Book VoIP Switch Support



Introduction

The Aarenet VoIP System supporting personnel find here links to detailed information about:

- How to support telephony users and solving user problems
 An introduction to the VoIP signaling protocols
 The Aarenet VoIP Switch on board support tools
 The Aarenet VoIP System monitoring and alarming
 The maintenance and problem solving of the Aarenet VoIP Switch
 The maintenance and problem solving of DELL server

User Guide for Solving Telephony Problems (Support Level 1)

Best Practice: How do I start to solve my problem?

	 Check that the telephone (VoIP device) is
	connected correctly
	→ Snow me now
	2. You are trying to get the phone (VoIP device) up
	and running, but now:
	▲ It doesn't load its configuration from the
	VolD Switch
	Show me how to
	check this
	You have already been able to make (inbound
	and outbound) phone calls with the VolP device
	and outbound) phone cans with the voli device,
	but now:
	I he telephone shows on its display that
	it has no connection to the VoIP Switch
	 The telephone (VoIP device) is no
Rest	longer available for incoming calls
Dreation	
Practice	
	CNECK THIS
	4. You have already been able to make (inbound
	and outbound) phone calls with the VoIP device.
	but now:
	You can no longer establish or receive
	▼ Tou call no longer establish of receive connections
	connections
	Show me how to
	check this
	5. You can make (inbound and outbound) phone
	calls with the VoIP device but now.
	▲ The voice quality is very poor
	 My counterpart description
	 iviy counterpart doesn't near me
	♦ I can't hear my counterpart
	We don't hear each other
	Show me how to
	check this

Basic Check of the VoIP Device

The following basic conditions must always be checked first:

- 1. Is the VoIP terminal correctly connected to the power supply?
 - Possible actions:
 - Replace the power supply cable
 - Use a different outlet
- 2. Is the VoIP terminal correctly connected to the data network?
 - · Plug the data cable into the correct port:
 - At the VoIP device
 - At the upstream IP device (IP router, xDLS modem, etc.)
 - Possible actions:
 - · Replace the data cable
- 3. Does the VoIP device display the behavior and indicators described in its user manual?
 - If it's not:
 - Possible actions:
 - Contact the seller's or device manufacturer's support
- 4. Does your data network connection work?
 - If your Internet connection for your PC and the VoIP device is running via the same upstream device (xDSL modem, FTTH modem (fibre optic modem), cable modem), can the Internet be accessed via your PC?
 - I don't know or if no: Possible actions:
 - Contact the support of the Internet provider

The VoIP Device doesn't load the Configuration from the VoIP Switch

	These instructions are only valid if:
Note	 You have an account for the provider's self-care GUI. The VoIP device type can be configured via the provider's self-care GUI. In case of doubt, contact the provider's support.
	For all other cases, the VoIP device must be configured according to the manufacturer's specifications!

How does the problem manifest itself:

You are trying to use the VoIP device for the first time or after a restart of the device with the default factory configuration, but:

• Nothing's working!

Verify in the user account of the self-care GUI:

Tab "Phones"

Click on the Button [State ...]

The "Last Access" parameter does not display the date/time and IP address of the VoIP device.
 The "MAC provisioning" parameter does not display "done".

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Is the VoIP device getting an IP address after connecting to the network?
 - Possible actions:
 - · Check network connection
 - · Check DHCP service in your local IP network
- 3. Is the web based user interface of the VoIP device accessible and can you log in?
 - Possible actions:
 - · Check network connection
 - · If the DHCP service is switched on in your local IP network, check via the telephone user
 - or console interface whether the VoIP device obtains its IP address via DHCP.
- 4. Is the configuration of the VoIP terminal in factory defaults?
- 5. If no:
- Possible actions:
 - Restart the device manually with the default factory configuration (see the user manual of the VoIP device)
- 6. Is the VoIP Switch available?
 - or is the redirection server of the device manufacturer configured correctly?
 - or is the redirection server of the device manufacturer reachable?
 - Possible actions:
 - · Contact the support of the telephony provider

If the problem cannot be solved, contact the provider's support with the following information:

- ◊ Telephone number of the device which causes problems
- ♦ Device type
- ◊ Date and time when the problem occurred
- Oescription of the problem:
 - "The VoIP device cannot load its configuration!"

The VoIP Device doesn't Register with the VoIP Switch

	These instructions are only valid if:
	1. You have an user account for the provider's self-care GUI.
Note	
	For all other cases, the VoIP device must be configured according to the manufacturer's operating instructions with the correct SIP credentials of your telephony provider !

How does the problem manifest itself:

The telephone (VoIP device) is used for the first time or it has already been possible to make a phone call (incoming and outgoing), but:

- Neither an incoming nor outgoing connection can be established with the VoIP device.
- An outgoing connection can be established with the VoIP terminal, but it is not possible to reach it inbound.

Verify in the user account of the self-care GUI:

Tab "Phones"
 Click on the Button [State...]
 At "Registrations" no user agent, no IP address, no contact is displayed.

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Did the VoIP device load the configuration?
- 3. If no:

Possible actions:

· Configure the device manually or via the VoIP Switch.

4. What does the log of the VoIP device show?

Possible actions

◊ Act according to the instructions of the VoIP device.

If the problem cannot be solved, contact the provider's support with the following information:

- ◊ Telephone number of the device which causes problems
- Oevice type
- Obte and time when the problem occurred
- Oescription of the problem:
 - "The VoIP device cannot register!"

The VoIP Device cannot Establish or Receive Connections

How does the problem manifest itself:

The telephone (VoIP terminal) has already been able to make (incoming and outgoing) calls, but now:

• The VoIP device cannot establish or receive connections to/from public or private vPBX phone numbers whose devices are verifiably working (e. g. checked with an mobile phone).

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Has this VoIP device registered?

Possible actions:

Check if the device is registered on the VoIP Switch.

- 3. For problems with incoming connections:
 - Is a call forwarding active?
 - Possible actions:

 - Check with *#00 if a call forwarding is configured and deactivate with *00 if necessary. If your VoIP device has a private vPBX phone number, have the vPBX administrator check if the call distribution is still working correctly.
- 4. For problems with outgoing connections:
 - · Check with another device, e.g. a mobile phone or other phone of the same vPBX, if the desired destination number is reachable.
- 5. If no:
- Possible actions:
 - · If you have a public phone number:
 - Check if a TopStop has been exceeded?
 - Is the desired destination number blocked by a RuleSet?
 - Contact the support of the telephony provider
 - · If you have a private vPBX number:
 - Check if you need a leading 0, an other digit or no digit for outgoing calls to the PSTN.
 - Check if a TopStop has been exceeded?
 - Is the desired destination number blocked by a RuleSet?
 - Contact the vPBX administrator

If the problem cannot be solved, contact the provider's support with the following information:

- ◊ Telephone number of the device which causes problems
- ◊ Date and time when the problem occurred
- ◊ Telephone numbers of the participating devices:
 - A Number of the calling side B Number of the called side
- Oescription of the problem:
 - "A cannot make calls"
 - "A cannot receive calls"
 - "A cannot make calls to certain B numbers:"
 - Ist of B numbers that cannot be called

Poor, Partly or Completely Missing Speech Transmission

How does the problem manifest itself:

The VoIP device can establish or receive connections. The voice transmission was fine on earlier connections, but not now.

- The voice transmission is disturbed:
 - OB hears A disturbed
 - A hears B disturbed
 - The speech transmission is disturbed in both directions A <-> B
- The voice transmission is missing in part or in full since beginning of the connection:
 - Object B does not hear A A does not hear B
 - A and B do not hear each other

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Is the handset or headset connected correctly?
- 3. Is the microphone of the handset or headset not muted?
- 4. Are the volume levels for the loudspeaker and microphone on your telephone set correctly?5. Is the problem only with a specific parter? If yes, the other party should check the volume of the
- microphones, headset and headset being used.
- 6. Remember:
 - Handsfree mode often produces poor voice quality.
 - Connections with mobile phones can be disrupted, especially when the call partner is traveling.

If the problem cannot be solved, contact the provider's support with the following information:

- ♦ Telephone number of the device which causes problems
- Obtain the broblem occurred
- ◊ Telephone numbers of the participating devices:
 - A Number of the calling side
 - B Number of the called side

- Description of the problem:
 "The voice transmission is disturbed:"
 - **OB** hears A disturbed
 - A hears B disturbed
 - The speech transmission is disturbed in both directions A <-> B
 - "The voice transmission is missing in part or in full since beginning of the connection:"
 - Object B does not hear A
 - A does not hear B
 - A and B do not hear each other

FAX Transmissions do not or Only Partially Work

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.

How does the problem manifest itself:

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

Check the following conditions and take action:

- 1. Adjust the FAX device configuration:
 - Reduce the transmission speed to max. 9600bds.
 - Switch OFF the error correction, e.g. EMC
 - If the device offers a "VoIP mode" then experiment with it and check if the results are better.

If the problem cannot be solved, contact the provider's support with the following information:

- Telephone number of the device which causes problems
- ◊ Device type
- Obte and time when the problem occurred
- ◊ Telephone numbers of the participating devices:
 - A Number of the calling side
 - B Number of the called side
- Obscription of the problem: "FAX Transmissions doesn't work"

Don't expect miracles from the support!

n style="color:#0061a0">

These instructions are only valid if:

1. You have an user account for the provider's self-care GUI.

For all other cases, the VoIP device must be configured according to the manufacturer's operating instructions with the correct SIP credentials of your telephony provider !

