Test Ports in Windows and MAC

Contents

Introduction

This document describes steps to test TCP SIP traffic ports in order to troubleshoot when supported Devices for Webex Calling are present.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understand of your Webex Calling environment and architecture
- Have read the Port Reference Information for Webex Calling
- Basic troubleshoot on device register issues.
- Have run the CSCAN tool Webex calling offers Use CScan to Test Webex Calling Network Quality

Components Used

This document is not restricted to specific software and hardware versions.

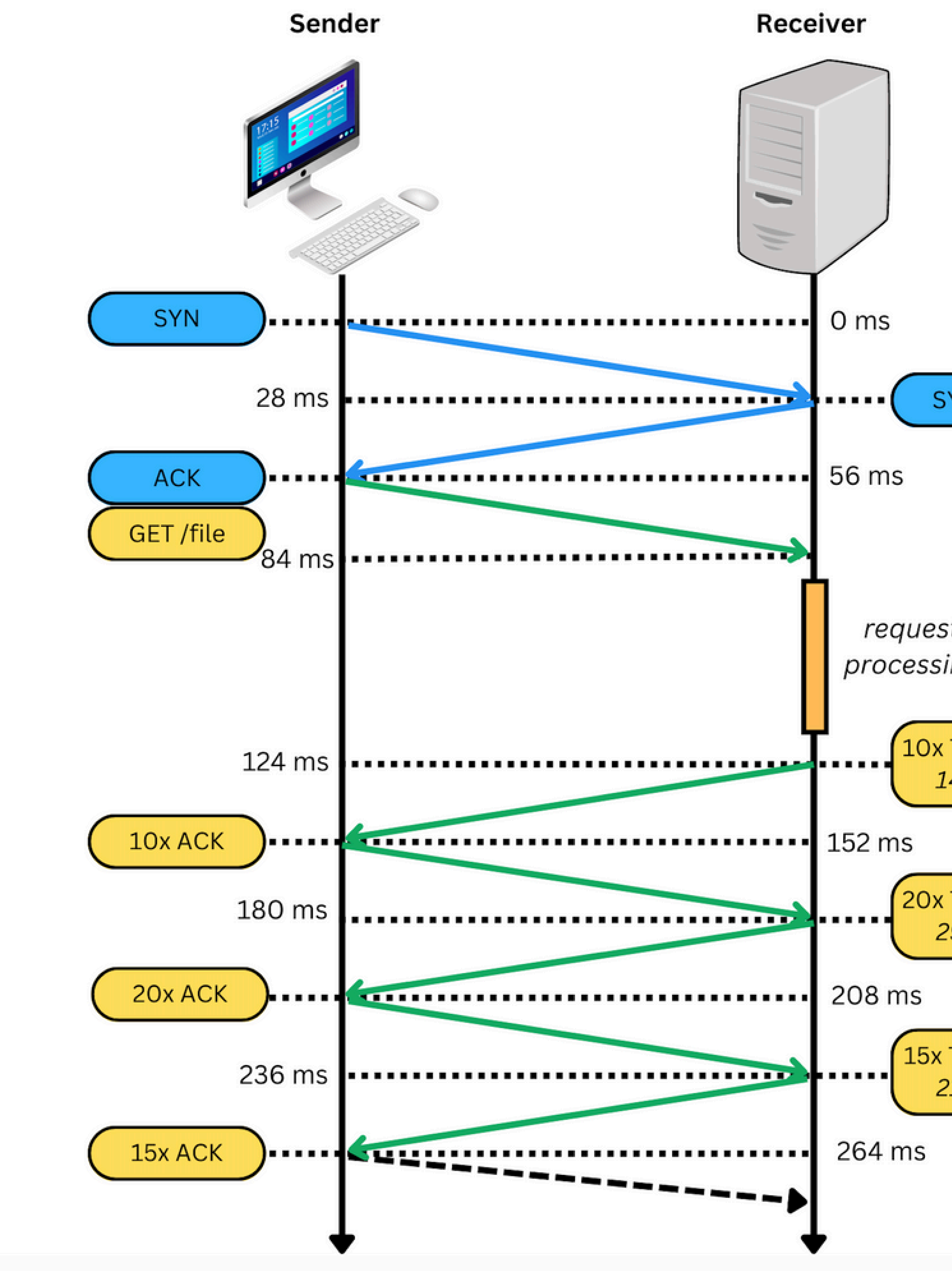
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes a basic way to troubleshoot and test whether you have access to the Webex Calling Signaling Session Initiation Protocol (SIP) ports.

