
Yealink VCS Network Deployment Solution

Oct. 2015

V10.6

Table of Contents

Table of Contents.....	iii
Network Requirements	1
Bandwidth Requirements	1
Calculating the Bandwidth of Head Office	1
Calculating the Bandwidth of Branch Office	2
Bandwidth Testing.....	2
IP Address Requirement for the Head Office	3
VCS Setup Scenarios.....	5
Scenario 1: Private IP Deployment (Behind Firewall with Port Forwarding)	5
Scenario 2: Public IP Deployment (Outside of Firewall).....	6
Scenario 3: Intelligent Traversal	6
VCS Network Deployment	7
VCS Network Settings.....	7
Related Port Usage for Firewall Setup.....	8
QoS Guarantees	8
Connectivity Testing.....	9
VCS Network Connectivity Testing	9
Troubleshooting	11
Branch Office Fails to Connect to Head Office	11
Abnormal Conditions during a Call	12

Network Requirements

Bandwidth Requirements

Video conferencing system (VCS) is a real-time network application. It has high network bandwidth requirements. To ensure the best performance, the recommended bandwidths are shown as below.

Recommended bandwidths for the Yealink video conferencing system:

Resolution	Recommended Bandwidth
Full HD 1080P (1920x1080)	1.3Mb
Full HD + Content: (people+ content)	2.6Mb
HD 720P (1280x720)	665Kb
HD + Content: (people + content)	1.4Mb
SD 448P (768x448)	333Kb
SD + Content (people + content)	666Kb

Other network requirements of the Yealink video conferencing system:

Delay	The delay should be less than 200ms
Jitter	The jitter should be less than 50ms
Packet lost	The packet loss should be less than 1%

Calculating the Bandwidth of Head Office

The bandwidth requirement of the head office is related to the numbers of branch offices.

The calculation formula is as follows:

Bandwidth of the head office = N (the number of branch offices) x bandwidth of a branch office

For example:

The head office is conducting a video conference with three branch offices, to achieve the full HD effect, the bandwidth of head office should be = 1.3Mbps x 3= 3.9 Mbps. If the head office needs to share content (e.g., video or PPT) during this video conference, the bandwidths will be doubled, so the bandwidth of head office will be = 1.3Mbps x 2 x 3 =7.8Mbps.

Calculating the Bandwidth of Branch Office

For example:

If the branch office is during a video conference, to achieve the full HD effect, the bandwidth of the branch office should be 1.3Mbps. If the branch office needs to share content (e.g., video or PPT) during the video conference, the bandwidths will be doubled, so the bandwidth of the branch office will be $= 1.3\text{Mbps} \times 2 = 2.6\text{Mbps}$.

Note

An independent optical fiber is recommended for the VCS.

Do not share the Internet connection with other devices. If this cannot be avoided, you are advised to take Quality of Service (QoS) measures to control the network traffic.

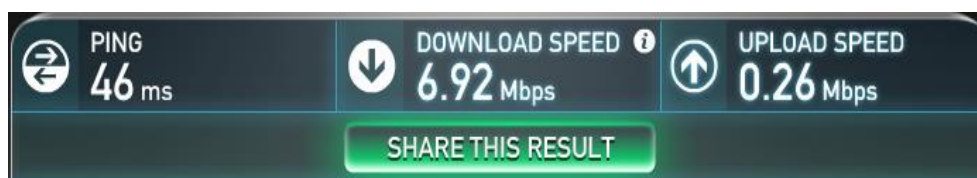
Bandwidth Testing

Once you know VCS bandwidth requirements, carry out the following steps to test whether your current bandwidth meets demand.

1. Enter <http://www.speedtest.net/> in the address bar of a web browser on your PC, and then press the **Enter** key.
2. Click **Begin Test** button.



3. Test result:



- **PING:** the ideal PING value should be less than 100ms. The lower the value, the lower the network latency.
- **DOWNLOAD SPEED:** Downlink bandwidth.
- **UPLOAD SPEED:** Uplink bandwidth.
- The ideal uplink and downlink bandwidths are 1.5Mb. We recommend that your uplink and downlink bandwidths should be 1.3Mb.
Downlink and uplink bandwidths may be asymmetric, so ensure the uplink bandwidth meets the demand during this test.

According to the test result, if your network cannot meet demand, please deploy the VCS after upgrading your network. Otherwise, your video conferences will not achieve good effects.

IP Address Requirement for the Head Office

At least one static public IP address is required in the head office to allow branch offices to connect.

