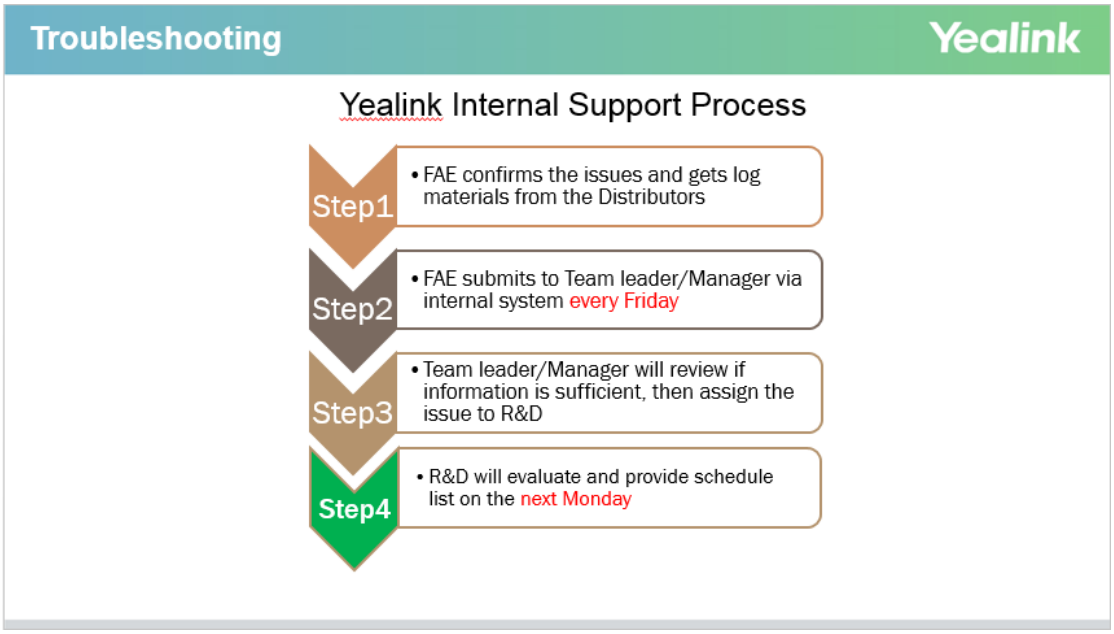
# How to Do the Troubleshooting

| Version | Change log | Editor | Review | Approval | Date |
|---|---|---|---|---|---|
| V1.0 | How to do the troubleshooting | Wilson | | | 2017-8 |
| V2.0 | Update the format ,change the info based on new product and new version features | Nicole | | | 2017-9-11 |
| V2.1 | Update the key of trace capture | Gerry | | | 2018-1-3 |
| V3.0 | Add how to do YMS troubleshooting<br>Update the info based on new product and new version features | Wilson | | | 2018-4-26 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# 1. Yealink Internal Support Process


# 2. Yealink Meeting Server (YMS)

## 2.1 Capturing Packets

To connect to the YMS via SSH connection.

The command to Start PCAP Trace.

```
tcpdump -i any -s 0 -w /tmp/test.pcap
```

The command to download to local tmp directory.

```
sz /tmp/test.pcap
```

## 2.2 Server Logs

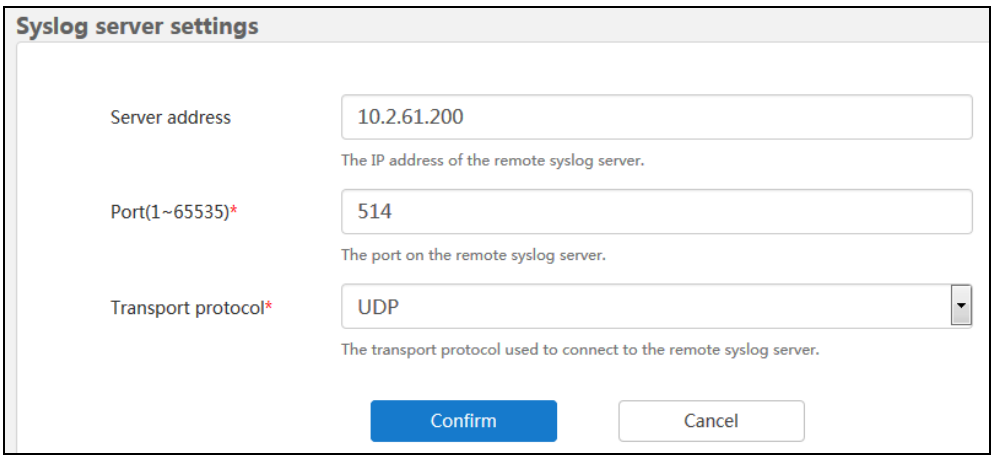
### 2.2.1Syslog Server Settings

You can configure remote syslog server to collect operation logs and system logs.

To configure the syslog server settings:

1. Click **System->System Log->Server log**.
2. On the top-right of page, click **Syslog server settings**.

3. Configure the syslog server.




Parameters are described below:

| Parameter | Description |
|---|---|
| Server address | Specify the IP address of the remote syslog server. |
| Port (1~65535) | Specify the port on the remote syslog server.<br>**Default:** 514 |
| Transport protocol | Configure the type of transport protocol used to communicate with the remote syslog server.<br>• **UDP**—provides best-effort transport via UDP.<br>• **TCP**—provides reliable transport via TCP.<br>• **TLS**—provides secure communication.<br>**Default:** UDP |

4. Click **Confirm**.

## 2.2.20peration Logs

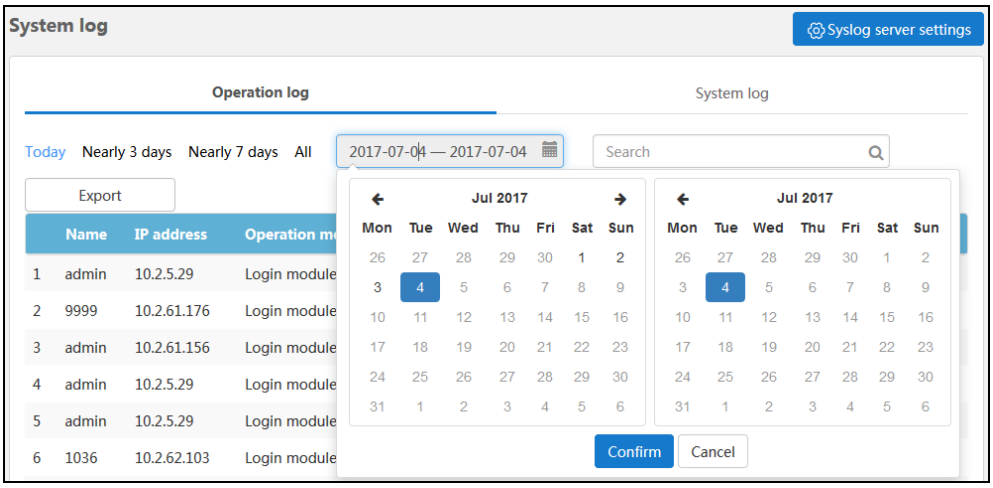
Operation logs record the change logs, including access logs or

configuration changes.

