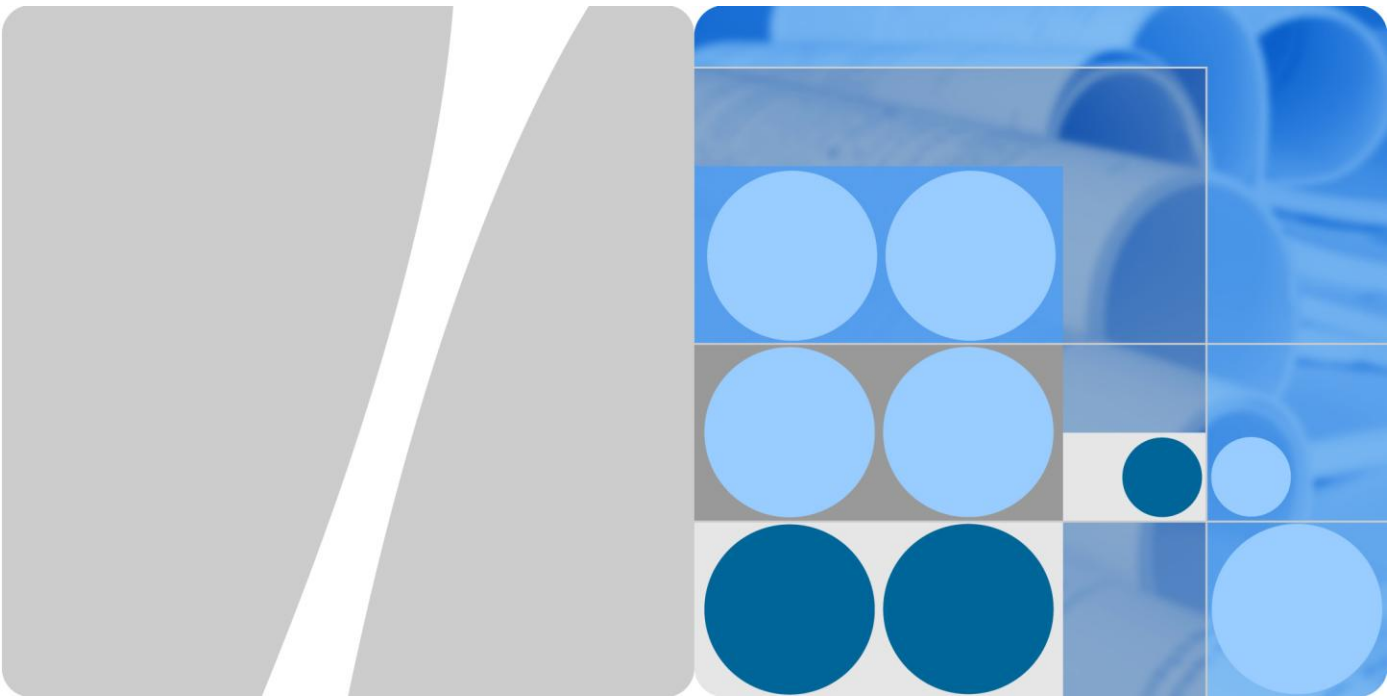


eSpace IAD
V300R001C04
Troubleshooting

Issue 03

Date 2012-06-11

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

This topic describes the flows, the methods for troubleshooting typical faults of the eSpace Integrated Access Device(IAD) and how to analyze and rectify faults.

Contents

About This Document ii

1 Troubleshooting 1

1.1 Overview 1
1.1.1 Fault Level 1
1.1.2 Precautions 2
1.1.3 Troubleshooting Process 2
1.2 Analyzing and Rectifying Faults 6
1.2.1 Call Faults 6
1.2.2 Fax and Modem Faults 25
1.2.3 Other Faults 32
1.3 Common Troubleshooting Methods 49
1.3.1 Observing Device Indicators 49
1.3.2 Collecting System Information (Web) 51
1.3.3 Viewing Call Failure Records 51
1.3.4 Checking the Network Status Automatically 52
1.3.5 Using the PING Command 54
1.3.6 Tracing Route 55
1.3.7 Tracing Signaling 56
1.3.8 Analyzing Packets Captured by Wireshark 57
1.3.9 Capturing the Network Packets Remotely 65
1.3.10 Bad AT0 Grounding 68
1.3.11 AT0 Ground Impedance Test 74
1.4 FAQs 77
1.4.1 Query-Related FAQs 77
1.4.2 Operation-Related FAQs 79

1 Troubleshooting

About This Chapter

This topic describes the flows, the methods for troubleshooting typical faults of the eSpace Integrated Access Device(IAD) and how to analyze and rectify faults.

1.1 Overview

This topic describes the fault severity, precautions, and troubleshooting process.

1.2 Analyzing and Rectifying Faults

1.3 Common Troubleshooting Methods

Common troubleshooting methods include the **ping** command, the **tracert** command (used to trace routes) on the IAD, and the **trace** command (used to trace signaling). The general packet capturing tool is Wireshark.

1.4 FAQs

This topic describes frequently asked questions (FAQs) of users when they use the IAD, including query FAQs and operation FAQs.

1.1 Overview

This topic describes the fault severity, precautions, and troubleshooting process.

1.1.1 Fault Level

Depending on the impact and scope of the fault, faults are classified as either emergency faults or ordinary faults.

Emergent faults refer to those that occur suddenly and affect a wide range of services or devices. Emergency faults, such as host breakdown and service congestion, seriously affect network operations and the quality of service (QoS).

The following faults are emergency faults:

- IAD voice and fax services are unavailable.
- The IAD restarts continuously.

Ordinary faults refer to those that are not emergency faults. The methods for locating and rectifying faults and the applicable reference documents are different for emergency and ordinary faults. For details, see Table 1-1.

Table 1-1 Methods for locating and rectifying faults

Fault Level	Processing Method	Reference Document
Ordinary	Locate and rectify the fault.	See the description for this document.
Emergency	Restore the service that has been affected as soon as possible, and then find the root cause of the fault.	Contact Huawei technical support for help.

1.1.2 Precautions

This topic describes the precautions for troubleshooting.

Before locating and troubleshooting faults, you must read and observe the following precautions:

- Strictly comply with the operation and industry rules and regulations to ensure safety of personnel and devices.
- Observe anti-static safety measures (for example, wear anti-static wrist straps).
- Record details about all the faults that occur during maintenance.
- Record all the important operations, for example, restarting a process and restoring factory settings. An important operation must be performed by qualified operators after the related data is backed up and proper measures are provided against security and emergency events.

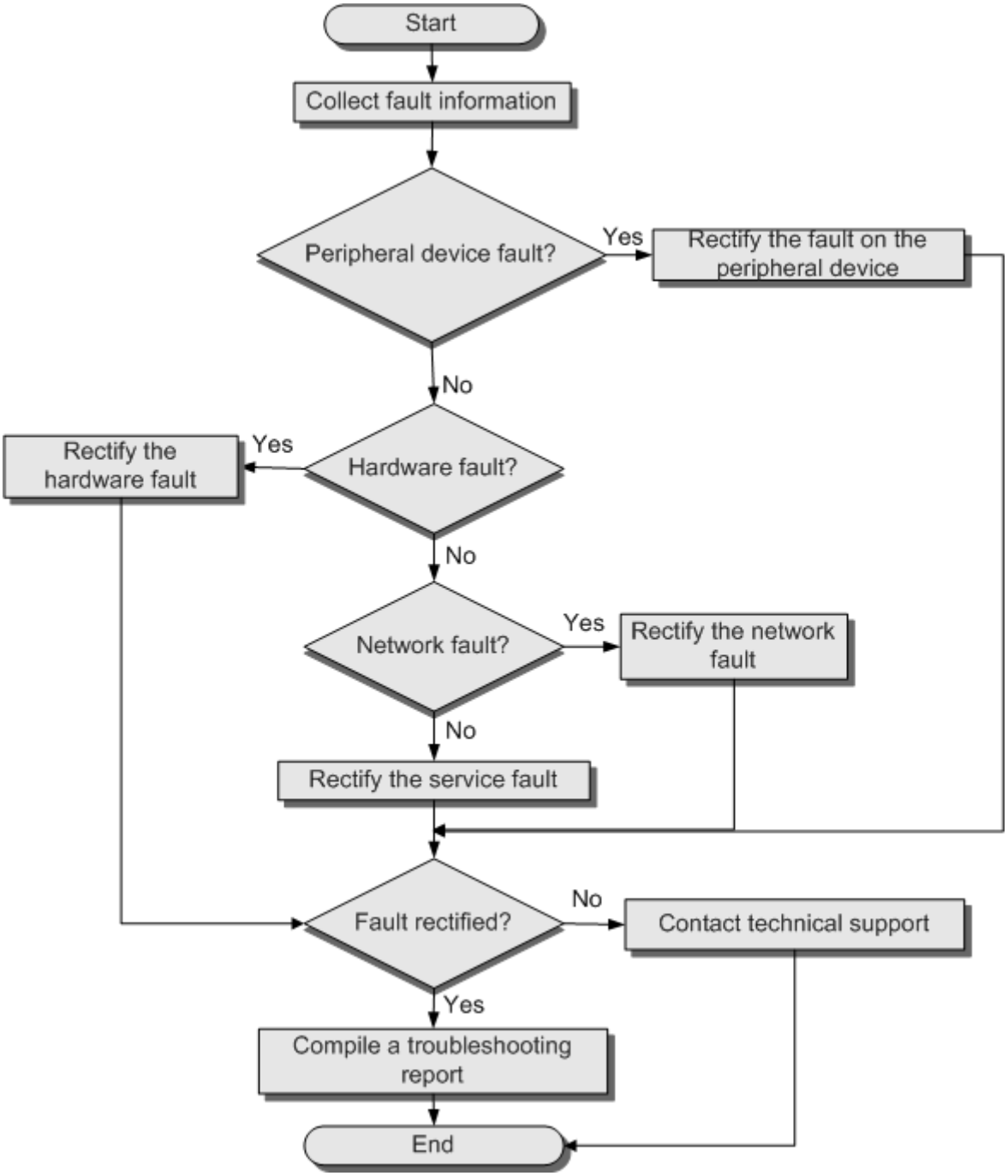
1.1.3 Troubleshooting Process

This topic describes the IAD troubleshooting process.

The IAD troubleshooting process involves collecting fault information, rectifying faults, verifying fault rectification, compiling troubleshooting reports, and obtaining Huawei technical support.

Figure 1-1 shows the troubleshooting flowchart.

Figure 1-1 Troubleshooting flowchart



Collecting Fault Information

Detailed fault description helps to quickly locate faults. The scenario information, networking information, and system information must be collected when a fault occurs.

Scenario Information

This topic describes the fault scenario information that must be collected when a fault occurs. Collect the following scenario information when a fault occurs:

- Fault occurrence time and place
- Fault symptom
- Operations that were performed before the fault occurred
- Measures that have been taken after the fault occurred and the results
- Services that were affected by the fault and the scope of the fault

Networking Information

Networking information helps maintenance personnel to simulate the fault scenario and locate the fault. The maintenance personnel must document and save the following onsite information:

- Physical network, including physical connections and connection media.
- Device names and versions.
- Logical connections between devices.
- Device interconnection information, such as the VLAN, IP address, subnet, gateway, or port of a device.

System Information

When a fault occurs, you can log in to the IAD web management system to obtain system information described in Table 1-2. The procedure is as follows:

1. Log in to the web management system. For details, see the *eSpace IAD Product Documentation*.
2. Choose **Diagnose** > **System Information** from the navigation tree on the left. The system information page is displayed.
3. Click **Download** to download the system information.

   Alternatively, you can view system information directly on the page.

Table 1-2 System information

Item	Description
Version	IAD software version information.
Network port information	Network port configuration information.
User registration status	For SIP services only.
Wildcard group registration status	For SIP services only.
Registration	(For MGCP services only) MG registration status and MGC server information.
VLAN configuration	Tag configuration for various packets generated by the IAD.

Item	Description
Current configuration	Current user configuration on the device.
Alarm history	Latest 10 alarms. To view more alarm information, view downloaded files.

NOTE
For details about how to query other system information, see the *eSpace IAD Product Documentation*.

Determining the Fault Category

Upon receiving fault information, determine whether the fault is an emergency fault. If the fault is emergent, contact Huawei technical support. If the fault is not emergent, locate and rectify the fault according to this document.

Locating and Rectifying a Fault

Troubleshooting refers to locating faults using fault locating methods provided by devices and rectifying the faults using various methods such as maintaining cables, replacing components, and modifying configuration data.

The procedure for locating a fault is as follows:

1. Verify that the fault is a peripheral fault.
2. Verify that the fault is an IAD hardware fault.
3. Verify that the fault is a network fault.
4. Verify that the fault is a service fault.

For details, see the common cases.

Verifying Fault Rectification

After taking measures to rectify a fault, verify that the fault is rectified.

If the fault is rectified, compile a troubleshooting report. If the fault is not rectified, contact Huawei technical support engineers..

Contacting Technical Support

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Email: support@huawei.com

Compiling a Troubleshooting Report

After verifying that a fault is rectified, record the fault rectification process and compile a troubleshooting report for future reference.

The troubleshooting report should include: fault symptom, fault location, fault rectification, and preventive suggestions.

1.2 Analyzing and Rectifying Faults

1.2.1 Call Faults

IAD Phone One-Way Audio Caused by the Defense Against UDP Flood Attacks

Symptom

When a user under the IAD makes a call to an onsite mobile phone user, the mobile phone user cannot hear the calling party's voice for several seconds. This fault occurs when the traffic is high.

Network:

IAD user-IAD-SBC-UMG

Cause

The defense against UDP Flood attacks is enabled for the SBC.

Solution

Step 1 Capture packets on the IAD, between the IAD and the SBC, and between the SBC and the UMG.

Step 2 Analyze the captured packets.

The packets from the IAD are normal; however, packet loss occurs during the transmission between the SBC and the UMG. The defense against UDP Flood attacks is enabled for the SBC. UDP packets bear the voice packets. When the traffic is high, the SBC discards the UDP packets that bear voice packets. Then one-way audio occurs.

Step 3 Disable the defense against UDP Flood attacks for the SBC.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

Voice Tremble Occurs During IAD Calls

Symptom

Voice tremble occurs during IAD calls.

Cause

- Phone fault
- Poor bearer network performance that causes the packet loss between the IAD and the peer gateway device
- Incorrect configuration for the Ethernet port on the IAD upper-level switch

Solution

Step 1 Change a phone, and check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 2.

Step 2 Ping the peer gateway device on the IAD to verify the network performance. If the delay time is less than 40 ms, and no packet loss occurs, the bearer network performance is good.

Step 3 Verify that each device that the media stream passes is configured to the full-duplex mode.

If a device is configured to the full-duplex mode, and the other device is configured to the automatic adaptive mode, the working mode may become half-duplex after negotiation, which affects the voice quality. You can configure the working mode to the full-duplex at a speed of 100 Mbit/s.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

Busy Tone When Picking Up or Dialing a Number

Symptom

- Beeps occur on phones connected to the IAD. Users cannot dial numbers.
- A user always hears the busy tone when dialing a number.

Cause

- The user is not registered with the softswitch.
- The called number does not exist.
- The short-circuit occurs.
- The IAD is faulty.
- The mapping between the cable sequence and ports is incorrect.

Solution

Step 1 Ping the softswitch IP address on the IAD.

- If the softswitch can be pinged, go to Step 2.
- If it cannot be ping through, check whether the network cable is well plugged (ensure that the uplink cable is plugged in the WAN port of the IAD).

Step 2 Run the **display protocol-mode** command to view the protocol used by the IAD.

Step 3 For SIP services, run the **display sip digitmap** command to query the digitmap configuration.

```
TERMINAL(config)#display sip digitmap
```

If the default digitmap **[XABCD*#].T** is deleted and other digitmaps are not configured, you cannot initiate any calls. For details about how to configure digitmaps, see the product document.

Step 4 View the user registration status.

- For MGCP services, run the **display mgcp attribute** command to view the user registration status.
- For SIP services, run the **display sip attribute all** command to view the user registration status.

Step 5 If the user is not registered with the softswitch, verify that the account of the user is enabled on the softswitch and is configured correctly on the IAD.

- For SIP services, you can query the attribute configuration of the SIP services as follows:
  - If the registration fails, check whether the data of the user is configured on the softswitch.
  - If the user ID or password is inconsistent with that on the softswitch, run the **sip user** command to configure the information.
  - If the IP address of the SIP server configured on the IAD is incorrect, run the **sip server** *index* **address** *ipaddress* command to configure the information.
- For MGCP services, you can query the attribute configuration of the MGCP services as follows:
  - If the IP address or domain name of the MGC (registration server) is not configured, run the **mgcp mgc** *index* **address** *ipaddress* command to configure the information. For example, if the IP address of the active MGC is 192.168.10.10, the operations are as follows:

    ```
    TERMINAL(config)#mgcp mgc 1 address 192.168.10.10
    ```
  - If the MG domain name is not the same as that set on the MGC server, run the **mgcp mg-domain-name** *domain-name* command to set the MG domain name again.
  - The interval for the IAD to register with the MGC may be too long after reboot (70s by default), you can run the **mgcp protocol mwd-val** *timer* command to decrease the registration waiting interval. For example, run the following command to set the interval to 20s:

    ```
    TERMINAL(advanced-config)#mgcp protocol mwd-val 20
    ```
  - Ensure that the authentication methods of the IAD and the MGC are consistent. If the authentication methods are inconsistent, run the **mgcp authentication** command in the global configuration mode to configure the authentication method.

Step 6 Check whether the mapping between the cable sequence and ports is correct. For details, see the product documentation.

- If no, reconnect cables.
- If yes, go to Step 7.

Step 7 Run the **display pstnport state** command to query the working status of the port.

For example, to query the user of **port 0** on the IAD132E(T), the operations are as follows:

```
TERMINAL#display pstnport state 0 /*If the port number is not specified, all ports are queried.*/
--------------------------------------
  Port    PortType       State
--------------------------------------
    0      FXS          IDLE
/*FXS is the port for SIP users, FXO is the port for PSTN users. State IDLE indicates that the port is in idle state. If the state is BUSY, it indicates that the port is occupied.*/
```

Step 8 Run the **display dsp-channel** command to query the configuration information such as DSP port status and send/receive gains.

Step 9 Run the **display dsp-chip** command to check whether the DSP chip is in normal state. If the DSP chip is damaged, return the IAD to the factory for repairing.

Step 10 Check whether the pickup event is correctly reported and whether the softswitch responses. For details, see Tracing Signaling.

Step 11 Configure the original IAD according to the configuration data on an IAD that is running properly, and check whether the fault is rectified.

- If yes, the IAD is not faulty.
- If no, go to Step 12.

Step 12 Contact Huawei technical support.

