



Improving Quality of Experience for Webex in Work from Home Environments

A Preferred Architecture Whitepaper

December 2020

© 2020 Cisco Systems, Inc. All rights reserved.





CONTENTS

PREFACE **3**

 PURPOSE 3

INTRODUCTION **4**

WEBEX MEETINGS WORK FROM HOME ENVIRONMENT **5**

 THE WEBEX MEETINGS CLIENTS AND DEVICES ROLES AND COMPONENTS 5

QOE RECOMMENDATIONS AND CONSIDERATIONS: **7**

 AUDIO AND VIDEO QUALITY 7

 NETWORK 8

 PHYSICAL SPACE 16

 PLATFORM 18

WEBEX CLIENTS AND DEVICES **22**

 MEDIA RESILIENCE AND RATE ADAPTATION 22

 WEBEX (FORMERLY WEBEX TEAMS) 22

 WEBEX MEETINGS DESKTOP APP 24

 CISCO WEBEX DESK DEVICES 27



Preface

Cisco Preferred Architectures provide recommended deployment models for common use cases. They incorporate a subset of products from the Cisco portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

Purpose

The purpose of this document is to describe the best practices and considerations for ensuring the best quality of experience in Work from home (WFH) environments using Webex Meetings Clients and Devices.

Documentation for Cisco Collaboration Preferred Architectures

- Cisco Preferred Architecture (PA) design overview guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.
- Cisco Validated Design (CVD) guides provide details for deploying components within the Cisco Preferred Architectures. These guides support planning, deployment, and implementation (PDI).
- Alternative Designs include supplemental documents such as overview and CVDs, whitepapers, and applications notes covering alternate designs, add-on applications and services, and optional functionality.

For more information go to the landing page of the [Cisco Collaboration Preferred Architectures](#)

About This Guide

The *Improving Quality of Experience for Webex in Work from Home Environments Whitepaper* is for Customers and Administrators who want to understand the best practices and recommendations for getting the best quality of experience in work from home environments using Cisco Webex technologies.



Introduction

In recent months, many organizations have found a majority or even all of their employees working remotely rather than working at an office or site location. These “work from home” users need to be able to continue to access work resources and need collaborative tools in order to communicate and stay in touch with their co-workers as well as customers and partners. Thankfully, there are many network and collaboration products and solutions which allow organizations to extend collaboration outside the walls of their businesses. Providing access to company resources and collaborative tools for employees outside the office is no longer a luxury; it is mandatory for businesses to stay relevant in today’s market. Today’s users expect immediate access to these tools from a wide variety of portable and mobile devices. Many of these same tools can be extended to customers and partners, helping strengthen these relationships.

Organizations realize the added value that remote worker and collaboration applications bring to their businesses through increased employee productivity and enhanced customer relationships. Not long ago, interoperability among collaboration applications was sparse, and applications were difficult to deploy and use. Since then, significant advances have been made in the secure remote work and collaboration space, simplifying deployment, improving interoperability, maintaining security, and enhancing the overall user experience. Additionally, individuals have adopted a wide variety of smart phones, social media, and collaboration applications in their personal lives.

Organizations can now feel comfortable providing remote workers with network connectivity and collaboration applications that employees will quickly adopt and that provide maximum value. These new connectivity tools enhance an organization’s overall business processes, make its employees more productive, and open the door to new and innovative ways for communicating with each other, business partners, and customers. Today’s work from home (WFH) solutions offer organizations the ability to support remote employees while maintaining productivity and ensuring business continuity.



Webex Meetings Work from Home Environment

The *Improving Quality of Experience (QoE) for Webex in Work from Home (WFH) Environments Whitepaper* is created to assist administrators and end users in learning about how to better improve the quality of their Webex meetings experience in WFH environments.

This document provides guidance (both general and specific) on achieving quality real-time audio and video collaboration in Webex Meetings. We start the document with a quick overview of the Webex Meetings clients and devices roles and components. We then discuss quality of experience recommendations and considerations by breaking up the subject matter into 3 areas network, platform and physical space. Specifically, a general audio and video quality discussion with guidance is provided however for the “Platform” portion voice headsets are also covered with specific Cisco examples including the Cisco 52x / 53x / 56x series and Cisco 730 series headsets. USB video or web cameras are also covered as it relates to video quality with the Cisco Webex Room USB as a specific example. We then dedicate the rest of the document to Webex apps and Devices specific information from client and device capabilities in providing quality in challenging network environment to how to specifically test meeting audio and video sources and preview your and test your environment.

The Webex Meetings Clients and Devices Roles and Components

In a Webex WFH environment a laptop or desktop is enabled with a Webex client, either the Webex (formerly Webex Teams) or Webex Meetings App. We also discuss Cisco Webex Devices as an alternative to a Webex clients and discuss some of the reasons why a dedicated video device might make sense in WFH environments.

[Cisco Webex Meetings Desktop and Mobile Apps](#)

[Cisco Webex Desktop and Mobile Apps \(formerly Webex Teams\)](#)

[Cisco Webex Devices \(Board, Room and Desk\)](#)

Cisco Webex Meetings Desktop and Mobile Apps

The Cisco Webex Meetings desktop and mobile app allows you to access your most commonly used Webex Meetings site controls all in one place. You can use the Webex Meetings desktop and mobile app to easily view your upcoming meetings, start and join your meetings, and connect to a video device.

The Webex Meetings desktop app is available for Windows and Mac OS platforms while the mobile app is available for Android, iPhone and iPad.

Cisco Webex Desktop and Mobile Apps (formerly Webex Teams)

Cisco Webex desktop and mobile apps are cloud-based applications with integrated voice/video meeting, calling, messaging, and content sharing for mobile devices, personal computers, and web browsers. The mobile and desktop clients are also capable of registering to Unified CM for voice/video calling.

The Webex desktop app is also available for Windows and Mac OS platforms while the mobile app is available for Android, iPhone and iPad.

Cisco Webex desktop and mobile apps support Unified CM registration which allows for Cisco Webex to register to both Webex Cloud as well as an On-Prem Unified CM call control simultaneously for both workloads. This document will not cover the Webex (Unified CM) workload. For more information on Webex (Unified CM) call flows and functionality please see the [Cisco Webex Hybrid Call Service](#) chapter of the [Preferred Architecture for Cisco Webex Hybrid Services, CVD](#).

Cisco Webex Devices (Board, Room and Desk)

Cisco Webex Devices come in 3 classifications based on usage, Webex Boards, Webex Room Devices and Webex Desk Devices.

The **Cisco Webex Board** is an all-in-one whiteboard, wireless presentation screen, and video conferencing system for smarter team collaboration.

The **Cisco Webex Room Devices** are Intelligent video conferencing devices for meeting rooms of all sizes.

The **Cisco Webex Desk Devices** are simple-to-use and compact video conferencing devices designed for desktops.

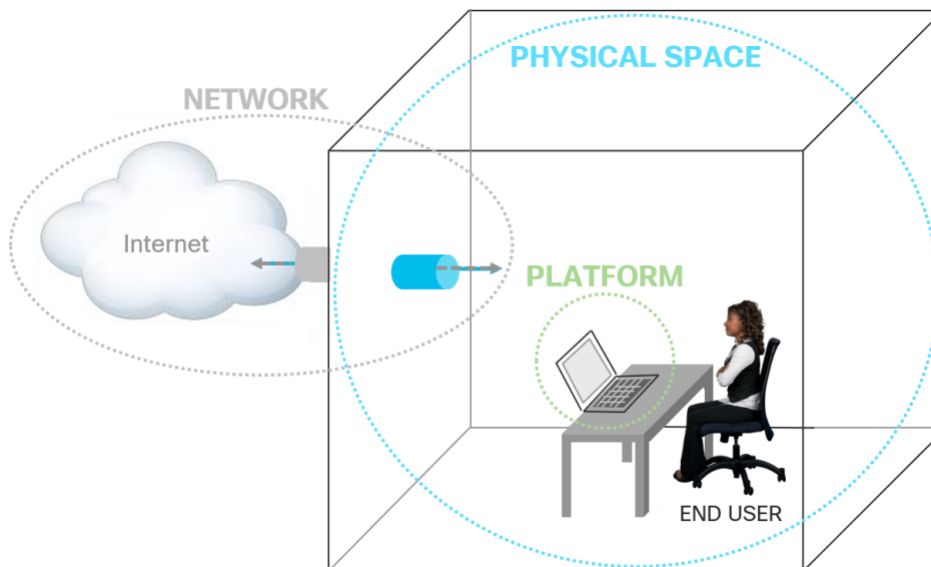
QoE Recommendations and Considerations:

Audio and Video Quality

Audio and video quality are critical components of successful real-time collaboration. Poor audio quality will cause breakdowns in real-time communication. If you cannot clearly hear another user or another user cannot clearly hear you, then no collaboration can move forward. Likewise, for video the added ability to see your interlocutors adds to the quality of a meeting experience and collaboration that can be achieved. When video quality is poor, this quality of meeting experience and collaboration is diminished.

When considering audio and video quality, it makes sense to break the overall environment into parts or layers which in combination determine overall quality. [Figure 1](#) shows the overall audio-visual environment broken into three layers: Network, Physical Space and Platform.

Figure 1. Audio and Video Quality: Three Layers of the Audio-Visual Environment



Poor quality can ruin the end user experience and in cases where audio is critical to the user's ability to get work done, it can render the WFH deployment unusable in many regards. To ensure a high-quality experience for the end user in a WFH deployment we must consider all three layers and take steps to ensure that best practices are implemented as much as possible at each layer. The following breaks each environment layer down with the important considerations and best practices for each layer.

Network

Network bandwidth, throughput, and reliability are critical for providing high quality audio and video. Generally, networks with very low delay and jitter, reliable delivery, and little to no packet loss are going to deliver higher quality audio and video.

Physical Space

The physical space consists of anything involved with the room environment that might affect both audio and video. Things such as size of the space, whether it's private/shared, background activity and noise and lighting.

