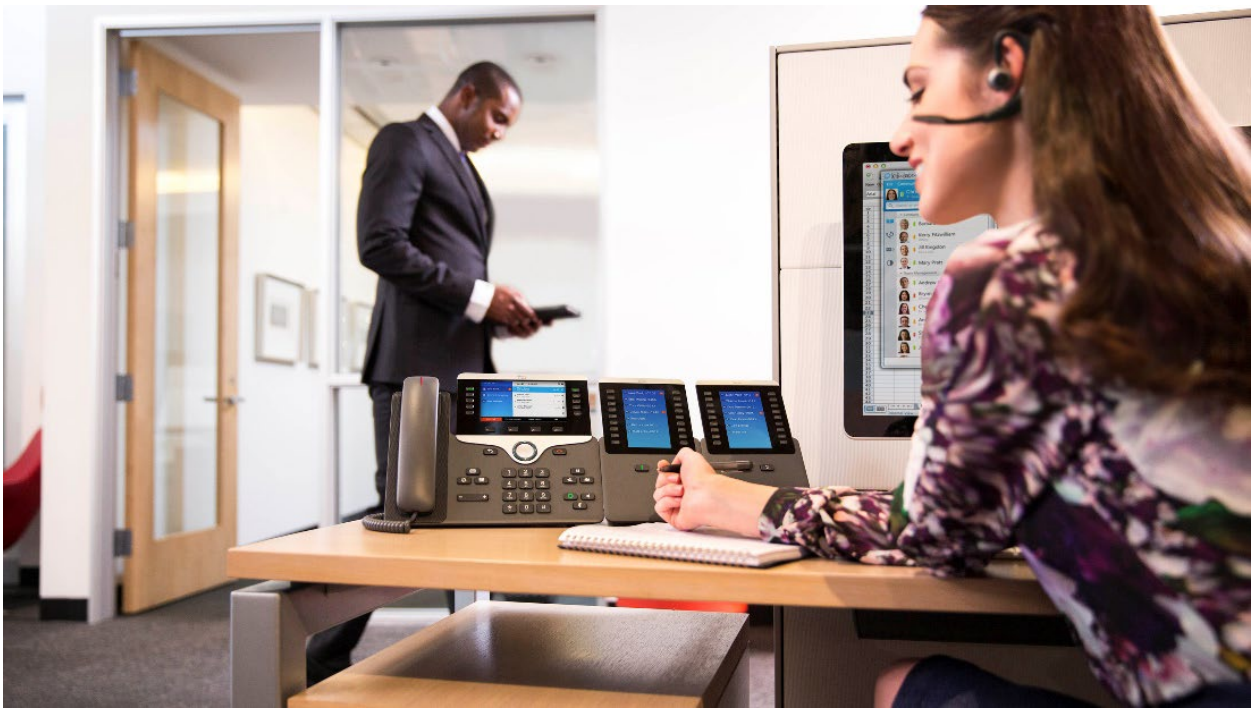
Webex Calling Service

Customer Requirements



December, 2020
Version 1.0

TABLE OF CONTENTS

About this document

Authors

Author(s): Quinton Parke-Thomas, Senior Product Manager – FirstLight Fiber, Inc.

Change Authority: FirstLight Engineering, FirstLight Operations, FirstLight Service Delivery, FirstLight Product Management.

Document Assumptions

This document assumes the reader has a high-level understanding of Voice over Internet Protocol, the general architecture of the Cisco Webex Calling Service, and the FirstLight Webex Calling Service offering.

Document History

Version	Issue Date	Change Reason
1.0	12/8/2020	First publication

Document Conventions

This symbol alerts the reader to critical information. By not following recommendations preceding this symbol there may be a risk of failure, equipment damage, connectivity loss or, data loss to the customer.

This symbol alerts the reader that there is further information about a given topic. There may be a hyperlink for the reader reference, or an external document referencing additional information that is important for a successful deployment.

This symbol alerts the reader to information that may be useful to the reader, but, is not critical to the customer experience. Rather, it may denote a best practice, or be useful information in general.