----End

Phones Connected to the IAD Can Ring but Nothing Is Heard After Pickup

Symptom

When outer-office user A dials IAD user B, user B's phone rings, and user A can hear the RBT. However, user B cannot hear user A's voice after user B picks up the phone.

Cause

The signaling carries events that the IAD does not support.

Solution

Step 1 Capture packets on the faulty IAD.

Step 2 Analyze the packets captured on the faulty IAD. Check whether the IAD sends a 518 error code to the softswitch.

NOTE
The IAD does not support softswitch messages that contain FXR/T38 events. Common MDCX messages do not contain FXR/T38 events.

- If yes, change the T38 mode to transparent transmission mode for the softswitch.
- If no, go to Step 3.

Step 3 Contact Huawei technical support.

----End

Phones Connected to IAD Cannot Make Calls to Fixed-Line Phones in a Specified Province

Symptom

Phones connected to IAD cannot make calls to fixed-line phones in a specified province but can make calls to fixed-line phones in other provinces. Fixed-line phones in the province can make calls to phones connected to IAD properly.

Network:

POTS-A-IAD-ZTE NGN

Cause

- Network exceptions
- Incorrect digitmap configuration on the softswitch

Solution

Step 1 Check whether the IAD is properly registered with the softswitch.

- If yes, go to Step 5.
- If no, go to Step 2.

Step 2 Check whether the network is disconnected.

- If yes, rectify the network fault.
- If no, go to Step 3.

Step 3 Run the **display sip attribute** command to view the IAD protocol mode.

Step 4 (For SIP mode only) Run the **display sip attribute** command to view the **digit-map position** value.

- If the digitmap of the softswitch is used, the softswitch sends the digitmap to the IAD in the 200 OK message. Check whether the digitmap delivered by the softswitch is correct, as shown in Figure 1-2.
  - If no, modify the digitmap configuration on the softswitch.
  - If yes, go to Step 6.

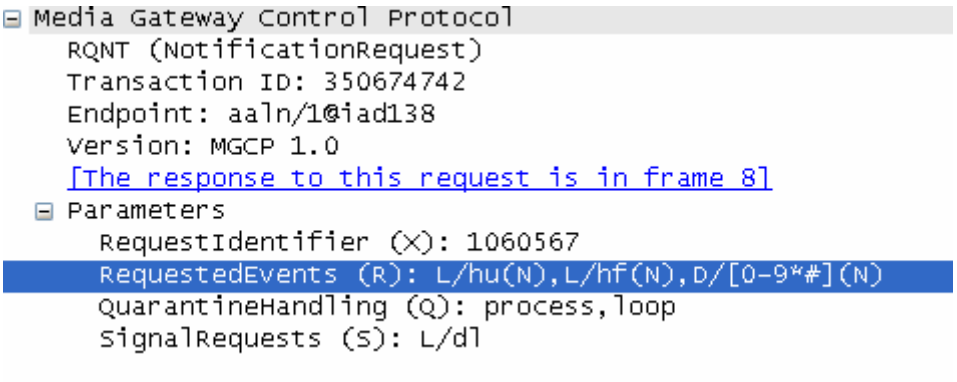
Figure 1-2 Digitmap delivered by the softswitch using SIP

Step 5 (For MGCP mode only) Capture packets to view the digitmap of the softswitch in the MGCP mode.

The softswitch sends the digitmap to the IAD in the RQNT message, as shown in Figure 1-3. If the number length in the digitmap is configured to 11 digits, but the called number consists of 12 digits, only 11 digits of the called number are reported. Therefore, an incorrect number is reported. Check whether the digitmap is correct.

- If no, modify the digitmap configuration on the softswitch.
- If yes, go to Step 6.

Figure 1-3 Digitmap delivered by the softswitch using MGCP



Step 6 Contact Huawei technical support.

----End

A User Cannot Hear Other's Voice on the Phone Connected to IAD After 5 to 10 Minutes

Symptom

When a user uses a phone connected to IAD to talk with others, the user cannot hear others' voice after 5 to 10 minutes. Other users can hear the user's voice.

Cause

- Phone fault
- Peer device fault

Solution

NOTE
The IAD configuration is correct when only one user encounters the problem.

Step 1 Change a phone, and check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 2.

Step 2 Check the peer device.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

POTS Phone Users Cannot Hear the Two-Stage Dialing Tone

Symptom

Users that use POTS phones connected to the IAD cannot hear the two-stage dialing tone.

Cause

- No two-stage dialing function for the office route corresponding to the SoftCo
- Inconsistency between the prefix in the number reported by the IAD and the prefix on the SoftCo
- Early IAD version

Solution

Step 1 Run the **show office selectcode no** *x* command to check whether the two-stage dialing function is enabled for office direction **x** corresponding to the SoftCo.

- If no, enable the function.
- If yes, go to Step 2.

Step 2 Check whether the prefix on the SoftCo maps the digitmap configured on the IAD.

- If no, modify the configuration on the IAD. Assume that the prefix is 99 on the SoftCo, the 99 digitmap must be added on the IAD. Ensure that the minimum length of outgoing numbers corresponding to the prefix on the SoftCo is 0.
- If yes, go to Step 3.

Step 3 Check whether the IAD version is V300R001C03SPC800 or later.

NOTE
Only V300R001C03SPC800 and later versions support the two-stage dialing function.

- If no, upgrade the IAD version to the latest version. For details, see IAD upgrade guide.
- If yes, go to Step 4.

Step 4 Contact Huawei technical support.

----End

000 Is Displayed to UAP3300 Agents for Incoming Calls

Symptom

The PSTN analog trunk is connected to the FXO port on the OSU board of the IAD132E(T). The original number of the analog trunk is 58836176. The access code of the UAP/CTI is 4006113006. A user can dial the original number or the access code. After dialing the access code, the user is connected to the IVR where the user can select the agent service. If the user dials the access code, 000 is displayed to the agent.

Network: PSTN analog trunk-IAD132E(T)-UAP3300

Cause

The possible causes are as follows:

- The calling number has enabled calling line identification restriction (CLIR) service.
- The receiving gain is not properly configured on the IAD132E(T).

Solution

Step 1 Contact the carrier to check whether the CLIR service is enabled for the calling number.

- If yes, disable the service.
- If no, go to Step 2.

Step 2 Run the **dsp fsk gain** command to lower the FSK gain gradually.

CAUTION

Do not reduce the FSK gain to a large scale. Large FSK gain charge may make the IVR two-stage dialing function unavailable. For example, when the gain is reduced to -5, the calling number is displayed to the UAP3300 agent when a phone or mobile phone user dials the access code; however, when the gain is reduced to -7, the IVR two-stage dialing function is unavailable.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

When the IAD Is Connected to the IMS, the Calling Number Cannot Be Correctly Displayed on Phones that are Connected to the IAD

Symptom

The customer requires that the short number is displayed when on-net users make calls on the IMS. However, the country code and the actual number are displayed no matter the call is made between on-net users or from an off-net user to an on-net user.

Cause

The possible cause is incorrect IAD soft parameter settings.

Solution

Step 1 Run the **display sip soft-parameter** command to check whether the **clip-mode** value is **PAI**.

- If yes, run the **sip soft-parameter clip-mode From** command to set **clip-mode** to **From**.
- If no, go to Step 2.

Step 2 Contact Huawei technical support.

----End

Incorrect SessionTimer Setting Causes the Five-Minute Disconnection

Symptom

When the IAD132E(T) is connected to the SoftX3000 using SIP, every call is disconnected after five minutes.

Cause

The possible cause is that SessionTimer is not enabled.

Solution

Step 1 Run the **display sip soft-parameter** command to check whether **SessionTimer** is **on**.

- If no, run the **sip soft-parameter sessionTimer on** command.
- If yes, go to Step 2.

Step 2 Contact Huawei technical support.

----End

Connecting Incoming Calls Through the FXO Port on the IAD Takes as Long as 15 Seconds

Symptom

If the carrier has not enabled the Calling Line Identification Presentation (CLIP) service for a PSTN number, an outer-office user has to spend as long as 15 seconds to connect a call to a PSTN user through the FXO port.

Cause

The possible cause is that the CLIP service has not been enabled for the PSTN number.

Solution

Step 1 Check whether the CLIP service is enabled for the PSTN number. (You can test the CLIP service directly on the PSTN network.)

- If no and the CLIP service is required, contact the carrier to enable the CLIP service.
- If no and the CLIP service is not required, go to Step 2.

Step 2 Configure the FXO port.

Run the following command:

```
TERMINAL(config)#sip user 0 fxo-clip no
```

NOTE

This command is available only for IADV300R001C03SPC900, IADV300R001C04SPC300, and later versions. You are advised to upgrade older versions to one of the preceding versions.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If yes, go to Step 4.

Step 4 Contact Huawei technical support.

----End

What should I do if the indicator of a phone is off when the phone is picked up?

Symptom

The IAD registration status is normal but the indicator of a connected phone is off when the user picks up the phone.

Possible Cause

The possible causes are as follows:

- The phone is faulty.
- The device is faulty.
- The subscriber line is unavailable.
- The power supply is abnormal.

Solution

Step 1 Replace the phone with another one.

- If the problem does not occur, the original phone is faulty. Replace the original phone.
- If the problem persists, go to Step 2.

Step 2 Connect the phone to the telephone line of the IAD and check whether there is feed.

- If yes, ensure that the cables in the cable distribution frame (CDF) are correctly connected.
- If no, go to Step 3.

Step 3 Use a telephone line delivered with the device to replace the existing one.

- If the problem is resolved, the procedure ends.
- If the problem persists, go to Step 4.

Step 4 Replace the board.

- If the problem is resolved, the procedure ends.
- If the problem persists, go to Step 5.

Step 5 Check the power supply, especial at small ports.

NOTE

- IAD1224: 110/220 V AC or 48 V DC.
- IAD132E(T): 100-240 V AC
- IAD208E(M) and IAD104H: 12 V DC (using the power adapter to convert 100-240 V AC to 12 V DC)
- IAD101/102H: 5V DC (using the power adapter to convert 100-240 V AC to 5 V DC)

- If yes, go to Step 6.
- If no, select the correct power supply.

Step 6 Contact Huawei technical support engineers.

----End

A Phone Connected to the IAD Does Not Ring for Incoming Calls

Symptom

Sometimes, a phone connected to the IAD does not ring for incoming calls. Users can use the phone to make outgoing calls.

Cause

The possible causes are as follows:

- The phone model is not supported.
- PCs connected to the IAD affect the voice service.

Solution

Step 1 Replace the phone with a phone of another model, and check whether the fault is rectified.

- If yes, the phone model is not supported. Replace the phone.
- If no, go to Step 2.

Step 2 Compare signaling streams and check whether the signaling stream is normal when the fault occurs.

- If yes, go to Step 3.
- If no, locate the fault based on the abnormal signaling.

Step 3 Check whether a PC or cascaded switch is connected to the IAD.

- If yes, connect the PC or cascaded switch to the upstream switch, because PCs or data communication devices cannot be directly connected to the IAD.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

When IAD Users Make Outgoing Calls Using the IMS, the Connection Rate Is Only 10%

Symptom

When IAD users under the SoftCo make outgoing calls using the IMS, the connection rate is only 10%. Incoming calls are normal.

Cause

The possible cause is that multiple IADs use one EID on the softswitch.

Solution

Step 1 Use the Wireshark to capture IAD1280 SIP signaling, and analyze these messages. If the softswitch returns a 403 error response message to the IAD INVITE message, the server recognizes but refuses to execute the request message.

Step 2 Check the data configuration, and clear conflict configuration to ensure that only one IAD uses one EID on the softswitch.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

When the IAD Is Connected to the IMS, Users Cannot Make Calls to Each Other

Symptom

When the IAD is connected to the IMS, users cannot make calls to each other.

Cause

The possible cause is that signaling interaction is abnormal.

Solution

Step 1 Capture IAD packets to analyze the signaling stream. If the IMS returns an error response message to the IAD INVITE message, the IMS does not support the URI TEL format that is used by the INVITE message.

Step 2 Run the **sip soft-parameter support-telurl off** command to change the TEL format to SIP format.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

When the IAD Is Directly Connected to the IMS, Blind Transfer or Transfer upon Inquiry Failed

Symptom

When the IAD is directly connected to the IMS, blind transfer or transfer upon inquiry failed. User A makes a call to user B (IMS user). The call is transferred to user C through the blind transfer or transfer upon inquiry service. When user B hangs up, users A and C are disconnected.

Cause

The possible cause is that signaling interaction is abnormal.

Solution

Step 1 Capture IAD packets to analyze the signaling stream. Normal signaling messages and signaling messages generated when the fault occurs have different TEL URI in the **from** and **to** fields. IMS messages do not support TEL URI.

Step 2 Run the **sip soft-parameter support-telurl off** command to disable **support-telurl**.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

Calls Between IAD Users Are Disconnected Sometimes

Symptom

A SoftCo9500 and 23 IADs are connected to the external network through the PRA trunk. Calls between IAD users or Outer-Office users are sometimes disconnected. The line disconnected is random. When a call is disconnected, a registration failure occurs on the IAD, but is automatically rectified in 10 seconds.

Cause

The possible cause is that the softswitch restricts the registration message traffic, resulting in registration of multiple times.

Solution

Step 1 Capture and analyze IAD logs. If the softswitch does not respond to the registration message sent by the IAD, the IAD sends a BYE message to terminate the session and re-sends registration messages until the registration is successful.

Step 2 Check whether the traffic is restricted on the softswitch.

- If yes, run the **fpga set limitflux enable protocol sipreg flux 50** command on the softswitch to disable the traffic restriction.
- If no, go to Step 3.

Step 3 Configure a different registration duration on the IAD. For example, run the **sip server 0 address 192.166.1.16 expire-time 200** command.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

One-Way Voice

Symptom

When making calls through the IAD, the calling party or the called party cannot hear any voice.

Cause

The possible causes are as follows:

- The local device cannot receive the RTP stream from the peer device due to network problems.
- The IAD's uplink port is set to half-duplex mode.
- The called party enables the RTP encryption function.
- The SIP signaling media negotiation is abnormal.

Solution

Step 1 Run the **display interface** command in the Ethernet switch mode to view the duplex mode of the IAD network port. If the duplex mode is half-duplex, run the **duplex** command to set the IAD to auto-negotiation mode.

Step 2 View the status of the network connection between the IAD and the opposite gateway (for example, IAD or trunk gateway). Firewalls or NATs between devices may cause the one-way data blocking. In this case, you can run the **ping** *a.b.c.d* command to check the fault cause.

Step 3 Ensure that the called party has not enabled the RTP encryption function. The IAD does not support the RTP encryption function.

Step 4 Capture and analyze IAD SIP signaling packets. Check whether the **session attribute** value in the IAD INVITE message is **sendrecv**.

- If the value is **sendonly**, the IAD sends RTP packets but cannot receive voice data packets, resulting in the one-way voice fault.
- If the value is **sendrecv**, go to Step 5.

Step 5 Check whether the IP address in the **connection information** attribute in the INVITE message sent by the IAD is the IP address of the local device. The peer device sends the RTP stream to the IP address in this attribute.

- If no, IAD users cannot hear the voice from the peer device.
- If yes, go to Step 6.

Step 6 Capture IAD packets to check whether the peer device has sent RTP packets to the local device.

- If yes, go to Step 7.
- If no, the local device cannot hear the voice from the peer device. Check the peer device.

Step 7 Contact Huawei technical support.

----End

No Voice

Symptom

The calling parties cannot hear each other.

Cause

The possible causes are as follows:

- Network quality issue
- Opposite gateway issue
- Inconsistence of codec between gateways
- IAD device issue

Solution

1. Check the status of the network that connects the IAD with the opposite gateway (IAD or trunk gateway) first. Firewalls or NATs between devices may cause the two-way data blocking. You can run the **ping** *a.b.c.d* command to check the network status.
2. When the IAD cooperates with some of the softswitches, no-voice faults may occur because the codecs supported by the gateways are inconsistent. You can run the **trace** command to trace signaling to determine the fault.
3. Run the **display rtp state** command to query the RTP statistics.
4. Check whether the fault is rectified.
   - If yes, the procedure ends.
   - If no, go to 5.
5. Contact Huawei technical support.

Phones Connected to the IAD Cannot Make Calls to Numbers Starting with 800

Symptom

Network: IAD-ZTE softswitch.

Phones connected to the IAD can make calls to other phone numbers except numbers starting with 800.

Cause

The possible cause is that the digitmap does not match.

Solution

Step 1 Capture IAD network packets and obtain MGCP packets. Check the digitmap information contained in RQNT messages. The digitmap delivered from the softswitch is **0[2-9]xxxxxx**. When the called number 08008302118 is matched to the digitmap, the number 08008302 is reported, which results in the call failure.

Step 2 Modify the digitmap delivered by ZTE softswitch to 0[2-9]xxxxxxXXX.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

No Prompt Tone Can Be Heard When a Phone Connected to the IAD Is Picked Up; When a User Dials the Number of the Phone, an Announcement Is Played, Indicating that the Phone Is on a Call

Symptom

No prompt tone can be heard when a phone connected to the IAD is picked up; when a user dials the phone, an announcement is played, indicating that the phone is on a call.

Cause

The possible cause is that the port is faulty.

Solution

Step 1 View the port registration status and port status.

1. Run the **display sip attribute** *port* command to view the port registration status.
2. Run the **display pstnport state all** command to view the port status.

The port is registered properly, but is in the locked state.

Step 2 Replace the IAD with an IAD that is running properly, and check whether the fault is rectified.

- If yes, the IAD board is faulty. Replace the IAD board.
- If no, go to Step 3.

Step 3 Contact Huawei technical support.

----End

IAD Registration Is Successful, but Intra-Office Calls Failed

Symptom

IAD registration is successful, but Intra-Office calls failed.

Cause

The possible cause is that **support-telurl** is set to **on**.

Solution

Step 1 Run the **display sip support-telurl** command on the IAD to view the **Support-Telurl** value. By default, the value is **off**. If the value is **on** and the domain name of the SIP Server is blank, the IAD cannot generate SIP messages. Run the **sip support-telurl off** command.

Step 2 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 3.

Step 3 Contact Huawei technical support.

----End

How to deal with slow call setup?

Symptom

It takes a long time to set up calls initiated by phones connected to an IAD.

Possible Cause

The possible causes are as follows:

- The network quality is poor.
- The digitmap used by the called number is unavailable on the IAD.

Solution

Step 1 Ping the IP address of the Softswitch to check the delay time and packet loss.

- If the delay time is too long and packet loss occurs, the network performance is poor.
- If the network is normal, go to Step 2.

Step 2 Log in to the IAD and run the **display sip digitmap** command to view the digitmap configuration in global mode. If the called number is 159xxxxxxxx, add 159xxxxxxxx to the digit map to ensure that numbers starting with 159 can be quickly connected.