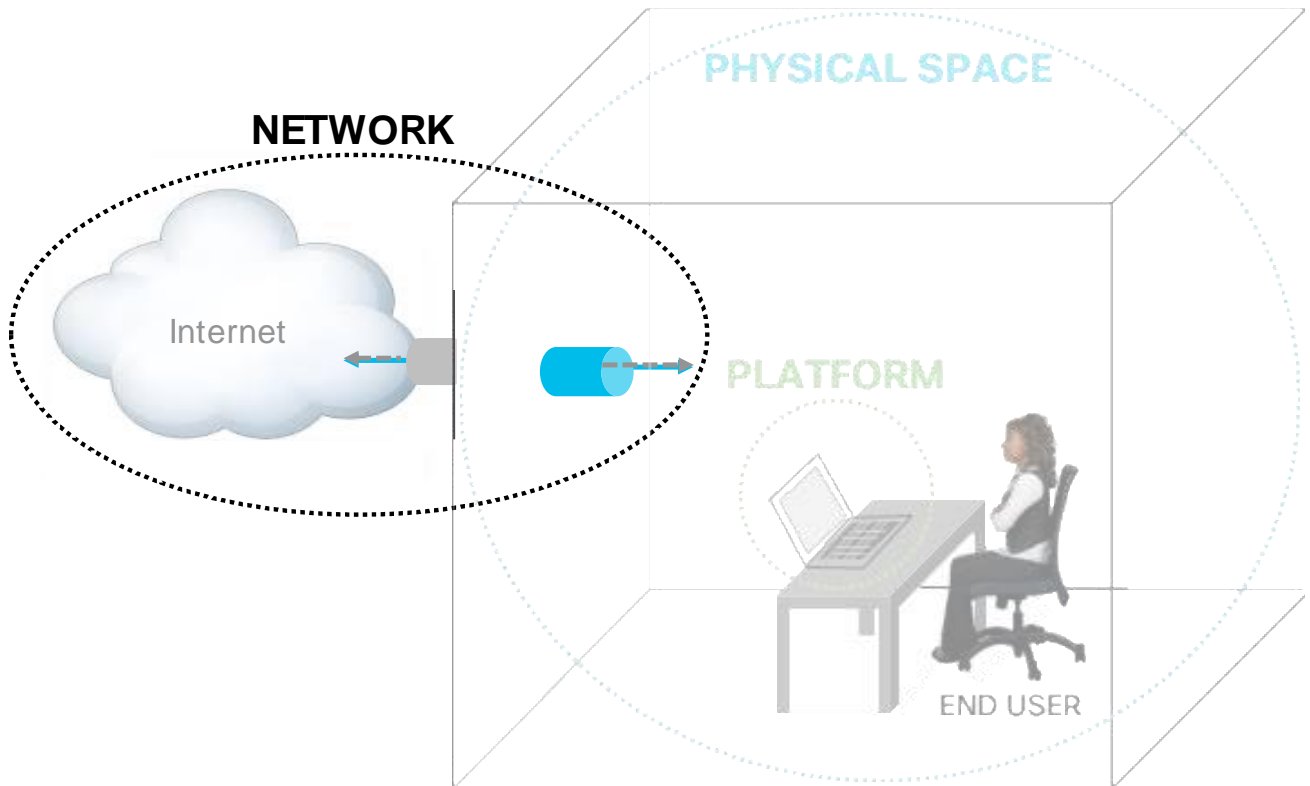
Platform

The platform consists of the Windows PC or Mac hardware and software components such as the operating system (OS), CPU, memory, Software running, hardware such as speaker, microphone and video camera.

Network

Network bandwidth, throughput, and reliability are critical for providing high quality audio and video. Generally, networks with very low delay and jitter, reliable delivery, and little to no packet loss are going to deliver higher quality audio and video.

Figure 2. Network



Network Readiness

Network readiness is a critical step in establishing a good working environment.

Without a proper network setup, home working might prove much less productive than working from the enterprise network. Insufficient upstream and downstream bandwidth can impact applications significantly, especially for real-time applications such as audio and video conferencing, to the extent that working from home becomes a frustrating experience. Although increasing the available Internet bandwidth that is offered by the Internet service provider can sometimes be an option, we can define a set of best practices that can help optimize the experience using the available network connection. In this section we will present some considerations to understand how well suited the network is when it comes to home working, and how to improve its usability.

The home network delivers Internet connectivity and, via Internet, access to the Enterprise. The home network is used by a number of different services, such as:

- Work from home
- Study from home
- Video surveillance
- Entertainment
- Home automation

All services can potentially be used concurrently by multiple users and thus potentially affect each other. To provide the best user experience it is critical to understand if and how these services can co-exist, and eventually how to prioritize certain services over others. The purpose of this section on network readiness is to prepare the network for a work from home / study from home consistent experience, even when multiple people are using the network at the same time.

Network devices provide network connectivity for user devices. Routers, switches, residential gateways, set-top boxes, home networking adapters and Internet access gateways are examples of network devices used to provide Internet access and interconnect devices within the home. User devices are those devices that exchange information with other user devices or servers (potentially via the Internet), and that ultimately present that information to the end-user. A mobile phone, a laptop or PC, a video surveillance camera, or a building automation sensor are examples of user devices.

End-to-end networks and components are involved in connecting home users to cloud services or to enterprise networks:

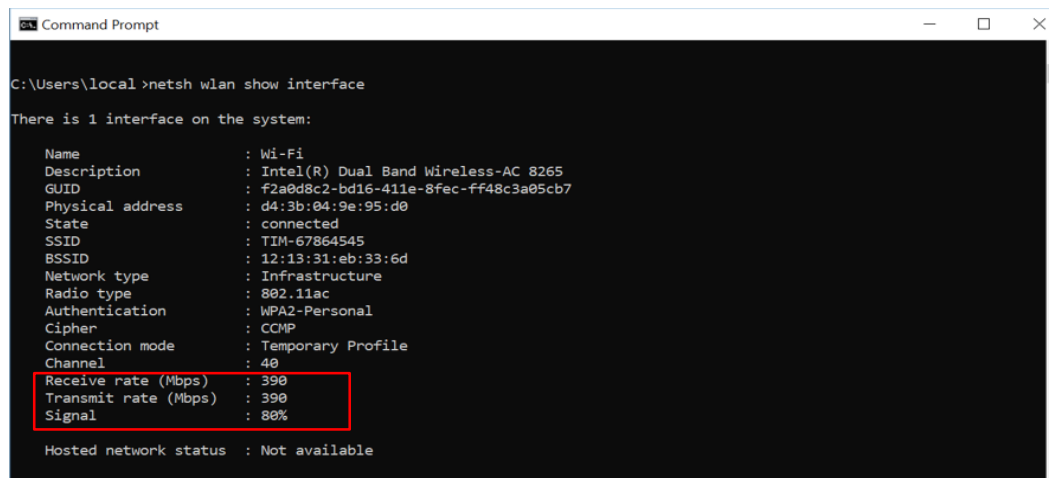
1. Internet
2. Demarcation point (router / cable modem / Internet gateway / Wifi access point)
3. Home network

The demarcation point marks the border between the home network and the Internet service providers infrastructure creating the connection to the Internet. Typical components at the demarcation point are routers, cable or DSL modems commonly combined with Wifi access points. The end user can only manage and control the home network and sometimes the equipment or CPE (customer premises equipment) at the demarcation point. Everything upstream from the CPE to the Internet is outside of the home user's control.

Every device inside the home network is under the user's control. As far as network quality is concerned, a wired connection is generally better than a Wifi connection. A wired connection is dedicated to a single device while Wifi capacity is shared between all devices concurrently using Wifi. Also signal quality on a network cable is superior, where noise and signal attenuation are much lower. In contrast, signal quality of Wifi connections is very sensitive to distance, physical obstacles, and other wireless networks in the same area. In order to check the quality of the Wifi signal it is possible to perform the following operations:

To view the Wifi signal information on Microsoft Windows PCs, open a Command Prompt session by typing "cmd" in the search. In the command prompt type "netsh wlan show interface (Figure 3). In the command prompt type "netsh wlan show interface". This command will return the percentage of signal strength and the available transmit and receive bitrate: below

Figure 3. Windows Network Statistics



```

C:\Users\local>netsh wlan show interface

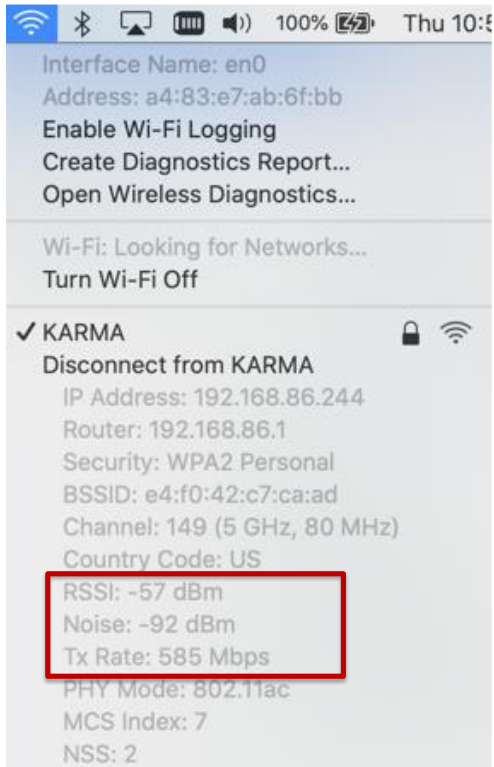
There is 1 interface on the system:

Name                : Wi-Fi
Description         : Intel(R) Dual Band Wireless-AC 8265
GUID                : f2a0d8c2-bd16-411e-8fec-ff48c3a05cb7
Physical address    : d4:3b:04:9e:95:d0
State               : connected
SSID                : TIM-67864545
BSSID               : 12:13:31:eb:33:6d
Network type        : Infrastructure
Radio type          : 802.11ac
Authentication      : WPA2-Personal
Cipher              : CCMP
Connection mode     : Temporary Profile
Channel             : 40
Receive rate (Mbps) : 390
Transmit rate (Mbps) : 390
Signal              : 80%

Hosted network status : Not available
  
```

On a Mac, select the Wifi icon located in the top bar while depressing the "option" key (Figure 4):

Figure 4. Mac Network Statistics



The RSSI (Received Signal Strength Indicator) value represents the power in the received radio signal. The unit dBm is used to express a power ratio in reference to 1 mW. An increase of 10 dBm in level is equivalent to 10-fold increase of power and an increase of 20 dBm is equivalent to a 100-fold increase. An RSSI of -100 dBm (equivalent to 0.1 pW) is the absolute minimum receive power on Wifi networks. An RSSI of -70 dBm is much worse than an RSSI of -50 dBm because the received power is less by a factor of 100. The higher the RSSI value the better. The receiver noise level is also expressed in dBm. The lower the Noise level the better; -90 dBm is better than -75 dBm. The difference between RSSI and noise is the signal to noise ratio (SNR). In the screenshot above the SNR would be calculated as $(-57 \text{ dBm}) - (-92 \text{ dBm}) = 35 \text{ dB}$. Typically, SNR values of at least 25 dB are required for good Wifi connections.

On Microsoft Windows platforms if the Wifi signal is less than 60% then the Wifi connection typically is not considered good enough for real-time traffic.

To improve SNR or Wifi signal quality either the received power has to be increased (move closer to the Wifi access point, remove obstacles) or noise has to be reduced (remove obstacles, chose a different channel to avoid overlap with other Wifi networks). Adding additional Wifi access points or Wifi repeaters is required if sufficient SNR or Wifi signal quality cannot be achieved by these methods. Additional Wifi access points with a wired connection to the CPE at the demarcation point are preferred over Wifi repeaters because they add less delay to the connection.

Besides the OS-embedded tools there are other tools available for Mac, Windows, Android and iOS that can give a comprehensive view of the Wifi quality.