VCS Setup Scenarios

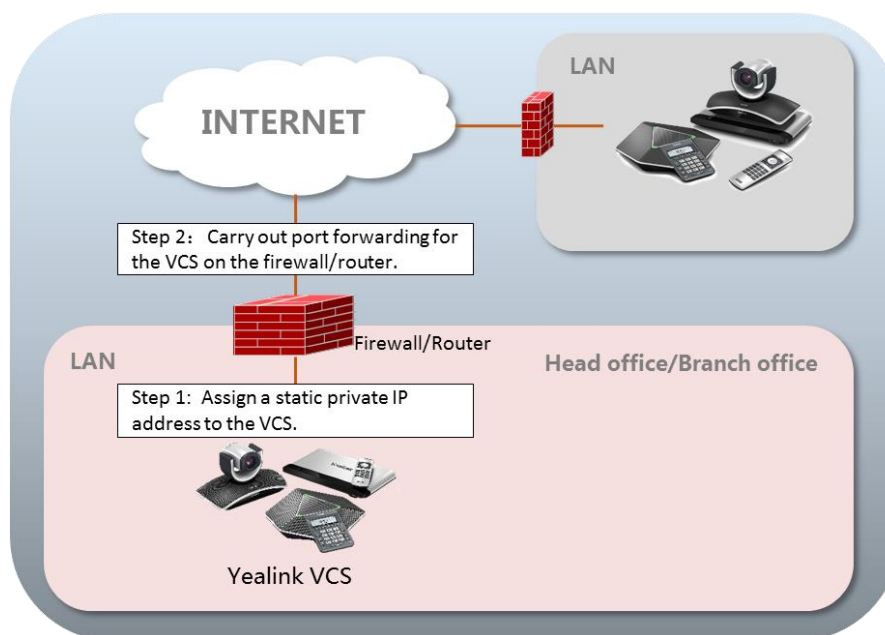
There are three general VCS setup scenarios. For the head office, you can deploy the VCS in the public network, or an intranet. For a branch office, you can follow the same steps as for the head office, or use intelligent traversal method to deploy the VCS.

Scenario	Description	Other
Private IP Deployment	To deploy the VCS in an intranet (behind a firewall), you must assign a static private IP address to the VCS. In the meantime, do port forwarding on the firewall/router.	This method is often used in the head office. Both inbound and outbound calls are available.
Public IP Deployment	To deploy the VCS in a public network, you need to assign a static public IP address to the VCS.	This method is often used in the head office. Both inbound and outbound calls are available.
Intelligent Traversal Deployment	Connect the VCS to the network. It is a plug-and-play solution, which means that you can deploy the VCS without any firewall configuration.	This method is often used in branch offices. Only outbound calls are available.

Scenario 1: Private IP Deployment (Behind Firewall with Port Forwarding)

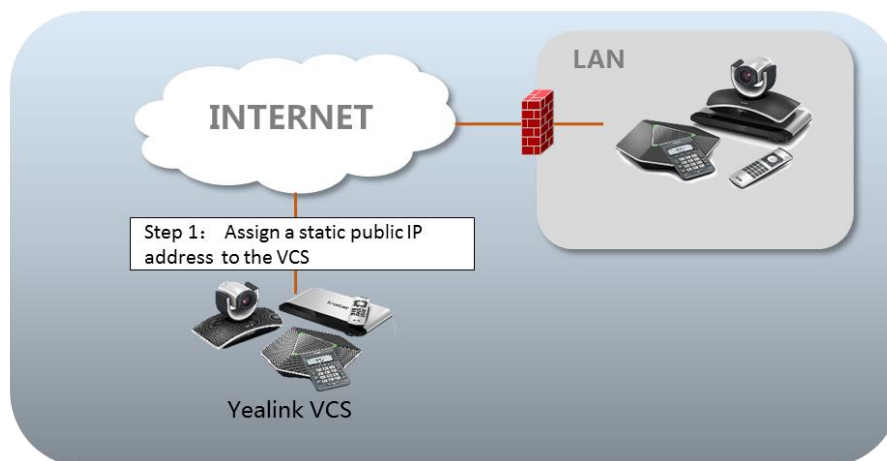
The most common deployment scenario is deploying the VCS in an Intranet (behind a firewall). You need to assign a static private IP address to the VCS. At the meantime, do port mapping on firewall/router for it.

This setup process is simple and with high security. In addition, it is a low cost solution. Both the head office and branch offices can deploy the VCS in this way.