How does the problem manifest itself:

The telephone (VoIP device) is used for the first time or it has already been possible to make a phone call (incoming and outgoing), but:

- Neither an incoming nor outgoing connection can be established with the VoIP device.
- An outgoing connection can be established with the VoIP terminal, but it is not possible to reach it inbound.

Verify in the user account of the self-care GUI:

Tab "Phones" Click on the Button [State...] ◊ At "Registrations" no user agent, no IP address, no contact is displayed.

Check the following conditions and take action:

- Are the basic conditions fulfilled?
- 2. Did the VoIP device load the configuration?
- 3. If no:
- Possible actions: · Configure the device manually or via the VoIP Switch.
- 4. What does the log of the VoIP device show?
 - Possible actions

◊ Act according to the instructions of the VoIP device.

If the problem cannot be solved, contact the provider's support with the following information:

- Telephone number of the device which causes problems
- Oevice type
- Oate and time when the problem occurred
- Obscription of the problem:
 - "The VoIP device cannot register!"

The VoIP Device cannot Establish or Receive Connections

How does the problem manifest itself:

The telephone (VoIP terminal) has already been able to make (incoming and outgoing) calls, but now:

 The VoIP device cannot establish or receive connections to/from public or private vPBX phone numbers whose devices are verifiably working (e. g. checked with an mobile phone).

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Has this VoIP device registered?
 - Possible actions:
- · Check if the device is registered on the VoIP Switch .
- For problems with incoming connections:
 - Is a call forwarding active?
 - Possible actions:

 - Check with *#00 if a call forwarding is configured and deactivate with *00 if necessary. If your VoIP device has a private vPBX phone number, have the vPBX administrator check if the call distribution is still working correctly.
- 4. For problems with outgoing connections:
 - Check with another device, e.g. a mobile phone or other phone of the same vPBX, if the desired destination number is reachable.
- 5. If no:

Possible actions:

- · If you have a public phone number:
 - Check if a TopStop has been exceeded?
 - Is the desired destination number blocked by a RuleSet?
 - Contact the support of the telephony provider
- · If you have a private vPBX number:
 - Check if you need a leading 0, an other digit or no digit for outgoing calls to the PSTN.
 - Check if a TopStop has been exceeded?
 - Is the desired destination number blocked by a RuleSet?
 - Contact the vPBX administrator

If the problem cannot be solved, contact the provider's support with the following information:

Telephone number of the device which causes problems
Date and time when the problem occurred
Telephone numbers of the participating devices:

A Number of the calling side
B Number of the called side

Description of the problem:

"A cannot make calls"
"A cannot receive calls"
"A cannot make calls to certain B numbers:"

List of B numbers that cannot be called

Poor, Partly or Completely Missing Speech Transmission

How does the problem manifest itself:

The VoIP device can establish or receive connections. The voice transmission was fine on earlier connections, but not now.

• The voice transmission is disturbed:

Observe B hears A disturbed

A hears B disturbed

◊ The speech transmission is disturbed in both directions A <-> B

• The voice transmission is missing in part or in full since beginning of the connection:

B does not hear A
 A does not hear B
 A and B do not hear each other

Check the following conditions and take action:

- 1. Are the basic conditions fulfilled?
- 2. Is the handset or headset connected correctly?
- 3. Is the microphone of the handset or headset not muted?
- 4. Are the volume levels for the loudspeaker and microphone on your telephone set correctly?
- 5. Is the problem only with a specific parter? If yes, the other party should check the volume of the microphones, headset and headset being used.
- 6. Remember:
 - ◆ Handsfree mode often produces poor voice quality.
 - Connections with mobile phones can be disrupted, especially when the call partner is traveling.

If the problem cannot be solved, contact the provider's support with the following information:

- Telephone number of the device which causes problems
- Obtain the problem occurred
- ◊ Telephone numbers of the participating devices:
 - A Number of the calling side
 - B Number of the called side
- Obscription of the problem:

"The voice transmission is disturbed:"

- ◊ B hears A disturbed
- A hears B disturbed
- ◊ The speech transmission is disturbed in both directions A <-> B
- "The voice transmission is missing in part or in full since beginning of the connection:"
 - OB does not hear A
 - A does not hear B
 - A and B do not hear each other

FAX Transmissions do not or Only Partially Work

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.

How does the problem manifest itself:

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

Check the following conditions and take action:

1. Adjust the FAX device configuration:

- Reduce the transmission speed to max. 9600bds.
- Switch OFF the error correction, e.g. EMC
 If the device offers a "VoIP mode" then experiment with it and check if the results are better.

If the problem cannot be solved, contact the provider's support with the following information:

- Telephone number of the device which causes problems
- ◊ Device type
- ◊ Date and time when the problem occurred
- ◊ Telephone numbers of the participating devices:
 - A Number of the calling side B Number of the called side

Obscription of the problem:

• "FAX Transmissions doesn't work" Don't expect miracles from the support!

-->

Introduction for Supporting User Problems (Support Level 2)

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.

-PBX Sur/ N. 10 1 Aarenet VolP Switch **S**\$7 or SIP Trunks nternational or SBC Mobile Telephone work **PSTN** Internet Service Telephony Customer Provider Provider an IP-Phone App an WebRIC-Phor 1 2 3

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: • Registration • SIP protocol • Device configuration Security: • TopStop • Password	ValP: • QoS for VolP	VolP System: • VolP Switch status • Access PSIN • Customer account configurations Security: • VolP ALG off
D - Data Transfer	IP Data Routing:	IP Data Routing:	IP Data Routing:
	• QoS for VoIP	• GoS for VoIP	Qos for VolP
	• IP routing	• Redundant IP routing	IP routing
	• Internet access	• Routing protocols	V Lan
	Security FW / Acc. Router:	Security:	Security:
	• IP policies	• IP link (redundant)	IP policies
	• NAT	• VPN	VolP ALG off
E - Equipment	Devices:	Devices:	Devices:
	• Telephone, DECT, FAX	• Router	• Router / Firewall / SBC
	• PBX / Gateway	• IP Switch	• IP Switch
	• Access Router / FW	• Redundant equipment	• VolP Server
	Cabling:	Cabling:	Cabling:
	• Supply	• Supply	• Supply
	• Patch cable	• Patch cable	• 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

 Record the customer's data and problem description: Get the customer data Get the problem description from the customer Show me how
 2. Cross check the user input against the VoIP switch configuration and logs. Via ConfigCenter check the users account configuration: Telephone number registration TopStop RuleSet Consult the "Call Data" for the last connection attempts and connections longer than 2min Show me how
 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. → Show me how 4. Check the big picture:



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 \rightarrow 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:

- Ocompany 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
- Vrong 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:

- Or 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
- O 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? Is the power cable correctly plugged in? Is the power cable not defect? Does the device show power on indication, e.g. display on, LED on? Actions: Replace the power cable Replace defect device if the powering is ok but no working indication is displayed 		



Defect power cables must be replaced! 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?		
	 Is the patch cable correctly plugged in? Is the patch cable not defect? Are there LED flashing or glow next to the network plug on the device or at the peer device (access router, IP switch)? 		
	Actions:		
	Replace the patch cable Plug in the patch cable at a different port at the peer device (access router, IP switch) 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?		
	The user must check the loaded firmware		
	Actions:		
	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?		
Transfer	Otheck on the device if it has received an IP address, e.g. via display or maintenance GUI.		
	Actions:		
	 If no IP address was assigned the user must: Check if the device is really connected to the IP network! Check if the device is configured with a fixed IP address! If it has a fixed IP does it match with the IP subnet? Is the default GW and DNS entry configured? Check if the device is configured to use DHCP! if the DHCP service in the IP network is running If the user cannot check the DHCP service he must contact the company IT responsible or the responsible of maintaining the access router. 		
	Other Check if the device makes contact with the VoIP Switch via Internet or any private IP Link.		
	Actions:		
	 If the device shall connect via the Internet: Connect a PC to the Ethernet port where the device usually is connected and try to connect to any public Web site. 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	Check via ConfigCenter:
	 Does the user account exist and is it "valid"? Does the telephone number exist and is it "valid"?
	Actions:
	 Check why the account, telephone number doesn't exist or is disabled 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.
			 Insert at "Text" the account name Insert at "From" - "Until" a reasonable time span where registrations could be expected Select the category: "Registration" Start the search and find out according the results what is going wrong. If needed repeat the search with the telephone number in the "Text" or other time spans
			\diamond Check the log results \rightarrow see below
			Actions:
			◊ → 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:

Output 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:		
	 ◊ Telephone number ◊ SIP credentials ◊ VoIP Switch domain configuration 		
	Actions:		
	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		
	For a automatically via AdminCenter configured device check that:		
	It the selected device type in the AdminCenter is identical to the physical one.		
	Actions:		
	If not the same type then the user must re-configure the device via AdminCenter		
	For a automatically via AdminCenter configured device check that:		
	◊ the user device has downloaded its configuration.		
	Actions:		
	If the configuration is not downloaded then it must be checked if the device:		
	has got an IP address in the local IP network		
	 has access to the Internet has access to the configuration download of the Telephony Provider. 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" 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		

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

f the device is connected to an IP-PBX then these problems must be solved with the responsible of the