Comparing the performance of wired network with Wifi performance helps understand which applications can run on Wifi and which require an Ethernet connection.

Use one of the free online tools to test your Internet access speed such as <https://www.speedtest.net/> and run two tests: one using the Ethernet connection of the user laptop, and another with the same laptop using the Wifi connection. If those tests give different results and the wired network is much better than the Wifi network despite being relatively close to the Wifi antenna, consider using a wired connection for real-time applications like voice and video.

Real-time applications are more demanding in terms of latency, jitter, packet loss, and overall bandwidth when compared to other non-real-time applications. For these reasons it's good to measure the impact of a collaboration-enabled device on the network. A way to check Webex running on the home network is by using the "Cisco Webex Network Test" available at <https://mediatest.webex.com>. Though specifically designed for Webex App (formerly Webex Teams), the tool can also be used to assess whether the network is suitable for collaboration endpoints which are registered to an on-premises call control via VPN or Mobile and Remote Access (MRA).

Network conditions may vary depending on utilization of the home network and the Internet. The networks test should be run under normal conditions: during regular working hours and under normal load of the home network. If many devices are usually connected to the network at the same, perform this test while all devices are connected and being used.

The tool shows detailed statistics for network parameters relevant for collaboration, such as delay, jitter and loss. However, you don't have to bother with this level of detail, as the output also has simple red, yellow, green classification for each parameter (Figure 5).

Figure 5. Cisco Webex Network Test: Success



In this test, Webex App, Room System and Call are good. By clicking the "More Details" link at the bottom of the page it is shown that a green circle means "good", a yellow circle means "fair", and a red circle means "bad".

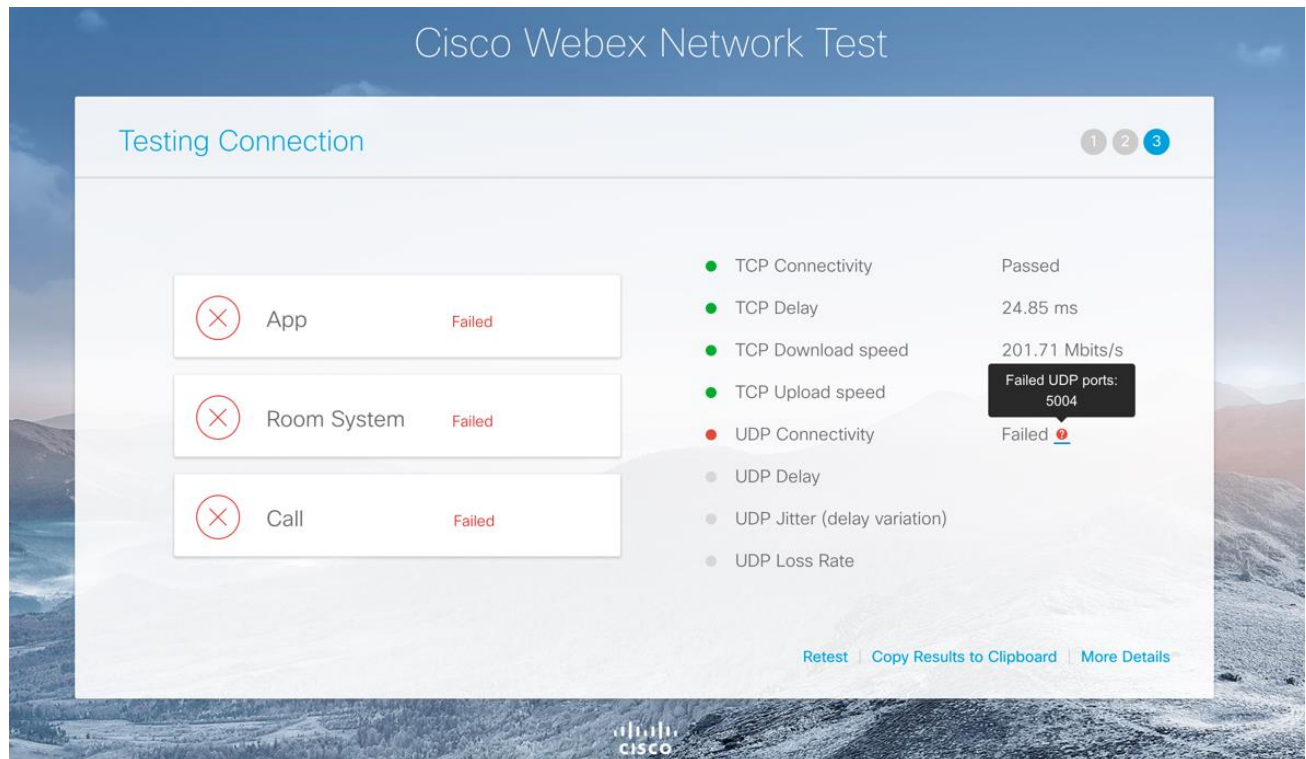
In this case TCP delay is "fair" and starts to be bad after 300 ms (click "More Details" for a legend).

If more than one bullet is yellow but still Webex App, Room System and Call show green, further investigation is required to improve the environment and change some of those parameters to green. One thing to check is whether the laptop is using the best network path. As an example, using a VPN connection can force all real-time traffic to travel via the Internet to the enterprise networks and then back out from the enterprise to the cloud service. Real-time cloud traffic hair-pinning through the enterprise leads to additional delay and potentially jitter and packet loss. To check the impact of VPN tunneling compare the results of media tests with VPN tunnel enabled and disabled. The enterprise administrator can enable split-tunneling for VPN so that traffic from the user machine to certain IP address ranges can egress to the Internet directly without being sent to the enterprise. Split-tunneling is recommended for all real-time cloud application traffic. If

split-tunneling cannot be implemented, then consider turning off your VPN tunnel during real-time collaboration sessions. See the [VPN Considerations](#) sub-section for more information on the impacts of VPNs.

In some cases, the tool suggests corrective actions. The next illustration shows that by hovering the mouse over the question mark the tool reports “Failed UDP ports: 5004”. This might be due to a firewall blocking UDP port 5004, and thus preventing communications when using Webex App (formerly Webex Teams). When UDP port 5004 is not functioning, the application will use TCP port 5004. Using TCP for real-time media adds additional delay and jitter compared to UDP. UDP is the preferred transport layer option for real-time media.

Figure 6. Cisco Webex Network Test: Failed



In terms of bandwidth, real-time traffic is more demanding than other technologies such as pure HTTP. Web technologies usually require less upload bandwidth, and more download bandwidth because the application in the cloud delivers content to the end user in response to requests sent from the application. Real-time voice and video instead create bidirectional data streams which for same bidirectional quality media have symmetric upload and download bandwidth requirements.

Video traffic requires more bandwidth than audio or content sharing. However, video traffic is self-adapting and able to down-speed if network conditions are suboptimal. In situations of constrained bandwidth or even asymmetric bandwidth in cases such as ADSL Internet access video traffic still adapts to the available bandwidth and can even use less upstream than downstream bandwidth.

It is worth noting that the available Internet connection bandwidth depends on many factors, and that the measured value might change over time. As an example, even if the measured upload bandwidth at one time is 20 Mbps, it might drop to 10 Mbps at other times. This still is more than sufficient for video transmission. A video client or endpoint, using an average of 1.5 - 2.5 Mbps or even more, would not detect this change, unless the Internet link is congested because some other users in the same network are uploading content at a high rate.

Having less than 2 Mbps upload or less than 5 Mbps download is problematic for video-based, real-time applications. In this case it's recommended to make sure that no other video conference is running at the same time, and that other video applications running at the same time such as entertainment applications do not interfere with the collaboration session.

In some cases, fluctuations in bandwidth occur because of other traffic on the home network or usage at the Internet Service Provider (ISP). For example, when a 2 Mbps upload bandwidth is reduced to 600 kbps. The endpoint down-speed algorithm will take some time to adapt to this bandwidth level. However, if the available bandwidth changes again, the adaptation algorithm will try to again adapt to the new condition. Frequent changes can result in video problems and audio gaps, leading to an unintelligible conversation during these spikes and changes.

In these cases, it is recommended to use a hardware video endpoint, as the overall quality improves if a standalone endpoint is used instead of a PC where many applications are running at the same time. See [Platform](#) section for more information on this.

Moreover, a video standalone device can be easily configured by the user to occupy a specific portion of the bandwidth. See [Cisco Webex Desk Devices](#) for more information on managing bandwidth controls for Webex Desk Devices.

In some cases when troubleshooting fluctuations in bandwidth utilization it is beneficial to reboot the home router (CPE) before raising a case with the Internet Service Provider (ISP). If the issue persists, then open a service request with the ISP.

When sufficient ISP bandwidth is shared between many different applications running on the home network, in some cases it is possible to prioritize real-time traffic.

As an example, Cisco Meraki devices allow for traffic prioritization. Traffic shaping and traffic prioritization are features for administrators and expert users, especially when real-time applications need to be prioritized over other non-critical applications running on the same computer. However, a cleaner separation between critical and non-critical applications simplifies the implementation of quality of service. As an example, if collaboration applications are standalone such as in the case of a video device, enabled for collaboration, they could be plugged into specific switch ports. Traffic from these ports then can be easily prioritized on the port level via the Cisco Meraki configuration. If it is difficult to use a cable between video-enabled devices and the switch, using a dedicated Wifi network for video devices can help, as Meraki is able to give priority to specific Wifi networks.

Wifi segmentation based on different Wifi networks is limited because technically the medium used for Wifi transport (air) is shared and all Wifi devices are competing for access at a given time and frequency. Wifi segmentation can still help to improve service quality if different Wifi channels (frequencies) are used for different Wifi networks and devices are assigned to the different Wifi networks according to their real-time application requirements. For example, one Wifi network can be dedicated to devices running any real-time application including video devices while another Wifi network is used by all other devices.