Scenario 2: Public IP Deployment (Outside of Firewall)

Some enterprises have high standards for the VCS. To avoid network congestion, you can configure a leased line for the VCS to make it access the public network directly. This setup process is simple and creates a stable network environment. However, this method is expensive due to the leased line costs and is often used for the head office.

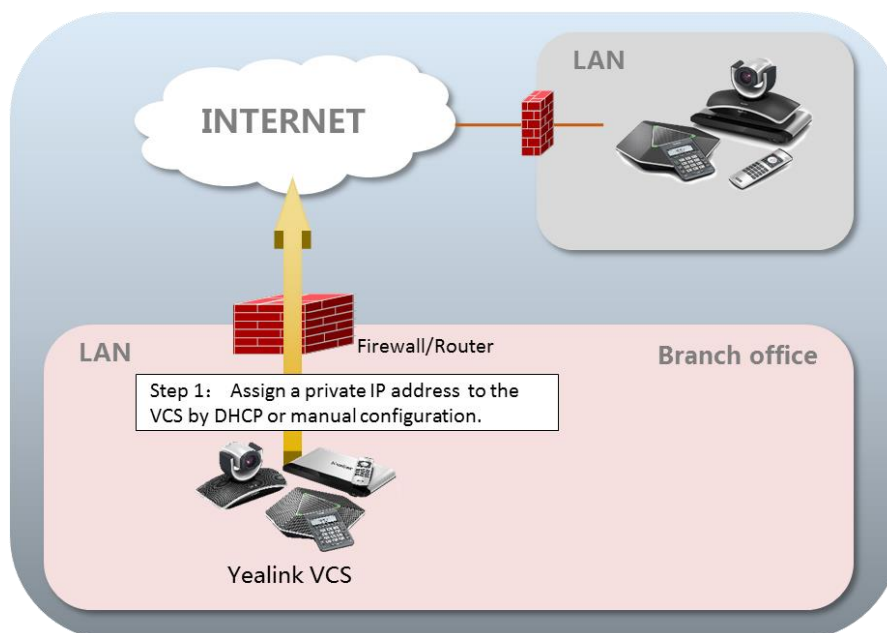


Scenario 3: Intelligent Traversal

Some branch offices lack IT professionals, which means that professional network configuration (e.g., port forwarding) cannot be done.

Yealink VCS supports intelligent traversal deployment. All you need to do is deploy the VCS in an intranet, and assign a private IP address to it by DHCP or manual configuration. Make sure the private IP can access the public network.

This setup process is simple, and is a plug-and-play solution which means that you can deploy the VCS without any firewall configuration. Using this method, inbound calls are unavailable, only outbound calls are available.



VCS Network Deployment

VCS Network Settings

Your video conferencing system can only work normally when the network settings are correct.

The system attempts to contact a DHCP server in your network to obtain an IP address by default. In most cases, the VCS dials the IP address of other system to establish call. So it is recommended that you configure a static IP address for the VCS.


To configure a static IP address via web the user interface:







1. Enter the IP address of the system in the address bar of a web browser on your PC, and then press the **Enter** key.
2. Enter the administrator user name and password.
The default user name is "admin" (case-sensitive), and the default password is "0000".
3. Click on **Network->LAN Configuration**.
4. Mark the radio box of the **Static IP**.
5. Enter IP address, subnet mask, gateway, primary DNS, secondary DNS in corresponding fields.

Lan Config	Port Type	Port Range
H.323	TCP	1720
Gatekeeper	UDP	1719
SIP	TCP/UDP	5060
Video, Audio & Data	TCP/UDP	50000-50499
HTTPS(Web)	TCP	443

6. Click **Confirm** to save the change.
The web user interface prompts "Warning: Settings will take effects after reboot. Reboot now?".
7. Click **Confirm** to reboot the system.

To configure a static IP address via the remote control:

1. Press  (**Menu** soft key) to enter the main menu.
2. Press **◀** or **▶** to scroll to the **Advanced** menu.
3. Enter the admin password (default password: 0000) in the **Admin Password** field.

4. Press  or Press  (Enter soft key).
5. Press  or  to scroll to **LAN Configuration**, and then press .
6. Uncheck the **DHCP** check box.
7. Enter IP address, subnet mask, gateway, primary DNS, secondary DNS in corresponding fields.
8. Press  (Save soft key) to accept the change
The LCD screen prompts: "Reboot now?".
9. Press **OK** to reboot the system.

Note

Wrong network settings may result in inaccessibility of your system and may also have an impact on your network performance. For more information on these parameters, contact your system administrator.