This symbol alerts the reader that additional technical information is available. Information preceding this symbol will provide technical details in relation to the topic being discussed. It will denote information that should be referenced while designing a solution.

FirstLight Webex Calling Solution Overview

FirstLight's Cisco Webex Calling solution consists of: Cisco Webex Calling, FirstLight PSTN Service for Cisco Webex Calling, and Network Assurance for Unified Communications.

Cisco Webex Calling is a service provided by Cisco Systems Inc. that provides PBX features to subscribers. Cisco Webex Calling is cloud based, with redundant infrastructure spanning the globe.

Cisco Webex Calling is offered from Cisco, and resold by FirstLight, in several license models that best fit the customers size and need.

Cisco Webex Calling only provides intra-company communications and does not provide any Publicly Switched Telephone Network services. FirstLight has integrated the calling services of the Cisco Webex Calling platform to the PSTN termination services offered by FirstLight. FirstLight PSTN Services for Cisco Webex Calling provide subscribers with inter-organizational calling capabilities over the traditional PSTN.

Customers purchasing both Cisco Webex Calling services and FirstLight PSTN Services for Cisco Webex Calling will receive a basic managed service and can contact FirstLight for support for the service. FirstLight offers optional managed service solutions for Cisco Webex Calling called Network Assurance for Unified Communications. This enhanced managed service provides customers a turnkey solution that includes: service activation, configuration, and ongoing support and management with a dedicated service level agreement.

Requirements Summary

Customer network design and configuration has many variables, many of which can affect the performance and quality of Voice over IP services (VoIP). For the Cisco Webex Calling VoIP service to work in most customer network environments there are a set of minimum requirements the customer network must meet to ensure service will function as expected. These requirements apply to both SIP phones and analog adapters (generally referred to from this point forward as SIP devices). Below is a summary of these requirements.

- Customer LAN must contain a DHCP server capable of providing an IP address to SIP devices when they boot.
- Customer LAN must contain a DNS server or provide DNS relay functionality to allow resolution of URL's used by SIP devices to communicate with external service platforms.
- DNS server must be capable of resolving both SRV and A records.
- Customer firewall must allow HTTP (TCP port 80) and HTTPS (TCP port 443) traffic for SIP devices to communication with external configuration servers.
- Customer firewall must allow SIP and RTP to allow SIP devices to place and receive calls.
- Customer router must set Network Address Translation (NAT) bind timer at a value greater than or equal to 30 seconds.
- Customer router/firewall must not manipulate the SIP or RTP packets at the application layer. If any CPE devices can function as a SIP Application Layer Gateway (SIP ALG), the ALG functionality must be disabled.
- Customer router should support Differentiated Service Code Point (DSCP) and ensure that higher priority packets take precedence over lower priority packets for all outbound packets.
- Customer router should be configured to mark all SIP and RTP packets from the Cisco Webex Calling control platforms as high priority to ensure these packets take priority over lower priority packets for all inbound packets. The Cisco Webex Calling control platforms can be uniquely identified by a set of specific IP addresses. SIP and RTP packets can be uniquely identified by the ports defined in the Firewalls section of this document.
- Customer Internet bandwidth must be sized to allow the minimum amount of required data bandwidth plus the total number of simultaneous voice calls required by the office.

- Customer Local Area Network (LAN) must be sized to allow the maximum amount of required data bandwidth plus the total number of simultaneous voice calls required by the office.

Minimum Requirements Summary

Customer Requirements	Minimum Internet Bandwidth	Recommended Internet Bandwidth
▪ DHCP Server ▪ DNS Server or Relay ▪ Allow TCP port 80 and 433 traffic ▪ Allow all necessary TCP ports to communicate through the customer firewall ▪ Disable SIP ALG ▪ Assign QoS to incoming SIP and RTP traffic and enable priority queuing on the outgoing router interface ▪ LAN sized to support SIP endpoints ▪ Separate subnet and VLAN for voice traffic	▪ Commercial Broadband Internet service ▪ 24 Kbps per simultaneous phone call ▪ 80 Kbps per simultaneous fax transmission ▪ 80 Kbps per non-compressed RTP stream ▪ 2.5 - 5 Mbps per video stream	▪ Direct Internet Access (DIA) featuring symmetrical service ▪ 200 Kbps (2x 100Kbps streams) per device or user (if employing softphones) ▪ 80Kbps per simultaneous fax transmission ▪ 2.5 - 5 Mbps per video stream ▪ Media bandwidth should be up to 50% or less of total available internet bandwidth, with the remaining allocated to data applications co-residing on the network. ▪ Internet should be sized to meet both voice and data requirements. Planned utilization of both voice and data should not exceed 80% of the available Internet bandwidth at expected peak usage.