VPN considerations

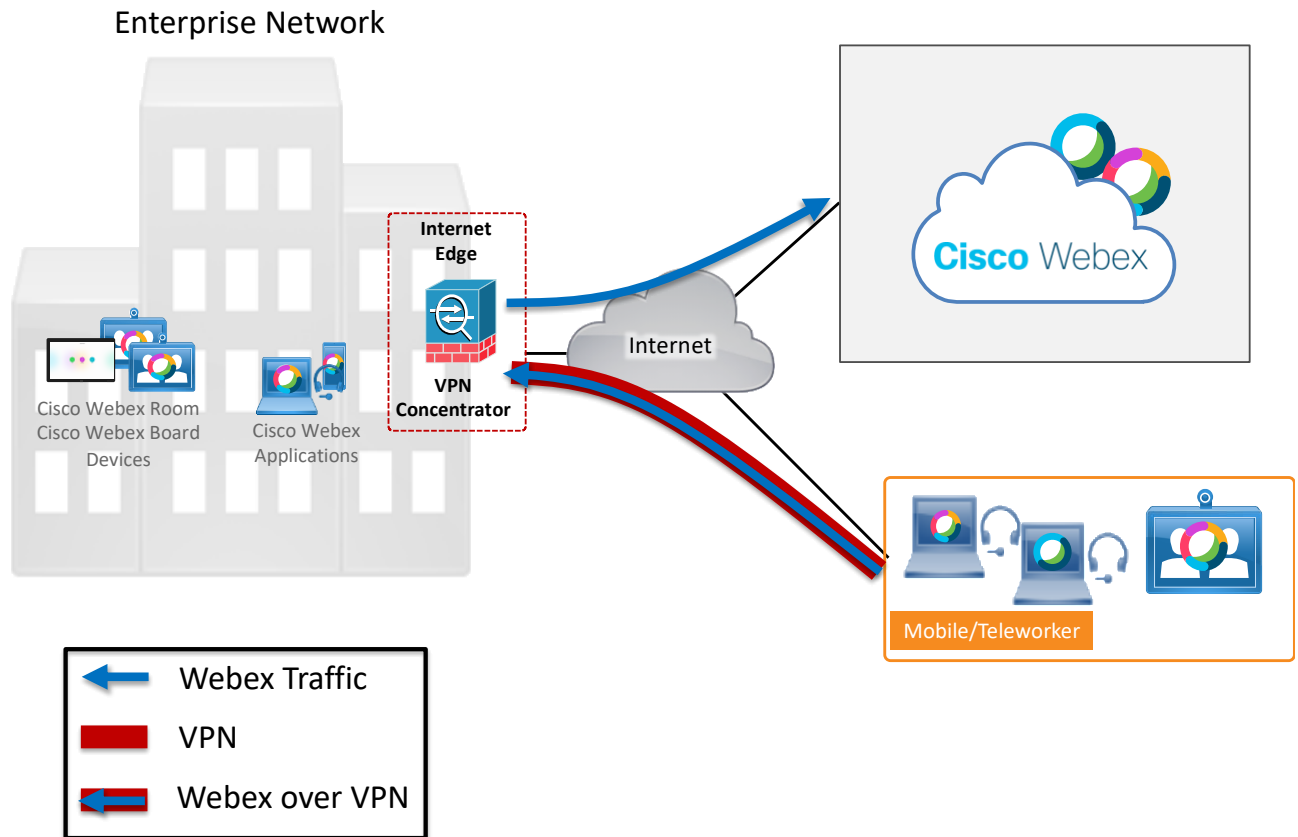
A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. It allows for teleworkers to connect securely to, and access services hosted in the enterprise network. In the past, teleworkers typically were always required to use a full-tunnel VPN in order to perform their work and access resources and services. However, with Cisco Webex and in general with cloud-based services becoming more and more prevalent, the requirements for a VPN are changing. A VPN connection to the enterprise network is typically required when teleworkers need access to enterprise services that are only internally available. Cisco Webex Meetings is a cloud service and direct routes to the Internet are all that is required, but VPN connections may be utilized depending on the enterprise security requirements. While all Cisco Webex Clients, Apps and Devices support VPNs of any type, the information provided here are design recommendations summarized to assist network engineers to promote the most optimized network path and remove possible areas of network delay, overhead and unnecessary load where and when applicable.

There are different approaches to VPN connections, but two classic models are full-tunnel VPN and split-tunnel VPN.

1. **Full-tunnel VPN:** Teleworkers establish a VPN connection during the entire workday and the VPN connection is configured as a full VPN tunnel. With a full VPN tunnel, the network traffic always flows through the enterprise network, even if the traffic destination is Cisco Webex or other cloud-based services. In this case, the network

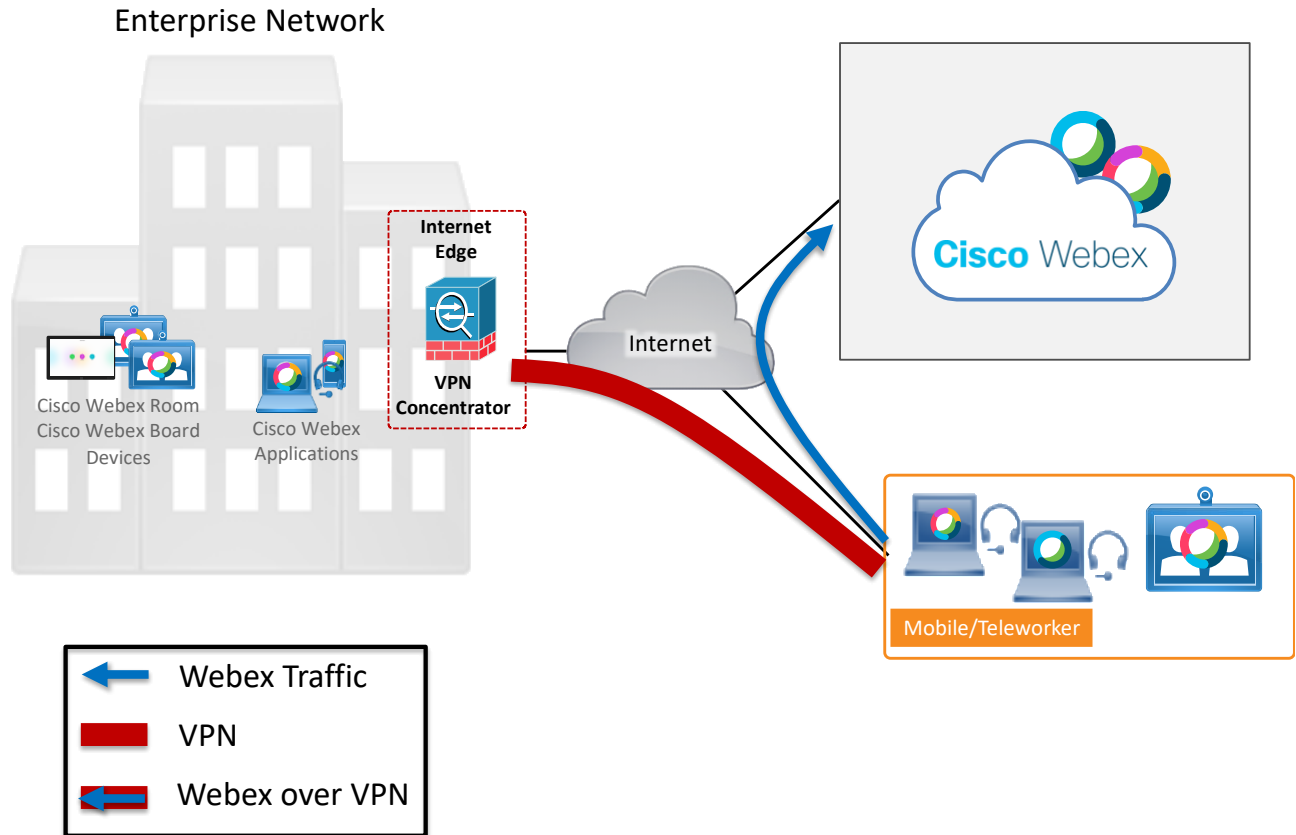
traffic flows to the enterprise network first and then goes to the cloud. The network traffic is hair-pinned at the enterprise network. This is illustrated in [Figure 7](#).

Figure 7. Webex traffic flow with full-tunnel VPN



2. **Split-tunnel VPN:** Teleworkers establish a VPN connection during the entire workday however, the VPN is configured so that the network traffic from the teleworkers' workspace goes to the enterprise network only if accessing on-premises based services. The network traffic to Cisco Webex or other cloud-based services go directly to the cloud, effectively bypassing the enterprise network. This is the recommended VPN configuration when Cisco Webex is deployed as it reduces the delay and potential packet loss that can occur with a longer path to the destination. This is illustrated in [Figure 8](#).

Figure 8. Webex Traffic flow with split-tunnel VPN



Split-tunnel VPN has a number of benefits over full-tunnel VPN by sending Webex meetings destined traffic directly to the Webex cloud rather than hair-pinning that traffic at the enterprise network. Benefits include:

- **Lowers delay and jitter.** Hair-pinning Webex traffic at the enterprise network adds unnecessary delay and delay variation (jitter) to the end-to-end media streams. This amount of the additional delay and jitter could be significant and could significantly impact real-time traffic such as Cisco Webex meetings and video calls and the quality of the voice and video connections could be severely impacted.
- **Decreases security encryption overhead.** Cisco Webex network traffic is already encrypted. Using a full VPN tunnel adds an unnecessary layer of encryption overhead which increases the network bandwidth due to the VPN packet overhead and adds further delay due to the encryption/decryption mechanism. While this delay is minimal it does add up against other delay factors that are unavoidable.
- **Decreases enterprise bandwidth utilization.** With a full-tunnel VPN, all traffic from the Teleworkers' workspace goes to the VPN concentrator in the enterprise network edge equipment, even when the destination is Cisco Webex. This unnecessarily increases enterprise Internet bandwidth consumption by bringing in the Webex destined traffic from the teleworker home to the enterprise Internet edge and then back out. The amount of this unnecessary network traffic could be significant as the number of teleworkers increases and with high bandwidth real-time media such as high-quality video and presentation sharing.
- **Reduce unnecessary load on the enterprise VPN concentrators.** As in the above example with full-tunnel VPN the VPN concentrator is using more resources to encrypt/decrypt this addition Webex traffic (signaling/media/share/files/messages). As mentioned, when the traffic is higher bandwidth real-time media and high-definition video this extra load can be significant and would otherwise be avoided with split-tunnel VPN.

Because of all those benefits, the general recommendation when a VPN is required is to use split-tunnel VPN. In some cases where a split-tunnel VPN is not an option, yet users do require a VPN tunnel for accessing internal enterprise resources such as wikis, internal web pages or on-premise application data from time to time during the workday, the teleworker can disable the VPN during meetings and enable it when access is required. This should be evaluated by the teleworker as in some cases the delay and loss are negligible over the VPN, however this technique offers the teleworker the ability to increase meeting quality if the VPN is causing quality related issues.

It should be noted that some IT organizations may still choose to have teleworkers use a full VPN tunnel for all workloads due to security concerns. The IT organization may want to have all network traffic anchored at the enterprise network and be able to perform traffic inspection or provide additional network security to teleworkers. For example, teleworkers could be victims of phishing attacks and unknowingly download malware onto their desktop or laptop. Home routers usually have only basic security features and cannot prevent this type of scenario while corporate security devices have enterprise-grade advanced security features and could prevent such scenarios.