To view the operation log:

1. Click **System->System Log->Server log.**
2. Select **Operation log** to enter the page of operation log.
3. Click **Today**, **Nearly 3 days**, **Nearly 7 days** or **All**, the page will display the operation log during the selected time.

You can also select the start time and end time in the date selection box.




4. Click **Export** to export the operation logs.

   The following is an example of operation logs:

| NO. | UserName | Module\|Menu | OperationTime | Remark |
|---|---|---|---|---|
| 1 | admin | SystemManager\|Configuration backup/restore | 2016-12-07T16:02:41Z | Download the backup successful! |
| 2 | admin | Login\|Login | 2016-12-07T16:01:05Z | Account:admin login success! |
| 3 | admin | Login\|Login | 2016-12-07T15:57:10Z | Account:admin login success! |
| 4 | 2221 | Login\|Login | 2016-12-07T15:56:45Z | Account:2221 login success! |
| 5 | admin | Login\|Login | 2016-12-07T15:42:32Z | Account:admin login success! |
| 6 | admin | SystemManager\|Configuration backup/restore | 2016-12-07T15:36:05Z | Download the backup successful! |
| 7 | admin | SystemManager\|Configuration backup/restore | 2016-12-07T15:36:01Z | Download the backup successful! |
| 8 | admin | SystemManager\|TerminalAutoUpgrade | 2016-12-07T15:21:53Z | Delete termianl config success! |
| 9 | admin | 登录模块\|登录模块 | 2016-12-07T15:19:28Z | 账号admin登录成功! |
| 10 | 4201 | Login\|Login | 2016-12-07T15:18:53Z | Account:4201 login success! |
| 11 | 4201 | Login\|Login | 2016-12-07T15:17:31Z | Account:4201 login success! |
| 12 | admin | 登录模块\|登录模块 | 2016-12-07T15:16:34Z | 账号admin登录成功! |
| 13 | 2221 | Login\|Login | 2016-12-07T15:14:44Z | Account:2221 login success! |
| 14 | admin | Login\|Login | 2016-12-07T15:14:31Z | Logout success! |
| 15 | 1222 | Login\|Login | 2016-12-07T15:13:08Z | Account:1222 login success! |
| 16 | admin | 登录模块\|登录模块 | 2016-12-07T15:10:39Z | 账号admin登录成功! |
| 17 | 1256 | 登录模块\|登录模块 | 2016-12-07T15:08:35Z | 账号1256登录成功! |
| 18 | admin | Login\|Login | 2016-12-07T15:02:09Z | Account:admin login success! |
| 19 | admin | SystemManager\|TerminalAutoUpgrade | 2016-12-07T15:00:53Z | Add termianl config success! |
| 20 | 4004 | Login\|Login | 2016-12-07T14:57:18Z | Account:4004 login success! |
| 21 | 4004 | Login\|Login | 2016-12-07T14:57:16Z | Account:4004 login success! |
| 22 | admin | Login\|Login | 2016-12-07T14:57:02Z | Logout success! |
| 23 | 4004 | Login\|Login | 2016-12-07T14:56:44Z | Account:4004 login success! |
| 24 | 4004 | Login\|Login | 2016-12-07T14:56:39Z | Account:4004 login success! |
| 25 | admin | Login\|Login | 2016-12-07T14:56:34Z | Logout success! |
| 26 | 4002 | Login\|Login | 2016-12-07T14:55:41Z | Account:4002 login success! |
| 27 | admin | Login\|Login | 2016-12-07T14:55:33Z | Logout success! |

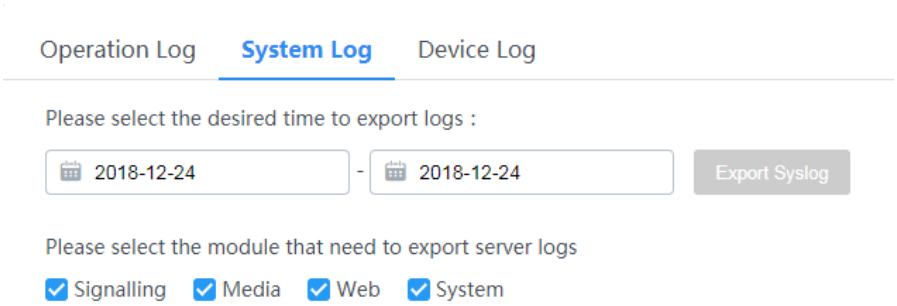
## 2.2.3 System Logs

System logs record conference logs.

You can export **Web**, **FreeSwitch**, **MCU**, **TURN**, **WebRTC** or **GateKeeper** logs and save these in your computer to view logs.

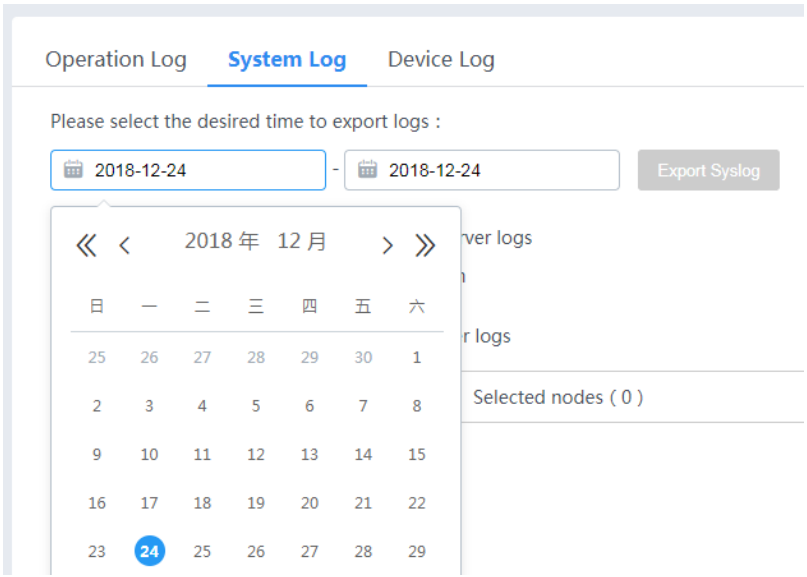
**To view the system log:**

1. Click **Maintenance->Support Log->Server log.**
2. Select **System log** to enter the page of system log.
3. Select the desired type of system logs, and then click **Signaling**, **media**, **Web**, or **system**, the selected type is blue.




