# User Support Level 2

**Introduction**
The supporter finds here instructions how to handle a user's level 2 telephony problems:

◊ Best Practice for Handling an User Problem
◊ Record the Customer's Data and Problem Description
◊ Analyzing the Customer Problem
◊ Solving the Customer Problem

## Contents

# Introduction Support Level 2

The level 2 support is the first instance where the user's telephony problems are handled that a user cannot solve himself. Additionally the level 2 supporter must be able to detect if the user problem is a "single" problem or if there is a large scale problem, that produces the same problem for multiple customers, e.g. data transfer problems in the Internet so that no VoIP call signaling is possible.

The level 2 supporter must be aware of the complexity of a VoIP system and the multitude of telephony solutions on the user side. Further he needs an understanding of:

      ◊ IP networking
      ◊ VoIP protocols SIP for signaling, SDP and RTP for speech transmission.

Overview of a VoIP system and the multitude of user telephony solutions:
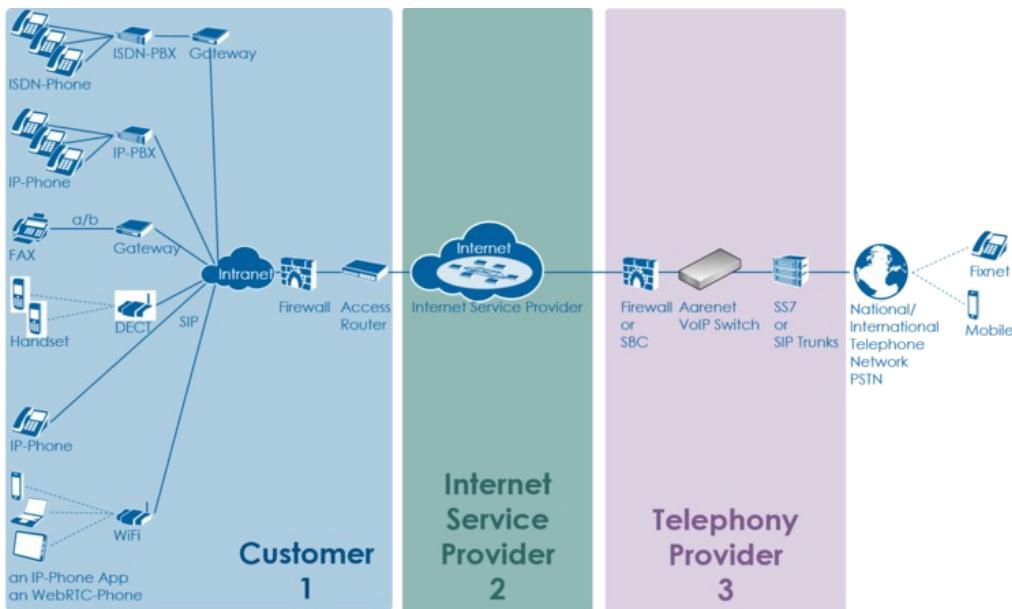


The level 2 supporter faces problems with the following layers:

    1. Equipment
    2. IP data transfer
    3. Telephony service

And each of this layer can be located into the following raw areas:

    1. Customer/User site
    2. Internet Service Provider ISP
    3. Telephony Provider

This layer and dividing into areas produces a "3x3 Support Matrix":

|  | 1 Customer | 2 Internet Service Provider | 3 Telephony Provider |
|---|---|---|---|
| **T - Telephony Service** | VoIP:<br>• Registration<br>• SIP protocol<br>• Device configuration<br>Security:<br>• TopStop<br>• Password | VoIP:<br>• QoS for VoIP | VoIP System:<br>• VoIP Switch status<br>• Access PSTN<br>• Customer account configurations<br>Security:<br>• VoIP ALG off |
| **D - Data Transfer** | IP Data Routing:<br>• QoS for VoIP<br>• IP routing<br>• Internet access<br>Security FW / Acc. Router:<br>• IP policies<br>• NAT | IP Data Routing:<br>• QoS for VoIP<br>• Redundant IP routing<br>• Routing protocols<br>Security:<br>• IP link (redundant)<br>• VPN | IP Data Routing:<br>• QoS for VoIP<br>• IP routing<br>• VLan<br>Security:<br>• IP policies<br>• VoIP ALG off |
| **E - Equipment** | Devices:<br>• Telephone, DECT, FAX<br>• PBX / Gateway<br>• Access Router / FW<br>Cabling:<br>• Supply<br>• Patch cable | Devices:<br>• Router<br>• IP Switch<br>• Redundant equipment<br>Cabling:<br>• Supply<br>• Patch cable | Devices:<br>• Router / Firewall / SBC<br>• IP Switch<br>• VoIP Server<br>Cabling:<br>• Supply<br>• Patch cable |

Within this "3x3 Support Matrix" the supporter can:

◊ advice the customer what to do when the problem is located in the nodes 1-T, 1-D and 1-E
◊ check the customer configurations on the VoIP Switch, node 3-T, and, if he has operator rights, adjust configurations.

For the other cases the level 2 supporter must be able to identify if:

◊ the user must contact his ISP, due to possible Internet access problems
◊ the VoIP System administrator must be involved, due to possible telephony service problems
Hint:
These cases indicate mostly large scale problems within the VoIP system!

# Best Practice for Handling an User Problem

| Best Practice | 1. Record the customer's data and problem description:<br>  ♦ Get the customer data<br>  ♦ Get the problem description from the customer<br>  → Show me how ...<br><br>2. Cross check the user input against the VoIP switch configuration and logs.<br>  Via ConfigCenter check the users account configuration:<br>  · Telephone number registration<br>  · TopStop<br>  · RuleSet<br>  · Consult the "Call Data" for the last connection attempts and connections longer than 2min<br>  → Show me how ...<br><br>3. Evaluate the user's VoIP setup:<br>  ♦ For questioning and analyzing the user's problem it is necessary that the supporter is aware of the VoIP setup of the user.<br>  → Show me how ...<br><br>4. Check the big picture: |
|---|---|

- ♦ If you are sure that the problem is "single" one continue with the next step "Solve the customer problem"
- ♦ If you suspect that the customer is not the only one with this problem within a short time range, e.g. 30min, then contact the VoIP switch administrator/operator if there is known issue in the VoIP system that causes this type of problem.
  → Show me how ...

5. Solve the customer's problem:
- ♦ You have now enough basic information for solving the customer's problem
  → Show me how ...

6. If you are not able to solve this problem then contact the provider support. Have ready all collected information and what you have done and found out until now.

