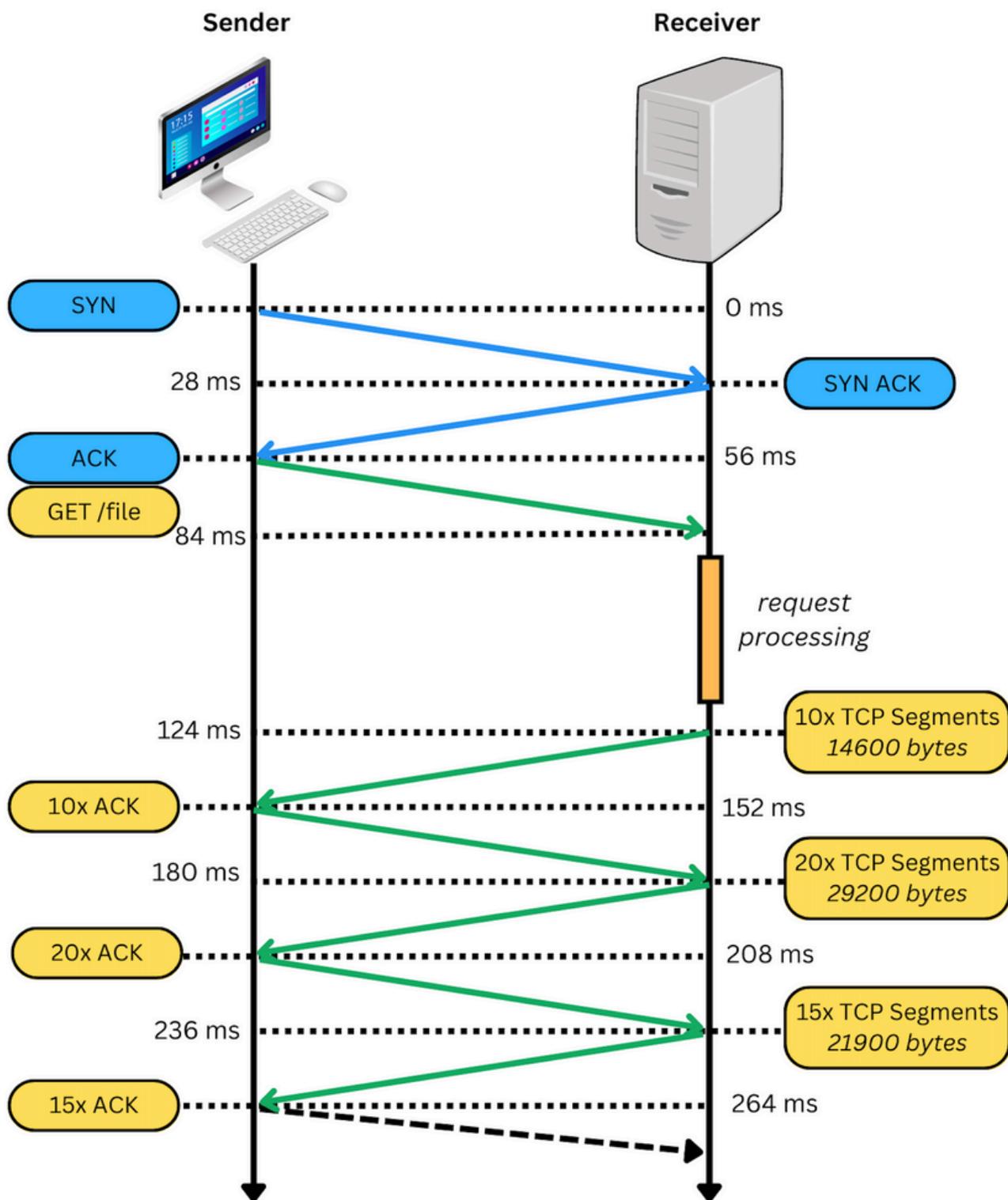
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto un modo di base per risolvere i problemi e verificare se si ha accesso alle porte SIP (Signaling Session Initiation Protocol) di Webex.