4. Click **Today**, **Nearly 3 days**, **Nearly 7 days** or **All**.

   You can also select the start time and end time in the date selection box.



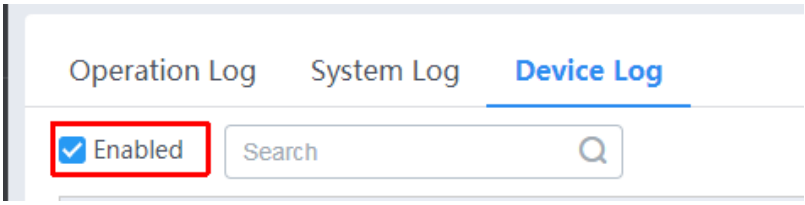

5. Click **Export** to export the system logs and save in your computer to view system logs.

## 2.3 Device Logs

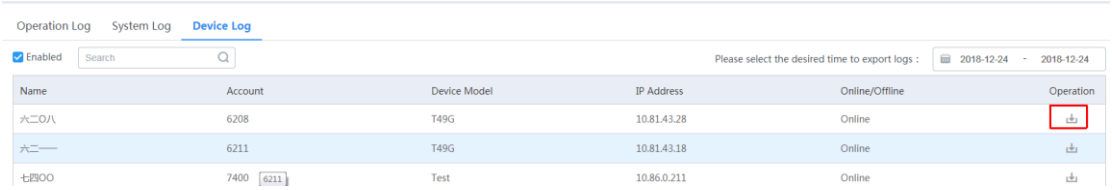
You can enable the **Device log** feature. After you enable it, the device logs will occupy a certain amount of bandwidth. System's actual performance may vary based on the number of devices. Device logs contain SIP information, when devices interact with YMS, the information are generated.

**To view the device log:**

1. Click **Maintenance->Support Log->Device log.**
2. Check the **Enable** checkbox to enable the Device log feature.




3. Click on the right download device log.




# 3 VCS

Troubleshooting Methods

The system can provide feedback in a variety of forms, such as log files, packets, status indicators and so on, which can help an administrator to find the system problem more easily and resolve it.

The following sections will help you to better understand and resolve the working status of the system.

- Viewing Log Files
- Capturing Packets
- Getting Information from Status Indicators
- Analyzing Configuration Files
- Viewing Call Statistics
- Using Diagnostic Methods

## 3.1 Viewing Log Files

The log files are Yealink specific debug files which may be requested by the Yealink support organization if you need

technical support. The current log files are time stamped event log files. You can export the log files to a syslog server or the local system. The administrator can specify the location where the log will be exported to and the severity level of the log.

System Log Level specifies the log level to be recorded. The default system log level is 6.

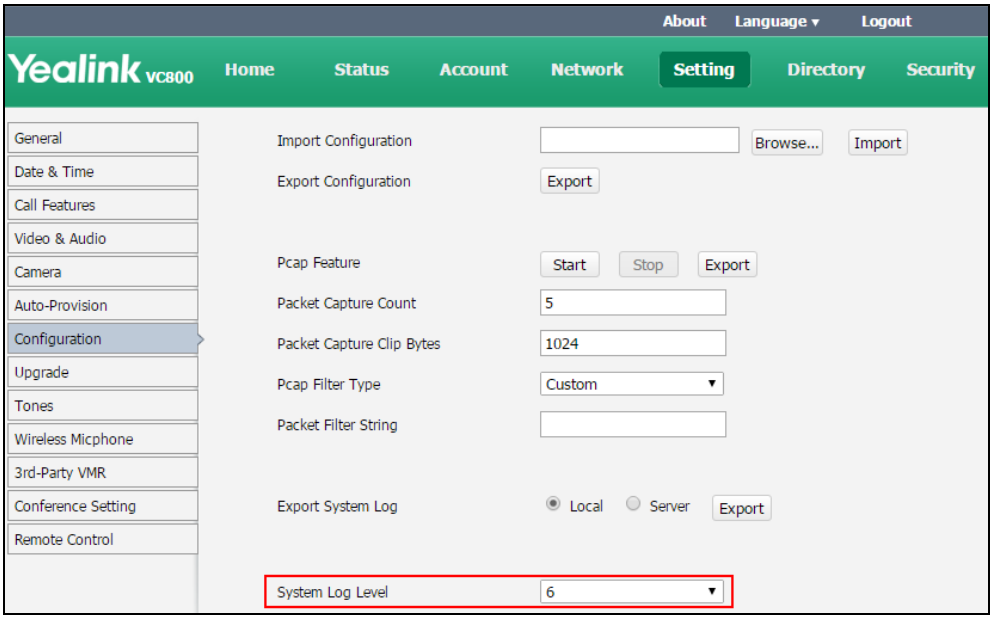
System log level parameters are described below:

| Parameter | Description | Configuration Method |
|---|---|---|
| Export System Log | Specify where the system log will be exported.<br>**Valid values:**<br>• **Local**-export the system log to the local computer.<br>• **Server**-export the system log to the specified server.<br>**Default:** Local | Web User Interface |
| Server Name | Specify the server address where the log will be exported.<br>**Note**: It only works if the parameter "Export System Log" is set to Server. | Web User Interface |
| System Log Level | Specify the system log level.<br>**Note**: The supported level is 0-6. | Web User Interface |

| Parameter | Description | Configuration Method |
| --- | --- | --- |
| | Higher value indicates more detailed content.<br>Default: 6 | |

To configure the system log level via web user interface:

1. Click on Setting->Configuration.
2. Select the desired level from the pull-down list of System Log Level.

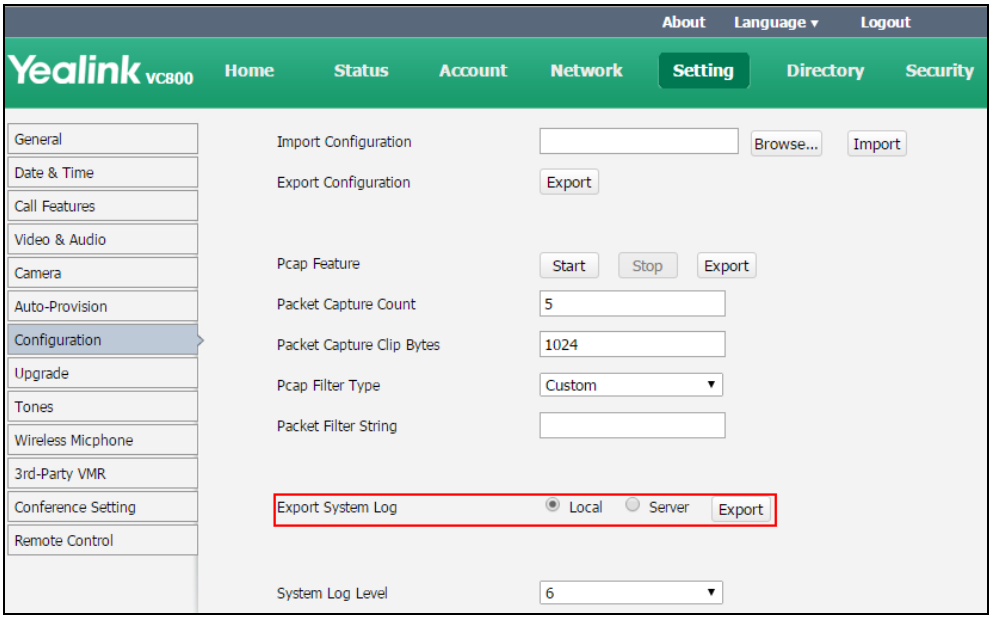



3. Click Confirm to accept the change.

To export a log file to the local system via web user interface:

1. Click on Setting->Configuration.

2. Mark the **Local** radio box In the **Export System Log** field.




3. Click **Export** to open the file download window, and then save the file to your local system.

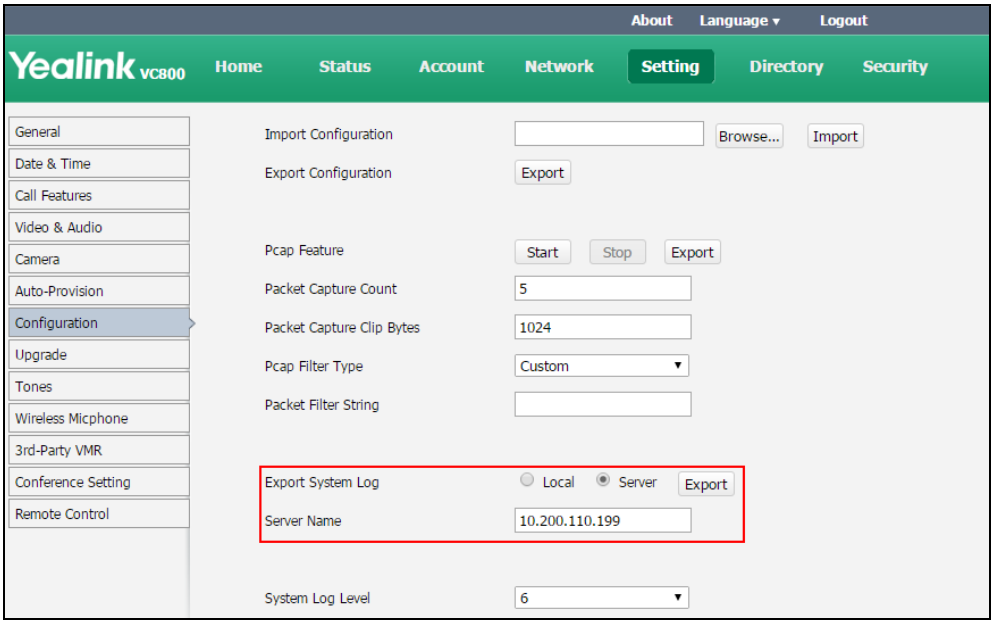
The following figure shows a portion of a log file:

```
  496 root       8876 SW  /yealink/bin/ggsvca_ipp
  497 root       8876 SW  /yealink/bin/ggsvca_ipp
  498 root       8876 SW  /yealink/bin/ggsvca_ipp
  499 root       8876 SW  /yealink/bin/ggsvca_ipp
  500 root       8876 SW  /yealink/bin/ggsvca_ipp
  501 root       8876 SW  /yealink/bin/ggsvca_ipp
  507 root      16424 SW  /yealink/bin/Screen.exe
  508 root      10344 SW  /yealink/bin/sipServer.exx
  509 root      10344 SW  /yealink/bin/sipServer.exx
  515 root      16424 SW  /yealink/bin/Screen.exe
  517 root      16424 SW  /yealink/bin/Screen.exe
  519 root      10344 SW  /yealink/bin/sipServer.exx
  521 root      16424 SW  /yealink/bin/Screen.exe
  522 root      16424 SW  /yealink/bin/Screen.exe
  523 root      16424 SW  /yealink/bin/Screen.exe
  524 root      10344 SW  /yealink/bin/sipServer.exx
  525 root            SW< [IRQ 45]
  526 root      10344 SW  /yealink/bin/sipServer.exx
  527 root      16424 SW  /yealink/bin/Screen.exe
  528 root      16424 SW  /yealink/bin/Screen.exe
  529 root      16424 SW  /yealink/bin/Screen.exe
 1147 root       1788 SWN sleep 1000
 1227 root      10120 SWN ConfigManApp.com
 1228 root       4624 SW  /yealink/bin/mini_httpd -p 80 -d /yealink/html -c cgi
 1229 root       2812 SWN sh -c cd /tmp;ifconfig >> Messages;ps >> Messages;tar
 1230 root       2812 RWN ps
Feb 29 06:01:09 mini_httpd[388]: mini_httpd.c(1510):child process 1227 exit!
Feb 29 06:01:12 mini_httpd[1232]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1232 exit!
Feb 29 06:01:12 mini_httpd[1233]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1233 exit!
Feb 29 06:01:12 mini_httpd[1234]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com, query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1234 exit!
```

**To export a log file to a syslog server via web user interface:**

1. Click on **Setting->Configuration**.

2. Mark the **Server** radio box in the **Export System Log** field.
3. Enter the IP address or domain name of the syslog server in the **Server Name** field.




4. Click **Confirm** to reboot the system immediately.

## 3.2 Capturing Packets

The administrator can capture packets in three ways:

- **Capturing the packets via web user interface** (Only using in issue happen within 20s)
- **Capturing the packets via remote control and USB flash driver**
- **Using the Ethernet software.**

Engineers can analyze the packets to troubleshoot problems.