Related Port Usage for Firewall Setup

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with video conferencing equipment, you must configure the firewall to allow incoming and outgoing traffic to the VCS through the related ports.

The following table lists the commonly used ports for the VCS. If these ports are restricted, you need to open firewall ports to allow incoming and outgoing video traffic.

If you deploy the VCS in an intranet, to make it access the VCS in the public network, you need to do port forwarding (the following table) on the firewall/router.

Function	Port	Type
Gatekeeper	1719	UDP
H.323 Call setup	1720	TCP
Signaling and control for audio, call, video, and data/FECC	50000-50499	TCP/UDP
HTTPS Interface (optional)	443	TCP
SIP port (optional)	5060-5061	TCP/UDP

Note

It is recommended that you forward the web management port (443/TCP) of the branch office to the public network, so that the head office can manage the branch office remotely.

QoS Guarantees

To ensure network stability, it is recommended that users enable the Quality of Service (QoS) feature for the VCS.



Quality of Service (QoS) is the ability to provide different priorities for different packets in the network. This allows the transport of traffic with special requirements. QoS guarantees are important for applications that require a fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss. For more information on QoS, refer to [Yealink_VC_Series_Video_Conferencing_System_Administrator_Guide](#).

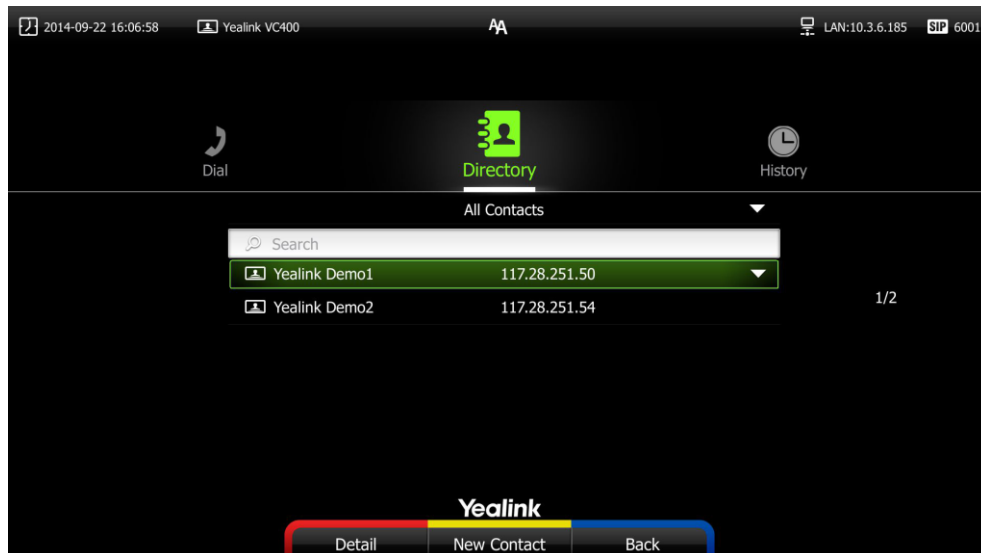
For more information on VCS bandwidth requirements, refer to [Bandwidth Requirements](#) on page 1.

Connectivity Testing

After the VCS is installed, you can test it by dialing Yealink demo contacts,.

To place a test call via the remote control:



1. Press  (Call soft key).
2. Press ◀ or ▶ to select the **Directory** menu.
3. Press ▲ or ▼ to select Yealink Demo1, and then press .



If the video call is established successfully, it means that the network is normal. If it fails, you can contact the system administrator to check the network and whether it can access the public network.