In some cases, devices fail to register, and show a **offline** or **issues** status on Control Hub.

You need a packet capture so you can investigate whether the device the expected SIP flow to register:



In a packet capture, if successful, it appears similar to the next image:

> : When you encounter this sort of issue, you need to investigate why this is blocked. In some cases, it is blocked on the Firewall side, however, further investigation needs to be done.

There are some steps that you can do to validate TCP connections from your Windows/MAC.

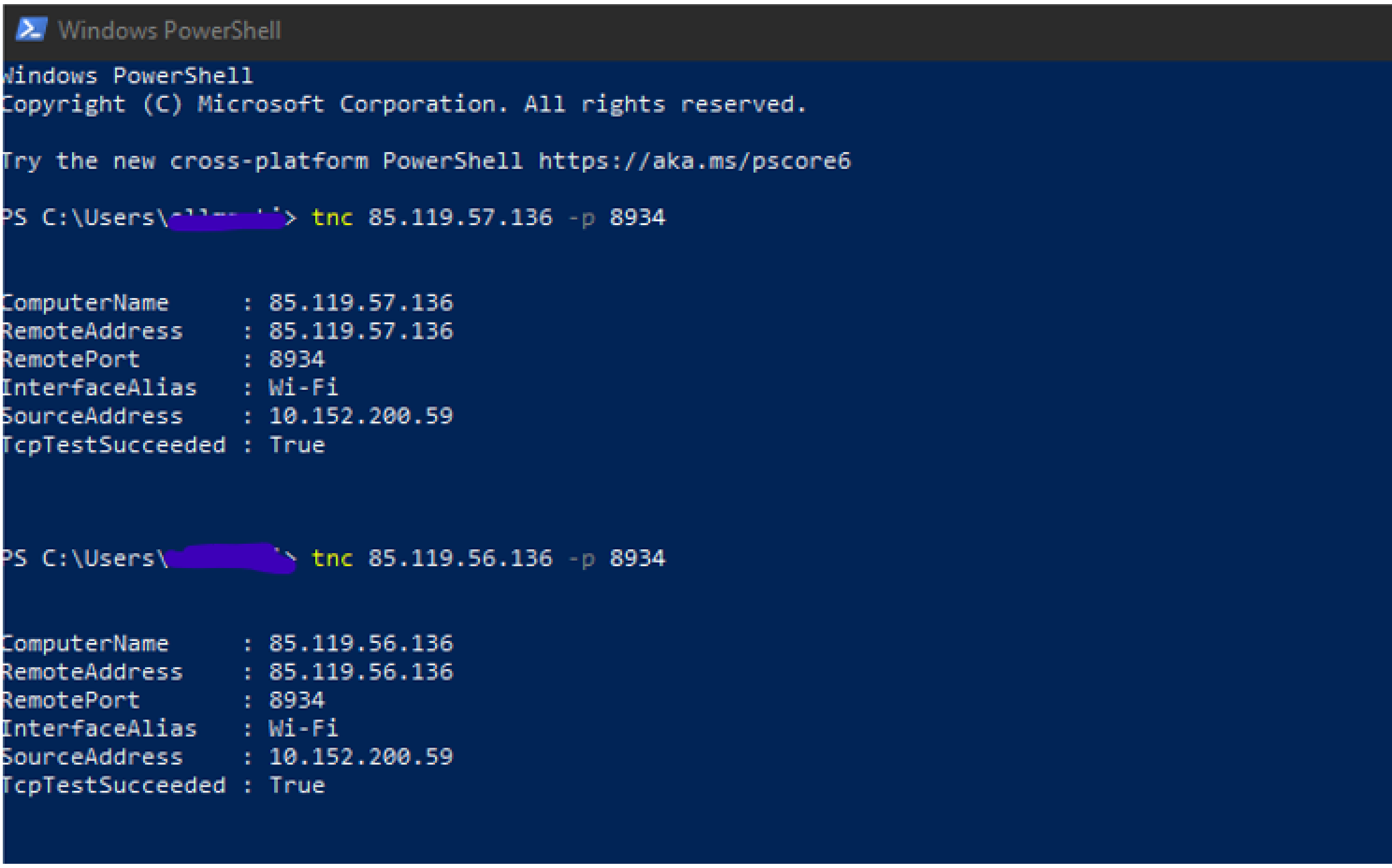
Test Ports

For Windows

Open the power shell, and use these commands:

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

Additionally, use `ipconfig` to check the source:



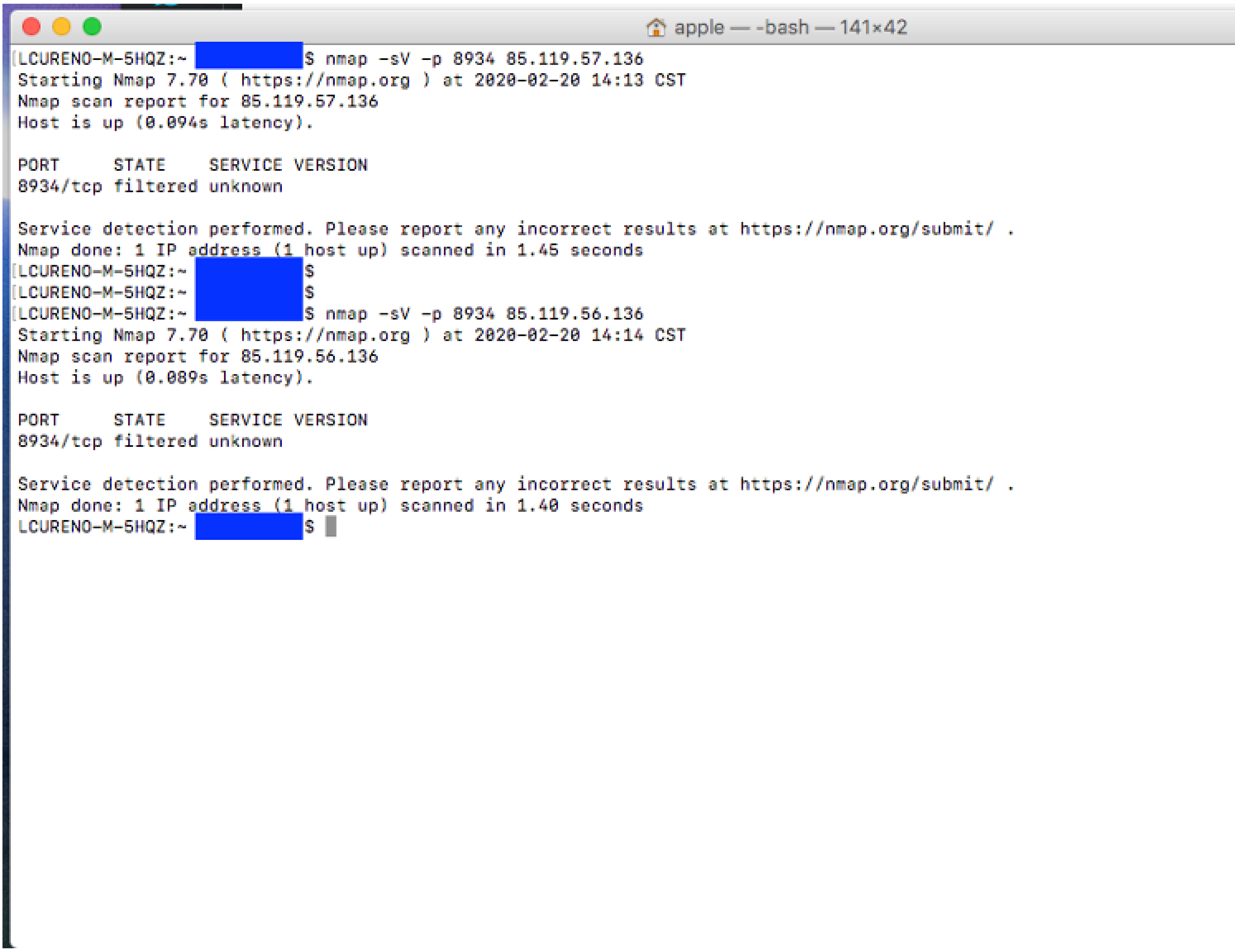
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\[redacted]> 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\[redacted]> 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
```

> **Note**: The IP addresses shown here are Webex Calling Session Border Controller (SBC).

Go to Terminal and use the next commands:

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

Additionally, use `ipconfig` to check the source:



```
LCURENO-M-5HQZ:~ [redacted]$ 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:~ [redacted]$
LCURENO-M-5HQZ:~ [redacted]$
LCURENO-M-5HQZ:~ [redacted]$ 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:~ [redacted]$
```

Related Information

- [Use CScan to Test Webex Calling Network Quality]
- [Cisco Technical Support & Downloads]