The supporter shall record the user information and the results of the own research:
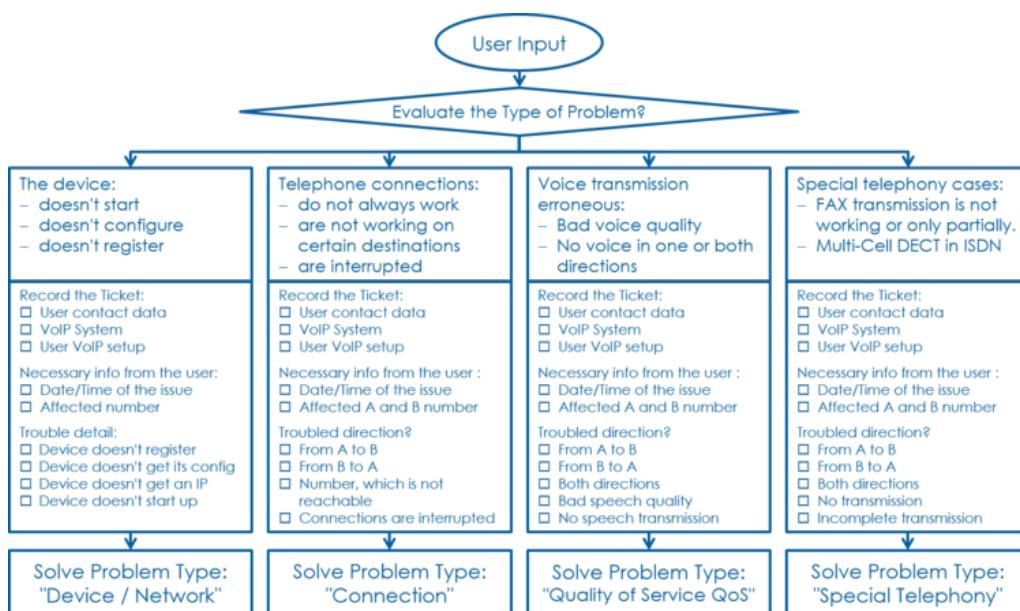


| Note | This information is most welcome if the supporter needs the support of the provider and has to inform him about the case. |
|------|--------------------------------------------------------------------------------------------------------------------------|

# Step 1: Record the Customer's Data and Problem Description

## Get the Customer's Data

From the customer get:

◊ Name of the caller
◊ Telephone number of the caller
◊ if applicable the company name

## Write down the Customer's Problem Description

From the customer get:

> ◊ Date and time of the issue
> ◊ The involved telephone numbers
> ◊ The problem description

If the customer doesn't know then identify via the ConfigCenter the telephone number and its associated account.

# Step 2: Cross Check the User Inputs

With this cross check the supporter can validate the user information, gets an impression of the state of the account and will probably find the reason for the user problem...

Via ConfigCenter check the users status and account configuration on the VoIP Switch:

1. Check "Validity":
   Check if the user account and its addresses are existing and "valid".
2. Check  the telephone number registration status.
   If there is no registration you can proceed directly with  ➔  The user device is not registered ...
3. Check "TopStop":
   Check if a TopStop in the account or address prevents the user from doing outgoing calls.
4. Check "RuleSet":
   Check if a selected RuleSet in the account or address configuration prevents the user from doing outgoing or receiving calls.
5. Check "Call Forwards" or "Call Rejecting":
   Check if a "Call Forwards" or "Call Rejecting" in the account prevents the user from doing outgoing or receiving calls.
6. Check "Call Data":
   Consult the  "Call Data" for the last connection attempts and connections longer than 2min of the user.

# Step 3: Evaluate the User's VoIP Setup

For questioning and analyzing the user's problem it is necessary that the supporter is aware of the VoIP setup of the user.

The experienced supporter knows of the user's VoIP setup after the  cross check . If not here the supporter finds the most implemented VoIP setup's.

## VoIP Setup: Residential

Characteristics:

> ◊ Private household
> ◊ Single or few telephone number
> ◊ Each telephone number registers individually

Most common problems:

> ◊ Account or telephone number blocked on the VoIP switch
> ◊ Telephone number not correctly ported to the telephony provider
> ◊ Telephone not correctly configured

◊ Telephone, cables defect
◊ Internet access fails

Overview VoIP Setup:
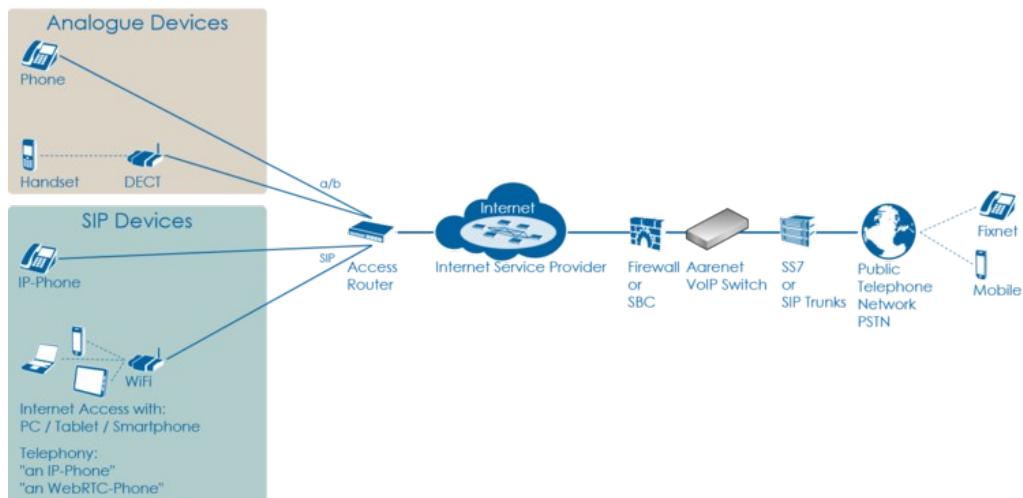


# VoIP Setup: Legacy ISDN PBX

Characteristics:

◊ Company PBX
◊ The ISDN PBX is connected via BRI or PRI to an ISDN-SIP Gateway
◊ One or more telephone number ranges
◊ The telephone numbers are registered via a main number
◊ The telephone number of incoming calls are signaled with only a few digits

Most common problems:

◊ Account or telephone numbers blocked on the VoIP switch
◊ Telephone number ranges not correctly ported to the telephony provider
◊ Telephone number ranges not completely configured on the VoIP Switch
◊ Wrong incoming telephone number signaling
◊ Internet access fails
◊ The company Firewall VoIP ALG interferes with the SIP signaling or needed IP ports are blocked.
◊ QoS problems for speech, Fax, DECT

Overview VoIP Setup:
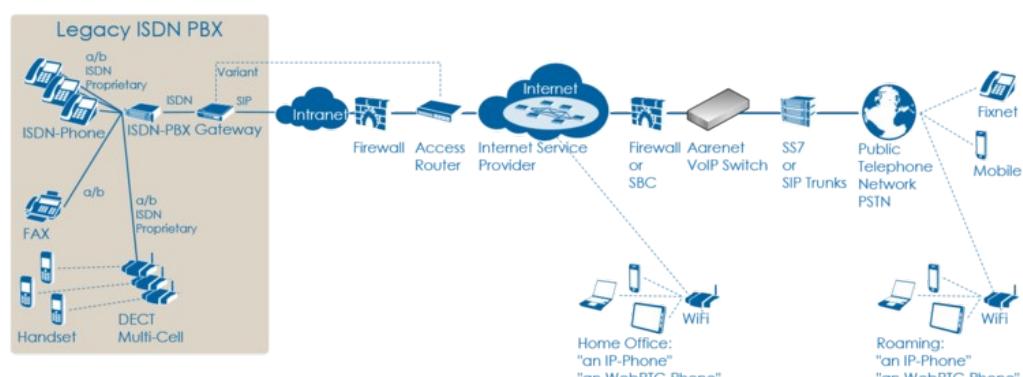
# VoIP Setup: IP PBX