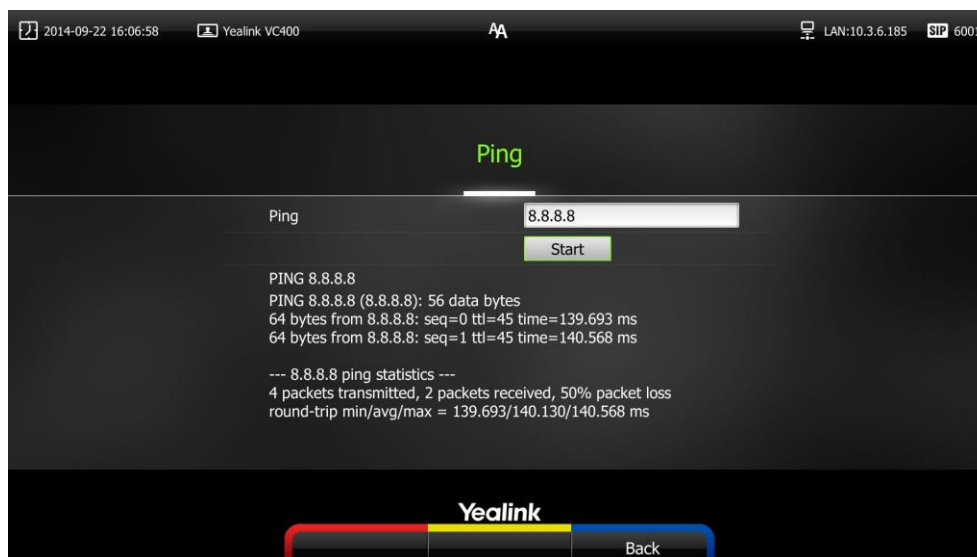
VCS Network Connectivity Testing

To check the network connectivity using the Ping test:

1. Press  (Menu soft key) to enter main menu.
2. Press ◀ or ▶ to select the **Diagnose** menu.
3. Press ▲ or ▼ to scroll to **Ping**, and then press .
4. Enter **8.8.8.8** in the **Ping** field.

This will test the connection between the local system and the public network.

- Once successful, the VCS receives a response. The time between these two transmissions is calculated to generate an average response or latency time.



- If the ping does not reach its destination due to an error or because it is being blocked, the sending device encounters a request timed out error or shows no received packets.
5. You can also test the network connection between the local VCS and other VCS.

Troubleshooting

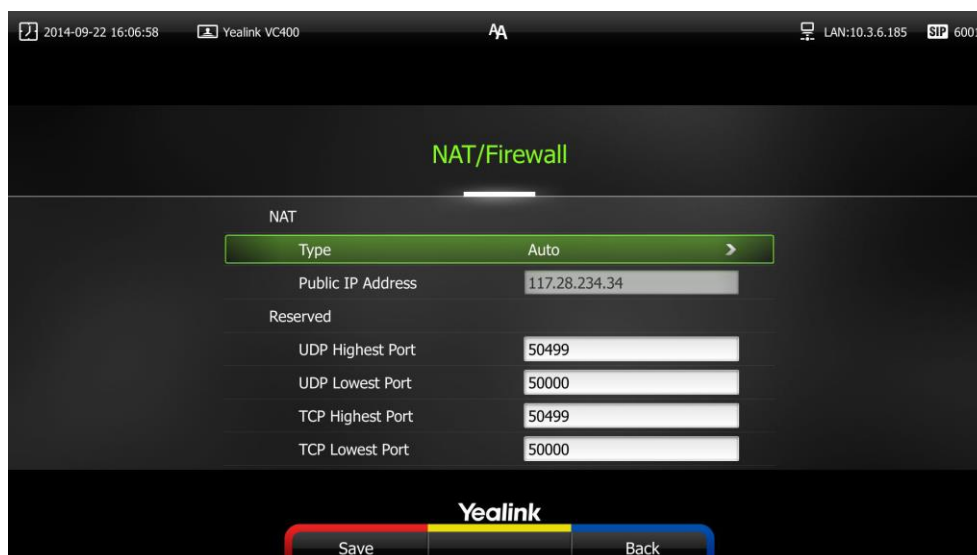
Branch Office Fails to Connect to Head Office

Assume that you are A in the head office. You have configured port forwarding for the VCS, but you find that you are able to call B in the branch office or Yealink demo contacts, but they cannot call you.

Please check whether the port forwarding configuration is correct. If it is correct, the most likely reason is that your firewall or router does not support the H.323 ALG feature. In this situation, please take the following actions to activate the NAT feature on the VCS.

To activate the NAT feature via the remote control:

1. Press **Menu->Advanced** (default password: 0000) -> **NAT/Firewall**.
2. Select **Auto** from the **Type** pull-down list, the system will obtain a public IP address automatically.
3. If the system does not obtain a public IP address automatically, select **Manual Settings** from the **Type** pull-down list, and then enter the public IP address in the **Public IP address** field.



4. Press  (**Save** soft key).

Abnormal Conditions during a Call

If extensive pixel mosaic appears on the screen during the video conference, this may be caused by network instability. You can press **More->Call Statistics** during the call to check network conditions. Please focus on the total packet loss and packet loss(%).



If total packet loss or packet loss rate is high, it is recommended that you check the causes of this problem.

Is it due to network instability, or network congestion? If the problem is resulted from network congestion caused by sharing Internet connection with other devices, please use QoS device to control the network traffic.