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.
			Check via ConfigCenter:
			 Does the telephone number exist? Is the telephone number valid? Is the user account valid? Is the telephone number correctly registered
			Actions:
			Check why the account, telephone number doesn't exist or is disabled and activate if allowed. 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: 1. In the "Call Data" search for the erroneous call: ◆ 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 and get the trace of the call, click the Button [Trace] 4. Check if the called number in the "TO-Header" in all INVITE messages is correct: Is the called number correct? Often the users don't dial all digits or wrong digits or the configured number on a direct call key is incorrect. If the number is dialed correctly then it can be that the destination is not reachable. Outgoing calls from a vPBX can miss the public prefix 5. Check the peers call cancel reason: SIP Failure Responses
	Actions:
	Inform the user to dial the correct number. Try to reach the called number via an alternative telephone network, e.g. from a mobile telephone. 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:		
	 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 Start the search and identify the CDR of the erroneous call in the list If no CDR was found search for the "Calling Number"! 		
	Open the identified CDR and check for the release or reject reason:		
	 Was the connection released by a peer, A or B side? Check cancel reason in "State" (SIP Failure Responses) 		
	Actions:		
	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.	
Data Transfer		
Equipment		

Solve "Quality of Service QoS" QoS-Problems

Introduction to QoS-Problems

	In most cases, QoS-problems can only be found and solved by means of an exclusion procedure.
Note	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 $A \rightarrow B$ nor $B \rightarrow A$? 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

It is very important that the supporter is aware of of the Note localization of the problem. QoS-problems in the range of the "2 Internet Service

1 Step: Check the "Big Picture"

	Customer	Internet ISP	Telephony Provider
Telephony			
Telephony Data Transfer	Check with the ISP where the user is connected to if there are outages in:	Check with the ISP where the VoIP System is connected to if there are outages in:	Check with the IT responsible of the IP network where the VoIP System is attached to:
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" Observe by By forcing the media stream through the MediaServer the routing of the RTP packets through the IP networks changes! ◊ If the QoS-problem disappears when Note 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":

On voice transmission, neither from A->B nor B->A

- O 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
- Oustomer firewall policies block IP range or UDP port range
- The peer devices negotiate not the same codec
 May occur when IP devices are defect
- Over device defect

	Customer	Internet ISP	Telephony Provider
Telephony			
Data Transfer			Assumption: The problem reporting user/customer shall be the A leg. 1st: Check if the negotiated "codec" are correct for both peers. \diamond Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A

 The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way connection

Actions:

- If the B side codec is not within the codec list of side A then check the configuration of the peer device B.
- Check the configuration of the device A why the codec of side B is not in its list.
- 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 and to the user/customer is not working:

Are there are no (or few) received packets from the user?
Are there packets sent toward the user?

- If Leg A "rec"=0 and Leg A "snt">0: no packets received
- from A but packets were sent toward A.
- 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.

4th: Check the "rtp data" records if the RTP transfer from and to the PSTN is not working:

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!

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

"One-Way Connection A->B":

Observe B hears A but A doesn't hear B

- 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: The problem reporting user/customer shall be the A leg.
			1st: Check if the negotiated "codec" are correct for both peers.
			 Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way connection Actions: If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list. 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?
	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":

O A hears B but B doesn't hear A

- Any 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 defeat

- May occur when IP devices are defect
 User device defect

	125	Provider
Telephony		
Data Transfer		Assumption: The problem reporting user/customer shall be the A leg. 1st: Check if the negotiated "codec" are correct for both peers. \diamond Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A \bullet The B side codec must be within the codec list of side A

	Possible problems: ouw-ing, No-Way or One-Way connection
	Actions: If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list.
	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 user is not working:
	Are there are no (or few) received packets from the user? If Leg A "rec"=0: no packets received from 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 sustamer IT responsible must check if the Internet or
	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.
	4th: Check the "rtp data" records if the RTP transfer to the PSTN is not working:
	Are there packets sent toward the PSTN? If Leg A "rec">0 and Leg B "snt">0: packets were received from the user but not sent toward the PSTN 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:
	<pre> Are there are packets received from the user but not sent toward the PSTN? If Leg A "snt">0 and Leg B "snt"=0, </pre>
	Actions: The supporter must inform immediately the telephony provider support!
Equipment	

Localize "Glitch Connection" and Possible Actions

"Glitch Connection":

◊ The voice transmission from A->B and B->A is disturbed

- A May occur when the customers Intranet is not optimized for VoIP
 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:
Transier			The problem reporting user/customer shall be the A leg.
			1st: Check if the negotiated "codec" are correct for both peers.
			 Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A: The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way connection
			If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list. Consider a firmware upgrade of either device!
			2nd: Check the "rtcp data" and "rtp data" records from and to the user/customer:
			Check the "rtcp data" (statistical data delivered from the device): "lost>0": Device A claimed not to receive all packets Possible problems: crackle, short interruptions
			"jitter>0": 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
			Other the "rtp data" (statistical data from the VoIP Switch): "rec" not equal "snt": The numbers of received "rec" and sent "snt" must be more or less equal since the last report. Possible problems: crackle, short interruptions "cpkl>0.1": The cumulated packet loss "cpkl" should be smaller than "<0.1"
			Possible problems: crackle, bigger interruptions
			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.
			3rd: Check the "rtcp data" and "rtp data"records from and to the PSTN is not working:
			Check the "rtcp data" (statistical data delivered from the device):
			"lost>0": Device B claimed not to receive all packets.

	Possible problems: crackle, short interruptions "jitter>0": Device B claimed to receive packets delayed or wavering (if the jitter values are different then wavering). Possible problems: crackle, short interruption, echo, ouw-ing Check the "rtp_data" (statistical data from the VoIP Switch): "rec" not equal "snt": The numbers of received "rec" and sent "snt" must be more or less equal since the last report Possible problems: crackle, short interruption "cpkl>0.1": The cumulated packet loss "cpkl" should be smaller than "<0.1" Possible problems: crackle, bigger interruptions Actions: If there are no similar problems in the big picture then the problem lies presumably in the network of side B. 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.

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

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

	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. 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.

- 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:
			The problem reporting user/customer shall be the A leg.
			1st: Check if the negotiated "codec" are correct for both peers.
			 Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A: The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way connection
			If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list. Consider a firmware upgrade of either device!
			2nd: Check the " <code>rtp data"</code> records if the RTP transfer to the user/customer is correctly working:
			Check the "rtp data" (statistical data from the VoIP Switch) toward the user/customer: Leg B "rec" not equal Leg A "snt": The numbers of received "rec" and sent "snt" 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 "rtcp data" records from the user/customer:
			Otheck the "rtcp data" (statistical data delivered from the device):
			"lost>0": Device A claimed not to receive all packets Possible problems: crackle, short interruptions "jitter>0": 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.
Equipment	

Solve "Voice Glitches with ISDN-PBX" Problem

This problem type covers the following erroneous conditions:

- **O Bad speech quality in an ISDN-PBX environment**
- Ilitches 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: Object the ISDN-PBX take its clock reference from a high precision clock?		
	Actions: Make sure the ISDN-PBX takes its reference clock from a high precision source. 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



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: the configuration of the FAX device		
	Adjust the FAX device configuration: • Reduce the transmission speed to max. 9600bds. • Switch OFF the error correction as e.g. EMC • 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.		
	Checks:		
	 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 Out band transmission with T.38 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:		
	 "In band transmission with codec G.711" If the user/customer has a lower quality IP network and the Telephone provider allows it then try: "Out band transmission with T.38" 		
Solve "DECT Multi-Cell with ISDN-PBX" Problem

This problem type covers the following erroneous conditions:

And over from cell to cell is not working ♦ Bad speech quality

Note If the DECT Multi-Cell system is connected to an IP-PB 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: Object the ISDN-PBX take its clock reference from a high precision clock?		
	Actions: Make sure the ISDN-PBX takes its reference clock from a high precision source. Use an ISDN-Gateway which provides a high precision clock.		

p>

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 \rightarrow 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:

- **Or 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:

- Ocompany PBX
- The IP PBX is connected directly or via SBC to the VoIP Switch
- One or more telephone number ranges
- Or 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:

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

Most common problems:

- Or 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
- Or The device doesn't register at the VoIP Switch

Note

Solve "Device Hardware & Firmware" Problem

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

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



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?	
	 Is the patch cable correctly plugged in? Is the patch cable not defect? Are there LED flashing or glow next to the network plug on the device or at the peer device (access router, IP switch)? 	
	Actions:	
	Replace the patch cable Plug in the patch cable at a different port at the peer device (access router, IP switch) 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?		
	◊ The user must check the loaded firmware		
	Actions:		
	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?

Telephony	
Data Transfer Has the device got an IP address? Ocheck on the device if it has received an IP address, e.g. via display or maintenance GUI. Actions: Ocheck if no IP address was assigned the user must: Ocheck if the device is really connected to the IP network! Ocheck if the device is configured with a fixed IP address! If it has a fixed IP does it match with the IP subnet? If it he device is configured to use DHCP! If the DHCP service in the IP network is running If the user cannot check the DHCP service he must contact the company IT responsible or the responsible of maintaining the access router. Has the device access toward the Volp Switch? Ocheck if the device makes contact with the VolP Switch via	

	 Actions: If the device shall connect via the Internet: Connect a PC to the Ethernet port where the device usually is connected and try to connect to any public Web site. 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:
			 Does the user account exist and is it "valid"? Does the telephone number exist and is it "valid"?
			Actions:
			 Check why the account, telephone number doesn't exist or is disabled 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. 1. Set the "Support Log" filters Insert at "Text" the account name Insert at "From" - "Until" a reasonable time span where registrations could be expected Select the category: "Registration" 2. Start the search and find out according the results what is going wrong. 3. If needed repeat the search with the telephone number in the "Text" or other time spans ◊ Check the log results → see below
			Actions: ◊ → 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:

Output 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:		
	 ◊ Telephone number ◊ SIP credentials ◊ VoIP Switch domain configuration 		
	Actions:		
	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		
	For a automatically via AdminCenter configured device check that:		
	It the selected device type in the AdminCenter is identical to the physical one.		
	Actions:		

	If not the same type then the user must re-configure the device via AdminCenter	
	For a automatically via AdminCenter configured device check that:	
	It the user device has downloaded its configuration.	
	Actions:	
	If the configuration is not downloaded then it must be checked if the device:	
	 has got an IP address in the local IP network has access to the Internet has access to the configuration download of the Telephony Provider. 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" 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?