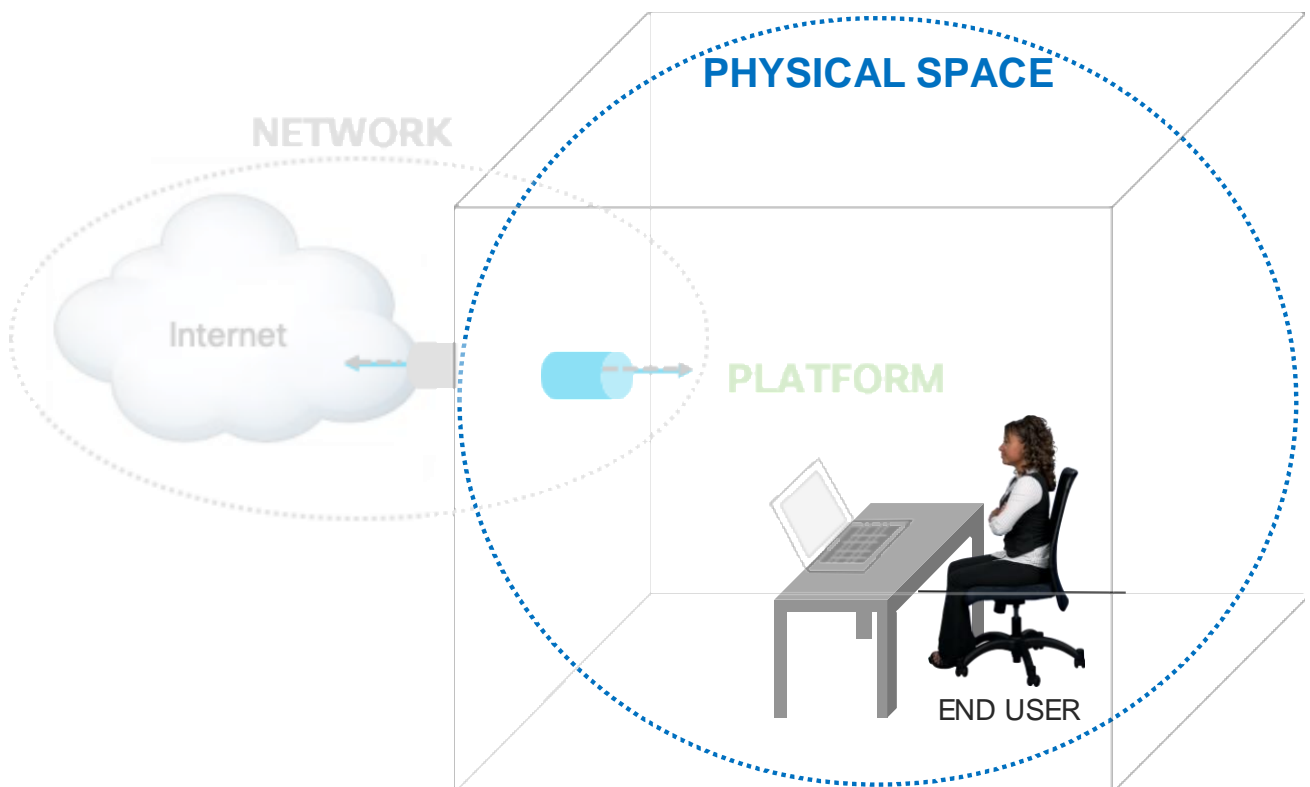
Hardware vs Software VPNs

As mentioned, split-tunnel VPNs are always recommended over full-tunnel VPNs in Cisco Webex designs due to the inherent benefits mentioned above. VPN clients typically come in either software-based versions like Cisco AnyConnect where it runs as software on the Windows PC/Mac or hardware VPNs solutions like Cisco Meraki or Cisco Virtual Office solutions with Cisco Integrated Services Routers (ISR). In the case of a software-based solution where a full-tunnel is configured it is easier for teleworkers to enable/disable the VPN ad-hoc. This is not the case with hardware-based solutions. As such it's even more important for hardware-based solutions to implement split-tunnel to ensure that Webex traffic is not hair-pinned through the enterprise.

Physical Space

The physical space consists of anything involved with the room environment that might affect both audio and video. Things such as size of the space, whether it's private/shared, background activity and noise and lighting.

Figure 9. Physical Space



Room environment:

Audio

- » Avoid larger open rooms and spaces to minimize echo and reverberation. Consider using sound dampening panels or other room sound-related remediation to improve audio quality.
- » Only use built-in or external speakers and microphones if the space is closed and private. Otherwise for shared spaces used by others, a noise cancelling headset is highly recommended.
- » Background noise (children, pets, others working, machinery, traffic, etc.) should be minimized as much as possible given that they distract not only the end user, but also other people communicating with the end user (far-end). In noisy environments, noise cancellation is a requirement if acceptable end user experience is expected.

Video

- » **Lighting:** Good front lighting is important so that you can be clearly seen, and the camera and software doesn't have to work harder to compensate for poor lighting with automatic light adjustments. Some cameras are great at this light adjustment, however most are not. When windows and light sources are behind a participant this backlighting can darken and shadow the subject's face creating poorer image quality for the viewing participants. You should always avoid back lighting and ensure that light sources are not in the video capture. So light sources from the side and behind the video camera are best.
- » **Background:** Background movement can cause distraction to the viewers but can also cause the video content to be more bursty and use more bandwidth and resources (CPU/memory). The less movement in the screen, typically equates to less bandwidth utilization. So, avoid busy and distracting backgrounds. Simple is best!
- **Virtual Backgrounds:** If you are a fan of the virtual backgrounds, blank walls are great. This is because it's much easier for the software to pick out the speaker when there is a simple distinction between the subject and the backdrop.
- **Ergonomics** A correct placement of the laptop or workstation is important to mitigate the Hunched over Laptop Syndrome (HOLS) or the Computer Vision Syndrome (CVS). The correct positioning should not require the user to bend over the laptop or to be relatively close to the monitor. If the daily job requires extensive use of collaboration and video sessions, it is recommended to use a dedicated device. Designed to be ergonomic, it helps mitigating both HOLs and CVS.

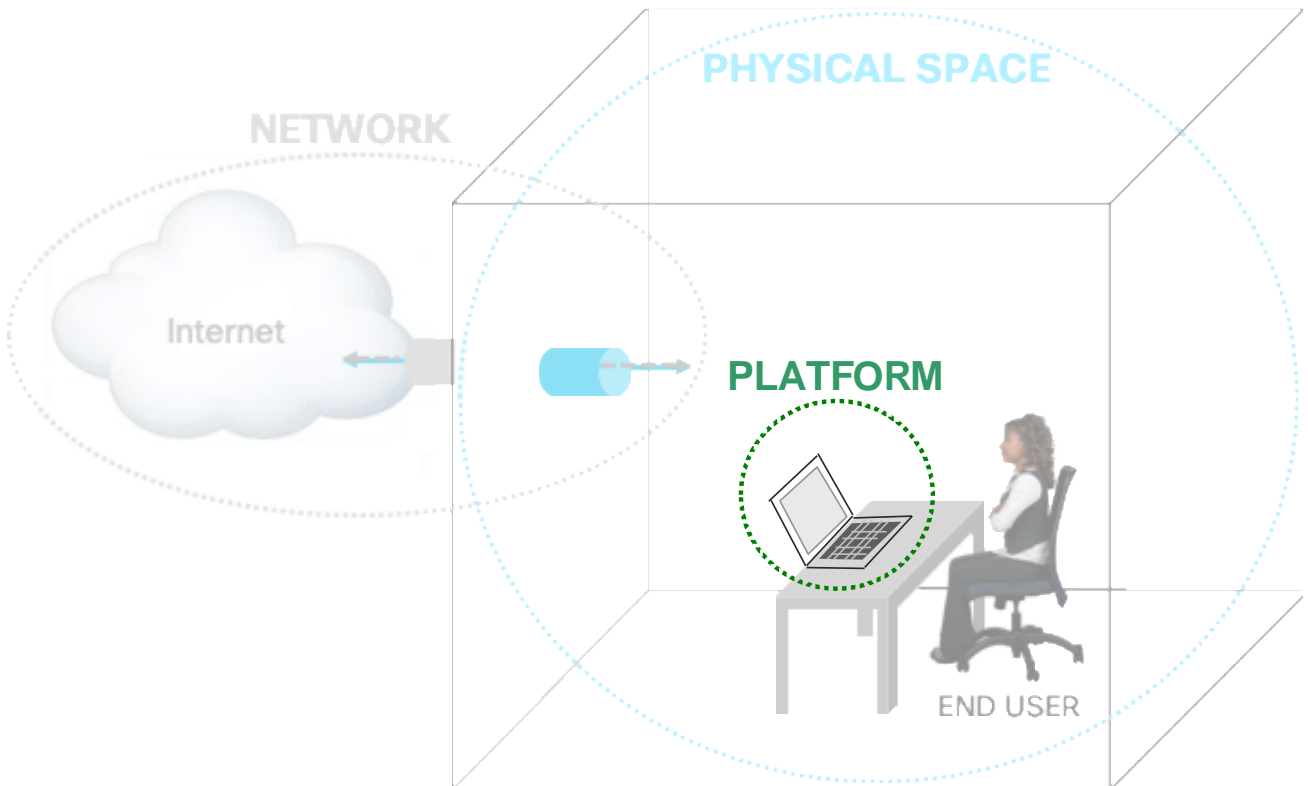
Audio and Video Input and Output

- » Ensure the laptop's built-in speakers and microphone are high quality or consider external speakers and high-fidelity microphone (USB or 3.5mm).
- » Optionally, use a good quality headset with high-fidelity microphone. Headset with noise canceling functionality is recommended.
 - » Some headsets come with a Bluetooth adapter (aka "dongle") and can add better Bluetooth capabilities for the headsets than the PC's built-in Bluetooth. Consider this as superior headset performance will be enjoyed if headset's Bluetooth adapter is used.
- » Ensure the laptop's built-in web camera is high quality or consider a high-definition external video camera (USB).
- » Refer to the [Headsets and Video Cameras](#) sub-section later in this document for more information about headsets and video cameras.

Platform

The platform consists of the Windows PC or Mac hardware and software components such as the Operating System (OS), CPU, memory, Software running, hardware such as speaker, microphone and video camera.