NOTE
To enable quick call connection, you can press the pound key (#) after dialing the called number.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support engineers.

----End

Voice Intermittence

Symptom

Voice of calls through the IAD is intermittent.

Cause

The network quality is poor.

Solution

1. Test the network quality (you can use the **ping** *a.b.c.d* command on the IAD to perform a simple test), or observe whether RTCP alarm exists on the IAD.

   The definition of the voice and video quality test network model in NGN is as follows:

Network Status	Packet Loss Ratio	Network Delay	Jitter
Good network	0	0 ms	0 ms
Poor network	1%	100 ms	20 ms
Extreme network	5%	400 ms	60 ms

2. If the network quality is poor (time delay > 100 ms), you can change the codec of the IAD. The default codec of the IAD is G.711A, you can run the **sip send-capability voip pri** command to change the codec to G.729 to adapt the poor network environment. The operations are as follows:

   ```
   TERMINAL(advanced-config)#sip send-capability voip pri 0 G729 ptime 30ms
   ```

   If voice intermittence still exists, you are advised to improve the network quality.

NOTE

When the G.711A codec is being used, one audio call of the IAD can occupy 100 Kbit/s of bandwidth at most.

What should I do if no prompt tone is played upon hangup?

Symptom

The IAD has been successfully registered with the softswitch using the MGCP, but users does not hear any prompt tone when hanging up a phone.

Possible Cause

The possible causes are as follows:

- The same IP address has been configured for MG domain names on the softswitch.
- Signaling delivered by the softswitch is abnormal.

Solution

Step 1 Check whether the IP addresses configured for MG domain names are the same on the softswitch.

- If the IP addresses are the same, modify the configuration.
- If the IP addresses are different, go to Step 2.

Step 2 Capture packets to check whether the signaling delivered by the softswitch is normal.

- If the signaling is normal, go to Step 3.
- If the signaling is abnormal, check the softswitch.

Step 3 Contact Huawei technical support engineers.

----End

1.2.2 Fax and Modem Faults

Faxes Can Be Received but Cannot Be Sent

Symptom

A fax machine connected to the IAD can receive but cannot send faxes.

Cause

The possible causes are as follows:

- Poor bearer network performance
- Inconsistent faxing modes
- Incorrect softswitch type

Solution

Step 1 Ping the softswitch IP address to check the delay time and packet loss.

- If the delay time is too long and packet loss occurs, the bearer network performance is poor. Verify the network connection.
- If the network is normal, go to Step 2.

Step 2 Check the consistency between the faxing modes of the softswitch and IAD.

Consult related personnel about the method for viewing the softswitch faxing mode.

To view the IAD faxing mode, proceed as follows:

1. Run the **display protocol-mode** command to view the protocol used by the IAD.
2. If MGCP is used, run the **display mgcp soft-parameter** command to view the faxing mode. If the faxing mode is different from that of the softswitch, run the **mgcp soft-parameter fax-mode** command to change the faxing mode. If the faxing modes are the same, go to Step 3.
3. If SIP is used, run the **display sip send-capability** command to view the faxing mode. If the faxing mode is different from that of the softswitch, run the **sip send-capability fax pri** command to change the faxing mode. If the faxing modes are the same, go to Step 3.

Step 3 Check the softswitch manufacturer and the softswitch type of the IAD.

The softswitch type configured on the IAD must be the same as the actual softswitch type.

1. Run the **display protocol-mode** command to view the protocol used by the IAD.
2. If MGCP is used, run the **display mgcp soft-parameter** command to view the softswitch type of the IAD. If the softswitch type of the IAD is different from the actual softswitch type, run the **mgcp soft-parameter mgc-type** command to change the softswitch type. If the softswitch types are the same, go to Step 4.
3. If SIP is used, run the **display sip soft-parameter** command to view the softswitch type of the IAD. If the softswitch type of the IAD is different from the actual softswitch type, run the **sip soft-parameter soft-switch-type** command to change the softswitch type. If the softswitch types are the same, go to Step 4.

Step 4 Contact Huawei technical support.

----End

IAD Fails to Send Faxes to ZTE Softswitches

Symptom

In the MGCP mode, the IAD fails to send faxes to ZTE ZS SS10.

Cause

By default, the T30 mode is configured on ZTE softswitches for ZTE IADs that use the H248 protocol. When Huawei IADs send or receive faxes using MGCP, the softswitch cannot recognize all information and the faxing fails.

Proprietary protocols are used to send heartbeat messages for devices of all manufacturers, and therefore 522 message will be displayed. This error does not affect communication.

Solution

Step 1 Configure a static attribute template, default attribute template, and packet template when adding an IAD.

Step 2 Modify the static attribute template.

When the fax service is enabled, MGCP faxing modes T30, T38, and T30 or T38 are displayed on the static attribute template.

Select T30.

Step 3 Modify the default attribute template.

In the SDP description, select **Fax**, and change the codec mode and packaging duration to **PCMA** and **20** respectively. If the default value is used, 510 error occurs in the faxing process.

Step 4 Modify the package template.

Select a package from the **IPFAX** drop-down list box, and add the package.

Step 5 Run the **#mgcp soft-parameter fax-mode 711v2 mgc-type zte** command to configure the faxing mode on the IAD.

Step 6 If the fault persists after you perform the preceding operations, contact Huawei technical support.

----End

Fax Machines Connected to the Counter Work Improperly

Symptom

Network:

Softswitch-IAD-Counter-Fax machine

A fax machine connected to the IAD through the counter cannot receive or send faxes properly.

Cause

The possible causes are as follows:

- Poor bearer network performance
- Inconsistent faxing modes
- Incorrect softswitch type
- Cable loss

Solution

Step 1 Ping the softswitch IP address to check the delay time and packet loss.

- If the delay time is too long and packet loss occurs, the bearer network performance is poor. Verify the network connection.
- If the network is normal, go to Step 2.

Step 2 Check the consistency between the faxing modes of the softswitch and IAD.

Consult related personnel about the method for viewing the softswitch faxing mode.

To view the IAD faxing mode, proceed as follows:

1. Run the **display protocol-mode** command to view the protocol used by the IAD.
2. If MGCP is used, run the **display mgcp soft-parameter** command to view the faxing mode. If the faxing mode is different from that of the softswitch, run the **mgcp soft-parameter fax-mode** command to change the faxing mode. If the faxing modes are the same, go to Step 3.
3. If SIP is used, run the **display sip send-capability** command to view the faxing mode. If the faxing mode is different from that of the softswitch, run the **sip send-capability fax pri** command to change the faxing mode. If the faxing modes are the same, go to Step 3.

Step 3 Check the softswitch manufacturer and the softswitch type of the IAD.

1. Run the **display protocol-mode** command to view the protocol used by the IAD.
2. If MGCP is used, run the **display mgcp soft-parameter** command to view the softswitch type of the IAD. If the softswitch type of the IAD is different from the actual softswitch type, run the **mgcp soft-parameter mgc-type** command to change the softswitch type. If the softswitch types are the same, go to Step 4.
3. If SIP is used, run the **display sip soft-parameter** command to view the softswitch type of the IAD. If the softswitch type of the IAD is different from the actual softswitch type,

run the **sip soft-parameter soft-switch-type** command to change the softswitch type. If the softswitch types are the same, go to Step 4.

Step 4 Connect the fax machine to the IAD without the counter, and check whether faxes can be sent and received properly.

- If yes, exceptions occur on the cable between the counter and the fax machine. You can connect the cable again.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

FAX Machines Connected to the IAD Cannot Send or Receive Faxes

Symptom

Fax machines connected to the IAD cannot send or receive faxes.

Cause

The possible causes are as follows:

- The fax service is not enabled on the softswitch.
- The fax machine is faulty.
- The network quality is poor.
- The media negotiation is abnormal.
- T.38 packets are not supported by the IAD.

Solution

Step 1 Check whether the fax service is enabled on the softswitch.

NOTE
The fax service must be enabled separately on some softswitch models.

Step 2 Check whether paper is put correctly in the fax machine. If the manual fax operation fails, the fax machine may send non-standard signaling. Ask the called party to press the start button on the fax device first, and then press the start button after hearing the prompt tone.

Step 3 Verify that the softswitch is grounded properly. Use a fax machine from another manufacturer, and check whether the fault is rectified.

- If yes, the fax machine is faulty. Replace the fax machine.
- If no, go to Step 5.

Step 4 Check the fax configuration.

- If SIP is used, run the **display sip send-capability** command to view the fax priority configuration.
- If MGCP is used, run the **display mgcp soft-parameter** command to view the MGCP software parameters:

```
TERMINAL#display mgcp soft-parameter
MGC-TYPE          REGISTER-MODE     CW-TONE-MODE
```

```
SoftX            Wildcard         mgc
=========================================================
FAX-MODE          HOLD-FLAG         CHARGE CONTROL
T38v3             Off              on
=========================================================
DUAL-TONE-DELAY
200 ms
```

NOTE

The faxing modes supported in the MGCP service are as follows:

- 711v2: Transfer mode (transparent)
- t38v2: T.38 mode
- t38v3: T.38 or transfer mode

Step 5 Verify that bearer network quality is good. For network quality definition, see Table 1-3.

Table 1-3 Network quality definition

Network Status	Packet Loss Ratio	Network Delay (ms)	Jitter (ms)
Good	≤ 0.1%	≤ 40	≤ 10
Poor	≤ 1%	≤ 100	≤ 20
Bad	≤ 5%	≤ 400	≤ 60

- If the network quality is poor, change the faxing mode. For relationships between fax/modem service performance and network quality, see Table 1-4.

Table 1-4 Fax/Modem service performance and network quality

Service Type		Performance in a Good Network	Performance in a Poor Network	Performance in a Bad Network
Modem	Transfer	Proved	Failed	Failed
Fax	Transfer	Proved	Failed	Failed
	T.38	Proved	Proved	Failed

For example:

- If SIP is used, run the **sip send-capability fax pri** command to set the faxing mode to T.38.

```
TERMINAL(advanced-config)#sip send-capability fax pri 0 t38 redundancy 2
```

NOTE

If the fax encoding/decoding priority configuration fails, run the **display sip send-capability** command to view the configuration result, and find out the priority for the required encoding/decoding type. Run the **undo sip send-capability fax pri** command to delete the priority, and run the **sip send-capability fax pri** command to set the priority again.

- If MGCP is used, run the **mgcp soft-parameter** command to set the faxing mode to t38v2.

  ```
  TERMINAL(advanced-config)#mgcp soft-parameter fax-mode t38v2
  ```

- If the network quality is good, go to Step 6.

Step 6 Capture IAD network packets to verify that both ends of media negotiation use the same codec. If downspeeding is performed, check whether downspeeding is successful.

- If no, the network quality is poor.
- If yes, go to Step 8.

Step 7 Check whether the packet consists of the following parameters:

- a=T38FaxFillBitRemoval:0
- a=T38FaxTranscodingMMR:0
- a=T38FaxTranscodingJBIG:0
- a=T38FaxUdpEC:t38UDPRedundancy

These parameters are not supported by the IAD.

Step 8 Check whether echo exists in the voice sent from the core network.

- If yes, contact the core network management personnel to find out the time when the echo is generated.
- If no, go to Step 9.

Step 9 Contact Huawei technical support.

----End

How to transfer remote faxes

Symptom

Faxes failed to be transferred.

Possible Cause

The V21 timer is incorrectly set.

Solution

Step 1 Check the setting of the V21 timer.

- For the IAD208E(M) and IAD132E(T), choose **Advanced Configuration** > **User Port Attribute**, or run the **display pstnport attribute** command to check the setting of the V21 timer. Generally, the value is set to 10 seconds. If the IAD can detect the signals sent from the timer in 10 seconds, the fax process starts. If the IAD fails to detect signals in 10 seconds, the modem service process starts.
- For the IAD1224, choose **Advanced Configuration** > **Setting the Fax Parameters**, or run the **display dsp fax-tone** command to check the setting of the V21 timer. Generally, the value is set to 500 (10 ms), that is, 5 seconds. If the IAD receives signals sent from the timer within 5 seconds, the fax process starts. If the IAD fails to detect signals in 5 seconds, the modem service starts.

Step 2 If the configuration is incorrect, adjust the setting as follows:

- For the IAD208E(M) and IAD132E(T), choose **Advanced Configuration** > **User Port Attribute** and adjust the V21 timer setting on the displayed page, or run the **pstnport attribute set** command to adjust the setting.
- For the IAD1224, choose **Advanced Configuration** > **Setting the Fax Parameters** and adjust the V21 timer setting on the displayed page, or run the **dsp fax-tone set** command to check the setting.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If yes, go to Step 4.

Step 4 Contact Huawei technical support engineers.

----End

Modem Dialing Failure

Symptom

Users on the IAD fail to dial up to the network (or dial the opposite modem).

Cause

- The service configuration of the softswitch is incorrect.
- The duration of the V21 timer on the IAD is too long. (The current default value is 10 ms.)
- The function of checking V21 signal that the calling party receives is enabled.

Solution

1. Ensure that the configuration of the softswitch of the user is correct. For example, for Huawei softswitch SoftX3000, deselect the no fax / no modem option in the gateway property.
2. You can shorten the duration of the V21 timer (scope: 0s to 30s) based on the site requirements. For example, to set the duration of the V21 timer to 10s, run the following command:

```
TERMINAL(advanced-config)#t38 v21TimerLen 10
```

NOTE
If the Internet access speed rate through modem is low, you can also use this method.

3. You can run the following command to check whether you have enabled the function of checking V21 signal that the calling party receives.

```
TERMINAL(config)#display system soft-parameter

      system soft-parameter
-------------------------------------
BusyTone Type    : DSP
Caller Detect V21 : on
-------------------------------------
```

If **Caller Detect V21** is **on**, run the following command to disable the function:

```
TERMINAL(advanced-config)#system soft-parameter caller-detect-v21 off
```

NOTE

If the function is enabled, the IAD will stop the modem service and start the fax service when the calling party receives the V21 signal sent by the called party.

4. If the fault persists, contact Huawei technical support. For details, see Contacting Technical Support.

1.2.3 Other Faults

Bad AT0 Grounding

Symptom

The IAD FXO port and the SoftCo AT0 trunk have noises or exceptions occur in call connections.

Cause

The IAD is not properly grounded.

Solution

Step 1 Check the AT0 grounding by referring to 1.3.10 Bad AT0 Grounding.

Step 2 Test the grounding resistance by referring to 1.3.11 AT0 Ground Impedance Test.

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

Port Indicator Is Off

Symptom

The LINK indicator of a port of the IAD is off after the network cable is connected.

Cause

The possible causes are as follows:

- The device is not powered on.
- The network cable and the port is in bad connection.
- Network cable is damaged.
- Network negotiation failed.

Solution

1. Ensure that the device is powered on.
2. Ensure that the network cable and the port is in good connection.
3. Check the network cable and replace the damaged cables.
4. Ensure that the dual-duplex mode of the WAN port of the IAD is consistent with that of the upper-level switch. Run the **duplex auto** *portid* command in the Ethernet switch mode to set the port to automatic negotiation mode. For IAD101H, IAD102H, IAD104H, and IAD208E(M), *portid* is WAN; for IAD132(E), *portid* is the number of the uplink port; for IAD1224, *portid* is FE1/FE2 network interface.

Network Connection Failure

Symptom

The network between the IAD and other devices on the network is disconnected (network status cant be tested by running the **ping** command).

Cause

The possible causes are as follows:

- Issues of network cables, power supply, or network negotiation.
- The IP address of the IAD conflicts with that of the other devices.
- Packet loss.
- When the Virtual LAN (VLAN) is used, the IAD is not connected to the same VLAN as the other devices.

Solution

1. Check whether the network indicator is on. For details, see Port Indicator Is Off.
2. If the network cable connection is good, run the **display ipaddress** command to check the IP address of the IAD. If the IP address of the IAD conflicts with that of other devices (shares the same IP address with other devices), change the IP address of the IAD.
3. If an IP network exists between the IAD and the network destination device, you can run the **tracert** command to check the connectivity of the network and ensure that the route between the packet and the IP network is reachable.
4. If no response is received after the **ping** *a.b.c.d* command is executed. The possible causes are as follows:
   - Some of the hosts or routers in the network closes the ping function.
   - The firewall used in the network can discard some of the packets according to the defined conditions.
   - If a network is undertaken massive traffic, the Quality of Service (QoS) mechanism may cause packet loss also.
   - If a packet is too big, the CPU usage of the IAD raises. Therefore, the IAD discards all packets that need to be divided into fragments.

NOTE

Fragment: The Internet protocol allows packets to be divided into fragments so that the fragments can go through a link in the form of Maximum Transmission Unit (MTU).

5. If VLAN is set on the IAD or the network destination device and the two devices are not in the same VLAN, packets cannot be sent between the two devices.

Loading or Backing Up File Failure

Symptom

When you load files from the FTP/TFTP server to the IAD or back the file up from the IAD to the FTP/TFTP server, the operation fails.

Cause

The possible causes are as follows:

- Network issue.
- FTP/TFTP server fault.
- Wrong file storage directory.
- When the load/backup operation is being implemented on the IAD, the parameter set on the IAD is inconsistent with that set on the server.

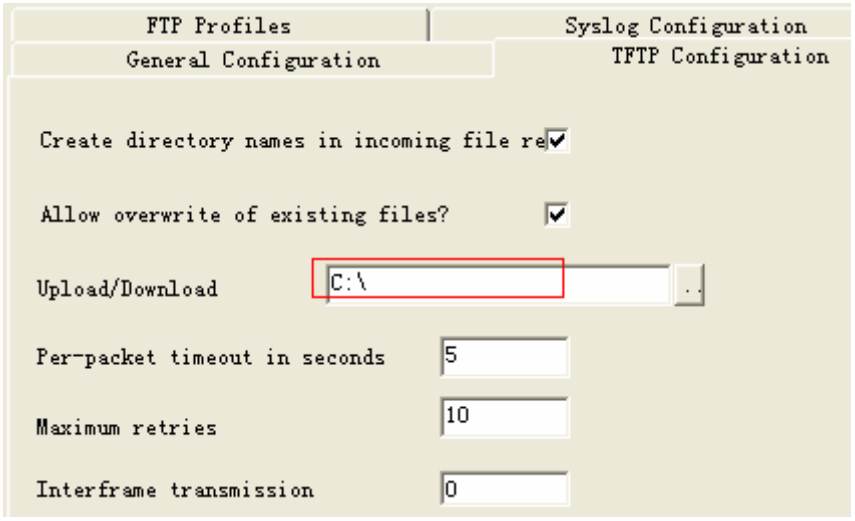
Solution

1. Check the network connection status between the IAD and the FTP/TFTP server by running the **ping** *a.b.c.d* command.

NOTE

If the network delay is too large, the loading may fail. For example, when you are accessing the Internet through ADSL and the connection speed is slow, the loading may fail.