ISP	Provider
	Do this check for the A and/or B telephone number if they are on-net numbers of the VoIP SWitch.
	Check via ConfigCenter:
	 Does the telephone number exist? Is the telephone number valid? Is the user account valid? Is the telephone number correctly registered
	Actions:
	Check why the account, telephone number doesn't exist or is disabled and activate if allowed.

Data
Transfer
Equipment

Hint:

 \Diamond 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:
			 In the "Call Data" search for the erroneous call: Set the "Call Data" filters:
			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: 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 Start the search and identify the CDR of the erroneous call in the list If no CDR was found search for the "Calling Number"! Open the identified CDR and check for the release or reject reason: 		

	 ◊ Was the ◊ Check of 	e connection released by a peer, A or B side? cancel reason in "State" (SIP Failure Responses)	
	Actions:		
	Inform device o probably	n the user about the release reason, e.g. his own or the peer device released the call regularly (but y nor expected).	
	Check if a call was relea	sed 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 Timer. 1 adjusted	n the user that his device did not restart the Session The device configuration must be inspected an d 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 messag manufa empty II	the user that his device did not answered INFO es. It must be checke with the support of the device cturer if the device doesn't send 200 ACK when an NFO message was received ("SIP ping").	
	 Variant This typ solve! I Media tr Switch, media s packets instance connect 	3: Missing RTP packets between the peers: e of problem is a difficult one and hard to check and t must be handled like a QoS problem. ransferring devices as the MediaServer of the VoIP SBCs, SS7-Gateways, SIP-Trunks supervise the tream of RTP packets. If after a certain time no RTP are transferred in a connection then such an e can release the call. Typically after 30secs a ion 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.	
Data Transfer			
Equipment			

Solve "Quality of Service QoS" QoS-Problems

Introduction to QoS-Problems

	In most cases, QoS-problems can only be found and solved by means of an exclusion procedure.
Note	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 Sad 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
- O The company Intranet is not made ready for VoIP
- ◊ Any device in the "D Data Transfer" laver

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 $A \rightarrow B$ nor $B \rightarrow A$?
- 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:	Check with the ISP where the VoIP System is connected to if there are outages in:	Check with the IT responsible of the IP network where the VoIP System is attached to:



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:

- Set the "Call Data" filters: 1.
 - · 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
 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"

	By forcing the media stream through the MediaServer the routing of the RTP packets through the IP networks changes!
Note	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

- Aay 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:
			The problem reporting user/customer shall be the A leg.
			1st: Check if the negotiated "codec" are correct for both peers.
			 Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way
			connection
			If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is
			not in its list. 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
			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 and to the user/customer is not working:
			 Are there are no (or few) received packets from the user? Are there packets sent toward the user? If Leg A "rec"=0 and Leg A "snt">0: no packets received from A but packets were sent toward A.
			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.
		4th: Check the " <code>rtp data"</code> records if the RTP transfer from and to the PSTN is not working:
		 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
Equipment		support!

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

"One-Way Connection A->B":

Or B hears A but A doesn't hear B

- Any 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 defeat

- May occur when IP devices are defect
 User device defect

	Customer	Internet ISP	Telephony Provider
Telephony			
Data Transfer			Assumption: The problem reporting user/customer shall be the A leg. 1st: Check if the negotiated "codec" are correct for both peers. \diamond Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A \bullet The B side codec must be within the codec list of side A

	Possible problems: ouw-ing, No-Way or One-Way connection
	Actions: If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is
	not in its list. 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
	Adjust the customers firewall policies Adjust the usable UDP port range in the customer peer device
	3rd: Check the " <code>rtp data"</code> 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.
	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.
	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.
	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 " <code>rtp data</code> " 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

- Any 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:	
			The problem reporting user/customer shall be the A leg.	
			1st: Check if the negotiated "codec" are correct for both peers.	
			 Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A The B side codec must be within the codec list of side A 	
			Actions:	
			the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list.	
			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	
			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 user is not working:	
			Are there are no (or few) received packets from the user? If Leg A "rec"=0: no packets received from 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,).	
			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.
	4th: Check the "rtp data" records if the RTP transfer to the PSTN is not working:
	 Are there packets sent toward the PSTN? If Leg A "rec">0 and Leg B "snt">0: packets were received from the user but not sent toward the PSTN 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 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":

◊ The voice transmission from A->B and B->A is disturbed

- May occur when the customers Intranet is not optimized for VoIP
 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: The problem reporting user/customer shall be the A leg. 1st: Check if the negotiated "codec" are correct for both peers.		

	<pre>"lost>0": Device A claimed not to receive all packets Possible problems: crackle, short interruptions "jitter>0": 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</pre>
	 Check the "rtcp data" (statistical data delivered from the device): "lost>0": Device B claimed not to receive all packets. Possible problems: crackle, short interruptions "jitter>0": Device B claimed to receive packets delayed or wavering (if the jitter values are different then wavering). Possible problems: crackle, short interruption, echo, ouw-ing Check the "rtp data" (statistical data from the VoIP Switch): "rec" not equal "snt": The numbers of received "rec" and sent "snt" must be more or less equal since the last report Possible problems: crackle, short interruption "cpkl>0.1": The cumulated packet loss "cpkl" should be smaller than "<0.1" Possible problems: crackle, bigger interruptions Actions: If there are no similar problems in the big picture then the problem lies presumably in the network of side B. If there are similar problems in the big picture then the supporter must inform immediately the telephony provider support or IT
Equipment	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:

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

Customer	Internet
	ISP

Telephony Provider

Telephony		
Data Transfer		Assumption: The problem reporting user/customer shall be the A leg. 1st: Check if the negotiated "codec" are correct for both peers. Check in the SDP information if the selected codec of the leg B side is in the offered list of leg A: The B side codec must be within the codec list of side A Possible problems: ouw-ing, No-Way or One-Way connection Actions:
		If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list. Consider a firmware upgrade of either device! 2nd: Check the "rtp_data" records if the RTP transfer to the PSTN is correctly working:
		Check the "rtp_data" (statistical data from the VoIP Switch) toward the PSTN: 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. Possible problems: crackle, short interruptions Actions:
		supporter must inform timediately the telephony provider support or IT emergency organization. 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 $B \rightarrow A$ ":

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

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

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

	Actions: If the B side codec is not within the codec list of side A then check the configuration of the peer device B. Check the configuration of the device A why the codec of side B is not in its list. Consider a firmware upgrade of either device!
	2nd: Check the " <code>rtp data"</code> records if the RTP transfer to the user/customer is correctly working:
	Check the "rtp_data" (statistical data from the VoIP Switch) toward the user/customer: Leg B "rec" not equal Leg A "snt": The numbers of received "rec" and sent "snt" 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 "rtcp data" records from the user/customer:
	 Check the "rtcp data" (statistical data delivered from the device): "lost>0": Device A claimed not to receive all packets Possible problems: crackle, short interruptions "jitter>0": 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
Fundament	working correctly. The user must check if the telephone device is ok.
Equipment	

Solve "Voice Glitches with ISDN-PBX" Problem

This problem type covers the following erroneous conditions:

 \Diamond Bad speech quality in an ISDN-PBX environment \Diamond 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:		

Does the	ISDN-PBX	take	its	clock	reference	from	а	high
precision	clock?							

Actions:

Make sure the ISDN-PBX takes its reference clock from a high precision source. Use an ISDN-Gateway which provides a high precision clock.

Solve "Special Telephony" Problem

 \Diamond

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:		
	Adjust the FAX device configuration: • Reduce the transmission speed to max. 9600bds. • Switch OFF the error correction as e.g. EMC • If the device offers a "VoIP mode" then experiment with it and check if the results are better.		

Customer

2 Step: Check the FAX transmission configuration of the gateway

Internet	Telephony
ISP	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.	
	Checks:	
	 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 Out band transmission with T.38 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:	
	 "In band transmission with codec G.711" If the user/customer has a lower quality IP network and the Telephone provider allows it then try: "Out band transmission with T.38" 	

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

This problem type covers the following erroneous conditions:

And over from cell to cell is not working
 Bad speech quality

Note If	f the DECT Multi-Cell system is connected to an IP-PBX hen DECT problems must be solved with the esponsible 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: Object the ISDN-PBX take its clock reference from a high precision clock?		
	Actions: Make sure the ISDN-PBX takes its reference clock from a high precision source. Use an ISDN-Gateway which provides a high precision clock.		