In alcuni casi, i dispositivi non vengono registrati e viene visualizzato lo stato offline o dei problemi in Control Hub.

È necessaria un'acquisizione di pacchetti per poter verificare se il dispositivo deve registrare il flusso SIP previsto:



In un'acquisizione pacchetto, se riuscita, appare simile all'immagine successiva:

No.	Time	Source	Destination	Protocol	Info
318	2023-03-08 17:46:43.463779	10.21.144.144	199.59.66.120	TCP	56959 - 8934 [SYN] Seq=0 Win=65535 Len=0 MSS=1356 WS=64 TSval=2164980443 TSecr=0 SACK_PERM=1
312	2023-03-08 17:46:43.283838	199.59.66.120	10.21.144.144	TCP	8934 - 56959 [SYN, ACK] Seq=1 Win=28948 Len=0 MSS=1208 SACK_PERM=1 TSval=3981894889 TSecr=2164980443 WS=1
313	2023-03-08 17:46:43.283115	10.21.144.144	199.59.66.120	TCP	56959 - 8934 [ACK] Seq=1 Win=32208 Len=0 TSval=2164980503 TSecr=3981894889
314	2023-03-08 17:46:43.285513	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=3981894958 TSecr=2164980505
318	2023-03-08 17:46:43.331761	199.59.66.120	10.21.144.144	TLSv1.2	Server Hello

La casella rossa indica che la connessione TCP è stata stabilita.

Nell'immagine seguente viene mostrato un esempio di connessione TCP non stabilita:

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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
518	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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
692	2023-03-07 16:58:29.970727	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
874	2023-03-07 16:58:42.611131	10.63.247.223	199.59.66.120	TCP	35421 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
922	2023-03-07 16:58:43.517171	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
970	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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1176	2023-03-07 16:58:49.381716	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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] 35421 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1352	2023-03-07 16:58:57.573748	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 35421 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1414	2023-03-07 16:59:02.614209	10.63.247.223	199.59.66.120	TCP	46199 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1533	2023-03-07 16:59:05.189733	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1632	2023-03-07 16:59:09.349728	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1777	2023-03-07 16:59:15.178733	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
1932	2023-03-07 16:59:22.810733	10.63.247.223	199.59.66.120	TCP	32213 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 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] 32213 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
2094	2023-03-07 16:59:25.669728	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 32213 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
2016	2023-03-07 16:59:27.019726	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 32213 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
3113	2023-03-07 16:59:29.829718	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 32213 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128
3212	2023-03-07 16:59:33.669739	10.63.247.223	199.59.66.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 46199 → 8934 [SYN] Seq=834218208 Len=0 MSS=1460 SACK_PERM=1 TSval=554864136 TSecr=0 WS=128

In questo caso, sull'acquisizione viene visualizzata solo la sintassi TCP SYN, quindi il dispositivo non è in grado di aprire la connessione TCP.

 Nota: quando si incontra questo tipo di problema, è necessario indagare perché questo è bloccato. In alcuni casi, è bloccato sul lato firewall, tuttavia è necessario eseguire ulteriori indagini.

È possibile eseguire alcune operazioni per convalidare le connessioni TCP da Windows/MAC.

Porte di test

Per Windows

Aprire Power Shell e utilizzare i seguenti comandi:

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

Inoltre, utilizzare `ipconfig` per controllare l'origine:

```
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
```

 Nota: gli indirizzi IP mostrati qui sono Webex Calling Session Border Controller (SBC).

Andare al terminale e usare i comandi successivi:

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

Inoltre, utilizzare `ipconfig` per controllare l'origine:

```
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

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

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:~] $
```

Informazioni correlate

- [Usa CScan per verificare la qualità della rete di chiamate Webex](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).