Requirements Detail

DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices to obtain various parameters necessary for the devices to operate in an IP network. The DHCP parameters provided by the site DHCP server that are necessary for Cisco Webex Calling service to function properly are IP address, subnet mask, default gateway, and DNS server.

DHCP servers are commonly integrated into the customer's router, but they can be a stand alone server dedicated to only performing the DHCP function. For most broadband applications, the DHCP server will be integrated into the broadband router provided by the service provider. In this case, the configuration of the DHCP server (including whether or not it is on or off) can be controlled by logging into the broadband router.

All Cisco Webex Calling SIP devices are configured by default to obtain IP address and DNS server information from a local DHCP server. When a SIP device is booted, it will attempt to locate the local DHCP server and obtain this information. If the customer network does not contain a DHCP server or does not provide the required information, the SIP device will not boot properly and will be unusable.

Some DHCP servers are capable of providing "options" as part of its response to a client's request. For SIP applications, Option 66 is commonly used to provide the client, in this case a SIP device, with the address of the configuration server it should contact to obtain its configuration. In the case of Cisco Webex Calling service, this option is not required. All Cisco Webex Calling SIP devices are hard coded to point to a specific configuration server address and if an Option 66 is received by the SIP device in response to a DHCP request, the SIP device will ignore it.

DNS Server

Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. It provides a method of naming Internet devices with words that are easier to remember than the devices' actual numeric IP address. Also, certain types of DNS records are capable of associating a single word name with a list of IP addresses. This functionality is useful for cases in which device redundancy is used to improve performance and/or reliability.

All Cisco Webex Calling SIP devices require DNS to translate domain names to IP addresses. During the boot process, the domain name of the SIP device configuration server is translated so the SIP device can locate and receive configuration information from the proper configuration server. Also, once the phone has completed the boot process, the domain name of the call control servers is translated so the SIP device can locate and communicate with these call control servers. If a DNS server is not available to provide name translation, the SIP device will not boot properly and will be unusable.

There are several types of DNS records. The Cisco Webex Calling service utilizes "A" (address) and "SRV" (service) record types. "SRV" records are used to provide a mechanism of redundancy for the call control platforms. For Cisco Webex to function properly, both of these record types must be supported on the customer network.

Firewalls

A firewall is a device or set of devices in a data network configured to protect the network from potentially harmful traffic. One general function of a firewall is to permit or deny services of specific types from passing across the public network interface. One application of this functionality is to restrict the types of

services users on the private network can publicly access or to restrict public access to the private network to ensure security of the network.

Firewalls can impede SIP devices from communicating with configuration servers, call control servers, network gateways, and other SIP devices. For Cisco Webex Calling service to function properly, firewalls must allow the following services:

- **HTTP** (port 80) – required for communication between the local SIP devices and the configuration servers which contain the SIP devices configuration information
- **HTTPS** (port 443) - required for communication between the local SIP devices and the configuration servers which contain the SIP devices configuration information
- **SIP** (port 5060) – required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other SIP devices
- **SIP** (port 8933 to 8943) - required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other SIP devices.
- Note: This port range is not commonly associated with SIP. In this instance, it is used to avoid encounters with Application Layer Gateway (ALG) functionality that may damage the payload of SIP packets. For more information, refer to the Application Layer Gateway section of this document
- **RTP** (ports 19560-65535) – required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other SIP devices.

Note: ports 19560-65535 are not commonly associated with RTP. In this instance, they are used to avoid encounters with Application Layer Gateway (ALG) functionality that may damage the payload of RTP packets. For more information, refer to the Application Layer Gateway section of this document. With these services allowed, SIP devices should be able to properly communicate with all necessary external sources.