Manual of the Aarenet VoIP Switch Support Tools

VoIP Switch ConfigCenter Support Tools

The ConfigCenter Support Log

The "Support Log" provides the supporter with information from the internal processes of the ServiceCenter:

- ◊ Registration
- Operation Setup, release and exceptions
- ♦ Call Routing
- Used Ruleset
 Emergency calls
- ♦ etc

The "Support Log" provides filters for:

- Time based selection: From ? Until, From ? Duration
 Text filter
 Registration events
- ◊ Call events
- ♦ etc.

The "Support Log" has a limited history. The history may last from a few hours up to some days. The length of the history may be different from VoIP switch to VoIP switch and depends on the length of log files and amount of logging events.

Note The "Support Log" is tenant sensitive. This means a supporter of tenant A is not able to see events of tenant B!

Navigate to the "Support Log"

ConfigCenter:

→ Menu "Support"

Menu "Support Log"

Get a "Support Log"

Dialog: "Support Log":

Optional Filter for Text	Support Log
String, e.g.: • Call Id • Telephone number	To limit the size of data the following restrictions can be configured: Text sci278747953657 From 2015/12/22 16:00:00
Time Span or Duration: Mandatory:	Duration 00:14:42
"From" "Until" or "Duration"	If at least one Category is selected, only matching entries are displayed:
• "From" • "Until" or "Duration"	If at least one Category is selected, only matching entries are displayed: All Registr. Routing Calls
• "From" • "Until" or "Duration"	If at least one Category is selected, only matching entries are displayed: All Registr. Routing Calls Timeout Authent. Config. Outported
• "From" • "Until" or "Duration" Optional Filters for Different Categories	If at least one Category is selected, only matching entries are displayed: All Registr. Routing Calls Timeout Authent. Config. Outported Emerg. Rules Alarm Presence Additional information to display:
• "From" • "Until" or "Duration" Optional Filters for Different Categories	If at least one Category is selected, only matching entries are displayed: All Registr. Routing Calls Timeout Authent. Config. Outported Emerg. Rules Alarm Presence Additional information to display: Domain Component Categories

When the dialog "Support Log" opens it contains by default in "From" the actual date/time (-5min) and in "Duration" a duration of 5min:

- 1. Click the Button [Download]
- 2. Via HTTP an ASCII formatted file with the last 5 minutes will be downloaded

Retrieving a "Support Log" in the past:

- 1. Insert the in "From" the desired start date/time 2. Insert in "Duration" the needed length
- 3. Press on the PC keyboard the 'Enter' key : The "Until" date/time will be computed 4. Click the Button [Download]

or

- 1. Insert the in "From" the desired start date/time 2. Insert the in "Until" the desired stop date/time
- 3. Press on the PC keyboard the 'Enter' key: The "Duration" will be computed 4. Click the Button [Download]

	Get the events of a connection in the past:	
Best Practice	 Search the Call ID of the connection in the "Call Data" Use the Call ID in the "Text" filter of the Support Log dialog Make sure that the connection date/time match "From"- "Until" Download the Support Log 	
	Get the events of a just finished connection:	
	 Set the "Duration" to 5min (or shorter) Download the Support Log Search for the connection 	

Interpretation of a "Support Log"

The interpretation of a "Support Log" is quite easy and straight forward. With a little experience one will be soon familiar with the interpretation.

Interpretation and example of a call setup and release:

Date/time of the event	
ServiceCenter where this event was logged, e.g.: sc1 → Host *-sc-01	
sc2 → Host *-sc-02	38 2010-03-19-13:17:28,410 sc1 sc1 100786539995 start call from 0110 to 0220 39 2010-03-19-13:17:28,414 sc1 sc1100786539995 routing call to address 0220 40 2010-03-19-13:17:28,418 sc1 sc1100786539995 rule 'Adjust Domain' rewrites 41 2010-03-19-13:17:30,475 sc1 sc1100786539995 rule 'Adjust Domain' rewrites 42 2010-03-19-13:17:33,229 sc1 sc1100786539995 [0110 disconnected]
Unique connection ID	_
Connection event description	

ConfigCenter Trace

The "Trace" provides the supporter with information from the message traffic between the VoIP switch and external VoIP devices, such as PSTN gateway, SIP CPE, SIP or MGCP telephones.

The "Trace" contains:

- Session Initiation Protocol SIP registration and connection signaling messages
 Media Gateway Control Protocol MGCP audit and endpoint control messages
 Session Description Protocol SDP streaming media initialization parameters

The "Trace" provides filters for:

Time based selection: From ? Until, From ? Duration ◊ Text filter

The "Trace" has a limited history. The history may last from a few hours up to some days. The length of the history may be different from VoIP switch to VoIP switch and depends on the length of log files and amount of logging events.

The interpretation of a "Trace" (PCAP formatted file) has to be done in an external application like Wireshark network protocol analyzer. Wireshark offers deep and rich VoIP analysis .

Noto	The "Trace" is not tenant sensitive. This means a supporter of tenant A is able to see signaling messages of tenant B!		
Note	Due to this open display of information it may be possible that the "Trace" is not available for the supporters and operators on a multi tenant VoIP Switch.		

Navigate to the "Trace"

ConfigCenter:

Menu "Support"

Menu "Trace"

Get a "Trace"

Dialog: "Trace":

Optional Filter for Text	Trace	×
Call Id Telephone number	Filter all messages that match ALL of the following rules: Text [0443027192	les:
	From (2015/12/22 16:00:00 (3)) Until (3) Duration (20:05:00	
Time Span or Duration: Mandatory: • "From"	Download	Close

When the dialog "Trace" opens it contains by default in "From" the actual date/time (-5min) and in "Duration" a duration of 5min:

- 1. Click the Button [Download]
- 2. Via HTTP an PCAP formatted file with the last 5 minutes will be downloaded

Retrieving a "Trace" in the past:

- 1. Insert the in "From" the desired start date/time 2. Insert in "Duration" the needed length
- 3. Press on the PC keyboard the 'Enter' key: The "Until" date/time will be computed
- 4. Click the Button [Download]

or

- 1. Insert the in "From" the desired start date/time
- 2. Insert the in "Until" the desired stop date/time
- 3. Press on the PC keyboard the 'Enter' key: The "Duration" will be computed 4. Click the Button [Download]

	Get the events of a connection in the past:
	 Search the connection in the "Call Data" Click the Button [Trace]
Best Practice	Get the events of a just finished connection:
	 Set the "Duration" to 5min (or shorter) Download the Trace Search for the connection

Interpretation of a "Trace"

The interpretation of a "Trace" needs experience!

For more information:

See also article "Brief Tutorial of the SIP Signaling and SDP Media Protocols" ◊ Get a Wireshark training

Example of a Wireshark call capture, SIP setup and release:

No.	Time	Source	Destination	Protocol L	ength Info
6426	4 2015-11-06 08:49:19.390000	81.	81.	SIP/SDF	794 Request: INVITE sip:043 081
6426	5 2015-11-06 08:49:19.408000	81.	81.	SIP	319 Status: 100 Trying
6426	6 2015-11-06 08:49:19.543000	192.168.222.53	192.168.222.53	SIP/SOF	947 Request: INVITE sip:mcf_conf@192.168.222.53:5062
6426	7 2015-11-06 08:49:19.544000	192.168.222.53	192.168.222.53	SIP	388 Status: 100 Trying
6426	8 2015-11-06 08:49:19.547000	192.168.222.53	192.168.222.53	SIP/SDP	692 Status: 200 OK
6426	9 2015-11-06 08:49:19.550000	81	81.	SIP/SDF	663 Status: 200 OK
6427	0 2015-11-06 08:49:19.573000	81	81	SIP	434 Request: ACK sip:04352105570815060
6427:	1 2015-11-06 08:49:19.574000	192.168.222.53	192.168.222.53	SIP	353 Request: ACK sip:mcf_conf@192.168.222.53:5062
6427	2 2015-11-06 08:49:43.095000	81.	81.	SIP	434 Request: BYE sip:0435210557081 :5060
6427	3 2015-11-06 08:49:43.095000	81	81.	SIP	353 Status: 200 OK
6427	4 2015-11-06 08:49:43.098000	192.168.222.53	192.168.222.53	SIP	342 Request: BYE sip:mcf_conf@192.168.222.53:5062
6427	5 2015-11-06 08:49:43.099000	192.168.222.53	192.168.222.53	SIP	372 Status: 200 OK
4					,
Fram	e 64264: 794 bytes on wire (63	352 bits), 794 byt	es captured (6352	bits)	
B Ethe	rnet II, Src: 00:00:00_00:5c:0	01 (00:00:00:00:50	:01), Dst: 00:00:0	0.00:00:00	(00:00:00:00:00)
. Inte	rnet Protocol Version 4, Src:	81 (81), Dst: 81.	(81	- ')
∎ User	Datagram Protocol, Src Port:	5062 (5062), Dst	Port: 5060 (5060)		
B Sess	ion Initiation Protocol (INVII	TE)			
B Rec	uest-Line: INVITE sip:04.	7081. ; SIP	/2.0		
III Mes	sage Header				
a V	ia: STP/2.0/UDP 81 :506	2: branch=z9hG4bKdf	chfbe3dadb48886		
	ax-Eorwards · 70		01009000010000		
	rom: <rin:07(************************************<="" td=""><td>>+++++++++++++++++++++++++++++++++++++</td><td></td><td></td><td></td></rin:07(>	>+++++++++++++++++++++++++++++++++++++			
	7081 (Sip.0/1 7081 3	17, cag=102a933002			
	all_TO: 2122cad24d6bbc47				
	all-10: 2152Ca0340000e4/				
B C	Sed: 28929 INVITE				
(i) C	ontact: <sip:0 4081.<="" td=""><td>:5062;transpor</td><td>'t=udp></td><td></td><td></td></sip:0>	:5062;transpor	't=udp>		
S	upported: replaces				
U	ser-Agent: Patton SN4960 4E60	V UI 00A0BA01CE73	R6.T 2013-03-14 H3	23 RBS SIP	MST SIP Stack/4.1.12.18
C	ontent-Type: application/sdp				
C	ontent-Length: 294				
8 Mes	sage Body				
85	ession Description Protocol				
	Session Description Protocol	Version (v): 0			
	Owner/Creator, Session Id (o)	: MxSIP 0 559 IN	IP4 81.		
	Session Name (s): SIP Call				
8	Connection Information (c): I	N IP4 81.			
8	Time Description, active time	(t): 0 0			
	Media Description, name and a	ddress (m): audio	4926 RTP/AVP 8 0	18 125 101	
18	Media Attribute (a): rtpmap:8	PCMA/8000			
	Media Attribute (a): rtpmap:0	PCMU/8000			
	Media Attribute (a): rtomap:1	8 6729/8000			
	Media Attribute (a): rtoman:1	25 CLEARMODE /8000			
	Media Attribute (a): rtnman:1	01 telephone-even	t/8000		
	Media Attribute (a): fmtn:18	annexh-no	.,		
	Madia Attribute (a): fmtp:101	0-16			
	Madia Attribute (a): condeacy	0-10			
	Media Accribute (a): Sendrecv	r			