Packets parameters are described below:

| Parameter | Description | Configuration Method |
|---|---|---|
| Pcap Feature | Start and stop capturing packets or export the captured packets. | Web User Interface |

| Parameter | Description | Configuration Method |
| --- | --- | --- |
| Packet Capture Count | Configures the count of the number of packets to capture.<br>**Default:** 5 | Web User Interface |
| Packet Capture Clip Bytes | Configures the number of bytes (in kb) of the packet to capture.<br>**Default:** 1024 | Web User Interface |
| Pcap Filter Type | Configures the filter type of the packet to capture.<br>**Valid Values:**<br>• **Custom**—Customize the packet filter string.<br>• **SIP or H245 or H225**—Capture SIP, H245 and H225 packets.<br>• **RTP**—Capture RTP packets.<br>**Default:** Custom | Web User Interface |
| Packet Filter String | Customizes the packet filter string.<br>**Syntax:**<br>Protocol+Direction+Host(s)+Value +Logical Operations+Other Expression<br>**Protocol:**<br>Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, | Web User Interface |

| Parameter | Description | Configuration Method |
| --- | --- | --- |
| | moprc, mopdl, tcp and udp.<br>Application-level protocol, such as http, dns and sip are not supported.<br>If no protocol is specified, all the protocols are used.<br>**Direction**:<br>Values: src, dst, src and dst, src or dst<br>If no source or destination is specified, the "src or dst" keywords are applied.<br>For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2".<br>**Host(s)**:<br>Values: net, port, host, portrange.<br>If no host(s) is specified, the "host" keyword is used.<br>For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1".<br>**Logical Operations**:<br>Values: not, and, or. | |

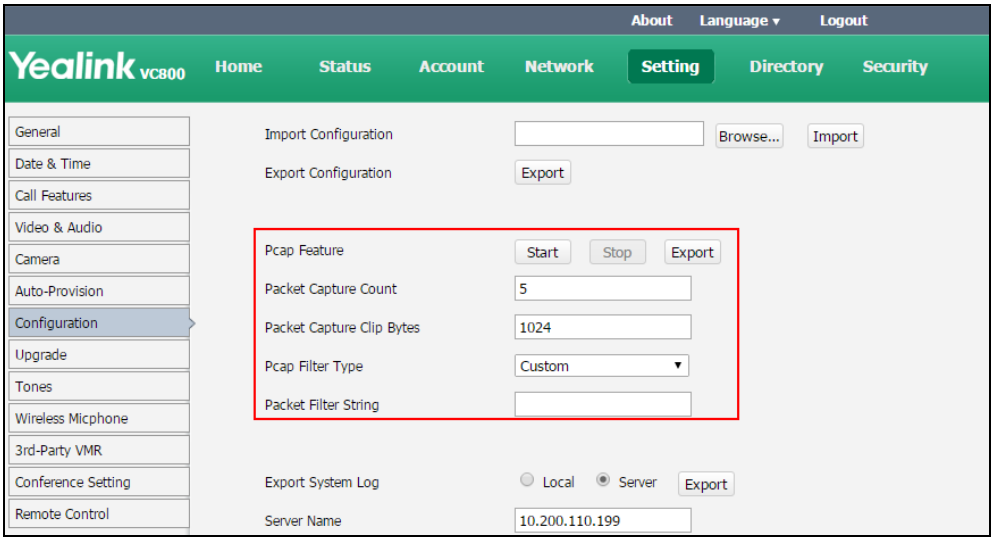
| Parameter | Description | Configuration Method |
| --- | --- | --- |
| | Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right.<br>For example:<br>"not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23".<br>"not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)".<br>**Example**: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8<br>Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and | |

| Parameter | Description | Configuration Method |
| --- | --- | --- |
| | destination IP network 10.0.0.0/8.<br>**Default**: Blank<br>**Note**: It only works if the parameter "Pcap Filter Type" is set to Custom. | |

To capture packets via web user interface:

1. Click on **Setting->Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.

   If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Click **Start** to start capturing signal traffic.
6. Reproduce the issue to get stack traces.
7. Click **Stop** to stop capturing.
8. Click **Export** to open the file download window, and then save the file to your local system.



**To export a PCAP trace via remote control and USB flash driver:**

Before capturing packets, make sure a USB flash driver is connected to VC800/VC500/VC200 codec, VCH50 video conferencing hub or CP960 conference phone and the USB feature is enabled.

1. Long press ⌫ when the system is idle or during a call.
   The display device prompts "Onekey-capture has been turned on, press the Backspace key for 2s to turn off it".
2. Long press ⌫ for 2 seconds to stop capturing packets.
   The packets are saved in the yealink.debug folder on your USB flash driver.

**To capture packets using the Ethernet software:**

Connect the Internet ports of the system and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic. You can also set mirror port on a switch to monitor the port connected to the system.

## 3.3 Getting Information from Status Indicators

In some instances, status indicators are helpful for finding system troubles. Status indicators may consist of the power LED, icons on the status bar of the display device or prompt messages.

The following shows two examples of obtaining the system information from status indicators:

- If a LINK failure of the system is detected, the status bar of the display device prompts "Network disconnected".
- If the power LED does not light, it indicates the system is not powered on.

## 3.4 Analyzing Configuration Files

Wrong configurations may have an impact on your system use. You can export configuration file to check the current configuration of the system and troubleshoot if necessary.

## 3.5 Viewing Call Statistics

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Uplink Bandwidth and Downlink Bandwidth.
- **Video**: Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost(%).
- Protocol used during a call.
- Device information of the far site.
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost(%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.

**To view call statistics during an all via web user interface:**

1. Click **Home**.
2. Hover your cursor over the desired particip, and then click to view call statistics.

**To view call statistics during an all via the remote control:**

1. Press ≡ or OK to open **Talk Menu**.
2. Press ▲ or ▼ to scroll to **Call Statistics** and then press OK.
3. Press ▲ or ▼ to view call statistics for every participant.
4. Press ↩ to return.

**To view call statistics during an all via the CP960 conference phone:**

1. Tap during a call.

The touch screen displays all participants.

2. Tap the desired participant to view call statistics.

## 3.6 Using Diagnostic Methods

The system supports the following diagnostic methods:

- **Audio Diagnose**: Test the audio input device and audio output device.
- **Camera Diagnose**: Test whether the camera can pan and change focus normally.
- **Ping**: Test whether the system can establish contact with a far-site IP address t entered.
- **Trace Route**: Tests the routing path between the local system and the IP address entered.

Above diagnostic methods can be configured using remote control.

Ping and Trance Route can also be configured via web user interface.

**To diagnose audio via the remote control:**

1. Select **More->Setting-> Diagnose.**
2. Select **Audio Diagnose**, and then press OK .
3. Speak into the microphone.
4. Check whether the microphone can pick up audio and play back the audio properly.

   If the system plays back the audio normally, it means that audio works well.
5. Press OK to stop audio diagnostics.

**To diagnose the camera via the remote control:**

1. Select **More->Setting-> Diagnose.**
2. Select **Camera Diagnose**, and then press OK .
3. Press navigation keys to adjust the camera position.
4. Press or to adjust the focus.

