Yealink VCS Network Deployment Solution

Aug. 2016

V21.20

Table of Contents

Network Requirements Overview

Bandwidth Requirements

Because the video conferencing system (VCS) is a real-time network application, it has high network bandwidth requirements. Recommended bandwidths to ensure the best VCS performance results are shown below.

Bandwidth requirements of the Yealink video conferencing system:

Video 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	General VCS delay is less than 200ms
Jitter	Jitter is less than 50ms
Packet lost	Packet loss is less than1%

Bandwidth Requirement for the Head Office

The total head office bandwidth requirement is related to the number of connected branch offices.

The calculation formula is as follows:

The total head office bandwidth requirement = N x bandwidth requirement for one single branch office

Take 3 branch offices as an example:

To achieve the full HD effect, the total head office bandwidth requirement = 1.3Mbps x 3= 3.9 Mbps.

Presentations are often needed during a video conference. This means that every office that runs presentations needs double bandwidth.

If a presentation is needed for 3 branch offices, then the total bandwidth requirement for the head office = 1.3Mbps x 2 x 3 =7.8Mbps.

Bandwidth Requirement for the Branch Office

Bandwidth requirement for the branch office = bandwidth requirement for a single branch office.

For example:

To achieve the full HD effect, the total bandwidth requirement is1.3Mbps. If presentation is needed, 2.6 Mb is needed.

Note

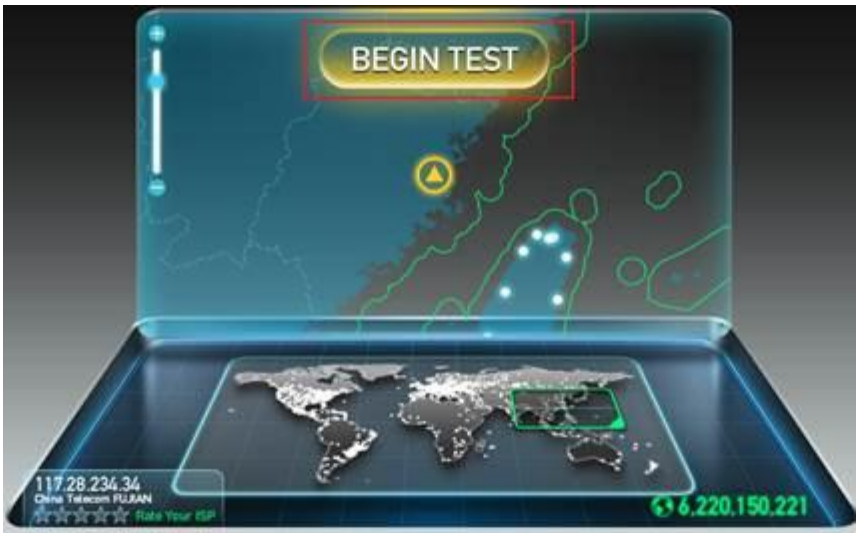
An independent fiber optic line is recommended for the video conferencing system instead of sharing bandwidth with other office systems. If network sharing cannot be avoided, you are advised to take QoS measures to control the network traffic.

Bandwidth Testing

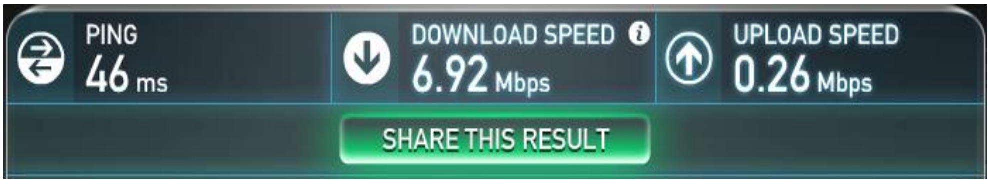
Once you understand your VCS bandwidth requirements, carry out the following steps to test whether your current bandwidth meets your new VCS needs.

Enter http://www.speedtest.net/ in the address bar of a web browser on your PC, and then press the **Enter** key.

Start you test when "**Begin Test**" is displayed on the webpage.