Characteristics:

◊ Company PBX
◊ The IP PBX is connected directly or via SBC to the VoIP Switch
◊ One or more telephone number ranges
◊ The telephone numbers are registered via a main number

Most common problems:

◊ Account or telephone numbers blocked on the VoIP switch
◊ Telephone number ranges not correctly ported to the telephony provider
◊ Telephone number ranges not completely configured on the VoIP Switch
◊ The company Firewall and/or SBC VoIP ALG interferes with the SIP signaling or needed IP ports are blocked.
◊ Internet access fails
◊ QoS problems for speech

Overview VoIP Setup:
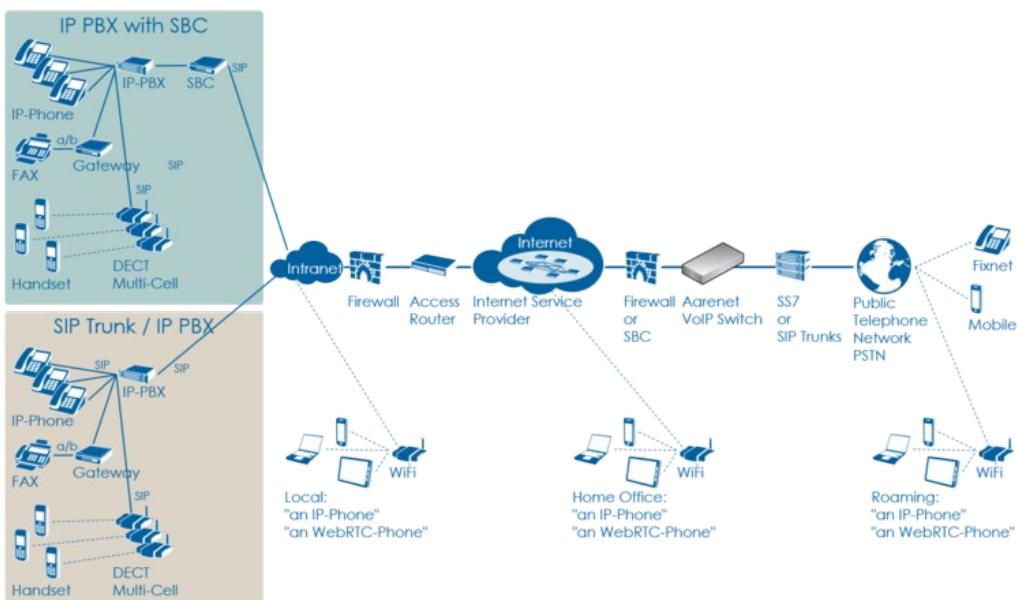


# VoIP Setup: vPBX

Characteristics:

◊ Company PBX
◊ The IP Phones are connected directly to the VoIP Switch
◊ One or more telephone number ranges

Most common problems:

◊ Public account and/or public telephone numbers blocked on the VoIP switch
◊ Public telephone number ranges not correctly ported to the telephony provider
◊ Telephone number ranges not completely configured on the VoIP Switch
◊ Private account and/or private telephone numbers blocked on the VoIP switch
◊ Provisioning of the SIP devices out of the AdminCenter
◊ The company or home office Firewalls and/or SBCs VoIP policies or ALG interferes with the SIP signaling or needed IP ports are blocked.
◊ Company/home office Internet access fails
◊ QoS problems for speech, FAX, DECT

Overview VoIP Setup:
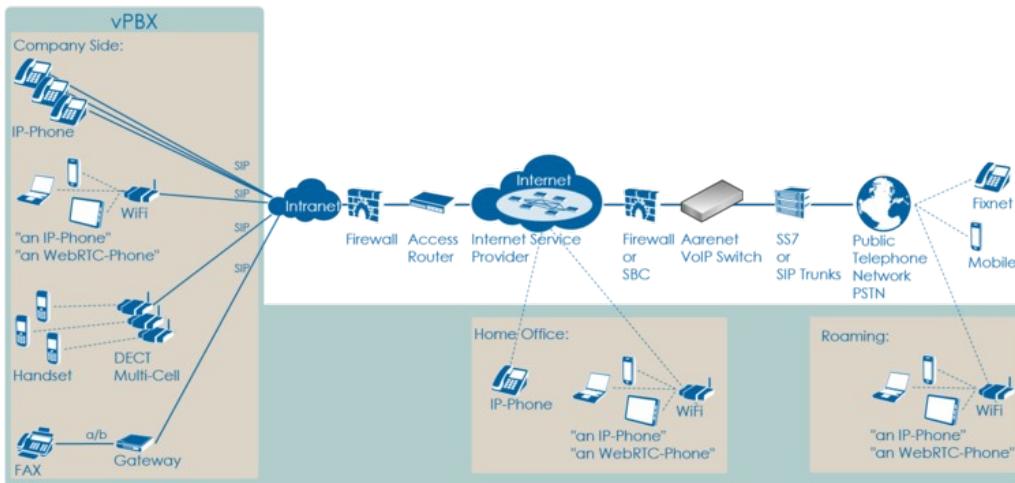


# Step 4: Check the "Big Picture"

At this point the supporter should get aware if the problem is limited to this user or if it could be large scale problem within the VoIP System.

If the supporter suspects a large scale problem, due to a great amount of the same ore similar user complains then he should contact the telephony provider support or emergency organization.

If the supporter has enough privileges he can check:

1. The   VoIP Switch component status
   This will show if the VoIP Switch itself has a problem.
2. The   VoIP System monitor
   Here you can check if:
   · The registrations dropped in a large scale
   · The calls dropped in a large scale
   · The IP connectivity somewhere in the VoIP system failed

At any rate the supporter **must inform** the VoIP system administrator!

# Step 5: Solve the Customer Problem

## Solve "Device / Network / Configuration / Registration" Problems

This problem type covers the following erroneous conditions:

◊ The device doesn't start
◊ The device doesn't integrate into the IP network
◊ The device is not correctly configured
◊ The device doesn't register at the VoIP Switch

| Note | If the device is connected to an IP-PBX then these problems must be solved with the responsible of the IP-PBX. |
|------|------|

### Solve "Device Hardware & Firmware" Problem

**1 Step: Is the device powered on, not defect?**

| | Customer | Internet ISP | Telephony Provider |
|------|------|------|------|
| **Telephony** | | | |
| **Data Transfer** | | | |
| **Equipment** | Check if the device correctly powered and shows basic activity?<br><br>◊ Is the power cable correctly plugged in?<br>◊ Is the power cable not defect?<br>◊ Does the device show power on indication, e.g. display on, LED on?<br><br>Actions:<br><br>Replace the power cable<br>Replace defect device if the powering is ok but no working indication is displayed | | |

| Warning | Defect power cables must be replaced!<br>Faulty power cables can be life-threatening! |
|------|------|

**2 Step: Is the device connected to the IP network?**

| | Customer | Internet ISP | Telephony Provider |
|------|------|------|------|
| **Telephony** | | | |
| **Data Transfer** | | | |
| **Equipment** | Is the device correctly connected to the IP network?<br><br>◊ Is the patch cable correctly plugged in?<br>◊ Is the patch cable not defect? | | |