2. Check the availability of the FTP/TFTP server. You are advised to enable the log function on the server. The records in the log file can help solving problems of this type.
3. Check whether the file to be loaded is stored in the file directory of the FTP/TFTP server. For example, the file directory of the TFTP server is C:\.



4. Check whether the file name and type of the file to be loaded or backed up are consistent with those typed on the IAD command line. If the file is loaded or backed up through the FTP server, when running the **load** or **backup** command, ensure the FTP user name and password are correct.

PPPoE Dialing Failure

Symptom

When you obtain IP address through Point-to-Point Protocol over Ethernet (PPPoE), the dialing fails.

Cause

The failure may be caused by network disconnection, invalid user name or password, or false login information after a fault occurs and the PPPoE server restarts.

Solution

1. Check whether the network is disconnected. For details, see Network Connection Failure.
2. Run the **display ipaddress** command to view the IP address obtaining mode. Ensure that the PPPoE mode is adopted.

```
TERMINAL>display ipaddress
-------------------------------------------------
DNS Domain Name..............: tele.com
Physical Address.............: 00-e0-fc-a8-d0-0d /*MAC address*/
IP Address Get Method.........: Static IP config /*Obtaining method of IP address*/
...
```

   The preceding information indicates that the IP address obtaining mode is static IP address. Run the **ipaddress pppoe** command in the global configuration mode to enable the PPPoE dialing mode, and then run the **pppoe** *user name* **password** *password* command to set the user name and password.
3. Run the following command to check whether the PPPoE is online. If the PPPoE is offline, check the correctness of the user name and password.

```
TERMINAL(config)#display ipaddress
-------------------------------------------------
  DNS Domain Name..............:
  Physical Address.............: 00-e0-fc-3e-57-2d
  IP Address Get Method.........: PPPoE
  cpm (unit number 0):
    Flags: (0x400) DOWN TRAILERS ARP
    IP Address..................: 192.166.1.102
    Subnet Mask.................: 255.255.255.0
    Default Gateway.............: 192.166.1.1
  Destination IP Address........:
  PPPoE Dialup on System Start..: yes
  PPPoE Online..................: yes /*yes indicates that the PPPoE is online.*/
  PPPoE Dialup Username.........: hHuawei
  PPPoE Dialup Password.........: ******
-------------------------------------------------
```

4. If the IAD is reset by accident or restarted because the power is off, the users may still be in online state in the PPPoE server. If you try to dial a number before the account times out and drops offline, the dial fails. You can wait for a few minutes before redial the number.

NOTE

If the IAD is reset using the **reboot** command, the user will be logged off before the IAD is reset. In this case, you can log in to the IAD right after the IAD is restarted.

5. Check the configuration of the PPPoE server.

PCs Connected to the IAD101H/102H/104H Cannot Access the Network

Symptom

The IAD uses the WAN port to connect to the switch and the LAN port to connect to a PC.

IAD users can use the voice service. The PC connected to the LAN port cannot access the network.

Cause

The possible causes are as follows:

- Network exceptions occur.
- Conflict between the NAT function and the static IP address occurs.
- The VLAN is configured on the upper-level switch, but not on the IAD; or the VLAN configuration is incorrect on the IAD.

Solution

Step 1 Connect the PC to the switch without changing the IP address, and check whether the fault is rectified.

- If yes, the IAD configuration is incorrect. Go to Step 2.
- If no, the upper-level network is disconnected. Check the upper-level network.

Step 2 Run the **display nat** command to verify that the NAT function is enabled for the IAD.

Step 3 Modify the IAD or PC configuration, and check whether the fault is rectified. If no, go to Step 4.

- If the NAT function is enabled for the IAD, the PC must not use a static IP address.
- If the PC needs to use a static IP address, run the **nat disable** command to disable the NAT function, and run the **lanswitch mode** command in the LAN switch mode to enable the LAN switch function.

Step 4 Check whether the VLAN is configured on the upper-level switch. If the VLAN is configured, verify that the VLAN configuration is correct. For details, see the product document.

Step 5 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 6.

Step 6 Contact Huawei technical support.

----End

IAD Cannot Register with the UCEMS After Startup

Symptom

Network:

UCEMS Client-UCEMS Server-IAD

The IAD online indicator on the UCEMS is gray. The IAD cannot be registered with the UCEMS.

Cause

The possible causes are as follows:

- Network exceptions occur.
- The physical serial number of the IAD is inconsistent with that set on the UCEMS.
- The IAD is disconnected from the UCEMS or the handshake function is disabled.
- The IAD uses an IP address for registration but the IP address setting is incorrect.
- The IAD uses a domain name for registration but the domain name fails to be parsed.

Solution

Step 1 Check whether the network quality is good.

- If no, rectify the network fault.
- If yes, go to Step 2.

Step 2 Run the **display physical-serial-num** command to verify that the physical serial number is the same as that set on the UCEMS. To obtain the physical serial number set on the UCEMS, contact the network administrator. If the configuration is inconsistent with that on the UCEMS, run the **physical-serial-num** *string* command in the global configuration mode to synchronize the physical serial number.

Step 3 Run the **display nms** command to verify that the communication parameter values set on the IAD are the same as those set on the UCEMS. If the values are different, run the **nms** command to set the communication parameters.

Step 4 If **nms access value** is **Disable**, run the **nms access on** command to allow the IAD to access the UCEMS. Run the **nms handshake switch on** command to enable the handshake function to ensure that the IAD information on the UCEMS is latest.

Step 5 Check whether the fault is rectified.

- If yes, the procedure ends.
- If yes, go to Step 6.

Step 6 Contact Huawei technical support.

----End

Frequent MG Disconnection Alarm

Symptom

The MG disconnection alarm is generated frequently. The registration status changes between **Normal** and **Fault** frequently. IAD users hear the busy tone after picking up phones.

Cause

The possible causes are as follows:

- Failure to be registered with the softswitch
- Poor bearer network performance
- IP address conflict
- Domain name conflict
- No heartbeat response
- Inconsistent heartbeat timeout durations on the IAD and softswitch
- MAC address conflict

Solution

Step 1 Check whether the IAD is registered with the softswitch.

- If no, verify that the IAD configuration is correct.
- If yes, go to Step 2.

Step 2 Ping the softswitch IP address to check the delay time and packet loss.

- If the delay time is too long and packet loss occurs, the bearer network performance is poor. Verify the network connection.
- If the network is normal, go to Step 3.

Step 3 Check whether the IAD registration status is synchronized with that on the softswitch.

- If no, verify the network connection.
- If yes, go to Step 4.

Step 4 Check whether IP addresses conflict.

- If yes, change the IAD IP address.
- If no, go to Step 5.

Step 5 Check whether the domain names conflict on multiple IADs.

- If yes, change the MG domain names on the IAD and MGC server to solve the conflict.
- If no, go to Step 6.

Step 6 Use the Wireshark to analyze packets to check whether the softswitch responds to the heartbeat message sent by the IAD.

NOTE

You can also run the **trace** command to trace signaling. For details, see signaling tracing in the common troubleshooting methods.

- If no, the softswitch is faulty.

- If yes, go to Step 7.

Step 7 Check whether the heartbeat timeout durations on the IAD and softswitch are the same.

- If no, run the **mgcp protocol** command on the IAD to change the heartbeat timeout duration. To change the heartbeat timeout duration on the softswitch, see the related softswitch document.
- If yes, go to Step 8.

Step 8 Check whether MAC addresses conflict.

- If yes, change the IAD MAC address.
- If no, go to Step 9.

Step 9 Contact Huawei technical support.

----End

When the IAD Is Connected to the Local PSTN Network Through the FXO Port, an Incorrect ID That Is Bound to the FXO Port Causes Incoming Call Exceptions

Symptom

Network: SoftCo-IAD-PSTN

A SoftCo user makes an outgoing call to a PSTN user through the FXO port on the IAD. An outer-office user dials the PSTN number to make an incoming call to the PSTN user through the FXO port. This implements the number retention service. The outer-office user hears the ring back tone twice before hearing the announcement indicating that the number dialed does not exist.

Cause

The possible cause is incorrect data configuration.

Solution

Step 1 Verify that a correct ID is bound to the FXO port. The ID bound to the FXO port must be the DN, that is, SoftCo number, not the EID.

NOTE
The ID configured on the FXS port is the SoftCo EID, but the ID bound to the FXO port is the DN. Generally, the EID is the same as the DN; however, there are some exceptions, especially when the virtual PBX exists. For example, the intra-office number is 1000, but its EID is 2000.

Step 2 Configure the ID bound to the FXO port. For example:

```
TERMINAL(config)#sip user 0 id 2000
TERMINAL(config)#sip user 8 id 1000
```

Step 3 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 4.

Step 4 Contact Huawei technical support.

----End

IAD Cannot Register with ZTE IMS Using SIP

Symptom

Network: IAD-ONU-ZTE IMS

ZTE IMS does not respond to the registration message sent by the IAD while the soft client can register with ZTE IMS.

Cause

The possible cause is that ZTE IMS cannot recognize the SIP registration message that contains **user=phone** sent from the IAD.

Solution

Step 1 Run the **sip soft-parameter sip-user-phone off** command to disable the **user=phone** information in the SIP message. The **sip-user-phone** attribute is enabled by default. You can run the **display sip soft-parameter** command to view the **sip-user-phone** value.

Step 2 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 3.

Step 3 Contact Huawei technical support.

----End

IAD Cannot Register with the Softswitch Using MGCP

Symptom

The IAD cannot register with the softswitch using MGCP.

Cause

The possible causes are as follows:

- The network is disconnected.
- The configuration is incorrect.
- The authentication information is configured on the IAD, but not on the softswitch.
- The soft parameter settings are inconsistent.

Solution

Step 1 Check whether the softswitch can be pinged on the IAD.

- If no, verify the network connection.
- If yes, go to Step 2.

Step 2 Check whether the authentication settings on the IAD and softswitch are the same.

- If the authentication information is configured on the IAD, but not on the softswitch, the IAD cannot register with the softswitch. Ensure that the authentication settings are the same on the IAD and softswitch.
- If the authentication settings are the same, go to Step 3.

Step 3 Run the **display mgcp soft-parameter** command to check the MG soft parameter settings. For Nortel devices, set **MGC-TYPE** to **nortel**, and registration mode to **individual**.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

Card Swiping Process Takes Long Time on the POS Device Connected to the IAD208E(M)

Symptom

Network: POS-IAD208E(M)-SoftCo9500-SBC-IMS

The point of sale (POS) device connected to the IAD takes 30 to 40 seconds to complete the card swiping process.

Cause

The possible causes are as follows:

- No digitmap is available for the card swiping number. The number is not reported until timeout.
- The network quality is poor.
- The card swiping server is faulty.

Solution

Step 1 Run the **display sip digitmap** command to check whether the digitmap is configured for card swiping numbers. If no, configure the digitmap, and verify that the fault is rectified.

Step 2 Capture network packets to analyze slow and fast card swiping processes. Verify that the IAD processing mechanism is the same, and no packet loss, delay, or jitter occurs.

Step 3 Verify that the card swiping server runs properly on the core network. If the server always responds to the connection request after several swiping attempts, the card swiping process is slow.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

What should I do if the IAD fails to register with the UAP3300?

Symptom

IAD users fail to register with the UAP3300.

Possible Cause

The possible causes are as follows:

- Network connection is unavailable.
- Configuration is incorrect.
- IAD is in local switch status.

Solution

Step 1 Check whether the softswitch can be pinged on the IAD.

- If no, verify the network connection.
- If yes, go to Step 2.

Step 2 Check whether the configuration on the IAD is consistent with that on the UAP3300.

- If yes, go to Step 3.
- If no, modify the IAD configuration.

Step 3 Run the **display sip local-call** command on the IAD to check whether the local switch is enabled.

- If the value of **Switch** is **on**, run the **sip local-call disable** command to disable the local switch and run the **write** command to save the configuration.
- If the local switch is disabled, go to Step 4.

Step 4 Contact Huawei technical support engineers.

----End

Why outgoing calls cannot be made when the IAD connects to the IMS?

Symptom

IAD users cannot make calls through the IMS.

Possible Cause

The possible causes are as follows:

- IAD users are not registered with the IMS.
- The URL mode is incorrect.
- The IMS does not support messages in which the user name is set to the phone number.

Solution

Step 1 Check the user registration status on the IAD.

- If the user has been registered, verify the network connection and the configuration data on the IAD.
- If the user has been registered, go to Step 2.

Step 2 Check whether the URL mode on the IMS and the IAD is the same.

- If no, run the **sip soft-parameter support-telurl** command on the IAD to adjust the URL mode.
- If yes, go to Step 3.

Step 3 Run the **sip soft-parameter sip-user-phone off** command on the IAD to delete the record where the user name is set to the phone number.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If yes, go to Step 5.

Step 5 Contact Huawei technical support engineers.

----End

Two Cascaded IAD132E(T)s Cannot Ping Each Other

Symptom

Two cascaded IAD132E(T)s cannot ping each other.

Cause

The possible causes are as follows:

- The two IADs are connected through a direct-connect cable, but the cable-check function is not enabled.
- The network is disconnected or the power supply is faulty.
- IP addresses are not in the same network segment.

Solution

Step 1 Run the **cable-check enable** command on the upstream IAD.

NOTE
The two IADs can be cascaded through a crossover cable. If a direct-connect cable is used, you must enable the cable-check function on the upstream IAD.

Step 2 Check whether network port indicators are normal.

- If no, check the network cable and power supply.
- If yes, go to Step 3.

Step 3 Verify that the IP addresses are in the same network segment.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

Multiple IADs Connected to the Same ONU/ONT Cannot Ping Each Other

Symptom

Multiple IADs connected to the same ONU/ONT cannot ping each other.

Cause

The possible causes are as follows:

- The configuration on the ONU/ONT is incorrect.
- The IP address of the IAD conflicts with that of another IAD.

Solution

Step 1 Verify that no IP address conflict occurs.

Step 2 Connect a switch to the ONU/ONT, and connect all IADs to the switch. Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 3.

Step 3 Modify the configuration on the ONU/ONT. For details, see the related ONU/ONT document.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

IAD Cannot Register with the SoftX3000

Symptom

The IAD cannot register with the SoftX3000.

Cause

The possible causes are as follows:

- The protocol mode is incorrect.
- The network is disconnected.

- The domain name is incorrect in the MGCP mode.
- The softswitch configuration is incorrect.
- The phone number is used by another phone.

Solution

Step 1 Run the **display protocol** command on the IAD or choose **Advanced Configuration** > **Protocol Mode** to view the protocol mode. Check whether the protocol mode is correct.

- If no, run the **protocol-mode** command or choose **Advanced Configuration** > **Protocol Mode** to change the protocol mode.
- If yes, go to Step 2.

Step 2 Check whether the softswitch can be pinged on the IAD.

- If no, verify the network connection.
- If yes, go to Step 3.

Step 3 If the protocol mode is MGCP, run the **display mgcp attribute** command on the IAD or choose **MGCP Service Configuration** > **MG** to check whether the MG domain name configuration is the same as that on the softswitch.

- If no, run the **mgcp mg-domain-name** command on the IAD or choose **MGCP Service Configuration** > **MG** to change the domain name.
- If yes, go to Step 4.

Step 4 Check whether the softswitch configuration is correct. For details, see the related softswitch document.

- If yes, go to Step 5.
- If no, modify the softswitch configuration.

Step 5 Verify that the phone number is not used by another phone.

Step 6 Run the **trace** command to trace signaling and locate the cause.

Step 7 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 8 Contact Huawei technical support.

----End

Two IADs on the Same VLAN Cannot Ping Each Other, and the Phone Does Not Ring When a User Under One IAD Makes a Call to Another User Under the Other IAD

Symptom

Two IADs on the the same VLAN cannot ping each other. When a user under one IAD makes a call to another user under the other IAD, the phone does not ring.

Cause

The possible causes are as follows:

- The network is disconnected.
- The IAD configuration is incorrect.

Solution

Step 1 Check whether the network cable is connected properly.

- If no, reconnect the network cable.
- If yes, go to Step 2.

Step 2 Check whether the configuration on the two IADs is correct. For details, see VLAN configuration in the product document.

- If yes, go to Step 3.
- If no, modify the configuration.

Step 3 Verify that the configuration on the upstream device connected to the two IADs is correct.

- If yes, go to Step 4.
- If no, modify the configuration.

Step 4 Check whether the fault is rectified.

- If yes, the procedure ends.
- If no, go to Step 5.

Step 5 Contact Huawei technical support.

----End

Unable to Run Commands

Symptom

The commands can be entered but cannot be run. Whenever a command is run, a message is displayed indicating that the system is busy and the command cannot be run.

Cause

Exceptions occur when commands are being run.

Solution

1. Pull off power supply, and then power on the device to restart it.
2. After the system is restarted, run the **display log** command to view the operation log, run the **display alarm history all** command to view the alarms, and enter the diagnose mode to view the exceptions.
3. Run a command again. If the command cannot be run, go to the next step.
4. Contact Huawei technical support.

Serial Port Failure

Symptom

After logging in to the IAD through the serial port, you cannot enter anything through the keyboard. In addition, no output or only illegible character is generated.

Cause

The possible causes are as follows:

- The scroll lock is on.
- If no output is generated, the serial cable may not be well connected.
- If illegible characters are generated, the fault may be caused by incorrect parameter configuration.
- The system is down.

Solution

1. Check whether the scroll lock on the keyboard is on, which prevents the automatic scroll of the command line interface (CLI).
2. Check the connection of the serial cable and the check the serial port number. You can switch the serial ports.
3. If illegible characters are generated but commands cannot be entered, the fault may be caused by incorrect serial port parameter configuration. Set **Baud Rate** to **9600**, **data bits** to **8**, **stop bits** to **0**, and **authentication** to **null**.
4. If the RUN indicator is not blinking, the IAD is down. For details, see 1.3.1 Observing Device Indicators. Press the Reset button to restart the device (do not turn off the power or the previously stored alarm records will be lost), and view and analyze the alarms.
5. (Optional) You can try to log in to the IAD through Telnet.

Start Slowness or Failure

Symptom

The start process is slow or stopped. No response is generated for inputs from the keyboard and the system does not automatically restart.

Cause

The possible causes are as follows:

- If the IAD uses the DHCP to automatically obtain the IP address, the fault may be caused because the IP addresses in the network are not sufficient for allocation and the waiting queue is too long.
- When domain name is used for registration to the UCEMS, if the DNS does not exist or has incorrect configuration, the domain name parse will fail and the system will wait for a long time.
- If it is set that the IAD upgrades through the FTP/TFTP server and the configuration of the IP address of the FTP/TFTP server is incorrect, the file request will wait for some time because no response message is received.

- System errors.