Test result:



PING 46 ms

DOWNLOAD SPEED 6.92 Mbps

UPLOAD SPEED 0.26 Mbps

SHARE THIS RESULT

a) **PING**: the ideal PING value is less than 100ms, so the test above shows that the network delay is low.

b) **DOWNLOAD SPEED**: Downlink bandwidth.

c) **UPLOAD SPEED**: Uplink bandwidth.

d) For a system with a 1080P video resolution: the proposed uplink and downlink bandwidths are 1.3Mb. The ideal uplink and downlink bandwidths are 1.5Mb. Downlink and uplink bandwidths may be asymmetric, so ensure the uplink bandwidth meets the requirements.

According to the result above, if the current network cannot meet the minimum VCS bandwidth requirements, please deploy the system after upgrading your network. Otherwise, your video conferences will not achieve the desired effects.

Static Public 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.

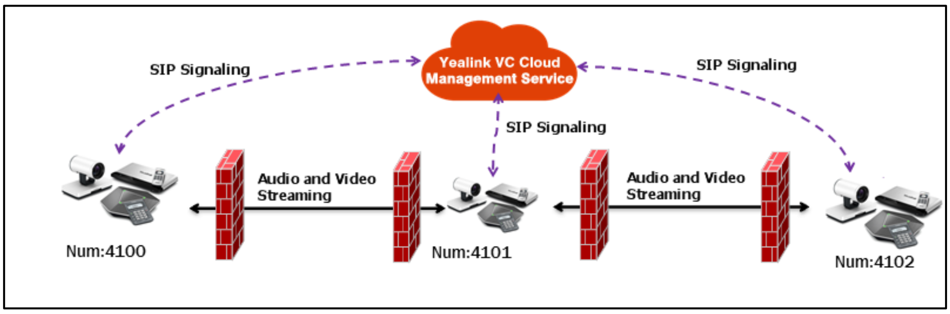
VCS Deployment

VCS supports two network deployment methods: Yealink Cloud deployment and traditional deployment. Choose the desired deployment method according to your needs.

Yealink Cloud Deployment Method

Cloud-based technology drives positive change in the way organizations communicate, especially when it comes to video. With Yealink's VC Cloud management service, organizations can communicate just using a Cloud account. Public IP address and complex network settings are unnecessary.

Challenges such as infrastructure costs and interoperability are eliminated. Both the head office and the branch offices can use the Cloud deployment method. Both inbound and outbound calls are available.


Yealink VC Cloud Management Service
SIP Signaling
SIP Signaling
SIP Signaling
Audio and Video Streaming
Audio and Video Streaming
Num:4100
Num:4101
Num:4102

Take above image as an example: three video conferencing systems are deployed in different networks, and they all register Cloud accounts.

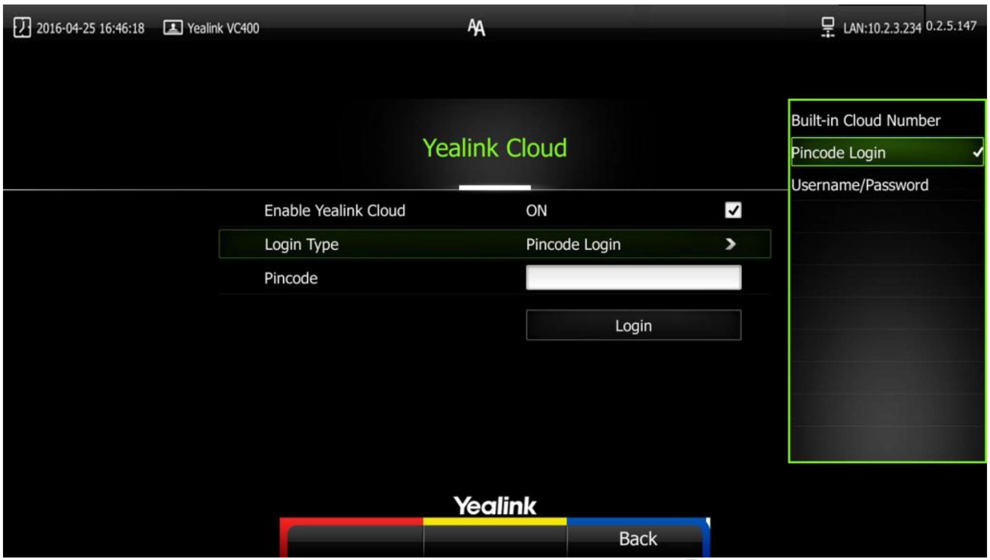
Yealink's VC Cloud management service deployed in public network can help traverse SIP signaling and media streaming, so that the video conferencing systems can call each other without public IP addresses and complex network settings