Example of a Wireshark call list:

Navigate in Wireshark:

→ Menu "Statistics"

→ Menu "VoIP Calls"

Wireshark dialog where all calls are listed of the actual trace:

Start Time -	Stop Time	Initial Speaker	From	То	Protocol	Packets	State	Comments	1000
52.373	253.222	85	sip:0 'Gsip01.tra	sip:04" @sip01	SIP	11	REJECTED		
64.130	287.793	213	sip:92@91	sip:008	SIP	15	IN CALL		
58.602	302.933	213. 1	sip:07: @21.	sip:09?************************************	SIP	13	COMPLETED		
58.784	276.349	85. *** 134	sip:04 +@sip01.tra	sip:04	SIP	13	REJECTED		
77.160	294.817	9:	sip:0(@9:	sip:04: @91 ?	SIP	19	COMPLETED		
79.900	285.546	21 57	sip:06 6@9'	sip:06 @91 ?	SIP	15	IN CALL		
84.561	297.739	91 1	sip:6161@91.	sip:08	SIP	15	IN CALL		
36.394	288.233	62.)	sip:00000000@91.	sip:08 1@9*	SIP	13	IN CALL		
\$7.277	293.579	80.	sp:313681415@91)	sip:03 /@91.	SIP	15	IN CALL		
\$7.406	296.029	21 1	sp:03 7@21	sip:09 3@91	SIP	12	IN CALL		
2.222	293.219	811	sp:80@91.)	sp:04	SIP	9	CALL SETUP		-
9 357	303,850	212	sia:00000000.#91	sip:004 3/801	STP	12	REJECTED		
0.358	300.786	21 1	sip: anonymous Ranonymou	sip:001)(801	STP	5	CALL SETUP		
14.164	304.579	213 1	sin:07 1@2	sin:09/ 5/891	STP	7	REJECTED		

Example of a Wireshark call flow:

Navigate in Wireshark:

- Menu "Statistics"
 - → Menu "VoIP Calls"
 - → Select the call of interest

Click Button [Graph]

Wireshark dialog where the message flow is shown of the selected call:

🗖 trace	[1].pcap - Graph Analysis	
Time	213. 1. 192.168.24.23 212. 1. 1.1.1	Comment
292.409 292.427 292.644 293.025 293.191 293.629 293.629 302.458 302.506 302.506 302.507	NVITE SDP (g711A g721 g728 g711U CLEARMODE t (5050) 100 Trying (5050) INVITE SDP (g711A g721 g729 g71 U 125 tel (5050) 100 Trying (5050) (5050) 100 Trying (5050) (5	SIP Prom: sip:01171110110213, 11,41101100 SIP Status SIP Request SIP Status SIP Status SIP Status SIP Status SIP Status SIP Status SIP Status SIP Status SIP Request SIP Request
	x	<
	Save As	Glose

The ConfigCenter Call Data

The "Call Data" lists the CDR of all incoming or outgoing connections or connection attempts. Extended filters enable the supporter to search for specific calls. The filters can be combined with logical AND.

Filter CDRs according:

- Ocall start and end date/time
- ◊ Call duration
- ◊ Call charges
- Telephone number of caller and/or callee.
- Tenants & account
- ◊ Price list attributes "Destination Type" & "Destination"

The "Call Data" has a limited history. The length of the history may be different from VoIP switch to VoIP switch and depends on the CDR storage length in the date base.

Selected CDR details allow direct access to the information of:

♦ SIP Trace:

The SIP message contents of this specific connection or call attempt is shown. For the interpretation of the trace consult the article "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow SIP Signaling".

The RTP/RTCP information and statistics of this specific connection or call attempt is shown. For the interpretation of the media information consult the article "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow Media Stream".

	 The "Call Data" has a limited history. The length of the history may be different from VoIP switch to VoIP switch and depends on the CDR storage length in the date base.
Note	 Not all filter options may be available on the VoIP Switch.
	• The "Call Data" is tenant sensitive. This means a supporter/operator of tenant A is not able to see events of tenant B!



Changing a CDR's contents may be a legal violation in the country of operation of the VoIP Switch!

Navigate to the "Call Data"

ConfigCenter:



→ Menu "Call Data"

Get the "Call Data"

Dialog: "Call Data":



By clicking on the line of a CDR a dialog pops up, which provides a) more details of the connection and b) one click access to the call's SIP trace and media RTP/RTCP information and statistics:

CDR: sc133665256	8403
Call ID Charges Account Charges Tenant Time Duration Restricted Calling Number Called Number Calle Called Number Called Number C	sc1336652568403 0.00 0.00 2017/08/24 10:54 00:00:00 ne 04 04 04 05 1 canceled A 0449980912 Switzerfand-058 (Corporate) VAS trace MediaTrace Close
Do not use for support reasons! Get a tra as PCAP	Get the RTP information and statistics of this call as HTML file.

	A loss been been been been been been been be						
	ALL						
	some with the state of a second with the lot of the lot of the lot of the second with the second control of the lot of th						
	And the second s						
•	NAME AND ADDRESS OF ADDRESS ADDRES						
	and an and an and an						
	BALL BALL AND REAL PROPERTY AND AN ADDRESS OF ADDRESS O						
	BOTT MOTOR MERCER CHARGE COLUMN TO THE AND AND AN ADDRESS AND ADDR						
	BUTT NOT TO AN AD AD ADDRESS AD. ADDRESS ADDRES						
	AND'S DOLY 12 MIL MILLION AND AND AND AND AND AND AND AND AND AN						
	BUT DEPENDENT OF THE DEPENDENT OF THE PARTY OF THE PARTY.						
	trans solidar. No home an array \$150 \$1951. The home company \$150 \$1951						
	entranne 11, bir berne an an de de an an de de la de la de la de						
	Internet Fridand Sectors 6, 511 IR. 18 3, 681 81 30 1						
	tor bragin relief, by het, bit could an het. San (1965)						
	Bastas Information Robert United						
	Line and Line recta signed. The Line a						
	- Nouse Num						
	3 Visit DEVI Artist B: 1980; A and all other had other bad others						
	No. 1011 ALL BUILD ALL AREAD AND AND AND AND AND AND AND AND AND A						
	A DECEMBER OF THE DECEMBER OF						
	View Constraint (Constraint) View Constraint) View Constraint) View Constraint) View Constraint)						
	 Const. (1971) 2011 (1971) Const. (1971) 2011 (1971) Const. (1971) 2011 (1971) Const. (1971) 2011 (1971) 2011 (1971) 2011 (1971) 2011 Const. (1971) 2011 (1971) 2011 (1971) 2011 (1971) 2011 (1971) 2011 Const. (1971) 2011 (1971) 20						
	 The start of the s						
	Vec (Vec (Vec (Vec (Vec (Vec (Vec (V						
	Conception and Conception and Conception and Conception Conception and Conception and Conception Conception and Conception and Conception C						
	The Control of the Theorem (Control of the Control of the Con						
	Line Unit and A Constant A Constant And						
	Line: Unit (1997) Biol (199						
	The second of the second						
	Provide and the second se						
	Provide State	_					
	The second	-					
	The second	-					
	The second	-					
	A second se	-					
	A second se	-					
		-					

For the interpretation of the trace consult the article:

"Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow SIP Signaling"



For the interpretation of the media information consult the article: "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow Media Stream"

The ConfigCenter Address Registration

The ConfigCenter "Address Registration" displays if a SIP device or MGCP MTA has registered the telephone number. The supporter finds the following information of the registering devices:

- ◊ Type of registration, SIP, notifications, presence, etc
- ◊ IP address
- ◊ SIP user agent
- Registration time left.

Registrations can be de-registrated on the VoIP Switch by force.

Hint:

The device cannot be informed that it was de-registerd on the VoIP Switch. That means you have to wait until it re-registers automatically or force the device manually to re-register.