Solution

1. If the method for obtaining the IP address of the IAD is DHCP, run the **ipaddress static** command to set a fixed IP address, and then run the **reboot** command to restart the system. Check whether exceptions occur.
2. Run the **display nms** command to view the nms status.

```
TERMINAL#display nms
  the config is DNS /*DNS indicates that the IAD is registered to the network
management platform through DNS.*/
domainName  /*Domain name*/
  iadms.com
get community   : ********
set community   : ********
trap community  : ********
trap port       : 162
nms access value: Disable
register nms ip : 0.0.0.0
register state  : no regist
handshake       : on
handshake time  : 30 S
register switch : on /*on indicates that the IAD registers to the network management
platform.*/
```

   - If it is set that IAD is registered to the UCEMS through DNS (domain name), ensure that the configuration on the DNS server in the network is consistent with the domain name on the IAD.
   - If the IAD is set that the IAD does not register with the network management platform and the automatic upgrade is performed through the FTP/TFTP server, run the **display auto-update** command to view the configuration of upgrade server and ensure that the IP address of the FTP server is correct.
3. If the fault still exists with the preceding factors excluded, the fault may be caused by system exceptions. Contact Huawei technical support. For details, see Contacting Technical Support.

IAD Restarts for No Reason

Symptom

The system automatically restarts when it is running.

Cause

The fault may be caused because a user who logs in to the IAD sends a command that leads to system restart or system exceptions occur.

Solution

1. Run the **display log** command in the privilege mode to view the operation log. Check whether other users send commands that may trigger automatic device reset such as the reboot command, command for IP address modification, or command for loading configuration file.
2. If exceptions occur, run the **load** command to reload the software.

3. If the IAD crashes, run the **display alarm history all** command to view the last alarms and contact Huawei technical support. For details, see Contacting Technical Support.

Automatic Upgrade Failure

Symptom

The FTP/TFTP server for automatic upgrade is set (If the IAD is registered to the UCEMS, you can specify an upgrade server to the IAD through the UCEMS) and the new version file is available on the server, but the automatic upgrade is not performed after the interval for detecting automatic update.

Cause

The possible causes are as follows:

- The network is disconnected.
- The IAD is not registered with the UCEMS.
- The upgrade configuration on the UCEMS or IAD (such as upgrade file path and FTP server) is incorrect.
- The version information in the upgrade file is the same as the current version.

Solution

1. Check whether the network is disconnected. For details, see Network Connection Failure.
2. If you need to specify an upgrade server to the IAD through the UCEMS, check whether the IAD is registered with the UCEMS.
3. If an upgrade server is set on the IAD, ensure that the correct IP address of the FTP server, FTP user name, password, and file path are set in the **auto-update ftpserver** command.
4. If the connection to the FTP server is available, you can check whether the IAD obtains the upgrade file and whether the software version in the configuration file is the same as the current software version on the host by viewing the output information through the command output line. If the software versions are the same, the current version on the host is the latest version and upgrade is not required. You can run the **display version** command to view the device version.

1.3 Common Troubleshooting Methods

Common troubleshooting methods include the **ping** command, the **tracert** command (used to trace routes) on the IAD, and the **trace** command (used to trace signaling). The general packet capturing tool is Wireshark.

1.3.1 Observing Device Indicators

By observing the indicators, you can monitor the operating status of the IAD.

Indicators of the IAD101H, 102H, and 104H

Indicator	Color	Item	Status	Description
PWR	Green	POWER indicator	On	Indicates that the power is on.
			Off	Indicates that the power is off.
WAN	Green	Uplink interface indicator	On (for the IAD101H and 102H only)	Indicates that a connection is set up on the WAN.
			Blinking (for the IAD104H only)	Indicates that a connection is set up on the WAN.
			Off	Indicates that no connection is set up on the WAN.
LAN	Green	Downlink interface indicator	On (for the IAD101H and 102H only)	Indicates that a connection is set up on the LAN.
			Blinking (for the IAD104H only)	Indicates that a connection is set up on the LAN and data is received and sent.
			Off	Indicates that no connection is set up on the LAN.
VoIP	Green	VoIP signal indicator	On	Indicates that the VoIP service is ready.
			Off	Indicates that no VoIP service is ready, or the system is saving data.
PHONE 1 - PHONE 4	Green	Voice phone port indicator	Blinking (0.25s on and 0.25s off)	Indicates that the phone of the corresponding port is ringing.
			Blinking (1.5s on and 0.5s off)	Indicates that the system is switched over to the backup PSTN and the phone is in use.
			On	Indicates that the phone is picked up or the phone is in lock state.
			Off	Indicates that the phone of the corresponding port is in hang-up state.

NOTE

The numbers of the voice telephone interface indicators of the IAD101H, 102H, and 104H are 1, 2, and 4 respectively.

1.3.2 Collecting System Information (Web)

This chapter is only for IAD208E(M), IAD132E(T) and IAD1224. Users can collect system information or download it for remote fault locating conveniently on the Web page.

The collected system information includes software version, network port setting, registration status of SIP users and Wildcard groups (only for SIP), or the registeration of the MG and MGC (only for MGCP), VLAN configuration, current system configuration, and history alarms.

Proceed as follows:

1. Choose **Diagnose** > **System Information** in the navigation bar. The system information page is displayed.
2. Click **Download** to save or open system information.

NOTE
The latest 10 alarms are displayed. To view more alarm information, view downloaded files.

1.3.3 Viewing Call Failure Records

This chapter is only for IAD208E(M), IAD132E(T) and IAD1224. You can view call failure records using web pages or CLI to locate and analyze call faults. The IAD records call failure information about all user ports, including calling number, called number, call start and end time, the party that releases the call, and the call release cause.

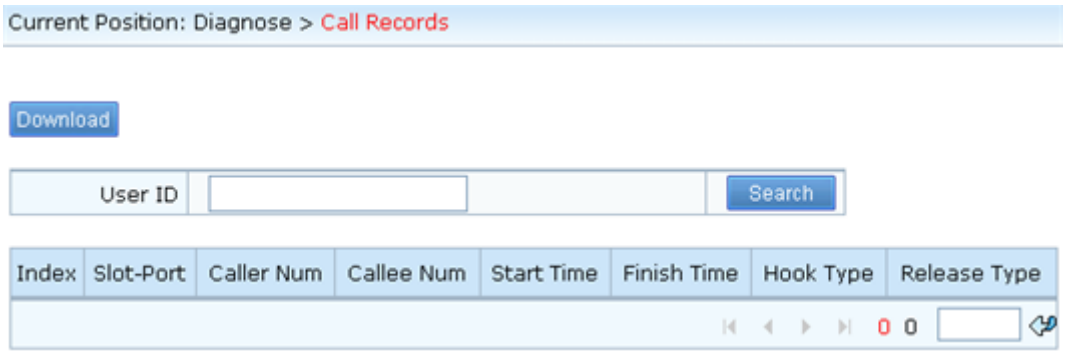
You can view all call failure records on the IAD and locate and analyze faults according to the call release causes. A maximum of 10 records of a user are saved.

NOTE
When the IAD restarts upon power outage, the original call failure records are lost.

Web Mode

Choose **Diagnose** > **Call Records** from the navigation bar. The page shown in Figure 1-4 is displayed.

Figure 1-4 Call failure records



You can click **Download** to download call failure records, or enter a user number to view the call failure records of a specified user.

NOTE
When the IAD is connected to the SoftSwitch, the user number is the same as **DN** on the SoftSwitch.

CLI Mode

Run the **display sip calloutrecords** command to view the call failure records. For example:

1.3.4 Checking the Network Status Automatically

By using this function, you can check the connection between an IAD and a specified device. If enable the function, the IAD generates the alarm information when the network connection is interrupted or restored. You can locate the faults according to the alarm information.

Application Instance

Network Requirements

The IAD is connected to the SIP server through LAN. The IP address of SIP server is 192.163.1.8. Problem description: The registered SIP users become unregistered.

CLI Mode

Step 1 Run the **network-auto-check on** to enable the automatic check function.

The command is as follows:

```
TERMINAL(config)#network-auto-check on
```

NOTE

- If the IP address of the SIP server , and the IP address of the device to be checked are not set, the IAD does not check the connection automatically.
- If the SIP server's IP address is set but the device's IP is not set, the IAD automatically check the connection with the first set SIP server .

Step 2 Run the **network-auto-check ipaddress** *ip-address* to set the IP address of a device to be checked.

The command is as follows:

```
TERMINAL(config)#network-auto-check ipaddress 192.163.1.8
```

Step 3 Run the **write** command to save the settings.

The command is:

```
TERMINAL(config)#write
```

Step 4 Run the **display network-auto-check** command to check the configuration.

The command is as follows:

```
TERMINAL(config)#display network-auto-check
----------------------------------------
server ipaddress:192.163.1.8
network-auto-check:on
----------------------------------------
```

Step 5 Query the network status according to the alarm information. For details, see *Processing IAD Alarms*.

The information is as follows:

```
IAD2000(config)#display alarm history alarmid 0x06010007
Command:
```

```
    display alarm history alarmid 0x06010007
 ALARM 38 FAULT WARNING 0x06010007 COMMUNICATION 2010-12-09 10:02:38
 ALARM NAME  : Network-autocheck fault
 PARAMETERS  : netcheck-ip : 192.163.1.8
 DESCRIPTION : Network-autocheck fault //Fault indicates network abnormality

 CAUSE      : Request timed out.
 ADVICE     : Request timed out.
 --- END
```

The information indicates that the connection between the standby SIP server and the IAD is restored.

Step 6 Rectify the network fault. For details, see the *IAD Troubleshooting Guide*.

Query the alarm information again. The information is as follows:

```
IAD2000(config)#display alarm history alarmid 0x06020007
Command:
      display alarm history alarmid 0x06020007
 ALARM 269 RECOVERY WARNING 0x06020007 COMMUNICATION 2010-12-09 10:25:16
 ALARM NAME  : Network-autocheck restore
 PARAMETERS  : netcheck-ip : 192.163.1.8
 DESCRIPTION : Network-autocheck restore //Restore indicates network resumption
 CAUSE      : Network restore
 ADVICE     : Need no process.
 --- END
```

Step 7 Run the command to query the users' registration state. The state is **registered**.

The command is as follows:

```
TERMINAL(config)#display sip attribute 0
             Sip User Information
-----------------------------------------------------
user-sn          : 0
id              : +8657187900066
password         : ********
name            : +8657187900066@ssg.comcast.net
local address     : 192.163.1.47
local-port       : 5060
registration state : registered //The user is registered
expire-time      : 0 sec
previous server   :
current server    : 192.163.1.8 : 5060
dm match delay    : 0 ms
digit-map position : remote
dial-delay position: remote
support no pound  : off
group id         : -
......
```

----End

1.3.5 Using the PING Command

By running this command, you can check the status of the network connection.

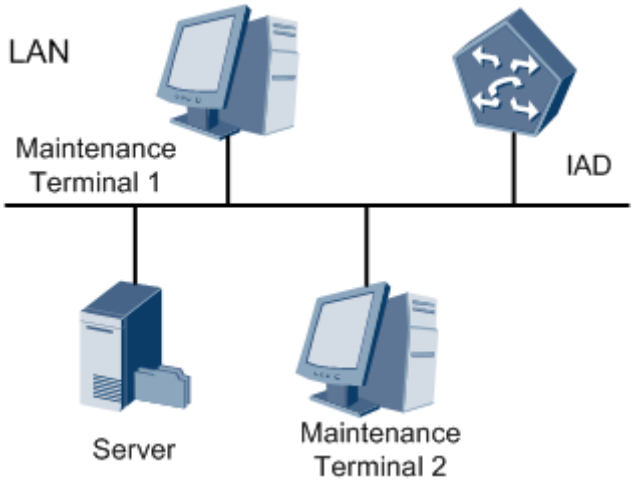
The example for running the**ping** command is as follows:

The IAD maintenance network port is connected with the maintenance terminal 1 and 2 through LAN. The IP addresses of the three equipment are shown in Table 1-5 and the networking status is shown in Figure 1-5.

Table 1-5 Example for Using the PING Command

Device	IP Address
IAD	172.21.100.16
Maintenance terminal 1	172.21.50.51
Maintenance terminal 2	172.21.50.84

Figure 1-5 Networking of the Example for Using the PING Command



Problem description: When a user uses maintenance terminal 1 to log in to the IAD through Telnet, sometimes the connection fails. However, the connection between maintenance terminal 2 and the IAD through Telnet is normal.

The troubleshooting method is as follows:

1. Use terminal 2 to log in to the IAD through serial port or Telnet.
2. Run the **ping** command to check the connection between the IAD and maintenance terminal 1. The operation is as follows:

```
TERMINAL>ping 172.21.50.51
  PING 172.21.50.51: 56  data bytes, press CTRL_C to break
  Request time out
  Request time out
  Request time out
  Request time out
```

```
Request time out

--- 172.21.50.51 Ping statistics ---
5 packets transmitted
0 packets received
100.00% packet loss
```

If the displayed result shows that the IAD cannot receive the data package, the network may be busy or disconnected.

3. You can set the **-c** parameter of **ping** command to adjust the sending packets.

   For example, to send 10 packets for testing the network, run the following command:

```
TERMINAL>ping 172.21.50.51 -c 10
  PING 172.21.50.51: 56  data bytes, press CTRL_C to break
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=0 ttl=128 time = 0 ms
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=3 ttl=128 time = 0 ms
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=5 ttl=128 time = 0 ms
  Request time out
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=7 ttl=128 time = 0 ms
  Reply from 172.21.50.51: bytes=56 Sequence=8 ttl=128 time = 0 ms

  --- 172.21.50.51 Ping statistics ---
  10 packets transmitted
  5 packets received  /*5 packets are received.*/
  50.00% packet loss  /*Packet loss rate is 50%.*/
  round-trip min/avg/max = 0/0/0 ms
```

In the preceding result, only five packets are received. The packet loss is severe. The packet loss may be caused by bad connection quality between maintenance terminal 1 and the IAD, busy network, or interference.

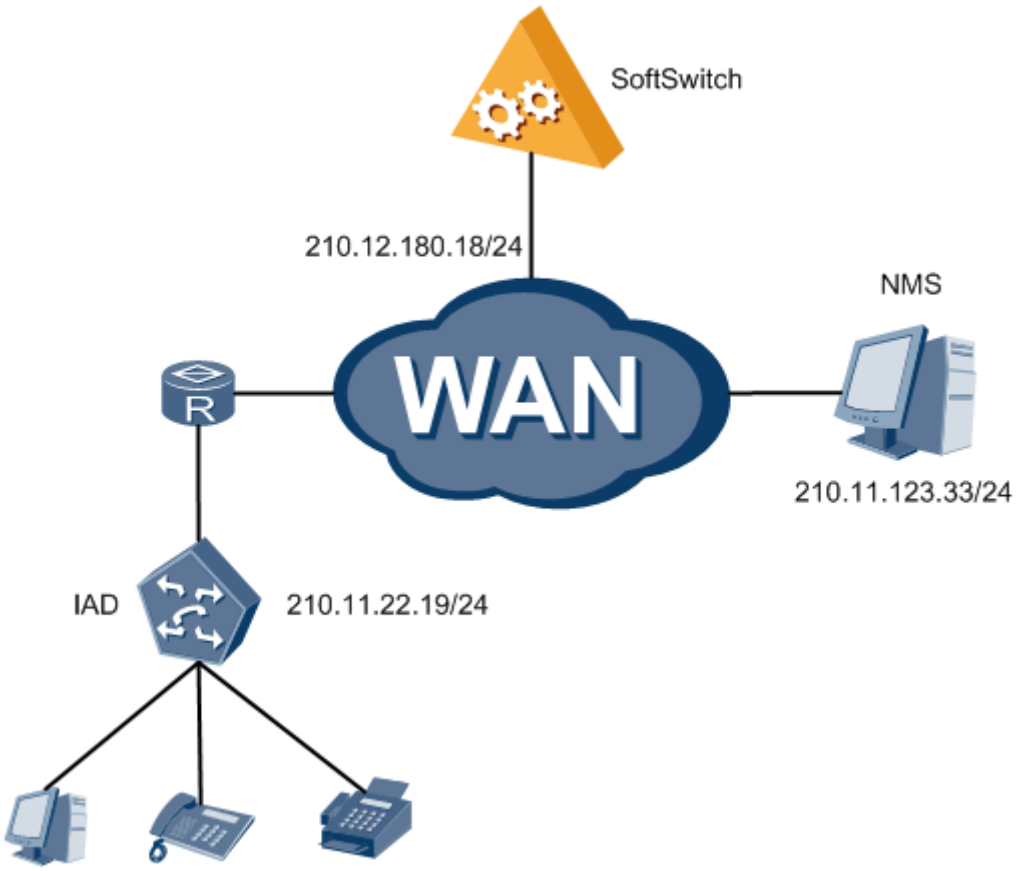
1.3.6 Tracing Route

By running the **tracert** command, you can display all the gateways that a test data package goes through from the sending host to the destination.

The example for running the **tracert** command is as follows:

Figure 1-6 shows the networking status.

Figure 1-6 Networking Instance



To analyze the network status between the IAD and SoftSwitch, the operation process is as follows:

1. Log in to the IAD from the maintenance terminal through serial port or Telnet.
2. Run the following command in the user mode:

```
TERMINAL>tracert 210.12.180.18
 traceroute to 210.12.180.18 max hops 30 ,packet 40 bytes
  press CTRL_C to break
 1    1 ms    <10 ms  <10 ms   210.11.22.254
 2    1 ms    2 ms    2 ms    210.110.0.17
 3    1 ms    1 ms    1 ms    210.11.180.18
Trace complete.
```

3. From the preceding result, you can find out the routes that the packet goes through from the IAD to the destination MGC.

1.3.7 Tracing Signaling

You can run the **trace** command to trace all messages transferred between the IAD and upper-level devices (SoftSwitch, IMS, and SIP server) and locate the signaling-related issues quickly.

Use SIP service of IAD132E(T) as an example, run the **trace** command to trace the signaling of port 0:

```
TERMINAL#trace 0
Execution of command succeeded

[2009/10/21 15:16:22 (910ms)]
UA->PROXY: Sip Message is going to be sent to 192.166.1.16:5060 through UDP
REGISTER sip:uap3;user=phone SIP/2.0
From:"8661"<sip:8667@uap3;user=phone>,tag=8f374716
To:<sip:8667@uap3;user=phone>
CSeq:46REGISTER
Call-ID:267503607886679f71cfae@192.166.1.132
Via:SIP/2.0/UDP 192.166.1.132:5060;branch=z9hG4bK<38ba526a7
Contact:<sip:8667@192.166.1.132:5060;user=phone>;expires=120
Expires: 120
Supported: 100rel
Max-Forwards: 70
...
```

NOTE

After the trace is completed, run the **undo trace** command to close the signaling tracing function.