Sign into the Yealink Cloud Account

To sign into the Yealink Cloud account via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Cloud.**
2. Select desired sign-in method from the pull-down list of **Login Type**
   - You can sign into the 9-digit enterprise Cloud account using PIN code or username/password (enterprise Cloud account can be managed via Yealink VC Cloud Management Service).

- You can also use 7-digit build-in Cloud number (build-in Cloud number cannot be managed via Yealink VC Cloud Management Service).



Enable Yealink Cloud ON ☑
Login Type Pincode Login >
Pincode

After successful registration, the display device displays ☁ , and the LCD screen of the video conferencing phone displays ☁ .

Traditional Deployment Methods

If you do not use Cloud accounts, you can choose traditional deployment method to deploy your VCS, and dial IP addresses of other devices to make a call.

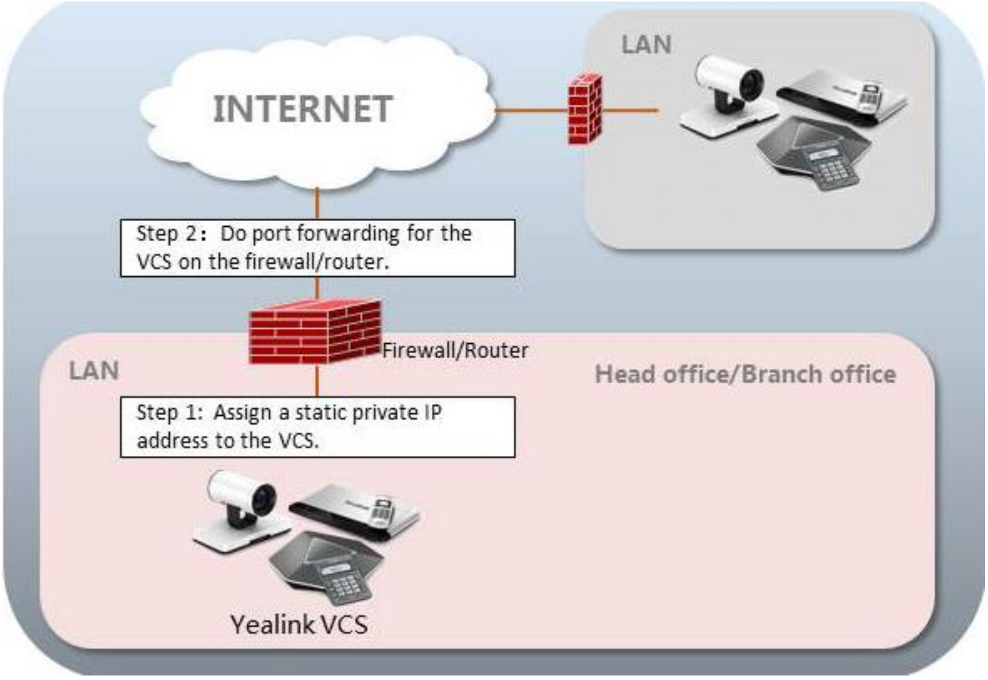
There are three common deployment scenarios. For the head office, you can deploy the VCS using the first two methods. For the branch office, you can follow the same deployment steps as for the head office, or use an intelligent firewall to deploy the VCS.