Network Address Translation

Network Address Translation (NAT) is a common router function which allows multiple private IP addresses on a LAN to be translated to a single public IP address on the WAN. The main reason NAT functionality exists is to conserve public IP addresses. There are not enough IP addresses within IPv4 to allow every computer connected to the Internet to have a unique public IP address. Also, NAT functionality does provide a level of security to devices with private IP addresses because those devices are not always publicly addressable.

Although necessary, NAT functionality creates issues for VoIP traffic. A typical NAT only translates IP information from private to public at the TCP/IP layer. It does not, however, translate any IP address information at the application layer. This means that any IP address information contained in the application layer payload of VoIP packets remains un-translated. Since these addresses are private, they are not routable in a public domain and are effectively unreachable. In the case of SIP, the IP address and port the SIP device wishes to advertise for establishing a connection is contained in payload of SDP attached to SIP messages. If this information is not translated, the far end will not be able to communicate with the SIP device. This usually creates a phenomenon commonly referred to as one-way RTP (voice path is only available in one direction).

Another issue with NAT functionality is that private devices are not reachable publicly unless a translation, commonly referred to as a bind, is created between the private IP address and the public IP address. This is done dynamically each time a private device attempts to communicate with a public device. The act of requesting communication causes the NAT to create a temporary bind between the private IP address requesting the communication and the public IP with which it is attempting to communicate. Bind duration is controlled by a timer which will expire and cause the bind to be removed if there is a period of inactivity

on the bind equal to the length of the timer. During the time the bind is active, public to private communication is possible, but once the bind becomes inactive, the private device is no longer publicly addressable. The most common duration for this timer is between 30 and 60 seconds. Also, binds can often be statically configured in a NAT. This functionality is often referred to as port forwarding. When this is done, the NAT is configured with a permanent bind between a private and public address.

With the Cisco Webex Calling product, the challenges presented by the presence of a NAT are addressed. A technique called NAT Traversal is used to overcome the issues created by the presence of a NAT. Part of the Cisco Webex Calling call control platform is responsible for maintaining constant communication with all SIP devices. This constant communication ensures that the NAT bind timer never expires, effectively making the dynamic bind permanent. Without this, a SIP device in a private network would not be able to receive calls. Also, the Cisco Webex Calling call control platform uses a technique called Media Relay to overcome the issue where the NAT does not manipulate application layer information. This functionality allows the call control platform to discover the public IP address and port of the RTP stream once the SIP device sends out its first RTP packet. The call control platform performs this function on both ends of a call and bridges the two legs of the call together, effectively relaying the traffic from one device to another.

Application Layer Gateway

Application Layer Gateway (ALG) is a method of manipulating IP address and port information at the application layer. It is similar to NAT functionality in that it typically translates private IP and port information created by a SIP device on a private network to public IP and port information on the WAN side of the router performing the ALG function. If done properly, this functionality negates the need for Media Relay functionality because all information advertised in the application layer is publicly routable.

Although this functionality is intended to improve the processing of VoIP traffic, not all ALG devices perform the application layer translation of packets properly. In many cases, portions of the packet are modified when they should not be which causes interworking problems between the SIP device and the call control platform. When this occurs, the ALG causes the SIP device to not function properly.

With the Cisco Webex product, it is recommended that all ALG functionality between the SIP device and the call control platform be turned off. Doing this eliminates the potential for the ALG to improperly translate packets which could render service unusable. However, in some cases, this functionality may not be configurable. To accommodate this case, the Cisco Webex product uses uncommon ports for SIP and RTP traffic. Port 8933 to 8943 is used instead of 5060 which is commonly used for SIP. Since most ALGs assume a SIP port of 5060, using port 8933 to 8943 will typically cause the ALG to ignore the packet completely and perform no manipulation. Also, the same is done for RTP. Although not specifically defined by any specific standard, the most common port range used for RTP is 16384-16482. To avoid the potential for ALG interaction, the Cisco Webex Calling product uses RTP ports 19560-65535.