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| | ◊ Are there LED flashing or glow next to the network plug on the device or at the peer device (access router, IP switch)?<br><br>Actions:<br><br>    Replace the patch cable<br>    Plug in the patch cable at a different port at the peer device (access router, IP switch)<br>    Replace defect device if the patch cable and peer port is ok but no working indication is displayed at the device port. | | |

**3 Step: Has the device a reasonable firmware loaded?**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | |
| **Equipment** | Has the device a reasonable firmware loaded?<br><br>    ◊ The user must check the loaded firmware<br><br>Actions:<br><br>    Replace the firmware if outdated or important bugs are fixed | | |

## Solve "Device Network" Problem

**1 Step: Has the device an IP address and can access the Internet?**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | Has the device got an IP address?<br><br>    ◊ Check on the device if it has received an IP address, e.g. via display or maintenance GUI.<br><br>Actions:<br><br>    ◊ If no IP address was assigned the user must:<br>    ◊   Check if the device is really connected to the IP network!<br>    ◊   Check if the device is configured with a fixed IP address!<br>          If it has a fixed IP does it match with the IP subnet?<br>          Is the default GW and DNS entry configured?<br>    ◊   Check if the device is configured to use DHCP!<br>          if the DHCP service in the IP network is running<br>          If the user cannot check the DHCP service he must contact the company IT responsible or the responsible of maintaining the access router.<br><br>Has the device access toward the VoIp Switch?<br><br>    ◊ Check if the device makes contact with the VoIP Switch via Internet or any private IP Link.<br><br>Actions:<br><br>    ◊   If the device shall connect via the Internet: | | |

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| | | | Connect a PC to the Ethernet port where the device usually is connected and try to connect to any public Web site.<br>◊ If the device shall connect via an private network check with the IT responsible if the access to the VoIP Switch is guaranteed. |
| **Equipment** | | | |

## Solve "Registration" Problem

**1 Step: Review the account and telephone number configuration**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | Check via ConfigCenter:<br><br>◊ Does the user account exist and is it "valid"?<br>◊ Does the telephone number exist and is it "valid"?<br><br>Actions:<br><br>◊ Check why the account, telephone number doesn't exist or is disabled<br>activate them if allowed. |
| **Data Transfer** | | | |
| **Equipment** | | | |

**2 Step: Where REGISTER messages received from the device on the VoIP Switch?**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | In the "Support Log" search for the device registration in the present and past time.<br><br>1. Set the "Support Log" filters<br>· Insert at "Text" the account name<br>· Insert at "From" - "Until" a reasonable time span where registrations could be expected<br>· Select the category: "Registration"<br>2. Start the search and find out according the results what is going wrong.<br>3. If needed repeat the search with the telephone number in the "Text" or other time spans<br><br>◊ Check the log results ➔ see below<br><br>Actions:<br><br>◊ ➔ see below |
| **Data Transfer** | | | |
| **Equipment** | | | |

Failed registrations due to disabled account or address:

2017-09-15-07:56:49.553 Registration failed, disabled account aan1-00093 tried to register number 0449980010

Actions:

◊ Check why the account is disabled and activate if allowed.


Failed registrations due to wrong SIP credentials:

> 2017-09-15-08:05:38.117 Registration failed, invalid credentials for account acc-01
> 2017-09-15-08:05:39.112 Registration failed, unknown username 'myusername' tried to register '0123456789'
> 2017-09-15-08:05:38.377 Registration failed, unknown number '0987654321' tried to register for account acc-01

Actions:

◊ The user must manually adjust the SIP credentials on the device
◊ The user must re-configure the device via AdminCenter


The device didn't refresh its registration:

> 2017-09-15-07:59:00.862 RegID989961 ended for 0987654321 ip=111.111.111.111:65398 ua=my-device v1.0

Actions:

◊ Order the user to check if the device is really on-line!
◊ Order the user to check if the device is defect? powered on? patch? IP address?    see below


For information a successful registration:

> 2017-09-15-07:59:30.383 RegID989965 started for 0987654321 ip=111.111.111.111:65398 ua=my-device v1.0


Hint:
The supporter might try to find REGISTER messages from the device in the  "Trace" . This gives the certainty that the message was received by the VoIP switch. The supporter can filter for the telephone number. If the IP address is needed then the customer must be able to tell or evaluate it, e.g.:

```
https://www.whatismyip.com/
```

**3 Step: Is the device correctly configured for registration??**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | For a manually configured device, check that the device has the correct configuration for:<br><br>◊ Telephone number<br>◊ SIP credentials<br>◊ VoIP Switch domain configuration<br><br>Actions:<br><br>The user must manually check the device configuration and if needed adjust its configuration of the telephone number, SIP credentials and VoIP Switch domain for registration<br><br>For a automatically via AdminCenter configured device check that:<br><br>◊ the selected device type in the AdminCenter is identical to the physical one.<br>Actions:<br><br>If not the same type then the user must re-configure the device via AdminCenter | | |

| | | | |
|---|---|---|---|
| | For a automatically via AdminCenter configured device check that:<br><br>◊ the user device has downloaded its configuration.<br><br>Actions:<br><br>If the configuration is not downloaded then it must be checked if the device:<br><br>◊ has got an IP address in the local IP network<br>◊ has access to the Internet<br>◊ has access to the configuration download of the Telephony Provider.<br>By default this is the IP address of the VoIP Switch domain and uses the protocol HTTPS on TCP port 443. Check with the Telephone provider or via ConfigCenter > Menu "System" > "Zone Profiles"<br>The user must check if the Firewall, SBC or Access Router doesn't block HTTPS traffic to and from the configuration download of the Telephony Provider | | |
| **Data Transfer** | | | |
| **Equipment** | | | |

# Solve "Connection" Problems

This problem type covers the following erroneous conditions:

◊ Incoming or outgoing calls are not working
◊ Wrong called number
◊ Call supervision
◊ User device not registered
◊ User device not correct configured
◊ SIP signaling in general

| | |
|---|---|
| **Note** | If the device is connected to an IP-PBX then these problems must be solved with the responsible of the IP-PBX. |

**1 Step: Review the account and telephone number configuration / registration?**

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | Do this check for the A and/or B telephone number if they are on-net numbers of the VoIP SWitch.<br><br>Check via ConfigCenter:<br><br>◊ Does the telephone number exist?<br>◊ Is the telephone number valid?<br>◊ Is the user account valid?<br>◊ Is the telephone number correctly registered<br><br>Actions:<br><br>Check why the account, telephone number doesn't exist or is disabled and activate if allowed.<br>Check why the device is not registered at the VoIP Switch |
| **Data Transfer** | | | |

| Equipment | | |
|---|---|---|

Hint:

◊ If the device is not registered outgoing calls might be working but NO incoming call will work.