Scenario	Description	Other
Private IP Deployment	To deploy the VCS over an intranet (behind a firewall), you must assign a static private IP address to the VCS. In the meantime, carry out port forwarding on the VCS firewall.	This is often used in the head office. Both inbound and outbound calls are available.
Public IP Deployment	To deploy the VCS over a public network, you need to assign a public IP address to the VCS.	This is often used in the head office. Both inbound and outbound calls are available.
Intelligent Firewall 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 is often used in branch offices. Only outbound calls are available.

Scenario 1: Private IP Deployment

The most common deployment scenario is deploying the VCS over an intranet (behind a firewall). The private IP address should be forwarded to the public network by port forwarding.

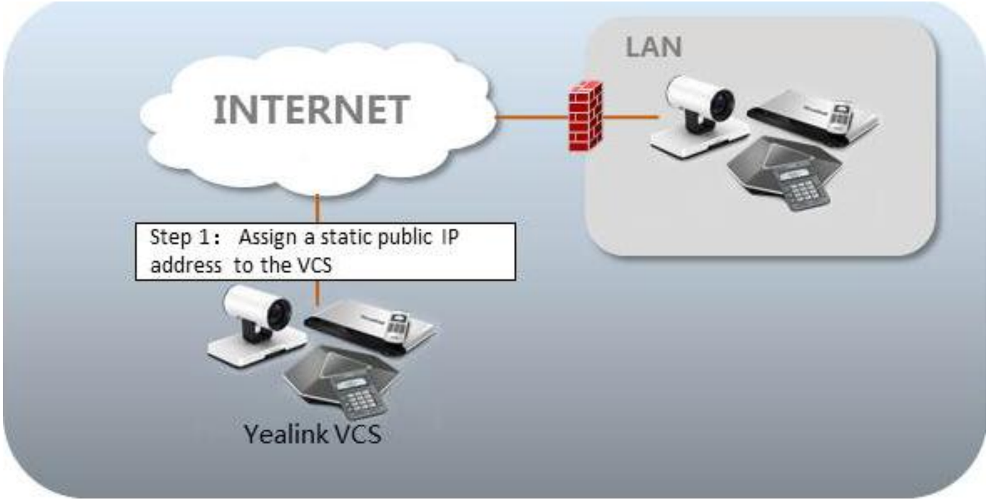
This deployment method involves a simple setup process and high security. In addition, it is a low cost solution. Both the head office and branch offices can deploy the VCS in this way.


INTERNET
LAN
Step 2: Do port forwarding for the VCS on the firewall/router.
Firewall/Router
LAN
Head office/Branch office
Step 1: Assign a static private IP address to the VCS.
Yealink VCS

Scenario 2: Public IP Deployment (leased lines)

Some enterprises have high video conference performance requirements. To avoid bandwidth congestion, you can configure a leased line to connect the VCS to the public network directly.

This deployment method involves a simple setup process and creates a stable network environment. However, it is more expensive due to leased line costs and is often used in the head office.