Figure 10. Platform



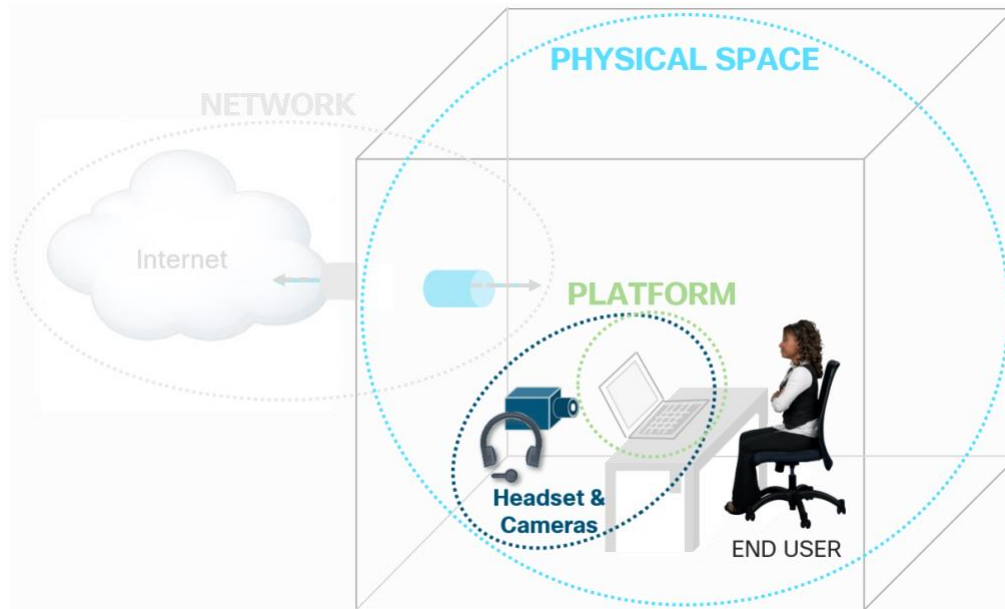
- **Operating System (Windows Mac, Linux, iOS, Android?):**
 - » Generally, the latest platform operating system (OS) is recommended.
 - » Apply all required and recommended OS updates – particularly those that may impact system sound and video camera as well as overall system performance.
- **Platform processor/CPU and memory:**
 - » Keep in mind that each active software application adds load to the system CPU and memory. Failure to deploy a system with ample CPU and memory will result in poor performance overall (e.g. delayed or slow system response, application, or system crashes). In the case of real-time audio functionality, poor voice quality including choppy, clipped, or even no audio at all.
 - » Ensure platform meets all minimum CPU requirements for any software running on the system. Generally, the more speed and CPU cores a system has, the better it will perform, particularly with processor intensive applications like those capable of sending and receiving audio in real time.
 - » Ensure platform meets all minimum memory requirements for any software running on the system. Generally, the more memory the system has the better it will perform, particularly if the system is running many applications at once.
- **Software and hardware:**
 - » Generally, the latest versions of all co-resident software and applications are recommended. This includes all required and recommended application specific updates – particularly collaboration applications which typically impact system sound as well as overall system performance.
 - » Built-in speakers and microphone should be in functioning order and of reasonable quality with all applicable hardware/software drivers up to date.

Headsets and Video Cameras

In most circumstances the use of a quality headset and a high-definition video or web camera are recommended when conducting real-time collaboration activities.

As shown in [Figure 11](#), headsets and video cameras span both the physical and platform layers of the audio-visual environment given that they are connected to the platform and address potential shortcomings in the physical environment.

Figure 11. Audio and Video Quality: Headset and Cameras in the Audio-Visual Environment



Headsets

In cases where the work area is private and closed with favorable acoustics (e.g., no echo or reverberation), a headset may not be needed, but even in those cases a headset may still provide improved audio quality especially when factoring in headset features like noise cancelation and mute notification.

Using a headset provides a number of improvements over built-in or external speakers and microphones including generally providing a more ergonomic benefit for the end user (e.g., freedom of movement). From an audio quality perspective, the two main improvements over built-in or external speakers and microphones are speaker-microphone separation reducing feedback and interference in the audio path as well as the directional nature of headset microphones ensuring the users voice is clearly captured.

Generally, headsets connect to the user's computer either directly (wired) or wirelessly. In the case of wired or direct connect headsets, most connect using USB or 3.5mm jack. In the case of wireless headsets, most connect over Bluetooth or DECT.

Note: Bluetooth wireless communication occurs on the 2.4 GHz wireless band. Some WiFi networks also communicate on the 2.4 GHz band (802.11b, 802.11g, 802.11n) and as such Bluetooth communications may impact 2.4 GHz wireless networks by causing interference. This interference which can lead to network throughput degradation can be avoided by moving wireless network traffic to the 5 GHz wireless band (802.11a, 802.11n, 802.11ac, and 802.11ax). If 2.4 GHz wireless networks cannot be avoided, consider connecting the headset directly rather than wirelessly to avoid the potential for Bluetooth interference.

Note: Bluetooth wireless devices can also interfere with other Bluetooth devices causing degraded performance for one or both devices. To avoid potential Bluetooth connection issues, refrain from using Bluetooth connected headsets in environments where other Bluetooth devices are in close proximity. If multiple Bluetooth devices will be nearby, consider connecting the headset directly to the computer using USB or 3.5mm.

Cisco offers several headset options for WFH users. Not only do these Cisco headsets provide high quality audio input and output as well as advanced audio quality features, the headsets may be centrally managed by the enterprise calling administrator ensuring WFH users have the latest headset firmware and optimized audio configuration.

- Cisco 500 Series Headsets:
 - » **Cisco Headset 521 / 522** – Features one or two ear cups and unidirectional boom microphone. This headset connects to the computer directly using 3.5mm or USB with an inline 3.5mm to USB adaptor connector.
 - » **Cisco Headset 531 / 532** – Features one or two ear cups and unidirectional boom microphone. These headsets have a quick disconnect cable which supports both a USB adaptor for connecting to computers and a RJ9 adaptor for connecting to IP phones.
 - » **Cisco Headset 561 / 562 with base station** – Features one or two ear cups and unidirectional boom microphone. These headsets connect via DECT to the base station. Base stations can be connected to computers via USB or Bluetooth.

For more information about Cisco 500 Series Headsets, refer to the product information available at <https://www.cisco.com/c/en/us/products/collaboration-endpoints/headset-500-series/index.html>

- Cisco 700 Series Headsets:
 - » Cisco Headset 730 – Features two over the ear cups with boom-less microphone. These headsets feature voice-honing, boom less Clear Voice technology coupled with adaptive noise cancellation and background noise reduction to provide crystal clear audio. These headsets connect to computers either wirelessly (Bluetooth) or directly (USB or 3.5mm).

For more information about Cisco 700 Series Headsets, refer to the product information available at <https://www.cisco.com/c/en/us/products/collaboration-endpoints/headset-700-series/index.html>

Cameras

In cases where video quality is paramount to collaboration or where the computer's built-in web camera does not provide acceptable quality an external USB video or web camera is recommended. High-definition USB cameras will generally provide larger field-of-view (FoV), improved focus distance and light compensation as well as overall better optical lenses than a computer's built-in camera. These capabilities can compensate at least in part for physical environment limitations mentioned previously like lighting and background, however, attention to lighting in the physical space as well as the framed background is still important. Some USB cameras also provide built-in microphones and in some case speakers to provide improved audio input and output. In some cases, external USB cameras are able to offload image processing from the computer to the built-in chipset of the camera potentially improving system performance and in turn the overall real-time collaboration experience.

Cisco offers the Cisco Webex Room USB camera option for WFH users. This USB passthrough camera enables 4K ultra high-definition video to computer-based collaboration. The camera not only delivers a 120° horizontal field of view, 1 meter to infinity focus range, and automatic brightness and white balance control, it also delivers high quality audio input and output from its built-in microphone array and speakers which have automatic gain control and built-in noise reduction.

For more information about the Cisco Webex Room USB, refer to the product information available at <https://www.cisco.com/c/en/us/products/collaboration-endpoints/webex-room-usb/index.html>.

Webex Clients and Devices

Media Resilience and Rate Adaptation

Webex apps leverage various media resilience and rate adaptation techniques. The Webex apps do adapt and will predict the network path capabilities on a real-time basis and freely adjust their strategies around available bandwidth to the client to keep the meeting experience in the best possible condition. The Webex Meetings, Webex App (formerly Webex Teams) and Webex Devices will adjust quality/resolution/framerate in a tradeoff as network conditions change.

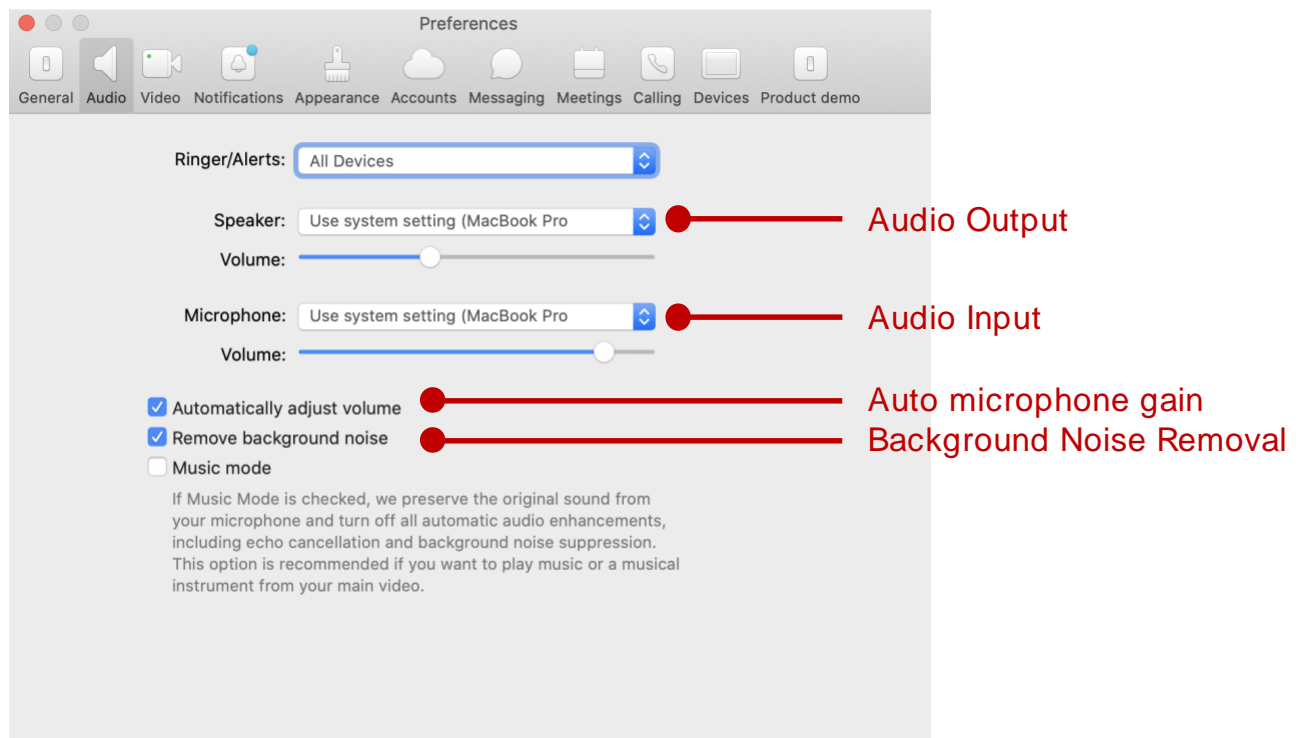
The next sections are recommendations and considerations specific to Webex apps and Devices.

Webex (formerly Webex Teams)

The Webex client application provides audio and video device selection under settings. The user can navigate to the application settings by clicking their profile picture (upper left-hand corner) and then selecting Preferences to load the options window.