## 2 Step: Was the called number correctly transmitted to the peer?

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | Check via ConfigCenter:<br><br>1. In the  "Call Data" search for the erroneous call:<br> ♦ Set the "Call Data" filters:<br>  · Insert at "Time" a reasonable time span where the erroneous call is to be expected.<br>  · Set "Duration" to 00:00:00<br>  · Insert at "Called Number" the called number<br>2. Start the search and identify the CDR of the erroneous call in the list<br>  If no CDR was found search for the "Calling Number"!<br>3. Open the identified CDR and get the trace of the call, click the Button [ Trace ]<br>4. Check if the called number in the "TO-Header" in all INVITE messages is correct:<br> ♦ Is the called number correct?<br>  Often the users don't dial all digits or wrong digits or the configured number on a direct call key is incorrect.<br> ♦ If the number is dialed correctly then it can be that the destination is not reachable.<br> ♦ Outgoing calls from a vPBX can miss the  public prefix<br>5. Check the peers call cancel reason:<br> ♦ SIP Failure Responses<br><br>Actions:<br><br> Inform the user to dial the correct number.<br> Try to reach the called number via an alternative telephone network, e.g. from a mobile telephone.<br> Check with the support of the telephony provider why the called number is not reachable. |
| **Data Transfer** | | | |
| **Equipment** | | | |

## 3 Step: What is the reason of an interrupted connection?

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | Search in the  "Call Data" for the erroneous call:<br><br>1. ♦ Set the "Call Data" filters:<br>  · Insert at "Time" a reasonable time span where the erroneous call is to be expected.<br>  · Set "Duration" to 00:00:00<br>  · Insert at "Called Number" the called number<br>2. Start the search and identify the CDR of the erroneous call in the list<br>  If no CDR was found search for the "Calling Number"!<br><br>Open the identified CDR and check for the release or reject reason:<br><br> ◊ Was the connection released by a peer, A or B side?<br> ◊ Check cancel reason in "State" ( SIP Failure Responses )<br><br>Actions: | | |

<table>
<tr><td></td><td colspan="2">

Inform the user about the release reason, e.g. his own device or the peer device released the call regularly (but probably nor expected).

Check if a call was released due to call supervision:

◊ Variant 1: Session Timer was not refreshed:
· Open the "Trace" of the connection and check if the connection was released due to missing RE-INVITE from the peers when the Session Timer run out.

Actions:

Inform the user that his device did not restart the Session Timer. The device configuration must be inspected an adjusted if needed.

◊ Variant 2: SIP INFO were not answered by the peer:
· Open the "Trace" of the connection and check if the connection was released due to not answered INFO messages that were sent from the VoIP Switch toward the peers. If activated the INFO's are sent usually every 120sec.

Actions:

Inform the user that his device did not answered INFO messages. It must be checke with the support of the device manufacturer if the device doesn't send 200 ACK when an empty INFO message was received ("SIP ping").

◊ Variant 3: Missing RTP packets between the peers:
This type of problem is a difficult one and hard to check and solve!  It must be handled like a QoS problem.
Media transferring devices as the MediaServer of the VoIP Switch, SBCs, SS7-Gateways, SIP-Trunks supervise the media stream of RTP packets. If after a certain time no RTP packets are transferred in a connection then such an instance can release the call. Typically after 30secs a connection is released if no RTP streams are detected.
◊          · Open the "Media Trace" of the connection and check if there are remarkable differences between the amount of sent and received or lost RTP packets.

Actions:

→  See "Quality of Service QoS problem" below.

</td><td></td><td></td></tr>
<tr><td>**Data Transfer**</td><td></td><td></td><td></td><td></td></tr>
<tr><td>**Equipment**</td><td></td><td></td><td></td><td></td></tr>
</table>

# Solve "Quality of Service QoS" QoS-Problems

## Introduction to QoS-Problems

| Note | In most cases, QoS-problems can only be found and solved by means of an exclusion procedure.<br><br>It is paramount that the customer/user knows that QoS-problems are difficult to track down and to solve. |
|---|---|

It's nerve-wracking and it is time consuming.

Solving QoS-problems often requires the cooperation and active co-testing from the customer/user with the support personnel! The active help of the customer/user is needed in most cases, e.g. by executing test connections.

The QoS-problem type covers the following erroneous conditions:

◊ No voice transmission in one or both directions from the beginning of the connection
◊ Bad voice quality during the connection

Naming and characteristics of QoS-problem:

**One/No-Way Connection**:

There is no speech transmission in one or both directions from beginning of the connection:

• Silence (Possible reason: Mostly due to no or blocked RTP data transmission)

**Glitch Connection**:
There is speech transmission but it is disturbed:
• Crackle, clicking (Possible reason: small packet loss, jitter)
• Short interruption (Possible reason: bigger packet loss)
• Ouw-ing (Possible reason: jitter, transcoding)
• Echo (Possible reason: jitter, big delay)

The source of the QoS-problems are all too often somewhere in the data transmission "D Data Transfer" layer (but sometimes they are surprisingly simple):

◊ The microphone or loadspeaker in the telephone handset defect
◊ Volume configuration in the telephone set wrong
◊ Telephone defect
◊ The company Intranet is not made ready for VoIP
◊ Any device in the "D - Data Transfer" layer

## 1st Step: Interview the User

**1 Step: Interview the user carefully and identify the type of QoS-problem**

Get all information from the user:

1. Occurs the the QoS-problem with all peers or just with the given B peer?
   Hint:
   If the problem occurs only with the B peer then this is a strong indication that something is wrong on the B side!
2. Is there no voice transmission, neither from `A->B` nor `B->A`?
   Type of QoS-problem:  "No-Way Connection"
3. Is there voice transmission from `A->B` (B hears you) but none from `B->A` (you don't hear B)?
   Type of QoS-problem:  "One-Way Connection `A->B`"
4. Is there voice transmission from `B->A` (you hear B) but none from `A->B` (B doesn't hear you)?
   Type of QoS-problem:  "One-Way Connection `B->A`"
5. Are there during the connection crackle, clicking, short interruptions, uow-ing in the voice transmission for both sides?
   Type of QoS-problem:  "Glitch Connection"
6. Are there during the connection crackle, clicking, short interruptions, uow-ing in the voice transmission from `A->B`?
   Type of QoS-problem:  "Glitch Connection `A->B`"
7. Are there during the connection crackle, clicking, short interruptions, uow-ing in the voice transmission from `B->A`?
   Type of QoS-problem:  "Glitch Connection `B->A`"
8. Uses the user an ISDN or DECT telephone behind an ISDN-PBX? Does the user have sharp clicking glitches in a regular or irregular interval? Do experience all users behind this ISDN-PBX this clicking?
   Remember :
   This points to a  synchronization problem of the ISDN-PBX!

9. Is one peer A or B a mobile user?

> Remember:
> Mobile networks often have QoS-problems on the wireless links between the base station and the mobile device!

Action:

> Cross check the users information by checking the media transfer statistics of the affected connection, see "2 Step" below!