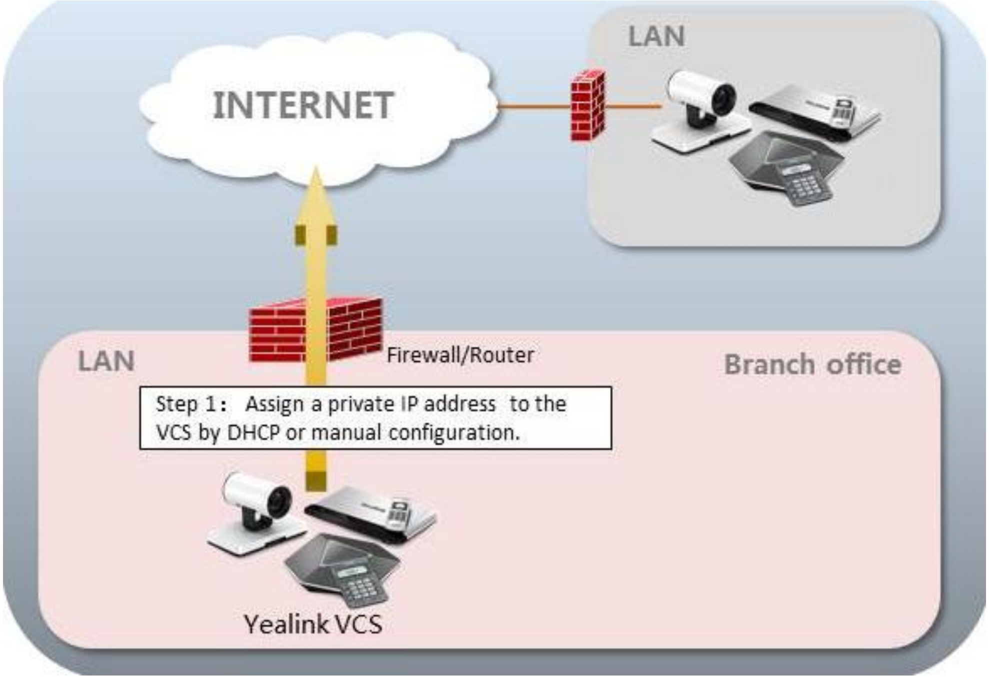


Scenario 3: Intelligent Firewall Deployment

Some branch offices lack IT professionals, which means that professional network configuration (e.g., port forwarding) is not possible.

Yealink VCS supports intelligent firewall configuration. You can deploy the VCS over an intranet, and make the VCS contact a DHCP server to obtain a private IP address which can access the public network. You can also configure a private IP address for the VCS manually.

This deployment method involves a simple setup process. It 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.



Step 1: Assign a private IP address to the VCS by DHCP or manual configuration.

VCS Network Deployment

VCS Network Settings

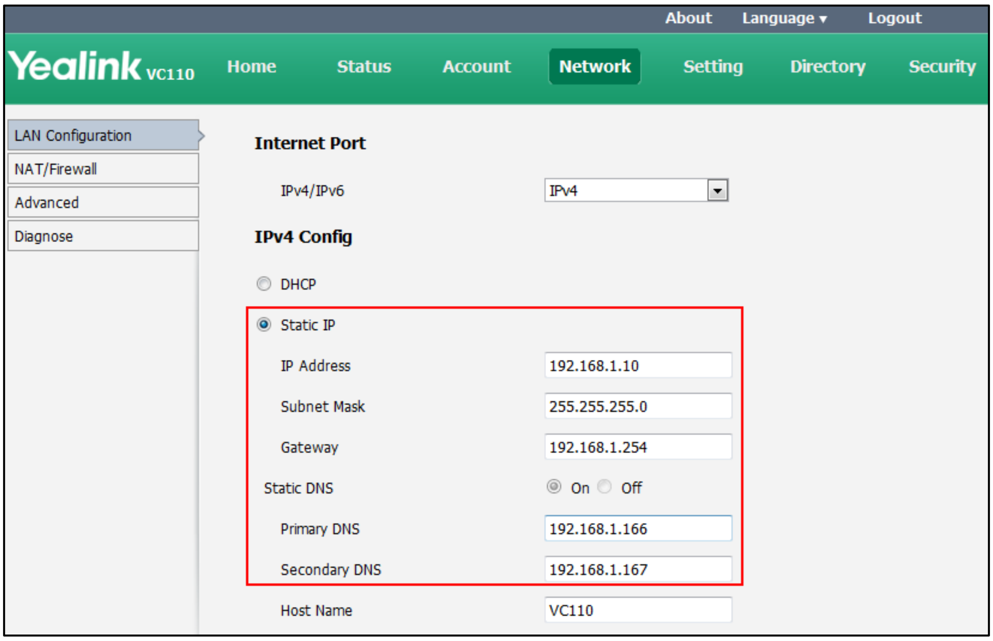
Your video conferencing system can only work normally when the network settings are correct.

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 IPv4 address to connect to the other system. So it is recommended that you configure a static IPv4 address for the VCS.

To configure a static IPv4 address via web 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. In the **IPv4 Config** block, mark the Static IP radio box.
5. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** fields.