The audio settings for the application are available on the Audio tab (Figure 12). The user can select the audio input and output device to use on a call or meeting. The user can also adjust the input and output volume levels for the client application.

Figure 12. Webex Client Audio Settings



Automatically adjust volume provides automatic gain control on the microphone (audio input) as the user speaks. If the user is speaking too loudly the volume is automatically adjusted down and vice versa if the user is speaking too low. This setting is on by default. Depending on the environment, the volume of the speakers and the quality of the microphone, this setting may cause a user's speaking volume to be lowered or raised making it harder for other participants to hear the speaker. If this happens consider disabling this setting when experiencing audio issues where your audio is too low or high for other attendees on calls and meetings.

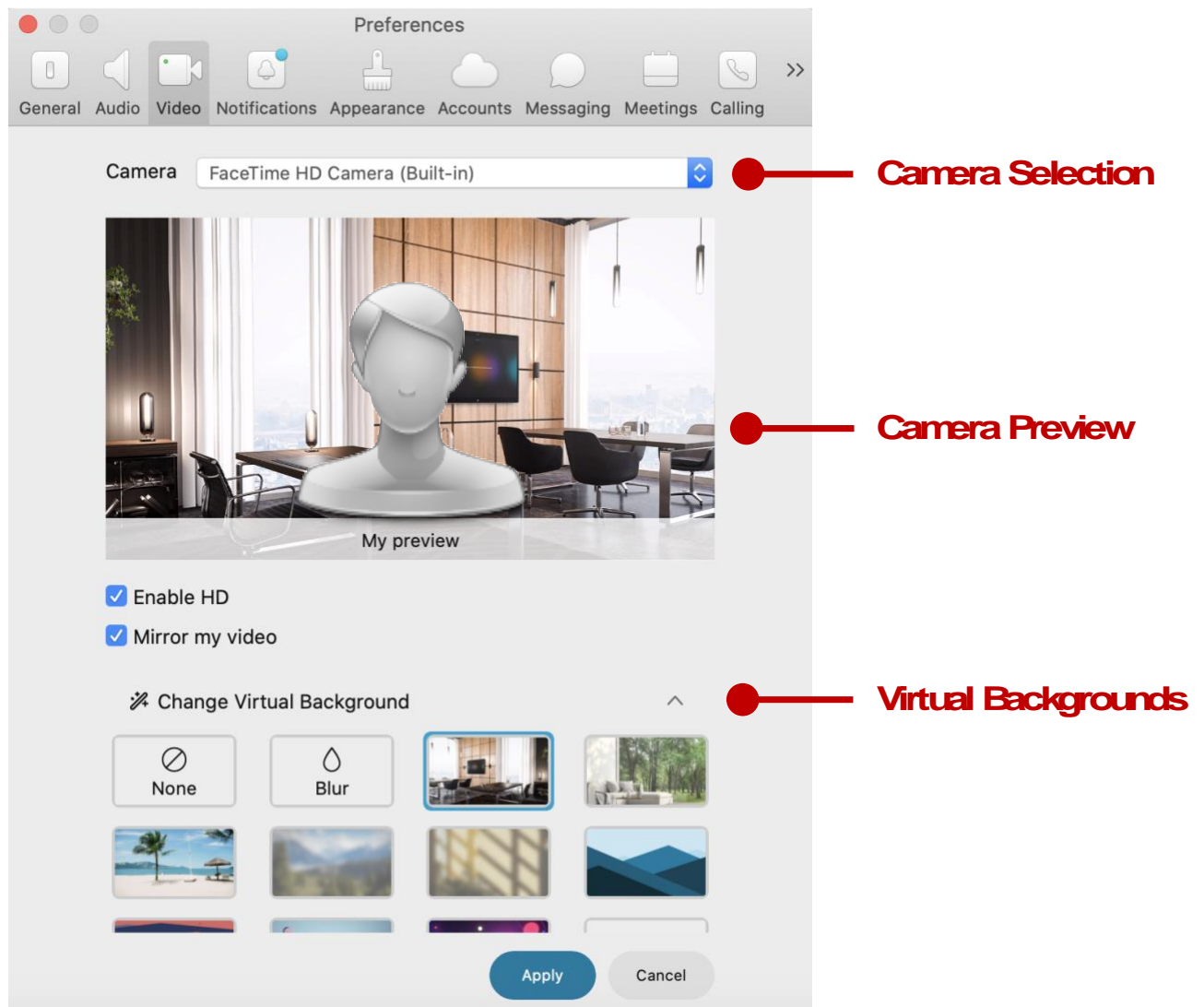
This setting can be affected by the speaker volume, that is when the output of the speakers is picked up by the microphone. This can cause the microphone auto adjustment to go too low for the user to be heard. In which case finding the right setting becomes very important, whether this is by adjusting the volume of the speakers or by disabling the auto adjustment and finding the right microphone volume. Some testing may be required with other meeting participants feedback in order to get this right in some cases. A clear sign this setting is not working for you is when participants tell you that you are speaking to low. That's a good indication that you need to adjust your settings. These issues can also be solved by using a good headset. See [Headsets and Video Cameras](#) for more information on benefits of headsets.

Remove background noise is a useful feature when there is expected background noises such as children, pets, others working, machinery, traffic, etc. This setting is on by default. If using a headset with built-in noise cancellation, you may consider disabling this feature as it will save on CPU resources used by the application.

Video settings for the application are available on the Video tab as shown in [Figure 13](#). Here the user can perform several tasks including:

- **Select the video camera device.** In cases where more than one camera is available on the system, the user can choose the desired camera for use on a call or meeting.
- **Preview the video camera picture.** This is an easy way for the user to check the video framing, background quality, and lighting of the environment and make adjustments as needed to improve the overall video quality prior to joining a call or meeting.
- **Configure virtual backgrounds.** In cases where the aesthetic of the physical space is not ideal or cannot be easily improved, the user can digitally blur the background of their video feed or apply a virtual background or to improve the overall appearance in a call or meeting.

Figure 13. Webex Client Video Settings



Webex Meetings is now integrated into the Webex application and can be administratively enabled to be utilized for Webex Meetings. In this case audio and video settings are synchronized between the two applications.

Webex Meetings Desktop App

Webex Meetings is now integrated into the Webex application. It is still possible to download Webex Meetings App to run separately and if you do so then these instructions apply to Webex Meetings Desktop App installed separately.

[Webex Meetings Desktop App Bandwidth Controls](#)

[User Audio and Video Test Meeting Functionality](#)

Webex Meetings Desktop App Bandwidth Controls

Webex administrators have controls to help manage video resolution and thus bandwidth used by clients that connect to Webex meetings should they choose to. Namely, you can cap the meeting layouts to 180p, 360p or 720p as the max available resolution. Whether your site is administered on Webex Control Hub or Webex Site Administrator, the following controls are available in Configuration > Common Site Settings > Options:

Figure 14. Webex Meetings Desktop App Bandwidth Controls

- Turn on high-quality video (360p) (Meetings, Training, Events and Support)
- Turn on high-definition video (720p) (Meetings, Training and Events)

Enable 180p video resolution – Nothing selected

Enable 360p video resolution – Select **Turn on high-quality video (360p)**

Enable 720p video resolution – Select both **Turn on high-quality video (360p)** and **Turn on high-definition video (720p)**

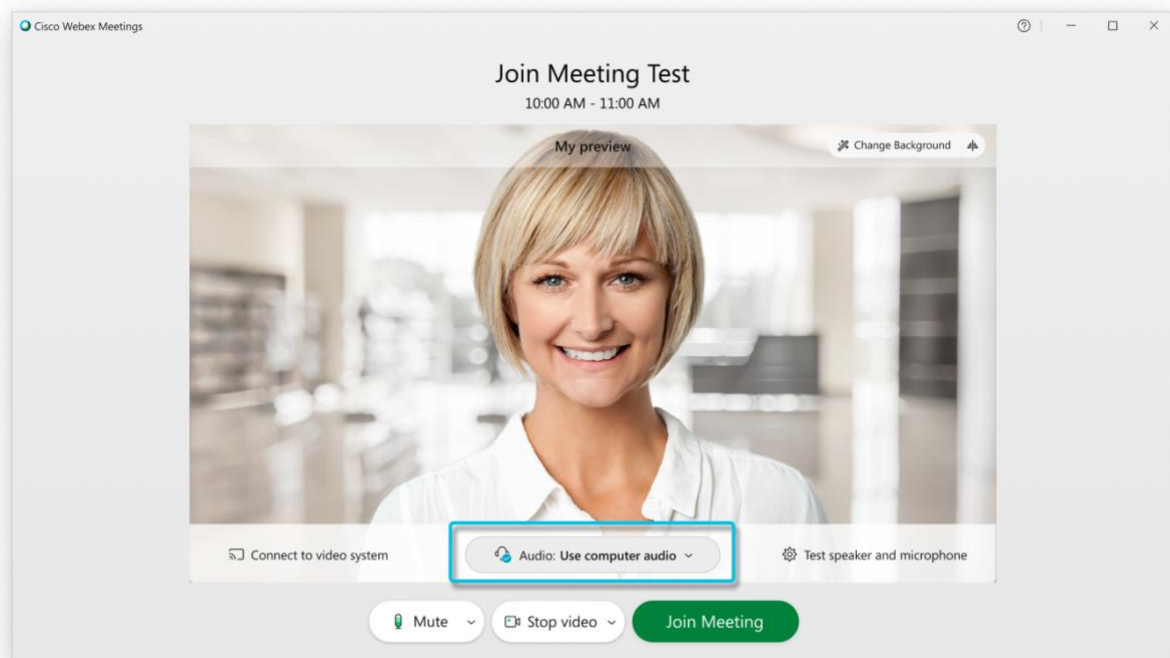
Note: These controls are also available at the user level settings

User Audio and Video Test Meeting Functionality

One way to evaluate your audio and video capabilities prior to a meeting is to join a test meeting and evaluate your speaker, microphone and video camera and video settings.

1. Go to <https://www.webex.com/test-meeting.html>.
2. Enter your name and email address, and then click Join.
3. If you don't already have the Cisco Webex Meetings app installed, you'll be prompted to click the installer file. On Windows, click Webex.exe. On Mac, click Webex.pkg.