## 2nd Step: Localize the QoS-Problem

| Note | It is very important that the supporter is aware of of the localization of the problem. QoS-problems in the range of the "2 Internet Service Provider ISP" or "3 Telephony Provider" will affect usually a lot of users immediately. |
|------|------|

## 1 Step: Check the "Big Picture"

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | Check with the ISP where the user is connected to if there are outages in:<br><br>◊ the ISP IP network<br><br>Actions:<br><br>Inform immediately the Telephone providers support or alarming organization.<br>If yes, just wait until the outage is solved | Check with the ISP where the VoIP System is connected to if there are outages in:<br><br>◊ the ISP IP network<br>◊ relevant national and/or international IP network<br><br>Actions:<br><br>Inform immediately the Telephone providers support or alarming organization.<br>If yes, just wait until the outage is solved | Check with the IT responsible of the IP network where the VoIP System is attached to:<br><br>◊ Are there known outages in the IP network where the VoIP System is attached to?<br>◊ Is there a large scale QoS-problem?<br>◊ Are users affected which are located:<br>   • in a certain private IP network of the telephony provider?<br>   • at a definable tenant?<br><br>Actions:<br><br>Inform immediately the Telephone providers support or alarming organization.<br>If the VoIP System is located in a pure private IP network then contact immediately the |

| | | | | IT responsible or IT emergency organization. If yes, just wait until the outage is solved |
|---|---|---|---|---|
| **Equipment** | | | | |

**2 Step: Identify the disturbed transmission direction from the VoIP Switch's view**

This identification bases upon the VoIP System setting that all media streams are routed via the MediaServer of the VoIP Switch. The MediaServer collects statistic information about all media stream that are routed through it. These statistics can help to identify the source of the QoS-problem.

Search in the "Call Data" the CDR of the erroneous call:

1. ♦ Set the "Call Data" filters:
   · Insert at "Time" a reasonable time span where the erroneous call is to be expected.
   · Set "Duration" to 00:00:00
   · Insert at "Called Number" the called number
2. Start the search and identify the CDR of the erroneous call in the list
   If no CDR was found search for the "Calling Number"!
3. Open the identified CDR
4. Get the RTP statistics of this connection, click Button [ Media Trace ]
   If there are no data in the "Media Trace" contained then the media stream is not routed via the MediaServer of the VoIP Switch. See below how to force the routing via the MediaServer.
   Depending of the identified QoS-problem type  analyze the RTP statistics detail, see below

If the media stream are not routed by default via MediaServer the supporter can force it for an account via the ConfigCenter:

→ Menu "Account"

→ Select the customers account

→ Tab "Advanced"

→ Set "Use always MediaServer" to `"Yes"`

| | |
|---|---|
| **Note** | ◊ By forcing the media stream through the MediaServer the routing of the RTP packets through the IP networks changes!<br>◊ If the QoS-problem disappears when forced via MediaServer and reappears when switched back then this is a strong indication that something is wrong in the direct IP routing path between the customer/user and the peer device. |

**Localize "No-Way Connection" and Possible Actions**

"No-Way Connection":

◊ No voice transmission, neither from A->B nor B->A

Knowhow background:

◊ May occur during commissioning of the customer connection for VoIP

◊ May occur when the telephony provider introduce now IP networks for new telephony users
◊ May occur when the Internet service provider or telephony provider modify the IP routing
◊ Customer firewall policies block IP range or UDP port range
◊ The peer devices negotiate not the same codec
◊ May occur when IP devices are defect
◊ User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>    ◊ Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A<br>        • The B side codec must be within the codec list of side A<br>        Possible problems: ouw-ing, No-Way or One-Way connection<br><br>Actions:<br>    If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>    Check the configuration of the device A why the codec of side B is not in its list.<br>    Consider a firmware upgrade of either device!<br><br><br>**2nd:** Check if the negotiated IP address and UDP ports are not blocked by any firewall.<br><br>    ◊ Check in the SDP information if the displayed IP addresses and UDP ports of the leg A and B are not blocked by any firewall<br>        Possible problems: No-Way or One-Way connection<br><br>Actions:<br>    Adjust the customers firewall policies<br>    Adjust the usable UDP port range in the customer peer device<br><br><br>**3rd:** Check the "`rtp data`" records if the RTP transfer from and to the user/customer is not working:<br><br>    ◊ Are there are no (or few) received packets from the user?<br>    ◊ Are there packets sent toward the user?<br>      If `Leg A "rec"=0` and `Leg A "snt">0`: no packets received from A but packets were sent toward A.<br>Actions:<br>    If there is a gateway on the user/customer side which is provided from the Telephony provider then check the correct working of this gateway.<br>    The user or customer IT responsible must check if the Internet or access to the Telephony network is ok.<br>    The user or customer IT responsible must check if the access router or Firewall are ok (no blocking policies, VoIP ALG off, ...).<br>    The user or customer IT responsible must check if its IT infrastructure is ok (no faulty IP switches, routers, ...).<br>    The user or customer PBX responsible must check if the ISDN- or IP-PBX is working correctly.<br>    The user must check if the telephone device is ok.<br><br><br>**4th:** Check the "`rtp data`" records if the RTP transfer from and to the PSTN is not working:<br><br>    ◊ Are there are no (or few) received packets from the PSTN? |

◊ Are there packets sent toward the PSTN?
If `Leg B "rec"=0` and `Leg B "snt">0`: no packets received from B but packets were sent toward B
Actions:
The supporter must inform immediately the telephony provider support or IT emergency organization.

**5th:** Check the `"rtp data"` records if the RTP handling in the VoIP Switch MediaServer is not working:

◊ Are there are packets received from the PSTN but not sent toward the user?
If `Leg B "rec">0` and `Leg A "snt"=0`: packets from B received but no packets sent toward A
◊ Are there are packets received from the user but not sent toward the PSTN?
If `Leg A "rec">0` and `Leg B "snt"=0`: packets from A received but no packets sent toward B
Actions:
The supporter must inform immediately the telephony provider support!

| Equipment | | | |
|---|---|---|---|

## Localize "One-Way Connection `A->B`" and Possible Actions

"One-Way Connection `A->B`":

◊ B hears A but A doesn't hear B

Knowhow background:

◊ May occur during commissioning of the customer connection for VoIP
◊ May occur when the telephony provider introduce now IP networks for new telephony users
◊ May occur when the Internet service provider or telephony provider modify the IP routing
◊ Customer firewall policies block IP range or UDP port range
◊ The peer devices negotiate not the same codec
◊ May occur when IP devices are defect
◊ User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>◊ Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A<br>• The B side codec must be within the codec list of side A<br>Possible problems: ouw-ing, No-Way or One-Way connection<br>Actions:<br>If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>Check the configuration of the device A why the codec of side B is not in its list.<br>Consider a firmware upgrade of either device! |

**2nd:** Check if the negotiated IP address and UDP ports are not blocked by any firewall.

> ◊ Check in the SDP information if the displayed IP addresses and UDP ports of the leg A and B are not blocked by any firewall
>
>> Possible problems: No-Way or One-Way connection
>
> Actions:
>> Adjust the customers firewall policies
>> Adjust the usable UDP port range in the customer peer device

**3rd:** Check the "`rtp data`" records if the RTP transfer from the PSTN is not working:

> ◊ Are there are no (or few) received packets from the PSTN?
>> If Leg B "`rec`"=0: no packets received from the PSTN.
>
> Actions:
>> The supporter must inform immediately the telephony provider support or IT emergency organization.

**4th:** Check the "`rtp data`" records if the RTP transfer to the user/customer is working:

> ◊ Are there are received packets from the PSTN and sent toward the user?
>> If Leg B "`rec`">0 and Leg A "`snt`">0: packets were received from the PSTN and sent toward the user.
>
> Actions:
>> If there is a gateway on the user/customer side which is provided from the Telephony provider then check the correct working of this gateway.
>> The user or customer IT responsible must check if the Internet or access to the Telephony network is ok.
>> The user or customer IT responsible must check if the access router or Firewall are ok (no blocking policies, VoIP ALG off, ...).
>> The user or customer IT responsible must check if its IT infrastructure is ok (no faulty IP switches, routers, ...).
>> The user or customer PBX responsible must check if the ISDN- or IP-PBX is working correctly.
>> The user must check if the telephone device is ok.