1.3.8 Analyzing Packets Captured by Wireshark

Network packets must be captured to locate faults about broadband voice quality, media, and signaling interaction. This topic describes how to use Wireshark (previously known as Ethereal) to capture data from the network for analysis.

Preparations

You need to establish network environment and configure the data before capturing packets.

NOTE

- If VPN(Virtual Private Network) software is installed on the PC, delete the VPN software before the packet capture. Otherwise the capture result will be affected because only the packets sent by the PC can be captured.
- Manage the captured packets carefully.

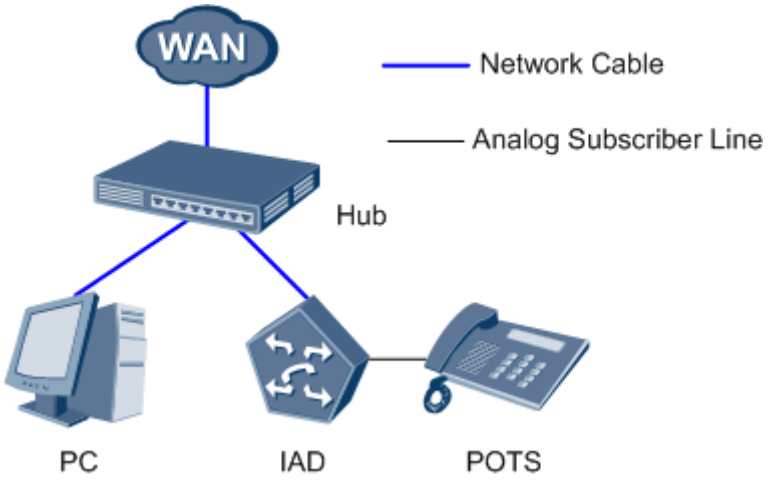
Capturing packets by means of the Hub

Set up the environment as follows:

1. Connect the Hub to the PC that is used to capture packets.
2. Connect the Hub to the WAN interface of the IAD.
3. Connect the Hub to the uplink network by using a LAN switch.

Make sure that the three cables are connected, as shown in Figure 1-7.

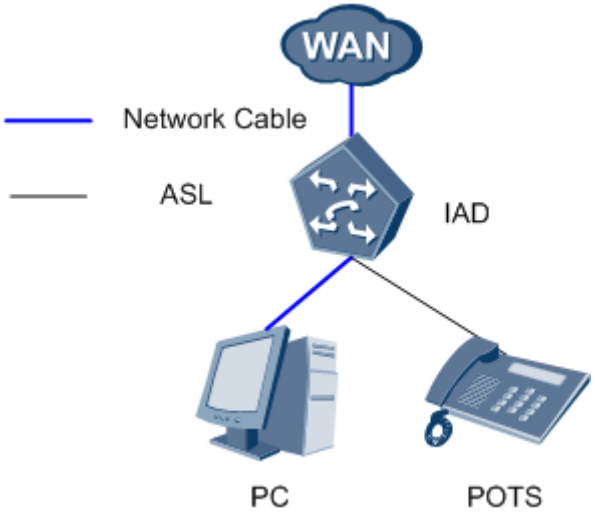
Figure 1-7 Capturing packets by means of the Hub



Capturing packets by using the mirror port on the IAD208E(M), IAD132E(T), and IAD1224

Connect the PC that is used to capture packets to the IAD. The networking scheme is shown in Figure 1-8.

Figure 1-8 Capturing packets by using the mirror port on the IAD



Configure the mirror port on the IADs by running the **TERMINAL(lanswitch)#monitor** *source-port* **observing-port** *destination-port* command. Table 1-6 describes the parameters in the command.

For example:

```
TERMINAL(lanswitch)#monitor 1 observing-port 2
 Monitor lsw interface succeed
```

After configuring the port, port 2 can capture packets of port 1.

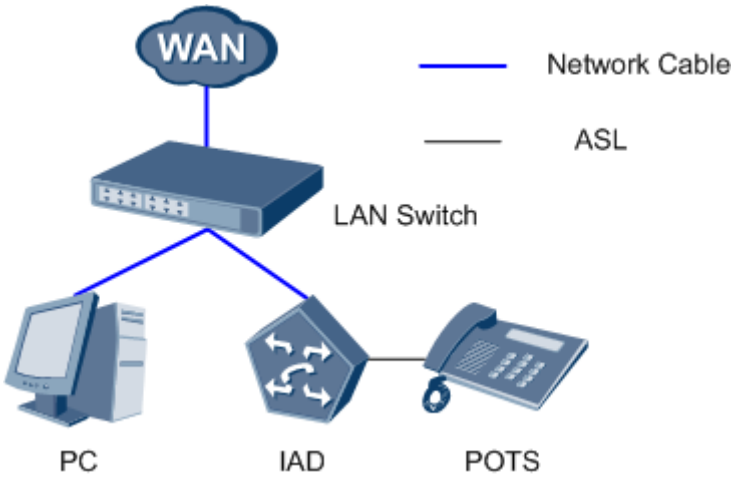
Table 1-6 Command description

Item	Description	Value Range		
		IAD208E(M)	IAD132E(T)	IAD1224
source-port	Source mirror port. Configure the uplink network port of the IAD as the source mirror port.	1 to 8	1 to 4	1 or 2
destination-port	Destination mirror port. Configure the port that is connected to the IAD on the PC as the destination mirror port.	1 to 8	1 to 4	1 or 2 **CAUTION** The uplink port of the IAD which is used to connect the IAD to the superior devices and the port which is used for cascading connections cannot be set as the destination mirrored port.

Capturing packets by using the mirror port on the switch

Connect the PC and the IAD to the same switch. The networking scheme is shown in Figure 1-9.

Figure 1-9 Networking example 3



CAUTION

Only one port can be set to the monitoring port on a switch. This port cannot monitor itself.

The method for setting mirror ports on switches varies according to the switch type. Huawei Quidway S3000 is used as an example.

Step 1 Connect the PC used to capture packets to port 24 to capture packets.

Step 2 Connect the WAN port of the IAD to port 18 on the switch.

Step 3 Log in to the switch through the serial cable.

Step 4 Run the **system-view** command to enter the system view.

Step 5 Run the **monitor-port ethernet 0/24** command to set port 24 as the destination mirror port to monitor other ports.

Step 6 Run the **mirroring-port ethernet 0/18** command to set port 18 as the source mirror port. The source mirror port is monitored by the destination mirror port.

Step 7 Run the **display mirror** command to view the configuration result.

NOTE

You can run the **mirroring-port Ethernet 0/1 to Ethernet 0/23 both** command to monitor ports 1 to 23 or run the **undo mirroring-port Ethernet 0/21 to Ethernet 0/23 both** command to cancel the monitoring on ports 21 to 23.

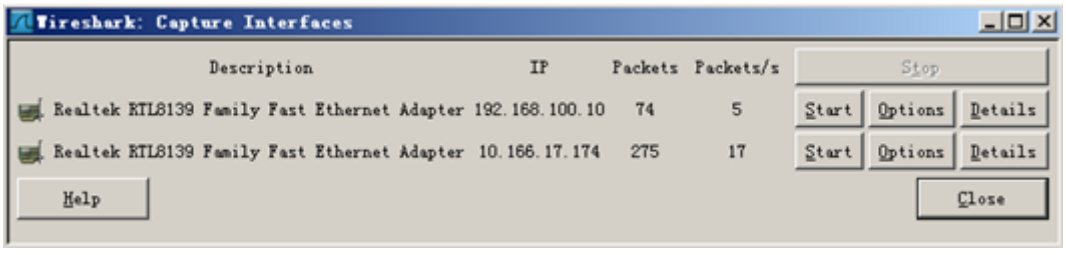
----End

Using the Wireshark to Capture Packets

Step 1 Open Wireshark (take version 1.0.6 for example), and then click  on the left of the toolbar.

A dialog box as shown in Figure 1-10 is displayed.

Figure 1-10 Selecting network adapters for capturing packets



Step 2 If multiple network adapters are available (in this example, it is dual-network adapter), select the network adapter whose IP address is in the same network segment as that of the IAD. Click the corresponding **Start** to start the packet capture.

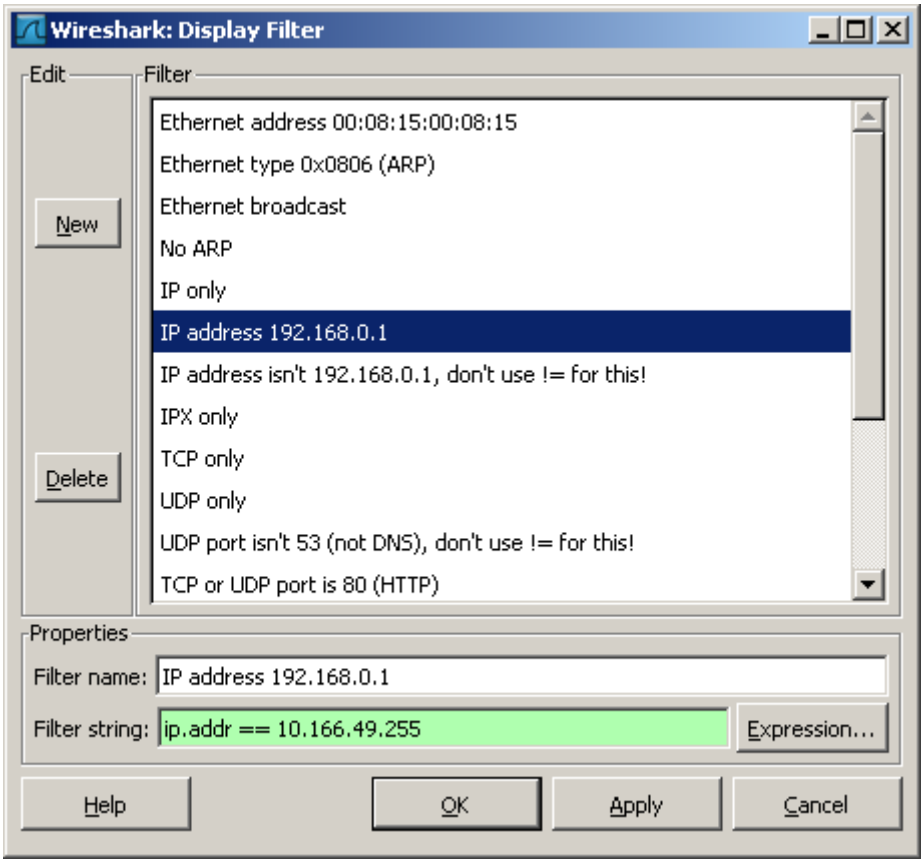
Step 3 Click  on the left of the toolbar to stop the packet capture when enough packets are captured.

Step 4 Use the filter.

- Enter filter condition in the **Filter** textbox under toolbar and then click **Apply** on the right (or press **Enter**). For example, if you enter **rtp**, only the packets in RTP protocol are displayed.
- Use defined filters:

1. Click  on the right of the toolbar to enable the common filtering conditions. A dialog box as shown in Figure 1-11 is displayed.

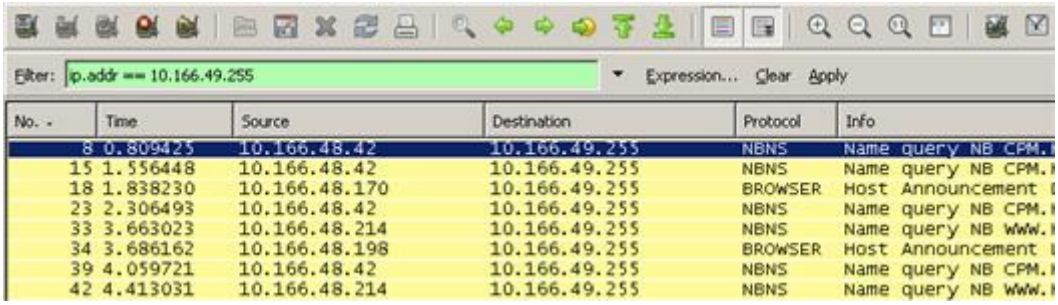
Figure 1-11 Setting Filtering Conditions



2. For example, to view only the packets whose destination IP address is 10.166.49.255, you need to select **IP address 192.168.0.1** in **Filter**, change the IP address in the **Filter string** text box to **10.166.49.255**, and then click **OK**.

   Only the packets whose destination IP address is 10.166.49.255 are displayed on the main page of Wireshark, as shown in Figure 1-12.

Figure 1-12 Running Filter Function



Voice services, call control, and remote (Telnet) maintenance involve packets of different types. You can set the filter criteria based on the following description.

- For SIP services, the structure of the protocol stack is shown in Table 1-7. You need to pay attention to the RTP and SIP protocols.

Table 1-7 Structure of SIP Signaling Protocol Stack

Remote Maintenance Through Telnet	Voice		Call Control
Telnet	RTP	RTCP	SIP
TCP	UDP		
IP			
MAC			

- For MGCP services, the structure of the protocol stack is shown in Table 1-8. You need to pay attention to the RTP and MGCP protocols.

Table 1-8 Structure of MGCP Signaling Protocol Stack

Remote Maintenance Through Telnet	Voice		Call Control
Telnet	RTP	RTCP	MGCP
TCP	UDP		
IP			
MAC			

Step 5 Choose **File** > **File Save as** to save the packet file in a specified folder.

----End

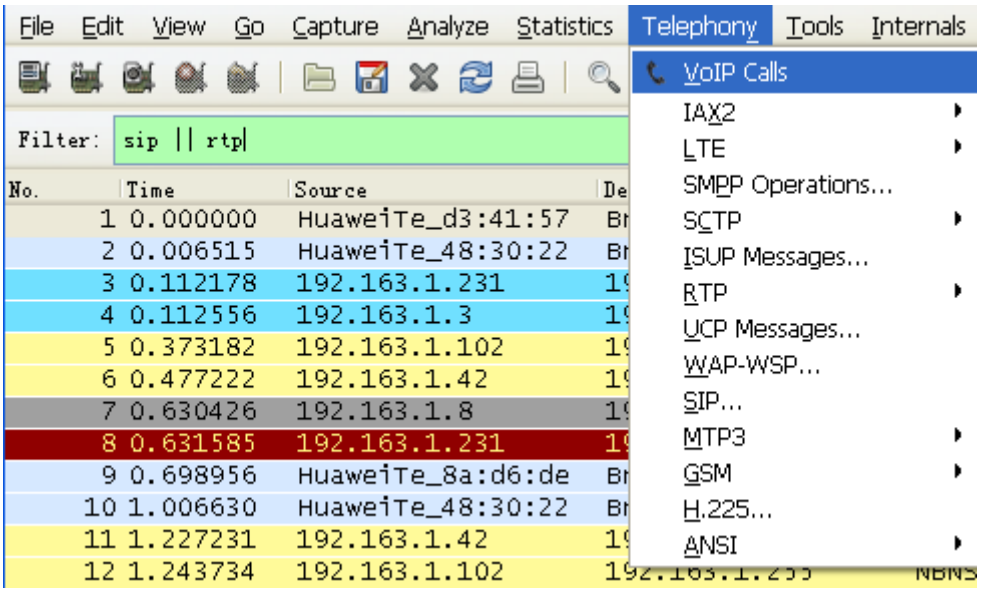
Examples for Analyzing Packets

Assume that the SIP and RTP packets need to be analyzed.

- Analyzing SIP packets

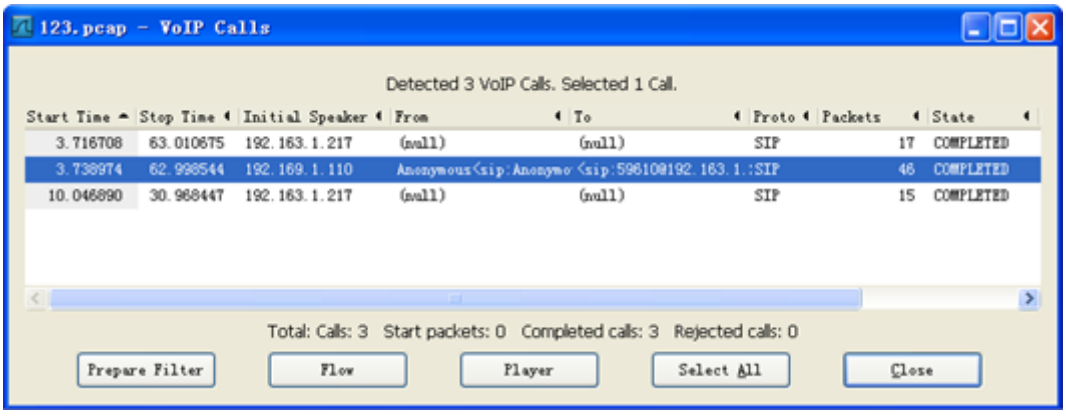
1. Choose **Telephony** > **VoIP Calls**, as shown inFigure 1-13.

Figure 1-13 Selecting call-related packets



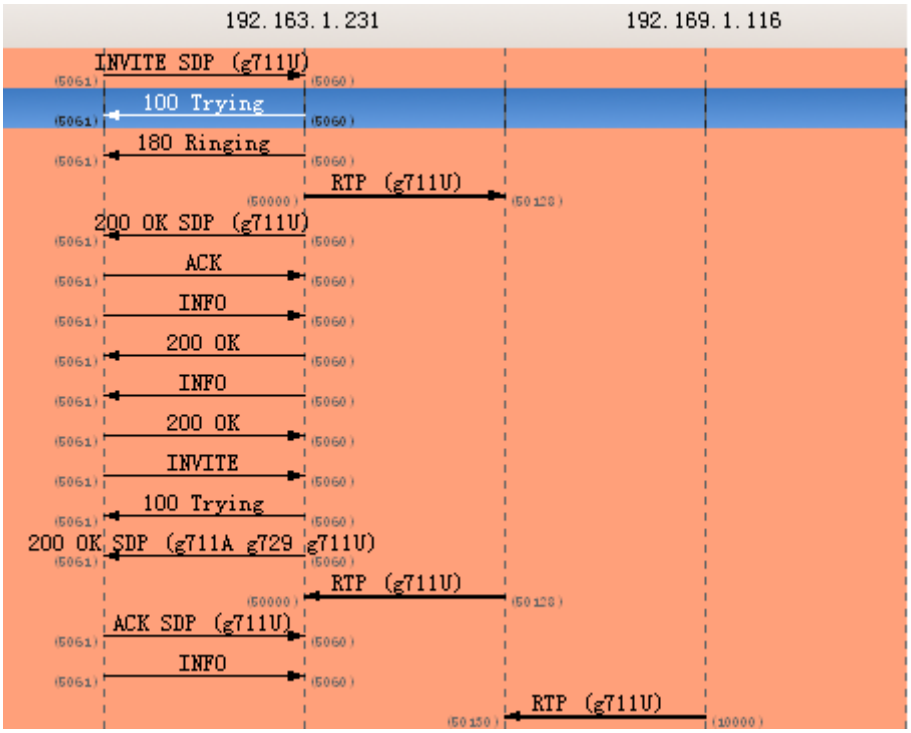
2. Select a call based on the calling number and called number, as shown in Figure 1-14.