Quality of Service Settings

Quality of Service (QoS) refers to the ability to provide different priority to different applications over a data network connection to ensure higher priority traffic takes precedence over lower priority traffic. A voice conversation is real-time and traffic associated with a voice call must process efficiently or issues such as clipping or choppy audio will occur. On the other hand, normal Internet traffic is best-effort. If packets are dropped or delayed, service is usually not noticeably disrupted. As a result, voice traffic generally is considered to be higher priority traffic than data traffic.

The Cisco Webex Calling product utilized Differentiated Services Code Point (DSCP), also commonly referred to as DiffServ, as the mechanism for marking packet priority. Each SIP device automatically sets every packet it sends as high priority. However, this does not ensure that all data network equipment in the traffic path will honor the setting and ultimately allow voice traffic to take priority of data traffic.

To ensure voice packets take priority over data packets, customer routers must be properly configured to handle DSCP. This functionality is sometimes referred to as Class of Service (COS) or priority queuing. In either case, it is recommended that the router be configured with strict priority queuing allowing packets marked with higher DSCP values to have higher priority. If this is not done properly, perceived call quality could noticeably deteriorate during peak traffic times.

Also, packets set with high priority by SIP devices only addresses traffic sent from the SIP device to other devices outside of the customer's network. It does not address packets inbound to the SIP device. These packets are normally not marked with a higher priority when received by the customer's router because priority values are normally not maintained across a WAN. As a result, without additional configuration these packets will not be prioritized over normal data traffic. To accommodate this case, it is recommended that priority rules be established to allow all inbound SIP and RTP traffic to have higher priority than all other traffic. The specific ports associated with SIP and RTP are defined in the Firewall section of this document. It may also be necessary to define the IP addresses of the Cisco Webex Calling call control platforms to have higher priority over all other traffic. A specific list of these IP addresses is not defined in this document because they are currently subject to change.

Internet Bandwidth

Internet bandwidth is the amount of capacity available for Internet traffic on a customer's network. This amount is determined by the service provided by the Internet Service Provider. The amount of bandwidth available will determine the amount of simultaneous voice calls and data traffic that the Internet connection will support. If properly sized and with the proper QoS settings in the customer router, the Cisco Webex Calling service will function properly. However, if undersized or if QoS is not provisioned correctly, perceived call quality could noticeably deteriorate during peak traffic times. The following information provides information and guidelines for properly sizing voice service for a given Internet bandwidth.

To determine the number of phones that can be supported over a given bandwidth, the maximum number of simultaneous calls that can be supported must first be calculated using one of the following formulas. There are two calculations that must be completed:

Worse Case Calculation (No Compression)

```
Max Calls = Available Voice Bandwidth (Kbps) / (SimCalls * 80Kbps)
```

Where,

- **Available Voice Bandwidth (Kbps)** – is the maximum amount of bandwidth allowed for voice traffic. This value is equal to the lower of the connection download and upload speeds minus an amount reserved for processing data traffic. Offices with routers provisioned to prioritize voice traffic over data traffic can process voice calls at up to 100% of total connection bandwidth without jeopardizing call quality. However, at sustained high call volumes, data traffic quality will be impacted. As a result, it is recommended that calculations for maximum calls and maximum phones be done assuming only a portion of the overall bandwidth can be used for voice traffic.

- **SimCalls** – the number of simultaneous calls coming out of a site
- **80Kbps** – is the bandwidth required for a fax/modem call

Best Case Calculation (With Compression)

```
Max Calls = Available Voice Bandwidth (Kbps) / ((Phone * 24Kbps)+(Fax *
                                    80Kbps))
```

Where,

- **Available Voice Bandwidth (Kbps)** – is the maximum amount of bandwidth allowed for voice traffic. This value is equal to the lower of the connection download and upload speeds minus an amount reserved for processing data traffic. Offices with routers provisioned to prioritize voice traffic over data traffic can process voice calls at up to 100% of total connection bandwidth without jeopardizing call quality. However, at sustained high call volumes, data traffic quality will be impacted. As a result, it is recommended that calculations for maximum calls and maximum phones be done assuming only a portion of the overall bandwidth can be used for voice traffic.
- **Phone** – the number of simultaneous phone calls with compression coming out of a site
- **24Kbps** – is the bandwidth required for a phone call with compression
- **Fax** – the number of simultaneous fax calls (no compression) coming out of a site
- **80Kbps** – is the bandwidth required for a fax/modem call

There are certain call flows in the Cisco Webex Calling PBX service that do not support compression, such as calls to Voice Mail or to the Conferencing service. Therefore, the actual amount of bandwidth required will vary between the best and worst case calculations.