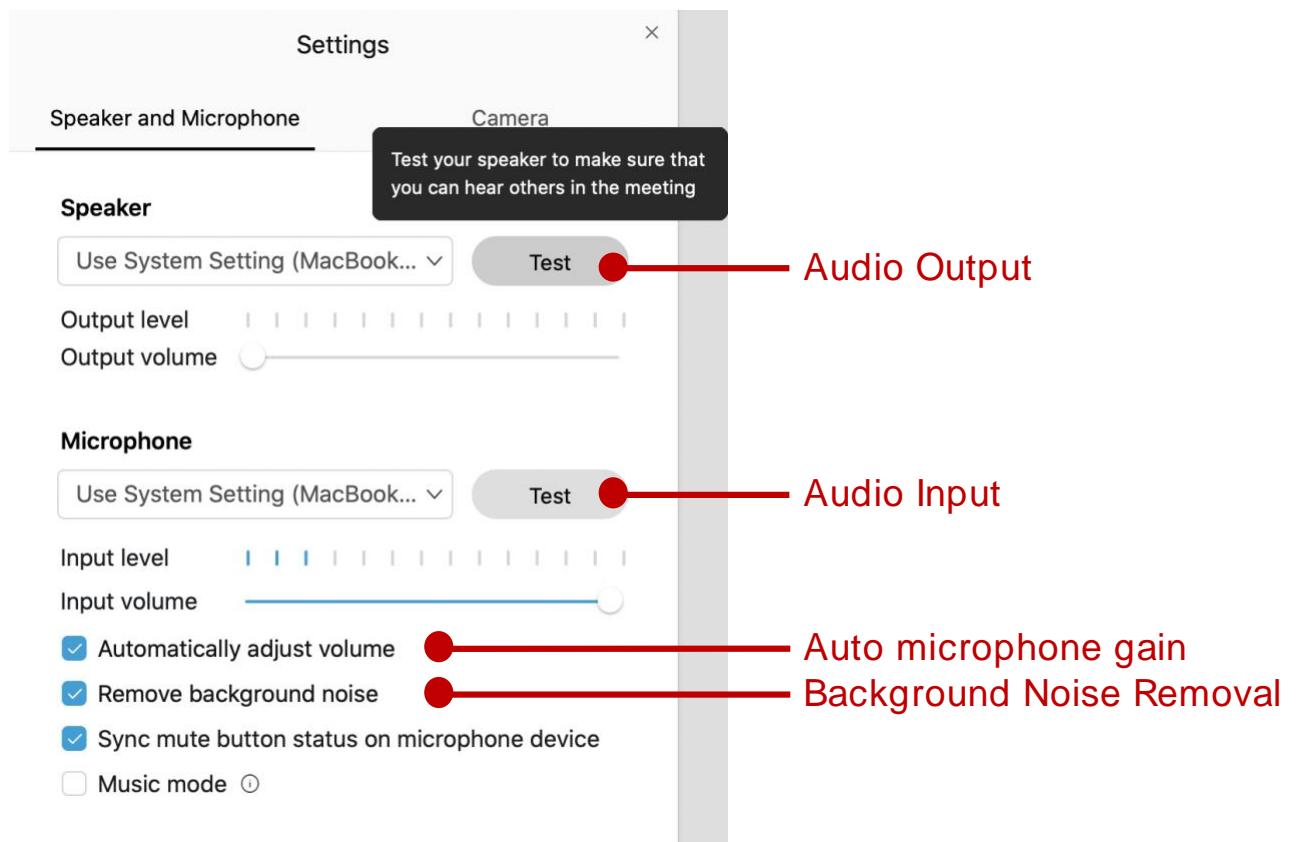
Figure 15. Cisco Webex Meeting App: Join Meeting Test




4. Check video settings

- a. Check to see if you see your self-view in the application ([Figure 15](#)). If you do not see your video, select the down arrow next to **Stop video** to select the camera and ensure that the camera is selected, is available for use and that video is not disabled or hidden by a camera cover/slider.
- b. Once the self-view is visible you can evaluate your surroundings, lighting, evaluate what is visible in your background or optionally select to change your background to a [virtual background setting](#) ([Figure 13](#)).
 - i. Click **Change Background** and then do one of the following:
 - ii. To blur your surroundings while remaining in focus, click Blur.
 - iii. To use a default virtual background, click the one you want.
 - iv. To use your own image for the virtual background, tap the + icon.
5. Next, select **Test Speaker and Microphone**
6. Test your speaker and microphone to make sure that you can hear everyone, and everyone can hear you, when using your computer for audio.
 - a. In the Speaker menu, click **Test** ([Figure 16](#)).
 - b. If you don't hear anything, try changing the speaker device in the drop-down list, or adjusting the Output volume slider.

Figure 16. Speaker Menu



- c. In the Microphone menu, click **Test**, and then speak into your microphone ([Figure 16](#)).
- d. After a moment, a recording of your test will automatically play back to you.

- 
- e. If you don't hear the audio play back, try selecting a different microphone from the drop-down list, or adjusting the Input volume slider.
7. Remove background noise is selected by default. This is a useful feature when there is expected background noises such as children, pets, others working, machinery, traffic, etc....
 8. Next, choose how you want to connect your audio to the meeting.
 - a. **Use computer for audio**(default): Use your computer with a headset or speakers.
 - b. **Call in:** If you prefer to use your phone for audio, dial in when the meeting starts. A list of the global call-in numbers is available after you join the meeting. Choose this option if your Internet connection is slow or low bandwidth.
 - c. **Don't connect audio:** Use this option when you need to join a meeting and share content, and don't need audio. For example, you're in a conference room with your team, or someone already connected to the meeting from a video device.

The settings are saved by default and the next time you join a meeting these settings will be used. To change this behavior, you can go to the **Meeting join options** in **Preferences** and change from **Use my last audio and video settings** to **Always use the following audio and video settings**. You'll find similar speaker, microphone and camera settings that were indicated above. This will allow you to run the same speaker, microphone and video camera tests above without joining a test meeting. See this article for more information: [Set your Meeting Join Preferences in the Cisco Webex Meetings Desktop App and Mobile App](#).

Cisco Webex Desk Devices

Being able to join a meeting and placing video calls with just an app that is installed on a desktop, laptop, or mobile device is very convenient and cost effective. There is no need to purchase additional hardware and the Cisco collaboration applications, Webex (formerly Webex Teams) and Webex Meetings clients, can simply be downloaded from the Cisco web site and are free of charge. However, the quality of the video and the meeting experience can be sub-optimal when using an application:

- The camera, microphone, and speakers that are built-in into laptops or mobile devices are often low-quality. If purchasing these accessories separately, quality could be better but still be suboptimal.
- The laptop or mobile device could be running other programs or running an anti-malware scan during a meeting and there could be high CPU or memory usage which could severely affect the real-time audio and video streams in the meeting,
- The laptop could be still powered off in the morning, could be rebooting due to an upgrade, or simply have an issue such as a driver not working after a upgrade or a virus/malware, and teleworkers could be unable to join their meeting for some time and run late for their meeting.

A dedicated collaboration endpoint eliminates those issues. And beyond that, it can offer a premium meeting experience. For example, the Cisco Webex Desk Pro is an all-in-one premium collaboration and productivity device featuring a 27-inch 4k display, 71-degree HD camera, superior sound system, advanced noise-canceling microphone array, and much more.

The Cisco Webex Desk Pro also offers smooth integration with the Cisco Webex and Cisco Webex Meetings applications for example through Proximity where the end user can for example place calls and control their Webex Desk Pro via their app or can wirelessly share their screen from their laptop or mobile device.

Another benefit of a video device is the overall ergonomics. A video device can be positioned sufficiently far from the user, thus mitigating the Computer Vision Syndrome, and the camera is high enough to reduce the Hunched over Laptop Syndrome (HOLS).

Webex Devices Bandwidth Recommendations and Considerations

Webex Devices offer the ability to set a maximum and transmit and receive bit rate. It is more appropriate to categorize these types of endpoints based on their maximum bit-rate support. At the time of this writing there are 2 categories of these devices, those which support up to 3 Mbps bit rate and those which support up to 6 Mbps. There are also devices which have dual screens and thus have a different level of bandwidth consumption in aggregate. Examples include:

3 mbps Bit-rate Support

- SX10
- DX Series

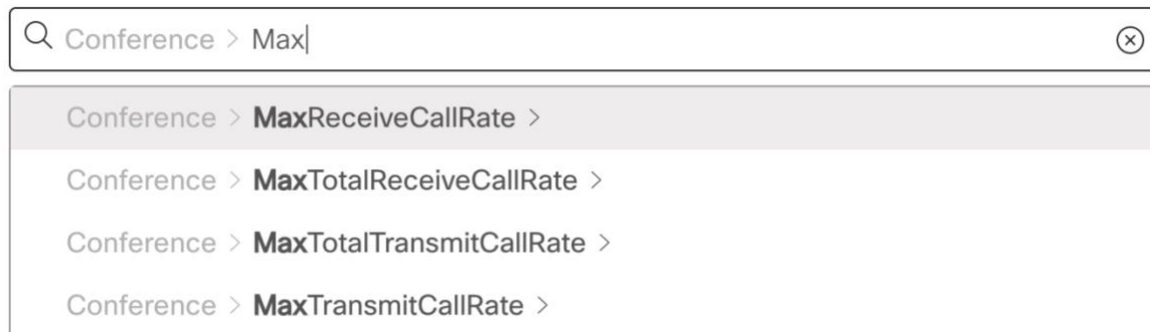
6 mbps Bit-rate Support

- Cisco Webex Desk Pro
- All Webex Room Series
- SX20, SX80, MX Series

Control Hub Device Level Bandwidth Controls

Control Hub (admin.webex.com) offers the ability to set a minimum and/or maximum transmit and/or receive bit rate for calls for Webex Devices in Webex Meetings. This allows the administrator to reduce the transmit or receive bit rate for specific devices if they are deployed in bandwidth constrained environments. [Figure 17](#) illustrates the Control Hub bit rate settings for Webex Devices. See this document for more information on accessing [Advanced Configurations for Room and Desk Devices and Webex Boards](#).

Figure 17. Control Hub bit rate controls for Webex Devices



The following are definitions for each bit rate setting:

MaxReceiveCallRate: Define the maximum receive bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call and is inclusive of all media bit rate: audio, video and presentation sharing.

MaxTransmitCallRate: Define the maximum transmit bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call and is inclusive of all media bit rate: audio, video and presentation sharing.

These settings apply to a video system's built-in MultiSite feature (optional), which is not applicable to Webex Meetings and can be disregarded for the purposes of this document:

MaxTotalTransmitCallRate

MaxTotalReceiveCallRate

One example of where it might be applicable to modify the bit rate settings is in environments where the transmit bandwidth is much lower than the receive bandwidth, such as home environments with limited upload speeds. These environments are prime candidates for this type of bandwidth control as the administrator can set the MaxTransmitCallRate to be lower than the device capability while leaving the MaxReceiveCallRate to the default or the maximum bit rate that the device can receive. So, as an example a Cisco Webex DX 80 can support up to 3 mbps of transmit or receive. If the site where the device is located only has a maximum of 2 mbps upload speed, then it might make sense to reduce the transmit for this device to something like 1.5 mbps so that during a meeting it doesn't attempt to transmit more leaving 500 kbps for other traffic during the meeting. [Figure 18](#) shows an example of this configuration in Control Hub.

Figure 18. Example: Changing MaxTransmitCallRate for a Device

Conference > MaxTransmitCallRate : 1500

64 1500 3072

Follow default value (3072)
Sets the configuration to always follow the default value, even if this changes in the future.

Cancel Save



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)