Figure 1-14 Selecting the number of calls



3. Click **Flow**. The SIP signaling flow for the call is displayed, as shown in Figure 1-15.

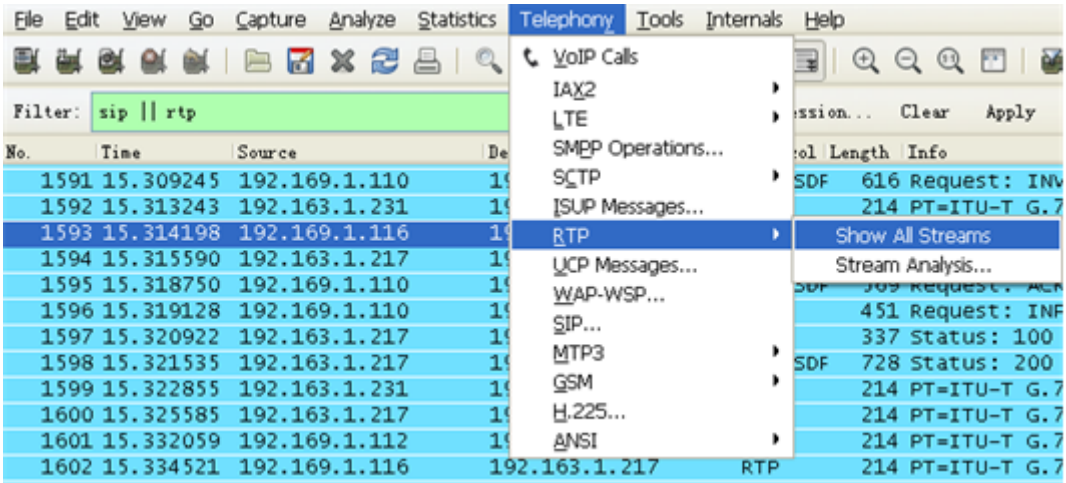
Figure 1-15 SIP signaling flow



- Analyzing RTP packets

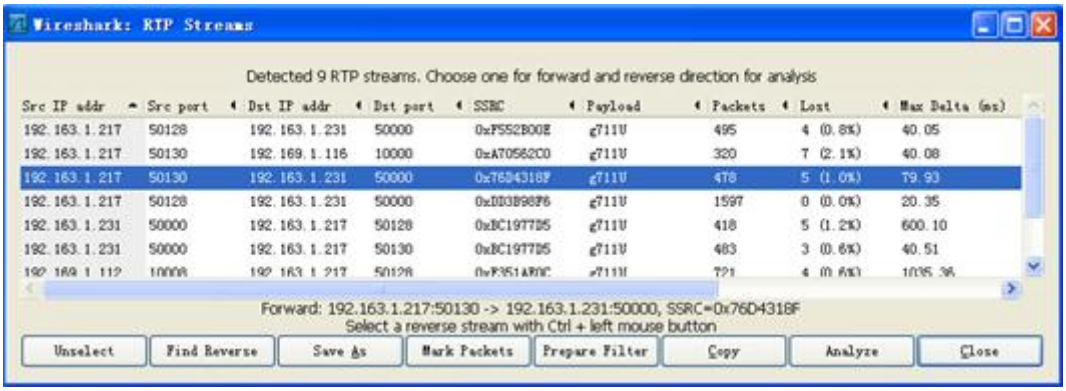
1. Choose **Telephony** > **RTP** > **Show All Streams**, as shown in Figure 1-16.

Figure 1-16 Selecting all RTP packets



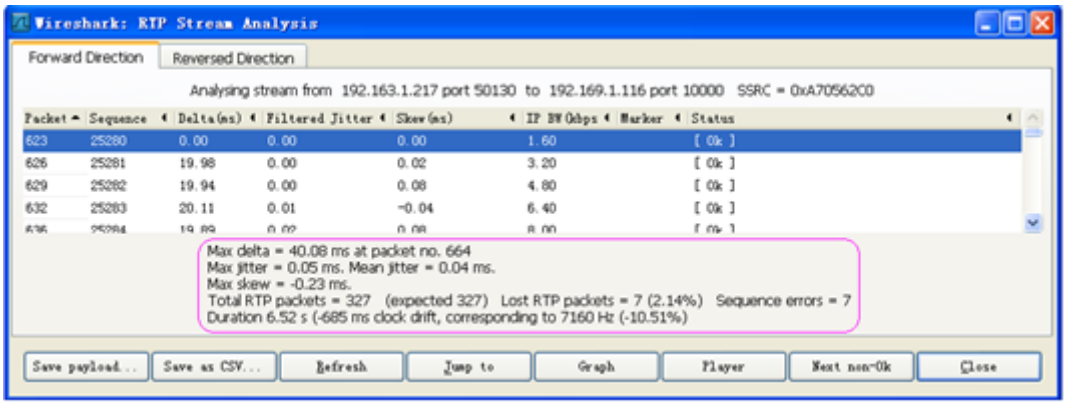
2. Select the data to analyze, as shown in Figure 1-17.

Figure 1-17 Selecting RTP packets to be analyzed



3. Click **Analyze**, as shown in Figure 1-18.

Figure 1-18 Checking the RTP packet analysis result



By performing the preceding steps, you can analyze the RTP stream and evaluate the quality of the bearer network based on the packet loss, jitter, and disorder data.

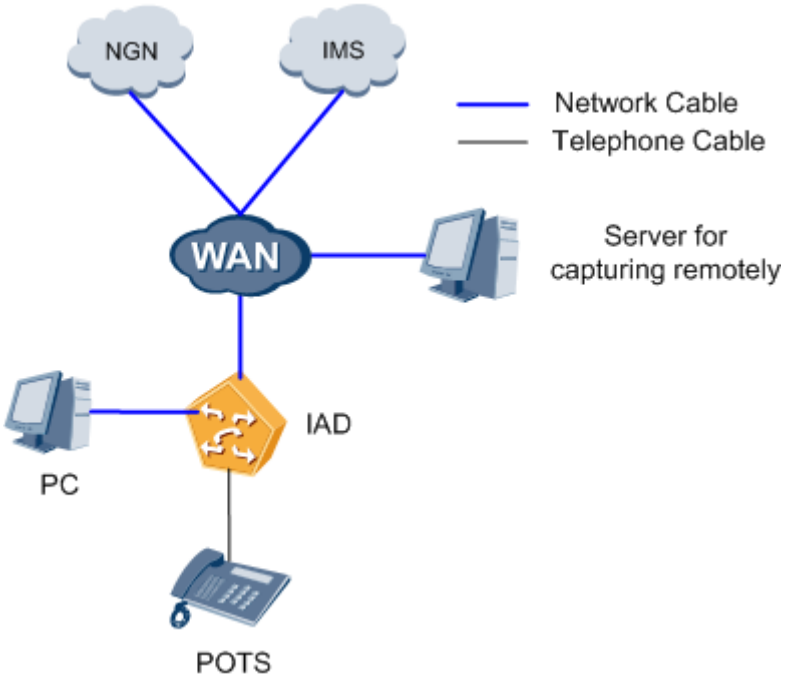
----End

1.3.9 Capturing the Network Packets Remotely

If the IADs are distributed widely and local capturing is not convenient, you can use the remote capture function of the IAD to capture data flow that interact with the IAD, according to certain users and the direction of data.

Example

Network Diagram

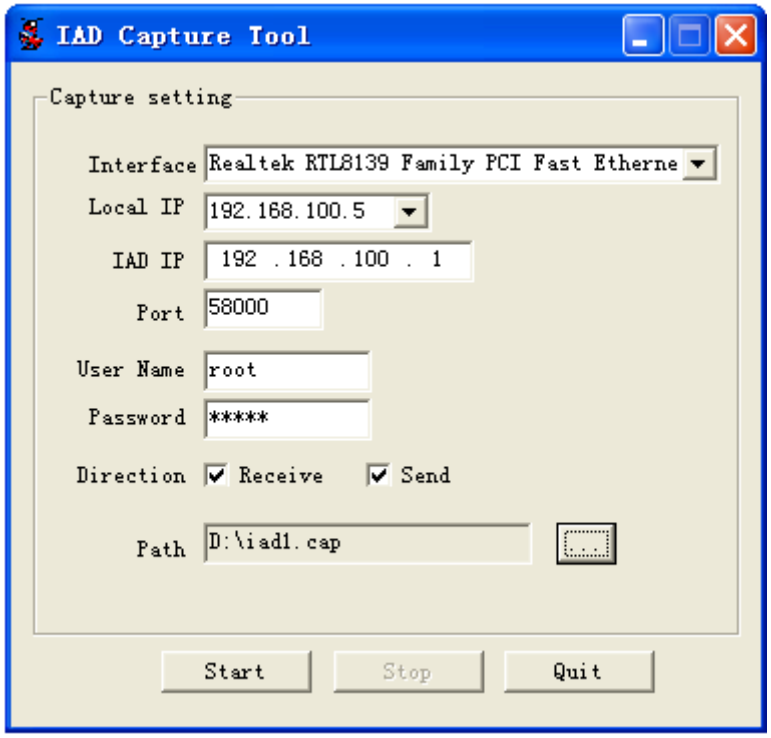


Procedure

1. Double-click 

to run the capture tool. The page is displayed, as shown in Figure 1-19.

Figure 1-19 Capture tool interface



2. According to Table 1-9 to set the tool.

Table 1-9 setting on the tool

Parameters	Description
Interface	Select the network card style for capturing.
Local IP	The IP address of the remote packet capture server
IAD IP	The IP address of the IAD.
Port	Port number. The default port number 58000 is proposed.
User Name	The user name for logging in the IAD.
Password	The password for logging in the IAD.
Direction	The capture direction.

3. click ... and enter the capture file name, for example, **iad1**. Then click **Save**.
4. Click **Start** to start capturing.

NOTE
When the size of the file that recvTool captured reaches 30 MB, the tool will create a file and save it, and then continue capturing flow.

5. If the capture process is complete, click **Stop** or **Quit** first, and then operate the capture file. Otherwise the capture file will be incomplete.

NOTE
Manage the captured packets carefully.

Related Commands

You can change the configuration on the IAD according to the following commands.

Table 1-10 Packet capturing commands of IAD101H, 102H, 104H, 208E(M) and 132E(T)

Operation	Command
Set the address and port of the capture server	**capture server ipaddress** <*a.b.c.d*> [**udpport** <*1-65534*>]
Open or close the signal capture switch	**capture signal** <**on** | **off**>
Open the RTP flow capture switch	**capture media start direction** <**receiveonly** | **sendonly** | **all**> [**userport** <*port-ID*>]
Close the RTP flow capture switch	**capture media stop**

1.3.10 Bad AT0 Grounding

The procedure is as follows:

Step 1 Verify that the device ground cables are connected to the ground bar of the equipment room.

Step 2 Verify that devices are installed in cabinets and the ground terminals of cabinets are properly connected to the ground bar of the equipment room.

Step 3 Verify that the ground bar of the equipment room is properly connected to the ground busbar (without paint) of the building.

Step 4 If the power supply cable is used as the ground cable, verify that the power supply cable is a three-core cable without extended two-core cables.

Step 5 Use multimeter to test the voltage difference between the chassis shell ground and the earth. If the voltage difference is greater than 10 V, the ground is poor.

Step 6 Use multimeter to test the impedance between the chassis shell ground and the earth. If the impedance is greater than 10 ohms, the ground is poor.

Step 7 If you cannot test the voltage of the earth, use the multimeter to test the voltage difference between the chassis shell ground and the live line, naught line, and earth line in the three-core ground cable. If the voltage difference is greater than 10 V, the grounding is poor.

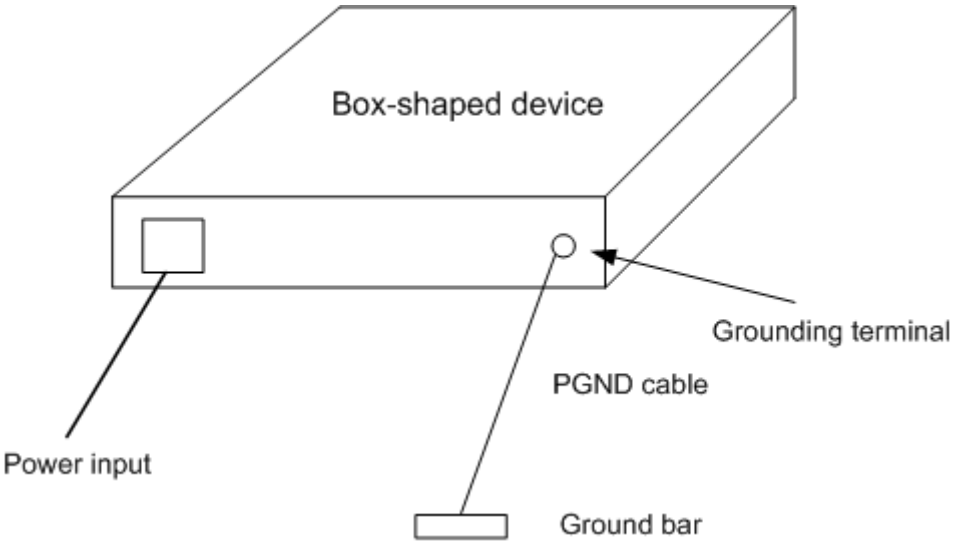
----End

Detailed ground requirements are as follows:

Ground Bar Is Installed in the Equipment Room

When the ground bar is already installed in the equipment room, check whether the ground bar is reliably grounded. If the ground bar is reliable, connect one end of the yellow-and-green protection ground (PGND) cable to the wiring terminal on the ground bar, and tighten the fixation nut firmly, as shown in Figure 1-20. The cross-sectional area of the PGND cable must not be less than 4 mm^2, and the PGND cable should be as short as possible. Do not wind the cable.

Figure 1-20 Grounding diagram when the ground bar is installed in the equipment room

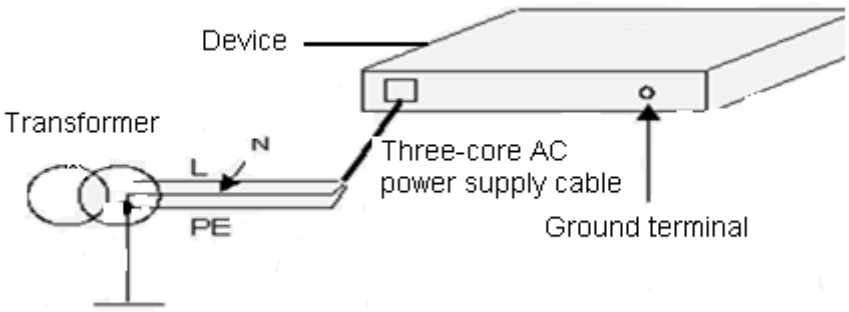


If a device is installed on a 19-inch cabinet, connect the yellow-green PGND cable of the device to the ground terminal on the 19-inch cabinet and connect the ground terminal to the ground bar of the equipment room.

Ground Bar Is Not Installed in the Equipment Room, and the Ground Electrode Cannot Be Buried Nearby

If a device uses 220 V AC power supply, the PE line of the AC power supply can be used as the ground cable. Ensure that the PE line of the AC power supply is properly grounded inside the power distribution room or beside the AC voltage transformer, as shown in Figure 1-21. In addition, ensure that the PE terminal of the device is reliably connected to the PE line of the AC power supply. Use the three-core cable with PGND cable as the power cable for the device.

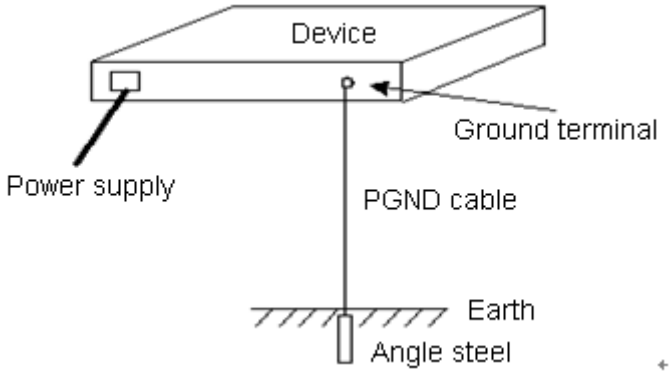
Figure 1-21 Grounding diagram when the PE line of the AC power supply is used as the ground cable



Ground Bar Is Not Installed in the Equipment Room, but the Ground Electrode Can Be Buried Nearby

When no ground bar is installed in the equipment room, and the ground electrode can be buried nearby, use an angle steel or steel pipe not shorter than 0.5 m. Bury the angle steel or steel pipe directly in the earth. The cross-sectional area of the angle steel should not be less than L x W x H = 50 x 50 x 5 (mm^2), and the steel pipe should not be thinner than 3.5 mm. The material used should be steel plated with zinc. Weld the yellow-green PGND cable of the device with the angle steel. Paint the surface of the welding point with anti-rustic paint. The cross-sectional area of the PGND cable must not be less than 4 mm^2, and the PGND cable should be as short as possible. Do not wind the cable. See Figure 1-22.

Figure 1-22 Grounding diagram when the ground electrode can be buried nearby



Ground Impedance Requirements

The ground impedance of an equipment room is determined by the equipment room environment. The ground impedance of a central equipment room must comply with standard YDJ26-89 (less than 1 ohm); that of a common equipment room must be less than 5 ohms; that of angle steel buried in the earth must be less than 10 ohms. In the area with high soil impedance ratio, spray some salt water or impedance-reducing agents to the earth.

Table 1-11 Common device ground specifications

No.	Specifications
1	The design for ground must follow the principle of equal voltage and equal electric potential. That is, the working ground and protection ground (including the shielded ground and the lightning-proof ground of the cable distribution frame) are jointly grounded in the same group of ground electrodes.
2	The cable tray, rack or shell, metal ventilation pipe, and metal door or window in the equipment room must be grounded for protection.
3	The metal device parts that are neutral in normal conditions must be grounded for protection.
4	The ground cable must be connected properly to the protection ground bar of the equipment room.
5	Only the specified device can be used as components for the electrical connection of the ground cable.