Maximum Supported Phones Calculation

The maximum number of phones that can be supported over a given bandwidth can now be calculated using the following formula:

```
Max Phones = Max Calls * Users per Simultaneous Call
```

Where,

- **Max Calls** – is the amount of simultaneous calls that can be supported over the given bandwidth
- **Users per Simultaneous Call** – is a statistical approximation of the total number of users that can share one call path with non-blocking results. The value of 4 is recommended for average office usage. However this number could vary drastically depending on the type and size of office.

Local Area Network Bandwidth

Local Area Network (LAN) Bandwidth is the amount of capacity a customer's internal network can support. This amount is determined by the throughput specification of the LAN infrastructure. In most customer applications, the LAN infrastructure is a single layer 2 switch. The amount of bandwidth

available will determine the amount of simultaneous voice calls and data traffic that the LAN will support. If properly sized, the Cisco Webex Calling service will function properly. However, if undersized, perceived call quality could noticeably deteriorate during peak traffic times. It is the customer's responsibility to ensure that their internal network is sized properly to support the addition of VoIP to their network.

Firewall Configuration Recommendations

A correctly configured firewall is essential for a successful calling deployment. We require ports for signaling, media, network connectivity, and local gateway.

Not all firewall configurations need ports to be open but if you're running inside-to-outside rules, you should open ports to allow the protocols required for service out. As long as you deploy NAT, define reasonable binding periods, and avoid manipulating SIP on the NAT device, you shouldn't need to open ports inbound on the firewall.

If a router or firewall is SIP Aware, meaning it has SIP Application Layer Gateway (ALG) or something similar enabled, we recommend that you turn off this functionality to maintain correct operation of service. See the relevant manufacturer's documentation for information about how to disable SIP ALG on specific devices.

Please refer to the following article for information regarding port and firewall configurations:
https://help.webex.com/en-us/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

Local Area Network Recommendations

Customers are required to maintain an ethernet based Local Area Network to provide connectivity between the SIP devices and the internet. The Local Area Network is generally comprised of either layer 2 ethernet switches or layer 3 ethernet switches. It is recommended the LAN meet the following requirements:

- Support for Power over Ethernet – it is recommended that SIP endpoints be powered via the LAN switching infrastructure. While AC power adapters are available for SIP endpoints offered with Webex Calling, PoE enabled switches reduce cabling requirements, lower power consumption, and enable centralized battery backup to ensure SIP endpoints can be used in the event of a power outage.
- Support for the following features or protocols:
  - VLAN Tagging
  - 802.1Q VLAN Trunking
  - CDP and/or LLDP-MED
  - Quality of Service
  - Class of Service

It is highly recommended that all switches that provide connectivity for SIP endpoints are connected to an Uninterruptible Power Supply (UPS), and in some cases utilizing a power redundancy strategy such as multiple power supplies and redundant power feeds. This is especially critical in situations where voice services are considered life saving and/or critical for health and safety purposes.

Cabling Recommendations

Customers are required to maintain a physical cable plant that will connect station ports to the ethernet LAN switch(s). Customers are also required to supply any patch cabling to connect SIP devices to station ports. It is highly recommended to follow all ethernet cabling standards.

Customers should not have more than one device connected to a single ethernet plenum cable run. At one time it was common practice to install low voltage twisted pair cabling termination half of the four copper wire pairs for an Ethernet device on one station port, and the other half for an analog device voice device. At the aggregation point, one half of the pairs would terminate in a patch panel to connect to a LAN switch, and the remaining half of the copper strands would be terminated into an analog PBX. This was done as several pairs were unused in the ethernet standard (10Base-T, 100Base-T non-duplex). Due to the 1000Base-T or Gigabit Ethernet standard, as well as Power Over Ethernet (which requires all 8 conductors to operate) standards, it is highly recommended, and in many cases required, to use all of the pairs in an ethernet cable run for a single device. FirstLight will only provide support for deployments where all eight of the conductors in the UTP plenum cable run are used in the termination of that device.