   If the camera can move and zoom normally, it means that the c

amera works properly.

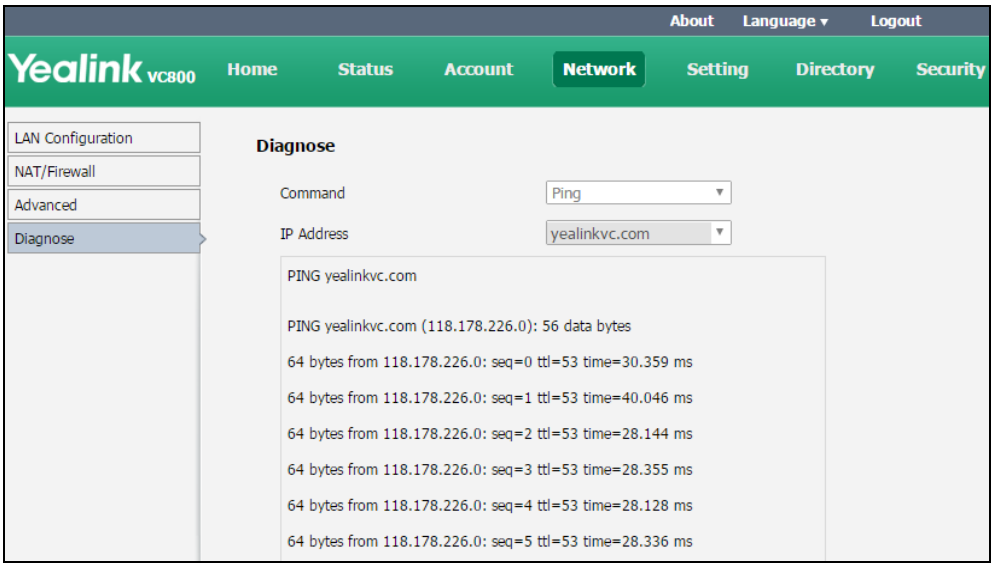
5. Press ↩ to stop camera diagnose.

**To diagnose network via web user interface:**

1. Click on **Network->Diagnose**.
2. Select the desired diagnostic method from the pull-down list of **Command**.
3. Click **Start** to start diagnosing.

   You can also enter any IP address in the **IP Address** field.

   The web page displays the diagnosis:




4. Click **Stop** to complete diagnosing.

   You can click **Copy** to copy the content to the clipboard.

To diagnose network via the remote control:

1. Select **More->Setting-> Diagnose->Ping.**
2. Select **Start**, and then press OK.
3. The system will Ping **yealinkvc.com** address by default. This will check whether the system can establish contact with the public IP address.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Ping** field.

   It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.
5. Press [↩] to return to the Diagnose menu.

**Trace Route:**

1. Select **More->Setting-> Diagnose ->Trace Route.**
2. Select **Start**, and then press OK.
3. The system will trace **yealinkvc.com** address by default.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Trace Route** field.

   If the test is successful, the system lists the hops between the system and the IP address you entered. You can check whether congestion happens via the time cost between hops.
5. Press [↩] to return to the Diagnose menu.

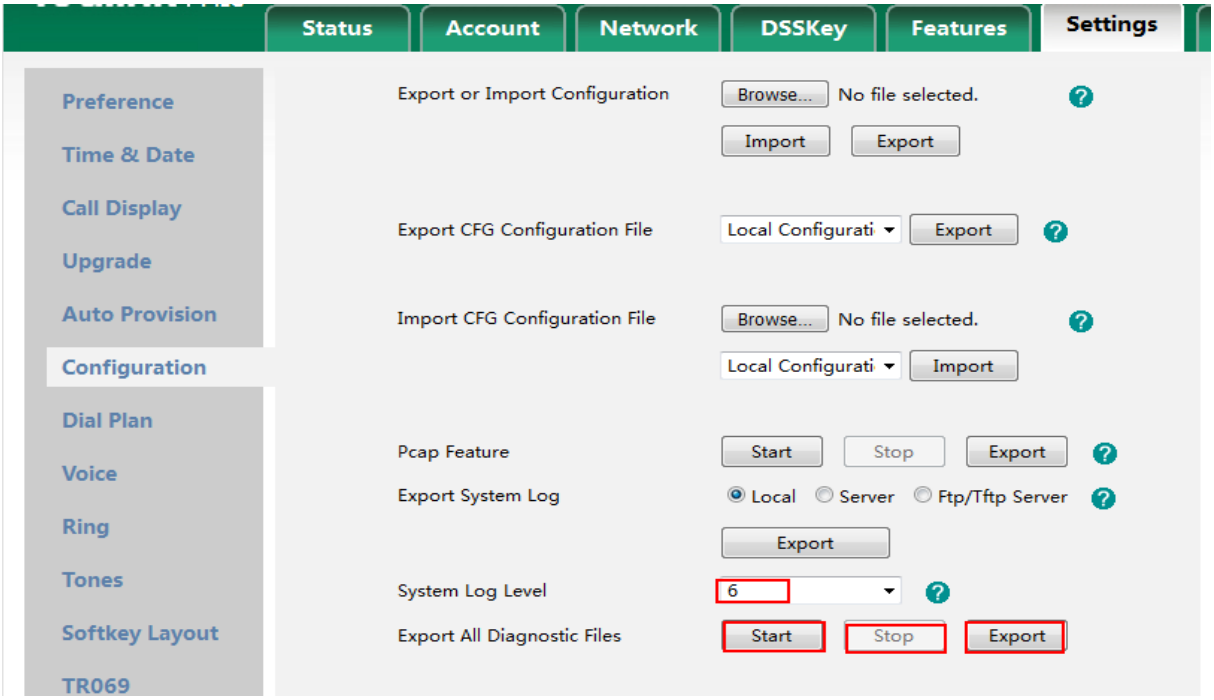
# 4 T49G

## 4.1 Situation 1: Web Interface

**The Issue is easy to be repeated within 20s, then to get information through web interface,**

Please see the picture below and follow the steps:

1) Login to the web interface of the device.
2) Go to **Settings->Configuration**: change the syslog log level to 6 and confirm, press **Start** button.
3) Repeat the issue step by step.
4) Press **Stop->Export** marked in red. You can get **pcap, syslog** and **config.bin** in one package



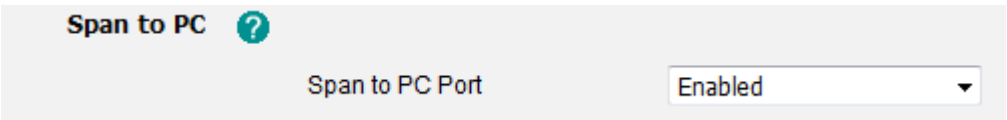

If the firmware on your device is lower than V80, please refer to: http://forum.yealink.com/forum/showthread.php?tid=1319