Internet Port

IPv4/IPv6: IPv4

IPv4 Config

○ DHCP

● Static IP

IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Static DNS	● On ○ Off
Primary DNS	192.168.1.166
Secondary DNS	192.168.1.167
Host Name	VC110

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 IPv4 address via phone user interface:

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

4. Press OK or press ▭ (**Enter** soft key).
5. Press ▲or ▼to scroll to **LAN Configuration**, and then press OK.
6. Press ▲or ▼to scroll to **IPv4**, and then press OK.
7. Uncheck the **DHCP** checkbox.
8. Enter the desired values in the IP Address, Subnet Mask, Gateway, DNS Primary Server and DNS Secondary Server fields respectively.
9. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
10. Select **OK** to reboot the endpoint immediately.

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.

Firewall/Router Settings

The following table lists the commonly used ports of the VCS. If the following ports are restricted in your network environment, you need to open these ports.

When the VCS is deployed over an intranet, and you want to solve the interconnection problem by port forwarding, you must forward the following ports to the public network on the firewall/router.

NO.	Function	Port	Type
1	H.323 signal port	1720	TCP
2	Audio & video media stream port	50000-50499	TCP/UDP
3	Web management port (optional)	443	TCP
4	SIP (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.

When the VCS is deployed over an intranet, you can also use the Cloud deployment method to solve the interconnection problem. Port forwarding is unnecessary. For more information, refer to Yealink Cloud Deployment Method on page 5.

QoS Guarantees

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

For more information on VCS bandwidth requirements, refer to Bandwidth Requirements on page 1

.

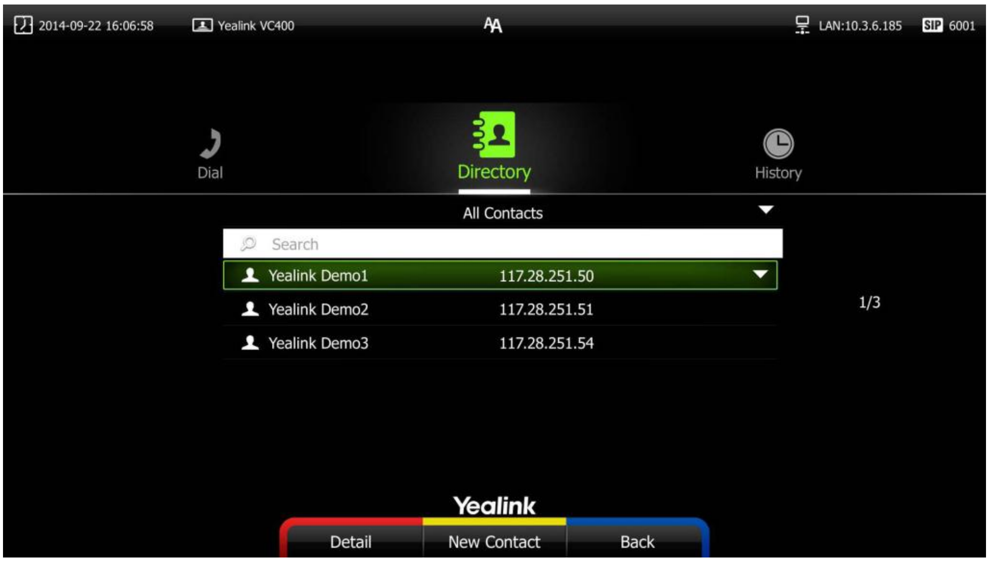
Connectivity Testing and Troubleshooting

Connectivity Testing

Yealink demo contacts can help users to test quickly whether the system is working normally after it has been installed.

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 ☎ .



Yealink Demo1	117.28.251.50
Yealink Demo2	117.28.251.51
Yealink Demo3	117.28.251.54

If the video call is established successfully, the network connectivity is normal. If the call fails, you can contact the system administrator to check the network connectivity and the access rights to the public network.