Legacy cabling should be avoided whenever possible. Using cabling that is not certified for at least 100Mbps full-duplex ethernet communication is not recommended. Generally cabling installed to be used with a premises analog PBX cannot support today's data networking requirements.

Testing Network Quality to Webex Calling Service – CScan

Cisco provides a web based tool, CScan, to measure the quality of the Internet connection from the PC the test is administered from to the Webex Calling service. This test checks the quality of the Internet connection including download and upload bandwidth, latency, packet loss, and jitter. The test also checks to see if the necessary TCP ports are open on any upstream firewall between the PC where the test is run and the Webex Calling service. The test can also perform a traceroute report to give insight into where issues might be occurring along the path between your computer and the Webex Calling data center.

The test provided by this tool is not, and should not be used as, a guarantee of performance. Since the CScan test is taken at a single point in time, the results are only an estimate of the expected performance at the time the test was performed.

Note: it is not possible to test all of the ports with a web-based application. It is still recommended to follow the port requirements guide to ensure your firewall is configured properly. See the document at the following hyperlink for more information:
https://help.webex.com/en-us/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

To access and run the test visit https://cscan.webex.com *in a supported web browser.*

For additional assistance regarding this tool, see the following help article:
https://help.webex.com/en-us/y27bej/Use-CScan-to-Test-Webex-Calling-Network-Quality#id_133930

Running a Cscan Test

1. To run the test, open a web browser, and navigate to the following URL: https://cscan.webex.com.
2. Select a location, choose your language, and click Pick server. Choose the location that is closest to you.
3. Choose either: **Advanced Diagnostic** Test, or **Basic** Test.

If you choose Advanced Diagnostic Test, you must allow CScan to access your microphone and camera. Generally, your browser will prompt you to allow this before the test begins. If your browser does not prompt you to provide CScan access to your microphone and camera, update your browser to the latest version and/or please check your browser's security settings to ensure this function isn't blocked.

Basic Test

The basic test will analyze download and upload bandwidth, latency, traceroute report, TCP ports between the PC it's executed from and the Webex Calling Data Center location you chose.

Note: The TCP ports that are tested are a subset of the ports required for Webex Calling. It isn't possible to test all the ports for a web-based application. Follow the port requirements guide to ensure that your firewall is set up correctly.

https://help.webex.com/en-us/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

Advanced Diagnostic Test

The Advanced Diagnostics test provides the same information as the Basic test but adds packet loss and jitter.

To carry out the Advanced Diagnostic test, CScan must open a WebRTC connection to your computer, this requires access to your computer's camera and microphone. CScan doesn't save any audio or video packets. This permission is used for measuring packet loss and jitter. CScan will never access your camera or microphone outside of running a test. The permissions can be revoked at any time.

Traceroute Report

A traceroute report is provided when you run a CScan test. To generate this, CScan initiates a traceroute from a Webex Calling data center to the public IP address of your computer. This can give insight into where issues might be occurring along the path between your computer and the Webex Calling data center.

Please note that traceroute reports can take a while to generate.

Interpreting Test Results

The CScan tool estimates potential concurrent calls that could traverse your network. This is an estimate based on the bandwidth that is required for audio calls, allowing for a buffer of extra internet traffic. Since the CScan test is taken at a single point in time, this is an estimate and not a guarantee of performance during peak traffic times.

If CScan indicates that ports are blocked, check your firewall configuration and the port requirements document. If ports are blocked, you may have issues registering devices or making calls. It's not possible to test all ports listed in the Port Requirements document, so if all ports on CScan are listed as open, there may still be other ports not tested that are causing issues.

If latency or bandwidth figures are low, you may have a lower quality Webex Calling experience. Ensure you have enough bandwidth from your ISP, and that your device has a strong connection to the internet. If you're using Wi-Fi, ensure that your signal is strong.