## 4.2 Situation 2: Span to PC

If you are suffering a randomly happened issue or need to do a long time test, phone's memory will not enough to record the useful information. Please use the method below:

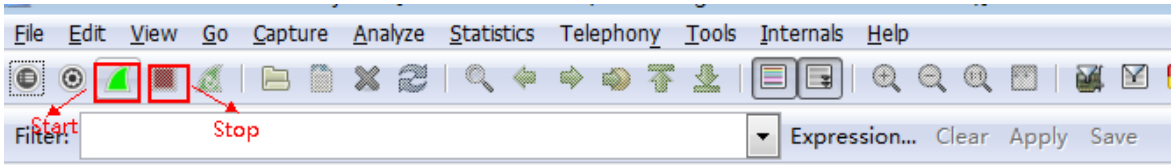
**Capture pcap with Wireshark:**

1) On Yealink IP phone, we have a feature named Span to PC. Please login to the web interface of Yealink Phone and go to **Network->Advance** page to enable Span to PC, then hit **Confirm.**

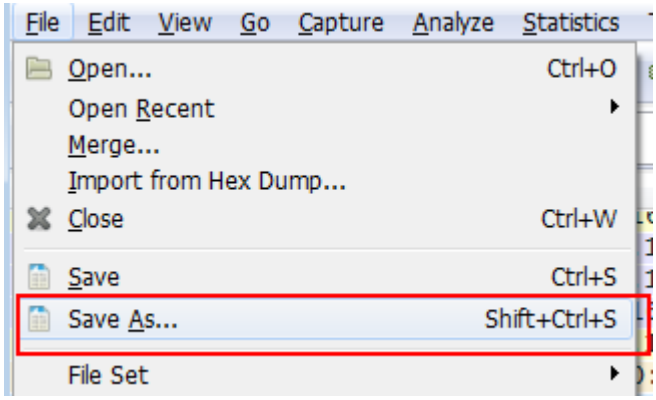



2) Connect PC port of Yealink phone to your PC and Internet port to network.

3) On Wireshark, press **Start**, repeat the steps on phone to reproduce the issue. All the pcap will be recorded. Then hit Stop to stop trace.

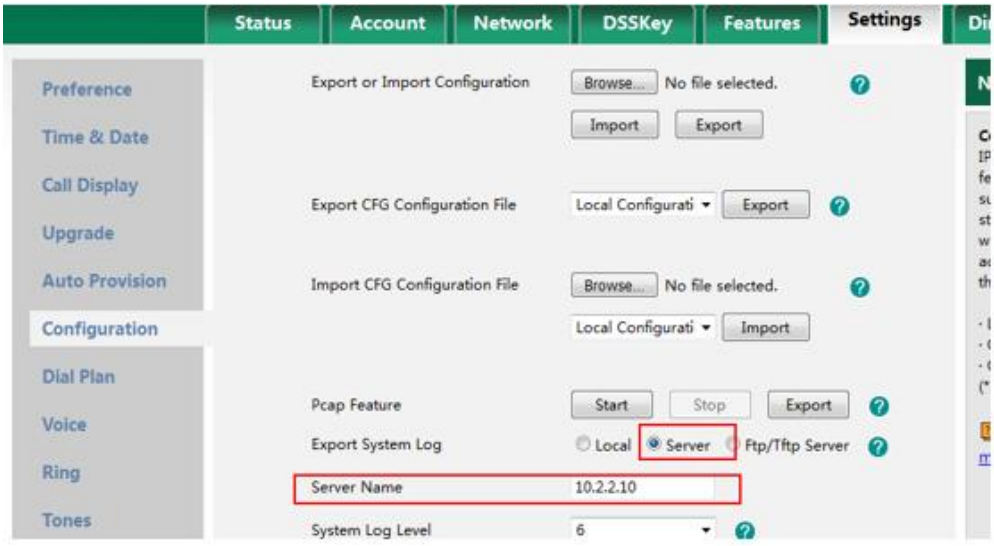



4) Save the file and send to Yealink support.

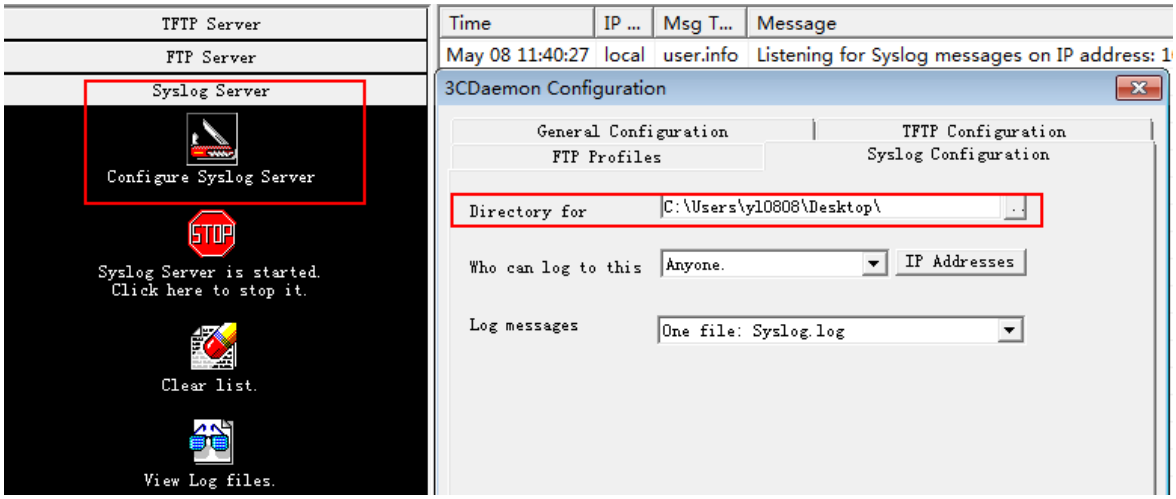



**Capture syslog using syslog server (please do it at the same time with pcap trace):**

1) On Yealink IP phone, please visit web below to change the configuration:




2) On syslog server (take 3CDaemon as an example): configure the syslog server and set up a directory to store the syslog file.




3) Repeat the operations on Yealink phone to reproduce the problem. All the messages will be recorded to syslog server.

# 5 VCD

**Troubleshooting Methods**

The Yealink VC Desktop can provide feedback in two forms, they are packets and call statistics, which can help you to find the problem more easily and then solve it.