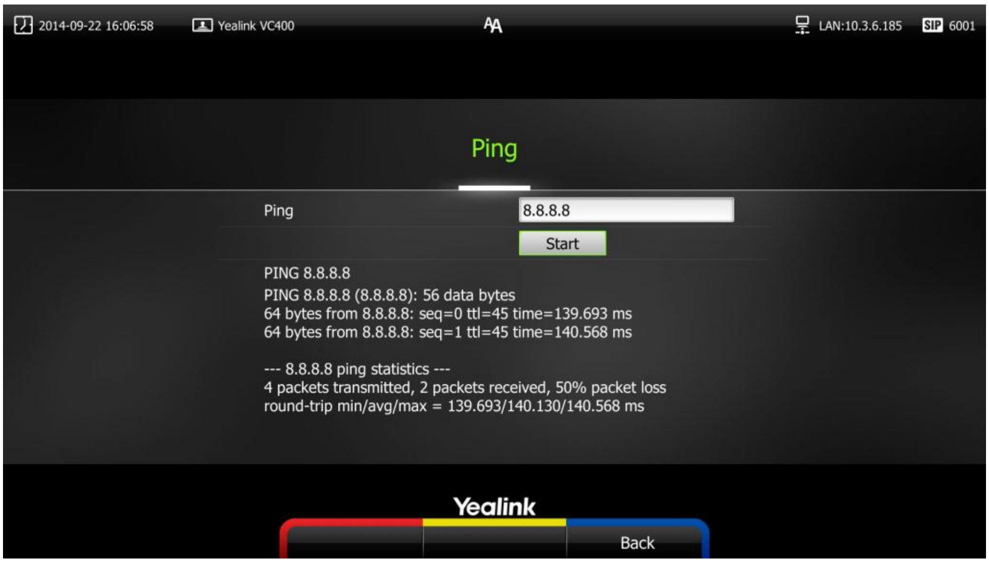
VCS Network Connectivity Testing

To check the network connectivity using the Ping feature:

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 OK.
4. Do the following:

   1) **Ping 8.8.8.8**: Test the connection between the local system and the public network. If successful, do the next test. If not, contact your administrator.

2) You can also test the network connection between the local system and any remote system.



```
PING 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=45 time=139.693 ms
64 bytes from 8.8.8.8: seq=1 ttl=45 time=140.568 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 2 packets received, 50% packet loss
round-trip min/avg/max = 139.693/140.130/140.568 ms
```

Branch Office Fails to Connect to Head Office

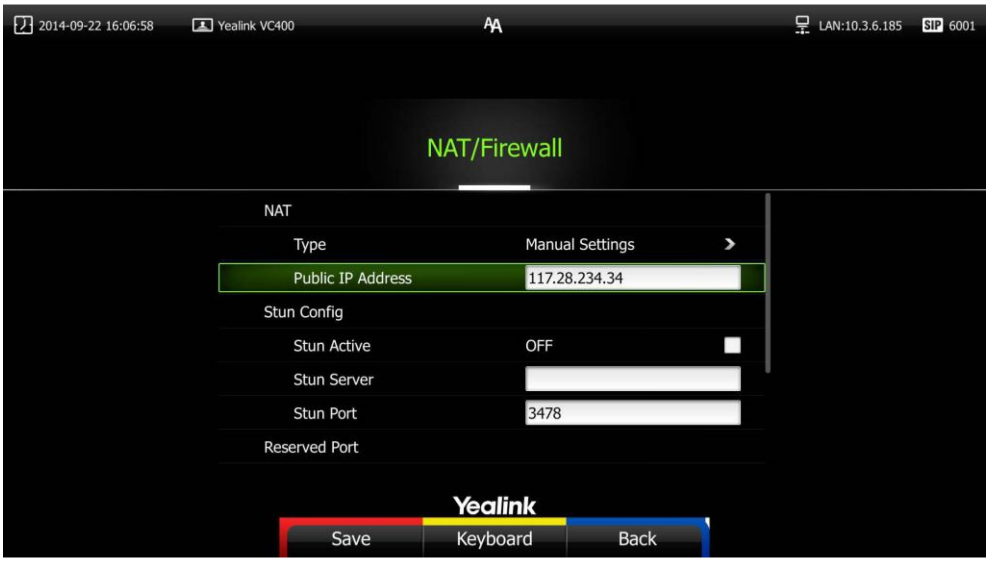
Assume that you are A in the head office. You have configured port forwarding for the VCS. You find that you able to call B in the branch office or Yealink Demo, but they cannot call you.