**5th:** Check the "`rtp data`" records if the RTP handling in the VoIP Switch MediaServer is not working:

> ◊ Are there are packets received from the PSTN but not sent toward the user?
>> If Leg B "`rec`">0 and Leg A "`snt`"=0: packets were received from the PSTN but not sent toward the user
>
> Actions:
>> The supporter must inform immediately the telephony provider support!

**Equipment**

---

**Localize "One-Way Connection B->A" and Possible Actions**

"One-Way Connection B->A":

> ◊ A hears B but B doesn't hear A

Knowhow background:

> ◊ May occur during commissioning of the customer connection for VoIP
> ◊ May occur when the telephony provider introduce now IP networks for new telephony users
> ◊ May occur when the Internet service provider or telephony provider modify the IP routing

◊ Customer firewall policies block IP range or UDP port range
◊ The peer devices negotiate not the same codec
◊ May occur when IP devices are defect
◊ User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>    ◊ Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A<br>        • The B side codec must be within the codec list of side A<br>        Possible problems: ouw-ing, No-Way or One-Way connection<br>Actions:<br>    If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>    Check the configuration of the device A why the codec of side B is not in its list.<br>    Consider a firmware upgrade of either device!<br><br>**2nd:** Check if the negotiated IP address and UDP ports are not blocked by any firewall.<br><br>    ◊ Check in the SDP information if the displayed IP addresses and UDP ports of the leg A and B are not blocked by any firewall<br>        Possible problems: No-Way or One-Way connection<br>Actions:<br>    Adjust the customers firewall policies<br>    Adjust the usable UDP port range in the customer peer device<br><br>**3rd:** Check the `rtp data` records if the RTP transfer from the user is not working:<br><br>    ◊ Are there are no (or few) received packets from the user?<br>      If Leg A `"rec"=0`: no packets received from the user<br>Actions:<br>    If there is a gateway on the user/customer side which is provided from the Telephony provider then check the correct working of this gateway.<br>    The user or customer IT responsible must check if the Internet or access to the Telephony network is ok.<br>    The user or customer IT responsible must check if the access router or Firewall are ok (no blocking policies, VoIP ALG off, ...).<br>    The user or customer IT responsible must check if its IT infrastructure is ok (no faulty IP switches, routers, ...).<br>    The user or customer PBX responsible must check if the ISDN- or IP-PBX is working correctly.<br>    The user must check if the telephone device is ok.<br><br>**4th:** Check the `rtp data` records if the RTP transfer to the PSTN is not working:<br><br>    ◊ Are there packets sent toward the PSTN?<br>      If Leg A `"rec">0` and Leg B `"snt">0`: packets were received from the user but not sent toward the PSTN<br>Actions:<br>    The supporter must inform immediately the telephony provider support or IT emergency organization. |

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|

**5th:** Check the `rtp data` records if the RTP handling in the VoIP Switch MediaServer is not working:

&#9671; Are there are packets received from the user but not sent toward the PSTN?
If Leg A `"snt">0` and Leg B `"snt"=0`,
Actions:
The supporter must inform immediately the telephony provider support!

**Equipment**

---

**Localize "Glitch Connection" and Possible Actions**

"Glitch Connection":

&#9671; The voice transmission from A->B and B->A is disturbed

Knowhow background:

&#9671; May occur when the customers Intranet is not optimized for VoIP
&#9671; The peer devices negotiate not the same codec
&#9671; May occur when IP devices are defect
&#9671; User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>&#9671; Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A:<br>The B side codec must be within the codec list of side A<br>Possible problems: ouw-ing, No-Way or One-Way connection<br>Actions:<br>If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>Check the configuration of the device A why the codec of side B is not in its list.<br>Consider a firmware upgrade of either device!<br><br>**2nd:** Check the `rtcp data` and `rtp data` records from and to the user/customer:<br><br>&#9671; Check the `rtcp data` (statistical data delivered from the device):<br>`"lost>0"`: Device A claimed not to receive all packets<br>Possible problems: crackle, short interruptions<br>`"jitter>0"`: Device A claimed to receive packets delayed or wavering (if the jitter values are different then wavering)<br>Possible problems: crackle, short interruptions, echo, ouw-ing<br>&#9671; Check the `rtp data` (statistical data from the VoIP Switch):<br>`"rec"` not equal `"snt"`: The numbers of received `"rec"` and sent `"snt"` must be more or less equal since the last report.<br>Possible problems: crackle, short interruptions<br>`"cpkl>0.1"`: The cumulated packet loss `"cpkl"` should be smaller than `"<0.1"`.<br>Possible problems: crackle, bigger interruptions |

| | | | Actions:<br>  If there is a gateway on the user/customer side which is provided from the Telephony provider then check the correct working of this gateway.<br>  The user or customer IT responsible must check if the Internet or access to the Telephony network is ok.<br>  The user or customer IT responsible must check if its IT infrastructure is ok (no faulty IP switches, routers, ...).<br>  The user or customer PBX responsible must check if IP-PBX is working correctly.<br>  The user must check if the telephone device is ok.<br><br>**3rd:** Check the `"rtcp data"` and `"rtp data"` records from and to the PSTN is not working:<br><br>  ◊ Check the `"rtcp data"` (statistical data delivered from the device):<br>  `"lost>0"`: Device B claimed not to receive all packets.<br>    Possible problems: crackle, short interruptions<br>  `"jitter>0"`: Device B claimed to receive packets delayed or wavering (if the jitter values are different then wavering).<br>    Possible problems: crackle, short interruption, echo, ouw-ing<br>  ◊ Check the `"rtp data"` (statistical data from the VoIP Switch):<br>  `"rec"` not equal `"snt"`: The numbers of received `"rec"` and sent `"snt"` must be more or less equal since the last report<br>    Possible problems: crackle, short interruption<br>  `"cpkl>0.1"`: The cumulated packet loss `"cpkl"` should be smaller than `"<0.1"`<br>    Possible problems: crackle, bigger interruptions<br>Actions:<br>  If there are **no** similar problems in the big picture then the problem lies presumably in the network of side B.<br>  If there are **similar** problems in the big picture then the supporter must inform immediately the telephony provider support or IT emergency organization. |
| **Equipment** | | | |

## Localize "Glitch Connection A->B" and Possible Actions

"Glitch Connection A->B":

    ◊ The voice transmission from A->B is disturbed. B claims to hear A with bad quality.