You can check the working status in the following two ways and find the fault cause quickly:

- Capturing Packets
- Capturing Logs File
- 
- Viewing Call Statistics

## 5.1 Capturing Packets

You can capture packets using the Ethernet software, and then analyze it to troubleshoot problems.

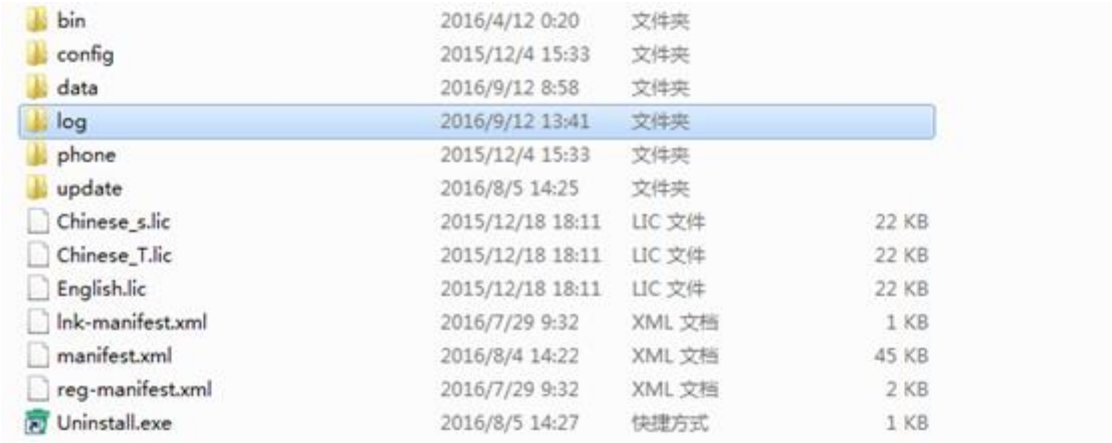
**To capture packets using the Ethernet software:**

Use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

## 5.2 Capturing Logs File

The log of VCD can be found under VCD installation directory. It is named as log. Compress the file and send it to Yealink.

From syslog, Yealink can detail information and confirm what cause an issue.




## 5.3 Viewing Call Statistics

If voice quality is poor during a call, you can enter the Call Statistics screen to view the current status of the call to find out the reason.

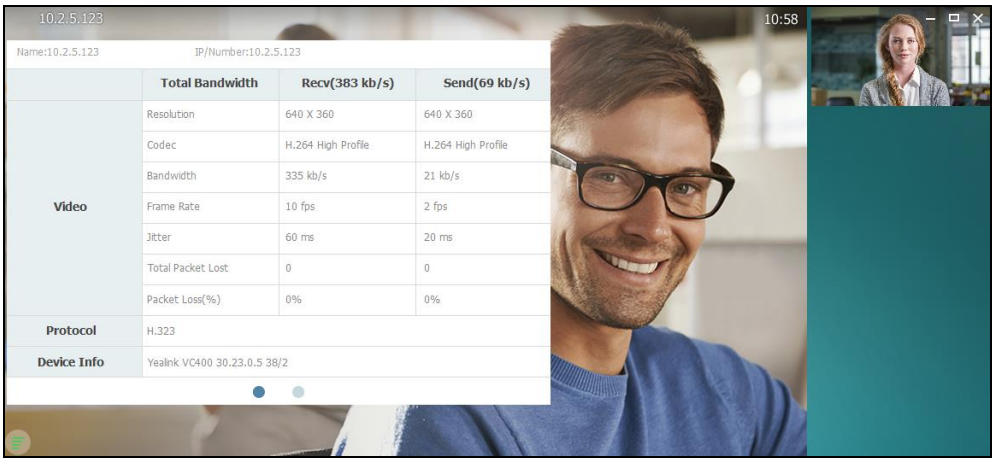
The call statistics mainly contain the parameters about audio, video and share. You can know about the call quality by viewing codec, bandwidth, total packet lost and other parameters. For example, when a delay occurs or the video has a ‘mosaic’ look, you can view the total packet loss to check whether the packet has been lost.

To view call statistics during a call:

1. On the lower-left of your screen, hover the mouse over  .

   The  icon changes according to your network signal strength.

**2.** (Optional) Clic ● to turn to the next page.




You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth**: Receive Bandwidth and Send Bandwidth.
- **Video: Resolution**, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost (%).
- **Audio**: Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost (%)
- Protocol used during a call.
- Device information of the far site.
- **Share**: Resolution, Codec, Bandwidth, Frame Rate.

# 6 VCM

## Troubleshooting Methods

The Yealink VC Mobile can provide feedback by viewing call statistics, which can help you to find the problem more easily and then solve it.

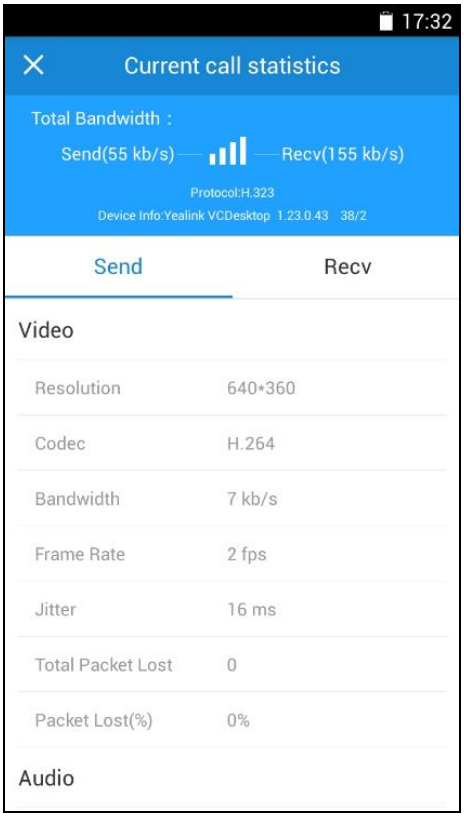
## 3.1 Viewing Call Statistics

If voice quality is poor during a call, you can enter the Call Statistics screen to view the current status of the call to find out the reason.

The call statistics mainly contain the parameters about audio, video and share. You can know about the call quality by viewing codec, bandwidth, total packet lost and other parameters. For example, when a delay occurs or the video has a ‘mosaic’ look, you can view the total packet loss to check whether the packet has been lost.

To view call statistics during a call:

3. Tap .




The icon changes according to your network signal strength.

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Receive Bandwidth and Send Bandwidth.
- Protocol used during a call.
- Device information of the far site.
- **Video**: Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost (%).
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost (%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.

## 3.2 Capturing logs file

**IOS** system: Settings->Diagnoses->send system logs->email to ios_support@yealink.com
**Android** system: VCM installation folder->log->copy log folder and send it to Yealink support team.