Please check whether the port forwarding configuration is correct. For more information, refer to Firewall/Router Settings on page 10. If it is correct, the most likely reason is that the firewall or gateway in the environment 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** soft key) to enter main menu.
2. Press ◀ or ▶ to scroll to the **Advanced** menu.
3. Enter admin password (default password: 0000) in the **Admin Password** field.
4. Press OK or press ▭ (**Enter** soft key).
5. Press ▲ or ▼ to scroll to **NAT/Firewall**, and then press OK .
6. Select **Auto** from the pull-down list of **Type**, the system will obtain a public IP address automatically.

7. If the system does not obtain a public IP address automatically, select **Manual Settings** from the pull-down list of **Type**, and then enter the public IP address in the **Public IP address** field.



NAT/Firewall

NAT

Type	Manual Settings
Public IP Address	117.28.234.34

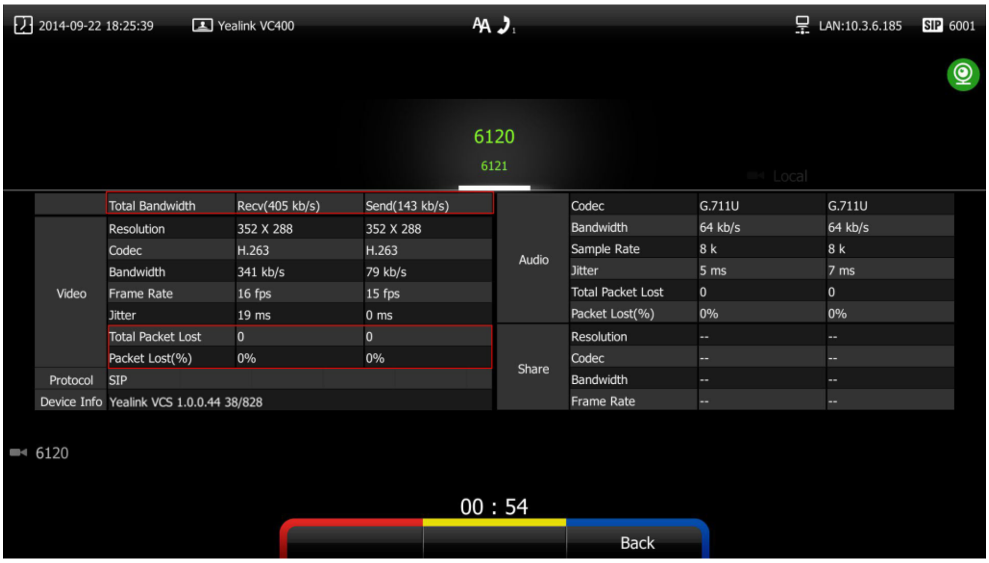
Stun Config

Stun Active	OFF □
Stun Server	
Stun Port	3478

Reserved Port

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 current network conditions. Focus on the total packet loss and packet loss(%).



	Total Bandwidth	Recv(405 kb/s)	Send(143 kb/s)
Video	Resolution	352 X 288	352 X 288
	Codec	H.263	H.263
	Bandwidth	341 kb/s	79 kb/s
	Frame Rate	16 fps	15 fps
	Jitter	19 ms	0 ms
	Total Packet Lost	0	0
	Packet Lost(%)	0%	0%
Protocol	SIP		
Device Info	Yealink VCS 1.0.0.44 38/828		

Audio	Codec	G.711U	G.711U
	Bandwidth	64 kb/s	64 kb/s
	Sample Rate	8 k	8 k
	Jitter	5 ms	7 ms
	Total Packet Lost	0	0
	Packet Lost(%)	0%	0%
Share	Resolution	--	--
	Codec	--	--
	Bandwidth	--	--
	Frame Rate	--	--

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

They may be due to network stability, or network congestion caused by network sharing. If either of these conditions are the cause of the problem, it is recommended that you use traffic control devices to guarantee the network traffic.