Table 1-12 IAD ground specifications

No.	Specifications
1	All communication devices and auxiliary devices (such as mobile base station, transmission devices, switches, power supply devices) in the equipment room must be grounded for protection. Connect all PGND cables for various devices jointly to a general ground bar, and then to the same PGND bar together with the PGND of devices in the room.
2	The PGND of the equipment is shorted to the copper protection ground bar provided by the customer. The short-circuiting cable used should be an alternating yellow and green plastic insulating one with copper core, with cross-sectional area greater than 35 mm^2.
3	There are ground terminals and ground flags at the lower part of the front door, rear door and side panel of the cabinet, connected to the ground terminals of the cabinet framework through connection cables with cross-sectional area no less than 1.6 mm^2.
4	Keep all metal components of a cabinet in good conductibility. No insulating coating can be sprayed on the connection between the metal components.
5	Connect the cabinets in the same row closely by fastening captive screws and gaskets on the top of the cabinets. Do not spray coating into a rectangle area of 30 x 50 mm around the connection hole for captive bolt. Measures to prevent rust and corrosion must be taken for this area. Zinc electroplating with iridescent yellow chromate conversion coating should be applied to the gasket and nut to ensure sufficient electric contact.
6	During combination cabinets of the same type, short-circuiting cables are used to connect the ground busbars (if any) of the cabinets. The cross-sectional area of the short-circuiting cable is 6 mm^2 and the length is less than 300 mm. Connect the two ends of the short-circuiting cable respectively to the ground busbar terminals on the neighboring cabinets and fix them firmly.

Table 1-13 Communication cable ground specifications

No.	Specifications
1	The AC power supply system of the equipment room uses the TN-S power supply mode.
2	The inlet for the AC power cable at the equipment room should be equipped with a lightning protection device with a nominal discharging current not less than 20 kA.
3	The protection ground for power supply and that for devices share the same group of ground electrodes. If the power supply and devices are in the same equipment room, try to use the same protection ground bar for them.
4	Add lightning protection circuit for the AC power interface.
5	The positive pole of the -48 V DC power supply (or negative pole of the 24 V DC power supply) must be grounded at the output of the DC power supply.
6	The working ground and protection ground of the DC power supply must use the same group of ground electrodes with the protection ground of the switches. If the power supply and devices are in the same equipment room, try to use the same protection ground bar for them.
7	Add surge protection for the DC power interface.

Table 1-14 Signal cable ground specifications

No.	Specifications
1	If there are digital trunks that connect a transmission device directly or indirectly to a wireless communication station, install an E1 lightning protection device for the relative interface of the transmission device.
2	Equip the cables laid outdoors with the metal jacket whose two ends are well grounded, or connect the cables to the protection ground bar of the equipment room. For cables inside equipment room, install the lightning protection device at the device interfaces. The PGND cable for the lightning protection device should be as short as possible.
3	Both ends of the external conductor of the coaxial cable and those of the shield layer of the shielded cable must have good electric contact with the metal shell of the device they connect to.
4	In the incoming and outgoing signal cables to and from the office, the idle line pair inside the cable must be grounded for protection.
5	The Tone & Data Access (TDA) cable will inevitably pass the Main Distribution Frame (MDF) with security unit when going out the office. Its shield layer must be connected to the protection ground of the MDF. The MDF must use the same group of ground electrodes with the cabinet.
6	The signal cables within the area of the communication office and mobile

No.	Specifications
	station should not be arranged aerially.

Table 1-15 Cable ground specifications

No.	Specifications
1	The ground leading cannot be arranged parallel to the signal cable, and crossover is not allowed.
2	The ground cable cannot be led in aerially, but buried in the earth globally or arranged indoor.
3	Do not extend the PGND cable, or add any switch or fuse.
4	The PGND cable used should be an alternating yellow and green plastic insulating one with copper core.
5	Do not connect the neutral line of the AC power cable with the protection ground of any telecom device in the equipment room.
6	The length of the PGND cable should not exceed 45 m and should be as short as possible. If it is longer than 45 m, you can ask the user to replace the ground bar nearby.

Table 1-16 Basic ground requirements

Requirements	Effect
• Ground mode Joint ground. Connect the working ground, PGND, and lightning protection ground to the same group of ground electrodes. • Ground impedance ≤ 10 ohms • Ground cable The cross-sectional areas of PGND cables are determined by the maximum current. The cables must be efficient conductor cables, for example, copper cable. Bare connector cables cannot be used.	Standard and efficient ground is a major measure to keep communication devices stable. It protects people and devices from static electricity, lightening, and electromagnetic interference.

1.3.11 AT0 Ground Impedance Test

Ground Impedance Test Principles and Precautions

Background

A ground is a conducting connection between an electrical circuit or device and the earth (generally a ground electrode in the earth) to discharge the system of current. The ground system includes the ground electrode and ground cables.

Ground Types

- PGND

  When an electrical device is leaking because of some faults, personnel and devices could be exposed to the risk of electric shock. The PGND is provided to connect the electrical device house to the ground to prevent electric shock.
- Lighting protection ground

  Lightning production ground deals with the protection of buildings and other structures due to direct damage from lightning.
- Working ground

  Working ground is to connect an electrical circuit to the ground as required by the normal work or fault location.

In a ground system, a ground electrode is buried in the earth and is connected to a ground conductor by a connector. The ground conductor connects to the ground bar or device houses. If multiple devices connect to the same ground electrode by conductors, a ground bar is required and the ground bar should be installed near to the ground electrode. The conductors from different devices must be connected to the ground bar separately.

Test Principles

The ground impedance is mainly affected by the following variables:

- Depth of the ground electrode
- Diameter and length of the ground electrode
- Number of ground electrodes
- Around geographical environment (plain, slop, or ditch)
- Soil humidity

The 3-pole Fall of Potential method is used to test the ground impedance. The method is as follows:

Position two ground stakes in the soil in a straight line on one side of the ground electrode (X), equidistant from one another. The stake (Y) is 20 m away from the ground electrode and stake (Z) is 40 m away from the ground electrode. The potential difference between X and Y and the current between X and Z are measured by a tester. Using Ohm's Law (V=IR), the tester automatically calculates the impedance.

Precautions

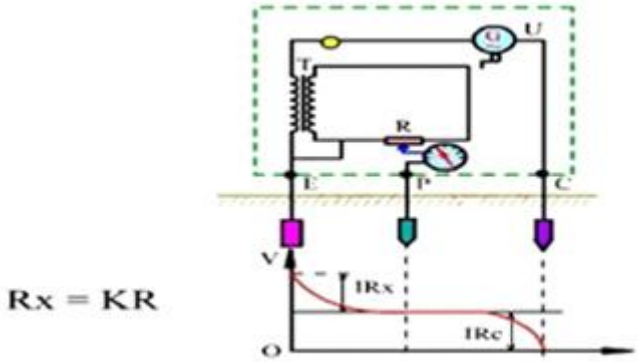
- The ground impedance changes with the season, weather, and soil humidity. Generally, the ground impedance tested in autumn is more precise.
- Before testing the PGND impedance, disconnect the ground cable from the device.

- If a ground electrode is severely rusty or corroded, polish the electrode and then test the impedance.
- Before testing the working ground (single-point ground), verify that the ground cable is connected to the device properly. If they are not connected, you cannot perform test; if the connection is abnormal, the test result is not accurate.
- Select a suitable test point because the test results on different points may vary greatly. If there is no available test point, you can remove the original ground conductor if necessary and connect a jumper cable that is easy to test.
- Prevent noise interference. If the current in the ground connector circuit is large, the test result will be inaccurate or even the impedance cannot be tested and noise may be displayed on the tester.

Normally, the PGND and working ground impedance of devices is less than 4 ohms and the lightning protection ground impedance of high buildings is less than 10 ohms. If the ground impedance does not meet the requirements, report the fact and monitor the rectification, such as, rebury the ground electrode or verify the ground conductor connections.

Figure 1-23 shows the ground impedance tester.

Figure 1-23 Ground impedance tester



Ground Impedance Test Method

Impedance Requirements

- AC working ground: not greater than 4 ohms.
- Security working ground: not greater than 4 ohms.
- DC working ground: determined by the actual devices.
- Lightning protection ground: not greater than 10 ohms.
- Joint shielded system ground: not greater than 1 ohms.

Resistance Tester Introduction

ZC-8 resistance tester is used to test the ground resistance of power supply systems, telecommunication devices, and lightning rods. IT can also test the resistance of low-resistance conductors and soil resistivity. The tester consists of a handle electric generator, current mutual-inductors, sliding resistor, and galvanometer. All these components are packed in plastic. In addition, probes and conductors are provided with the tester.

Preparation for Resistance Test

Prepare the following tools:

- ZC-8 resistance tester.
- Two test probes.
- Three conductors with the length of 5 m, 20 m, and 40 m.

Before impedance test, connect a 5 m conductor to point E, a 20 m conductor to point P, and a 40 m conductor to point C, and connect the other ends of the conductors to ground electrode E', potential probe P', and current probe C' respectively. Points E', P', and C' must be on a straight line and the distance between each other is 20 m.

Figure 1-24 shows the connection diagram for testing impedance greater than or equal to 1 ohm.

Figure 1-24 Connection diagram for testing impedance greater than or equal to 1 ohm

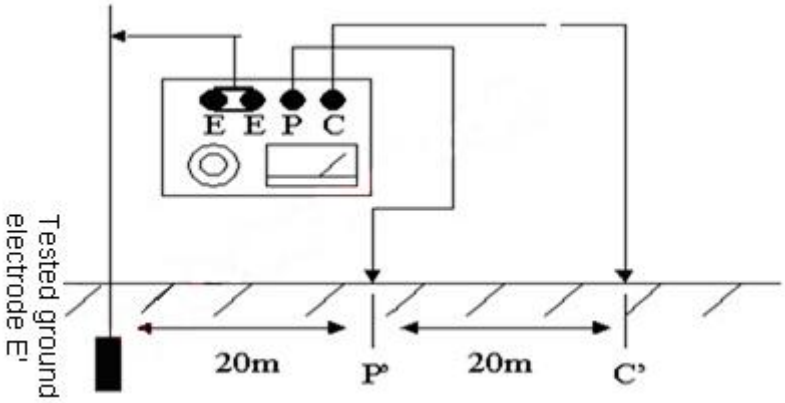
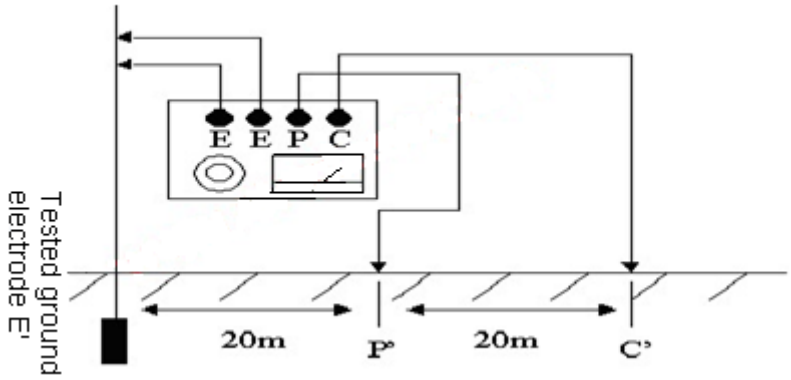


Figure 1-25 shows the connection diagram for testing impedance less than 1 ohm (both conductors on points E are connected to the ground electrode).

Figure 1-25 Connection diagram for testing impedance less than 1 ohm



Test Procedure

1. Ensure that the connections between the tester, ground electrode, and probes are correct.
2. Place the tester horizontally and ensure that the pointer is on the central line.

3. Set the ratio scale to the maximum, rotate the electric generator handle slowly, and move the tester until the pointer is on the central line.
4. When the pointer becomes stable on the central line, rotate the electric generator quickly (more than 150 rounds per minute), and move the tester until the pointer is on the central line again.
5. If the reading is less than 1, change the ratio scale to a smaller one and perform the test again.
6. If the pointer shakes, change the handle rotating speed until the pointer becomes stable.

Precautions

- Place and take the tester carefully and avoid severe shake.
- The ground conductor must be disconnected from devices.
- The ground electrode to be tested cannot be surrounded by scattered current or polarized soil.
- Do not test the ground impedance when the soil humidity is too high (for example, after rain) or the temperature, pressure, and climate changes greatly.
- The probe must be far away from the big metal entities, such as pipes, cables, and railways. The current probe must be 10 m away from the metal entities and the potential probe must be 50 m away. If a metal entity does not connect to the ground system, the distance can be shortened by 1/2 to 1/3.
- The conductor must be well insulated.
- Select a proper position for the current probe and ensure that the potential of the ground electrode is 0 after the current probe is inserted to the soil.
- Test the impedance when the soil impedance ratio is high, such as in earlier winter.
- No electrolyte is allowed around the test area.
- If the tester is highly sensitive, plug the potential probe shallower; if the tester is not sensitive, moisten the probe.

1.4 FAQs

This topic describes frequently asked questions (FAQs) of users when they use the IAD, including query FAQs and operation FAQs.

1.4.1 Query-Related FAQs

This topic provides query-related FAQs, including how to query devices' IP addresses and version information.

What Are the Default IP address, User Name, and Password Used to Log In to the IAD

Q: What are the default IP address, user name, and password used to log in to the IAD?

A: The default IP address for IAD208E(M), IAD132E(T), IAD1224, and LAN port of IAD101H/102H/104H is **192.168.100.1**. The default user name is **root**, and the default password is **admin**.

How Do I View the IP Address of the IAD

Q: How do I view the IP address of the IAD?

A: The method varies according to the IAD model:

- For IAD208E(M), IAD132E(T) and IAD1224, connect a phone to the IAD, and dials *127. The IAD automatically plays an announcement indicating the IP address. For details, see the product document.
- For IAD101H/102H/104H, use a network cable to connect a PC to the LAN port on the IAD, and enter **telnet 192.168.100.1** in the **Run** dialog box to log in to the IAD. The default user name is **root**, and the default password is **admin**. In the privilege mode, run the **display ipaddress** command to display the IP address. For details, see the *eSpce IAD Product Documentation*.

How Do I View the MAC Address of the IAD

Q: How do I view the MAC address of the IAD?

A: You can view the MAC address in either of the following ways:

- Log in to the web management system, and choose **Basic Configuration** > **Network Parameter**.
- Log in to the CLI, and run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode. Then run the **display mac-address** command.

NOTE
IAD101H/102H/104H supports only the CLI mode.

How do I view the physical sequence number of the IAD

Q: How do I view the physical sequence number of the IAD?

A: You can view the physical sequence number in either of the following ways:

- Log in to the web management system, and choose **Advanced Configuration** > **UCEMS Configuration**.
- Log in to the CLI, and run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode. Then run the **display physical-serial-num** command.

NOTE
IAD101H/102H/104H supports only the CLI mode.

How do I view the software version of the IAD

Q: How do I view the software version of the IAD?

How do I view the system information

Q: How do I view the system information?

A: For details, see **Maintenance** > **Viewing the System Information** in the *eSpce IAD Product Documentation*.

How do I view the elabel of the IAD

Q: How do I view the elabel of the IAD?

A: You can view the MAC address in the following ways:

- IAD101/102/104H, IAD208E(M) and IAD132E(T)

  Log in to the CLI, and run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode. Then run the **display elabel** command.
- IAD1224

  Log in to the CLI, and run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode. Then run the following commands:
  - For the CVP, run the **display elabel cvp** command.
  - For the backboard, run the **display elabel backboard** command.
  - For the ASI or OSU board, run the **display elabel pots** command.

1.4.2 Operation-Related FAQs

This topic provides operation-related FAQs, including how to resolve problems that users encounter in product configuration and information query.

How do I log in to the IAD management system

Q: How do I log in to the IAD management system?

How Do I Log In to the IAD If I Forget the Password

Q: How do I log in to the IAD if I forget the password?

A: You can log in to the IAD in either of the following ways when you forget the password:

- Log in to the IAD using Telnet: Enter the user name **system** and password **login** on the Telnet login page to log in to the IAD. Manually restore factory settings in the global configuration mode, and restart the IAD. When the IAD restarts, use the default IP address **192.168.100.1**, user name **root**, and password **admin** to log in to the IAD.
- Log in to the IAD using the serial port:

1. Use a serial cable to connect the PC and IAD, and restart the IAD.
2. View the messages displayed on the serial port interface. When the following message is displayed, press Ctrl+R:

   ```
   Press CTRL+R to restore vendor-config  3s
   ```
3. When the following message is displayed, enter Y or y. The IAD automatically restores to factory settings and restarts.

   ```
   Confirm to restore vendor-config? [Y|N] :
   ```
4. When the IAD restarts, use the default IP address **192.168.100.1**, user name **root**, and password **admin** to log in to the IAD.

How do I restore the IAD to factory settings

Q: How do I restore the IAD to factory settings?

How to restart the IAD

Q: How to restart the IAD?

How do I change the IP address of the IAD

Q: How do I change the IP address of the IAD?

A: For details, see **Maintenance** > **Changing IP address** in the *eSpce IAD Product Documentation*.

How do I set the upper and lower limits of the hookflash duration

Q: How do I set the upper and lower limits of the hookflash duration?

A: Log in to the CLI, and run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode. Then run the **dev parameter set** command in the following modes:

- IAD101H/102H

  Run the **devasi parameter set 1** command to set the upper limit, and run the **devasi parameter set 2** command to set the lower limit.
- IAD104H

  Run the **devasi parameter set 3** command to set the upper limit, and run the **devasi parameter set 4** command to set the lower limit.
- IAD1224

  Run the **devasi parameter set 1** command to set the upper limit, and run the **devasi parameter set 2** command to set the lower limit.
- IAD208E(M), IAD132E(T)

  Run the **devasi parameter set 3** command to set the upper limit, and run the **devasi parameter set 4** command to set the lower limit.

How do I change the protocol mode

Q: How do I change the protocol mode?

- A: You can do as follows:
  - To change to the SIP mode, log in to the CLI, run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode, and run the **protocol-mode sip** command.
  - To change to the MGCP mode, log in to the CLI, run the **enable** and **configure terminal** commands in sequence to enter the global configuration mode, and run the **protocol-mode mgcp** command.

NOTE
IAD101H/102H/104H supports only the CLI mode.

How do I set the VLAN priority on the IAD

Q: How do I set the VLAN priority on the IAD?

How do I set the fax function on the IAD

Q: How do I set the fax function on the IAD?

How do I enable the pulse dialing function

Q: How do I enable the pulse dialing function?

A: You can do as follows:

- IAD101H/102H/104H

  Log in to the CLI, and run the **enable**, **configure terminal**, and **advanced** commands to enter the advanced mode. Then run the **pstnport attribute set 0 enable** command. If port 0 needs to be connected to the DTMF phone, run the **pstnport attribute set 0 disable** command to disable the pulse dialing function.

- IAD208E(M), IAD132E(T) and IAD1224

  Log in to the web management system, and choose **Advanced Configuration** > **PSTN Port Attribute Configuration**. The page for setting the PSTN port attributes is displayed. Select a port and click **Modify**. On the page that is displayed, enable the pulse dialing function and click **OK**.