Knowhow background:

    ◊ May occur when the customers Intranet is not optimized for VoIP<br>
    ◊ May occur when IP devices are defect<br>
    ◊ User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>  ◊ Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A:<br>  The B side codec must be within the codec list of side A<br>    Possible problems: ouw-ing, No-Way or One-Way connection |

| | | | |
|---|---|---|---|
| | | | Actions:<br>    If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>    Check the configuration of the device A why the codec of side B is not in its list.<br>    Consider a firmware upgrade of either device!<br><br>**2nd:** Check the `"rtp data"` records if the RTP transfer to the PSTN is correctly working:<br><br>        ◊ Check the `"rtp data"` (statistical data from the VoIP Switch) toward the PSTN:<br>        `Leg A "rec"` not equal `Leg B "snt"`: The numbers of received `"rec"` and sent `"snt"` must be more or less equal since the last report.<br>                Possible problems: crackle, short interruptions<br>    Actions:<br>    If the received packets are very different to the sent ones then the supporter must inform immediately the telephony provider support or IT emergency organization.<br>    If the received packets are quite equal to the sent ones then the problem must be on the B side |
| **Equipment** | | | |

 

**Localize "Glitch Connection B->A" and Possible Actions**

"Glitch Connection B->A":

        ◊ The voice transmission from B->A is disturbed. A claims to hear B with bad quality.

Knowhow background:

        ◊ May occur when the customers Intranet is not optimized for VoIP
        ◊ May occur when IP devices are defect
        ◊ User device defect

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | Assumption:<br><br>The problem reporting user/customer shall be the A leg.<br><br>**1st:** Check if the negotiated "codec" are correct for both peers.<br><br>        ◊ Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A:<br>        The B side codec must be within the codec list of side A<br>                Possible problems: ouw-ing, No-Way or One-Way connection<br>    Actions:<br>    If the B side codec is not within the codec list of side A then check the configuration of the peer device B.<br>    Check the configuration of the device A why the codec of side B is not in its list.<br>    Consider a firmware upgrade of either device!<br><br>**2nd:** Check the `"rtp data"` records if the RTP transfer to the user/customer is correctly working:<br><br>        ◊ Check the `"rtp data"` (statistical data from the VoIP Switch) toward the user/customer: |

<table>
<tr><td></td><td></td><td>

<code>Leg B "rec"</code> not equal <code>Leg A "snt"</code>: The numbers of received <code>"rec"</code> and sent <code>"snt"</code> must be more or less equal since the last report.

    Possible problems: crackle, short interruptions

Actions:
    If the received packets are very different to the sent ones then the supporter must inform immediately the telephony provider support or IT emergency organization.

**3rd:** Check the <code>"rtcp data"</code> records from the user/customer:

◊ Check the <code>"rtcp data"</code> (statistical data delivered from the device):

<code>"lost>0"</code>: Device A claimed not to receive all packets
    Possible problems: crackle, short interruptions

<code>"jitter>0"</code>: Device A claimed to receive packets delayed or wavering (if the jitter values are different then wavering)
    Possible problems: crackle, short interruptions, echo, ouw-ing

Actions:
    If there is a gateway on the user/customer side which is provided from the Telephony provider then check the correct working of this gateway.
    The user or customer IT responsible must check if the Internet or access to the Telephony network is ok.
    The user or customer IT responsible must check if its IT infrastructure is ok (no faulty IP switches, routers, ...).
    The user or customer PBX responsible must check if IP-PBX is working correctly.
    The user must check if the telephone device is ok.

</td></tr>
<tr><td>**Equipment**</td><td></td><td></td></tr>
</table>

## Solve "Voice Glitches with ISDN-PBX" Problem

This problem type covers the following erroneous conditions:

◊ Bad speech quality in an ISDN-PBX environment
◊ Glitches in the voice transmission, it "clicks"

ISDN-PBX environment usually provide an excellent voice quality. In an VoIP environment this excellent voice quality can be only maintained if the ISDN-PBX can synchronize with high precision clock source.

### 1 Step: Check the ISDN reference clock

| | Customer | | Internet ISP | Telephony Provider |
|---|---|---|---|---|
| **Telephony** | | | | |
| **Data Transfer** | | | | |
| **Equipment** | Checks:<br><br>◊ Does the ISDN-PBX take its clock reference from a high precision clock?<br><br>Actions:<br><br>    Make sure the ISDN-PBX takes its reference clock from a high precision source.<br>    Use an ISDN-Gateway which provides a high precision clock. | | | |

# Solve "Special Telephony" Problem

## Solve "FAX Transmission" Problem

This problem type covers the following erroneous conditions:

◊ FAX transmission doesn't start
◊ FAX transmission is dropped
◊ The transmitted document is incomplete

| Note | If the FAX is connected to an IP-PBX then FAX problems must be solved with the responsible of the IP-PBX. |
|------|------|

In a VoIP environment FAX no longer achieve the same degree of reliability as before in an analogue or ISDN one. The FAX reliability depends on various factors such as the type of device, device settings and the way the device is connected to the IP network. It depends also on the quality of the transmitter and receiver of the peer FAX devices. Getting all these factors together a transmission may not even start or dropped unexpectedly. The transmitted documents may be incomplete.

The users must expect increasing difficulties in the future, especially for international transmissions.

### 1 Step: Check the FAX device configuration

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | |
| **Equipment** | Check:<br><br>◊ the configuration of the FAX device<br><br>Actions:<br><br>Adjust the FAX device configuration:<br><br>• Reduce the transmission speed to max. 9600bds.<br>• Switch OFF the error correction as e.g. EMC<br>• If the device offers a "VoIP mode" then experiment with it and check if the results are better. | | |

### 2 Step: Check the FAX transmission configuration of the gateway

| | Customer | Internet ISP | Telephony Provider |
|---|---|---|---|
| **Telephony** | | | |
| **Data Transfer** | | | |
| **Equipment** | Depending on the quality of the IP network the supporter and/or administrator of the gateway can experiment with the FAX transmission protocol of the gateway device.<br><br>Checks:<br><br>◊ Check with the Telephony provider if there are recommendations or directives which type of FAX transmission protocols are to use, e.g.: | | |

| | · In band transmission with codec G.711alaw or G.711ulaw<br>· Out band transmission with T.38<br>◊ Check the configuration of the gateway device | | |
| Actions: | | | |
| | If the user/customer has a good quality IP network and the Telephone provider allows it then try:<br><br>• "In band transmission with codec G.711"<br>If the user/customer has a lower quality IP network and the Telephone provider allows it then try:<br>• "Out band transmission with T.38" | | |

## Solve "DECT Multi-Cell with ISDN-PBX" Problem

This problem type covers the following erroneous conditions:

◊ Hand over from cell to cell is not working
◊ Bad speech quality

| Note | If the DECT Multi-Cell system is connected to an IP-PBX then DECT problems must be solved with the responsible of the IP-PBX. |
|---|---|

DECT-Multi-Cell systems connected to an ISDN-PBX which is working with in a VoIP environment experience special issues. Most issues are interconnected with accuracy of the synchronization clock of the ISDN-PBX. If this synchronization clock is not especially precise then the reference clock of the DECT-Multi-Cell system will have problems as described above.

### 1 Step: Check the ISDN reference clock

| | Customer | | Internet ISP | Telephony Provider |
|---|---|---|---|---|
| **Telephony** | | | | |
| **Data Transfer** | | | | |
| **Equipment** | Checks:<br><br>◊ Does the ISDN-PBX take its clock reference from a high precision clock?<br><br>Actions:<br><br>Make sure the ISDN-PBX takes its reference clock from a high precision source.<br>Use an ISDN-Gateway which provides a high precision clock. | | | |