Navigate to "Registrations"

ConfigCenter:



or

→ Menu "Accounts"

Click on the line of the desired account

Click on the right arrow at "Addresses"

For details:

Click on the line of the desired address

→ Click on the right arrow at "Registration"

Interpretation of "Registrations" Information

Display of "Addresses" and registration overview:

	Addres	ses of Account: 2				×
	End	Number Name		(* or ? as wild (* or ? as wild (* or ? as wild	dcards) dcards) dcards)	
Chatwa and tyme of	Page	or 1 (10 Entrie	es) 🖤			Search
Status and type of	Numbe	rv	Endpoint r	name	Registrat	ion 🔶
registration:	0.	30			sip	×
	02				sip	
 Active registration 	04	-			sip	- 2
No registration	04	1			• sip	x
- -	04	j			sip	×
F	04	3			sip	×
Note:	04	1			• sip	×
If no icon is shown then	02	5			sip	
more than 100	04	,			- sip	-
	Start	Wizard		_	_	Close
dudiesses die listed.					•	
	04	ł	0@8(1	mgcp	×
	04	3	1@8c		mgcp	×
	11				3	
	1:				3	2

By clicking on the line of an address and then the right arrow at "Registration" a dialog pops up, which provides informations of all registrations of the address:

	Status	registered		
	Registration Time left 00	00:06:41		
Release all registrations of all	IP Address	9 2:5060		
	User Agent Connection Weight	FPBX-13.0.192.8(13.14.0) SIP 1.000		
				devices on the VoIP
Switch.				Endpoint
	Delete	CI	ose	

The ConfigCenter Components

The "Components" displays the state and activity of the VoIP Switch components. The components are the entities of the VoIP Switch that provide all functionality and features. The display is automatically updated every few seconds and shows the actual state and load of every component.

Navigate to "Components"

ConfigCenter:

- → Menu "System"
 - Menu "Components"

Interpretation of "Components" Information

Display of "Components":

Name of all installed					
	Con onents				
Presents the state of a connection: active: The component is working correctly and is active. Passive: The component is correctly working and ready for jump in.	Name HealthCheck 1 HealthCheck 1 LoadBalancer 1 LoadBalancer 2 CallBalancer 2 MediaServer 1 MediaServer 2 ServiceCenter 1 ServiceCenter 1	State agrive passive active passive active active active active active active	Remark 153/558 messages 0/0 messages 919 stleams 914 stleams 434 ca is		
 barred: The component is correctly working but is suspended from its task. unavailable: The component is not working correctly! 	MediaCenter 1 MediaCenter 2 FaxServer 1 FaxServer 2 CallAgent 1 CallAgent 1 CallAgent 2 CdrCollector RatingCenter 1 RatingCenter 2	active active active active active active passive passive	108 endpoints 102 endpoints		
In the remarks mostly the load of an active component is displayed. In an exceptional situation a short description is given.	AdminCenter 1 AdminCenter 1 ConfigCenter 1 ConfigCenter 2 Database 1 Database 2	 active active active active active active active 	28 sestions 6 sessions 209 connections 95 connections	Close	

By clicking on the line of a component a dialog pops up, which provides more informations or enables to send messages or handle the work load of the component:

IP address of the component within the	ServiceCenter	X
VoIP Switch internal communication.	Name Servie Center State ad Te IP Address 192.168.32.12	
Installed software version of the component	Version 6.8.10542 Remark	Change Enables the possibility to generate a message with a certain severity
The Acceptance defines the work load that a component has	Test-Alarm Info •	Send and any text in the lo files of the component With a severity higher
to take over. A value of 0 puts the component in the "barred" state.		than "Info" an E-mail will be sent to the defined addressees i the Xymon alerting.

The ConfigCenter Channels

The ConfigCenter "Channels" is a live display of the current active connections and connection build-up. The administrator can filter an search the connections. If needed a connection can be forced to be released.



Navigate to "Channels"

ConfigCenter:

Interpretation of "Channels" Information

Display of "Channels":



The ConfigCenter System Utilization

The "System Utilization" gives a statistical overview of the VoIP Switch resource utilization:

- Number of accounts
- ◊ Number of addresses (telephone numbers)
- Number of registrations
- ◊ etc

Note On most VoIP Switches the "System Utilization" display is not available for the supporters and operators.

Navigate to "System Utilization"

ConfigCenter:

→ Menu "System"

→ Menu "Utilization"

Interpretation of the "System Utilization" Information

The "System Utilization" provides the numbers of used resources:


'Enter' key: The "Duration" will be computed Click the Button

	Get the events of a connection in the past:
Rest	 Search the connection in the "Call Data" Click the Button [Trace]
Practice	Get the events of a just finished connection:
	 Set the "Duration" to 5min (or shorter) Download the Trace Search for the connection

Interpretation of a "Trace"

The interpretation of a "Trace" needs experience!

For more information:

 \diamond See also article "Brief Tutorial of the SIP Signaling and SDP Media Protocols" \diamond Get a Wireshark training

Example of a Wireshark call capture, SIP setup and release:

No.	Time	Source	Destination	Protocol L	ength Info
6426	4 2015-11-06 08:49:19.390000	81.	81.	SIP/SDF	794 Request: INVITE sip:043 081
6426	5 2015-11-06 08:49:19.408000	81.	81.	SIP	319 Status: 100 Trying
6426	6 2015-11-06 08:49:19.543000	192.168.222.53	192.168.222.53	SIP/SOF	947 Request: INVITE sip:mcf_conf@192.168.222.53:5062
6426	7 2015-11-06 08:49:19.544000	192.168.222.53	192.168.222.53	SIP	388 Status: 100 Trying
6426	8 2015-11-06 08:49:19.547000	192.168.222.53	192.168.222.53	SIP/SDP	692 Status: 200 OK
6426	9 2015-11-06 08:49:19.550000	81	81.	SIP/SDF	663 Status: 200 OK
6427	0 2015-11-06 08:49:19.573000	81	81	SIP	434 Request: ACK sip:04352105570815060
6427:	1 2015-11-06 08:49:19.574000	192.168.222.53	192.168.222.53	SIP	353 Request: ACK sip:mcf_conf@192.168.222.53:5062
6427	2 2015-11-06 08:49:43.095000	81.	81.	SIP	434 Request: BYE sip:0435210557081 :5060
6427	3 2015-11-06 08:49:43.095000	81	81.	SIP	353 Status: 200 OK
6427	4 2015-11-06 08:49:43.098000	192.168.222.53	192.168.222.53	SIP	342 Request: BYE sip:mcf_conf@192.168.222.53:5062
6427	5 2015-11-06 08:49:43.099000	192.168.222.53	192.168.222.53	SIP	372 Status: 200 OK
4					
Fram	e 64264: 794 bytes on wire (63	352 bits), 794 byt	es captured (6352	bits)	
B Ethe	rnet II, Src: 00:00:00_00:5c:0	01 (00:00:00:00:50	:01), Dst: 00:00:0	0.00:00:00	(00:00:00:00:00)
. Inte	rnet Protocol Version 4, Src:	81 (81), Dst: 81.	(81	- ')
∎ User	Datagram Protocol, Src Port:	5062 (5062), Dst	Port: 5060 (5060)		
B Sess	ion Initiation Protocol (INVII	TE)			
B Rec	uest-Line: INVITE sip:04.	7081. ; SIP	/2.0		
III Mes	sage Header				
a V	ia: STP/2.0/UDP 81 :506	2: branch=z9hG4bKdf	chfbe3dadb48886		
	ax-Eorwards · 70		01009000010000		
	rom: <rin:07(************************************<="" td=""><td>>+++++++++++++++++++++++++++++++++++++</td><td></td><td></td><td></td></rin:07(>	>+++++++++++++++++++++++++++++++++++++			
	7081 (Sip.0/1 7081 3	17, cag=102a933002			
	all_TO: 2122cad24d6bbc47				
	all-10: 2152Ca0340000e4/				
B C	Sed: 28929 INVITE				
(i) C	ontact: <sip:0 4081.<="" td=""><td>:5062;transpor</td><td>'t=udp></td><td></td><td></td></sip:0>	:5062;transpor	't=udp>		
S	upported: replaces				
U	ser-Agent: Patton SN4960 4E60	V UI 00A0BA01CE73	R6.T 2013-03-14 H3	23 RBS SIP	M5T SIP Stack/4.1.12.18
C	ontent-Type: application/sdp				
C	ontent-Length: 294				
8 Mes	sage Body				
85	ession Description Protocol				
	Session Description Protocol	Version (v): 0			
	Owner/Creator, Session Id (o)	: MxSIP 0 559 IN	IP4 81.		
	Session Name (s): SIP Call				
8	Connection Information (c): I	N IP4 81.			
8	Time Description, active time	(t): 0 0			
	Media Description, name and a	ddress (m): audio	4926 RTP/AVP 8 0	18 125 101	
18	Media Attribute (a): rtpmap:8	PCMA/8000			
	Media Attribute (a): rtpmap:0	PCMU/8000			
	Media Attribute (a): rtpmap:1	8 G729/8000			
	Media Attribute (a): rtoman:1	25 CLEARMODE /8000			
	Media Attribute (a): rtnman:1	01 telephone-even	t /8000		
	Media Attribute (a): fmtn:18	annexh-no	.,		
	Madia Attribute (a): fmtp:101	0-16			
	Madia Attribute (a): condeacy	0-10			
	Media Accribute (a): Sendrecv	r			

Example of a Wireshark call list:

Navigate in Wireshark:

→ Menu "Statistics"

→ Menu "VoIP Calls"

Wireshark dialog where all calls are listed of the actual trace:

Start Time -	Stop Time	Initial Speaker	From	То	Protocol	Packets	State	Comments	
252.373	253.222	85	sip:0 'Csip01.tra	sip:04" @sip01	SIP	11	REJECTED		
64.130	287.793	213	sip:92@91	sip:008	SIP	15	IN CALL		
68.602	302.933	213. 1	sip:07: @21.	sip:090	SIP	13	COMPLETED		
268.784	276.349	85. *** 134	sip:04 +@sip01.tra	sip:04 :@sip01.tra	SIP	13	REJECTED		
277.160	294.817	9:	sip:0(@9:	sip:04. @91 ?	SIP	19	COMPLETED		
279.900	285.546	21 57	sip:06 6@9'	sip:06 @91 ?	SIP	15	IN CALL		
284.561	297.739	91 1	sip:6161@91.	sip:08 @91	SIP	15	IN CALL		
286.394	288.233	62	sip:00000000@91.	sip:08 1@9*	SIP	13	IN CALL		
287.277	293.579	80	sip:313681415@91)	sip:03	SIP	15	IN CALL		
287.406	296.029	21 1	sip:03 7@21	sip:09 3@91	SIP	12	IN CALL		
292.222	293.219	811	sip:80@91	sip:04 \$91	SIP	9	CALL SETUP		_
92.409	302.507	211	sp:0 021	sip:09 22@91	SIP	12	IN CALL		
298.357	303.850	21. 5	sip:00000000@91. ?	sip:004	SIP	13	REJECTED		
300.358	300.786	21	sip:anonymous@anonymou	sip:09(SIP	5	CALL SETUP		
304.164	304.579	213	sip:07 1@2:	sip:09L	SIP	7	REJECTED		

Example of a Wireshark call flow:

Navigate in Wireshark:

- Menu "Statistics"
 - → Menu "VoIP Calls"
 - → Select the call of interest

Click Button [Graph]

Wireshark dialog where the message flow is shown of the selected call:

🗖 trace	[1].pcap - Graph Analysis	
Time	213. 1. 192.168.24.23 212. 1. 1.1.1	Comment
292.409 292.427 292.644 293.025 293.191 293.629 293.629 302.458 302.506 302.506 302.507	NVITE SDP (g711A g721 g728 g711U CLEARMODE t (5050) 100 Trying (5050) INVITE SDP (g711A g721 g729 g71 U 125 tel (5050) 100 Trying (5050) (5050) 100 Trying (5050) (5	SIP Prom: sip:01171110100213, 11, 1101170 SIP Status SIP Request SIP Request
	x	र ा) । ,
	Save As	Glose

The ConfigCenter Call Data

The "Call Data" lists the CDR of all incoming or outgoing connections or connection attempts. Extended filters enable the supporter to search for specific calls. The filters can be combined with logical AND.

Filter CDRs according:

- Ocall start and end date/time
- ◊ Call duration
- ◊ Call charges
- Telephone number of caller and/or callee.
- Tenants & account
- ◊ Price list attributes "Destination Type" & "Destination"

The "Call Data" has a limited history. The length of the history may be different from VoIP switch to VoIP switch and depends on the CDR storage length in the date base.

Selected CDR details allow direct access to the information of:

♦ SIP Trace:

The SIP message contents of this specific connection or call attempt is shown. For the interpretation of the trace consult the article "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow SIP Signaling".

The RTP/RTCP information and statistics of this specific connection or call attempt is shown. For the interpretation of the media information consult the article "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow Media Stream".

	 The "Call Data" has a limited history. The length of the history may be different from VoIP switch to VoIP switch and depends on the CDR storage length in the date base.
Note	 Not all filter options may be available on the VoIP Switch.
	• The "Call Data" is tenant sensitive. This means a supporter/operator of tenant A is not able to see events of tenant B!



Changing a CDR's contents may be a legal violation in the country of operation of the VoIP Switch!

Navigate to the "Call Data"

ConfigCenter:



→ Menu "Call Data"

Get the "Call Data"

Dialog: "Call Data":



By clicking on the line of a CDR a dialog pops up, which provides a) more details of the connection and b) one click access to the call's SIP trace and media RTP/RTCP information and statistics:

CDR: sc133665256	8403
Call ID Charges Account Charges Tenant Time Duration Restricted Calling Number Called Number Calle Called Number Called Number C	sc1336652568403 0.00 0.00 2017/08/24 10:54 00:00:00 ne 04 04 04 04 04 04 04 05 1 canceled A 04 04980912 Switzerland-058 (Corporate) VAS to see the second se
Do not use for support reasons! Get a tra as PCAP	Get the RTP information and statistics of this call as HTML file.

	A - 10 - 10 - 10 - 10 A - 10 - 10 - 10 - 10
	A
	a - 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10
	a
	1.10.11.000 1 1000 1
How determine the set of the	
Received and the second s	
Report Los Reis Las Reis (Series 100 - 100	
Here and the second secon	
Even (a) and (b)	
No investory 11 (1997) - 2010 - 2010 - 2010 - Prime story 11 (2010) - 2010 - Prime story 2010 - Prime s	
the second of the second	
No	
Color Dr. Etterstellinger Color Statistics (ed.) (2015)	
 Cong. 2010 INVEX Cong. 2010 To 2010	
Contact, etc. 67, 100, 100, 100, 100, 100, 100, 100, 10	
Instantiant reprint the second statement of antipactory's and approximate the second s	
that agent forms taken some of minimulat?) as 7 201-01-14 will see the set of the taken 1.1.18	
Called Top: and Laborate	
· Third Int	
- Next and Next Sector 1	
Resides Bencharter Fraherst service (12) 8	
a Barter, Comptony, Sanadary 14 Lab. Wellin 8 100 10 100 101 10.	
Resultant Name Auto 1977 (1977)	
a particular information only in the sta-	
a The Best States, with the ISL III	
a bails bearinging, can out attain this work and a to be in the	
a Marine and Tanke 100 - Hannah & Kimin Mills	
- Build and finds (a) - respect to the line	
a field and the second se	
a Barling with Charles (and) and and a strength of the second stre	
a particular to a second and a particular second second	
- Budy attribute (c): Sale M examines	
A REAL AND A	
And all had been and and and all had been al	

For the interpretation of the trace consult the article:

"Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow SIP Signaling"



For the interpretation of the media information consult the article: "Brief Tutorial of the SIP Signaling and SDP Media Protocols", chapter "Knowhow Media Stream"

The ConfigCenter Address Registration

The ConfigCenter "Address Registration" displays if a SIP device or MGCP MTA has registered the telephone number. The supporter finds the following information of the registering devices:

- ◊ Type of registration, SIP, notifications, presence, etc
- ◊ IP address
- ◊ SIP user agent
- Registration time left.

Registrations can be de-registrated on the VoIP Switch by force.

Hint:

The device cannot be informed that it was de-registerd on the VoIP Switch. That means you have to wait until it re-registers automatically or force the device manually to re-register.

Navigate to "Registrations"

ConfigCenter:



or

→ Menu "Accounts"

Click on the line of the desired account

Click on the right arrow at "Addresses"

For details:

Click on the line of the desired address

→ Click on the right arrow at "Registration"

Interpretation of "Registrations" Information

Display of "Addresses" and registration overview:

	Addres	ses of Account: 2				×
	End	Number Name		(* or ? as wild (* or ? as wild (* or ? as wild	cards) cards) cards)	
	Page	1 of 1 (10 Entrie	es) 🌳			Search
Status and type of	Numbe	r 7	Endpoint r	name	Registrat	ion 🔶
registration:	0.	30			sip	×
registration.	04	1			sip	×
Active registration	04	2			• sip T	×
No registration	04	3			e sip	×
	04	1			sip	
	04	,			sip	- 0
Note:	04	;			sip	2
	04	3			sip	×
If no icon is shown then	04)			sip	×
more than 100 addresses are listed.	Start	Wizard	_			Close
	04	ł	0@8(,	mgcp	×
	04	i	1@80	1	mgcp	×
	1:				0	×
	1;				0	×

By clicking on the line of an address and then the right arrow at "Registration" a dialog pops up, which provides informations of all registrations of the address:

	Status Registration Time left IP Address User Agent Connection Weight 1	registered				
		00:06:41				
Release all registrations of all devices on the VoIP Switch.		9 2:5060				
		FPBX-13.0.192.8(13.14.0) SIP 1.000 Public IP				
				Endpoint		
					Delete	Clos

The ConfigCenter Components

The "Components" displays the state and activity of the VoIP Switch components. The components are the entities of the VoIP Switch that provide all functionality and features. The display is automatically updated every few seconds and shows the actual state and load of every component.

Navigate to "Components"

ConfigCenter:

- → Menu "System"
 - Menu "Components"

Interpretation of "Components" Information

Display of "Components":

Name of all installed components.				
	Conconents			×
Presents the state of a connection: active: The component is working correctly and is active. passive: The component is correctly working and ready for jump in.	Name HealthCheck 1 HealthCheck 2 LoadBalancer 1 LoadBalancer 2 CallBalancer 2 MediaServer 2 MediaServer 1 MediaServer 1 ServiceCenter 1 ServiceCenter 1	State agive passive active passive active active active active active	Remark 153/558 messages 0/0 messages 919 streams 914 streams 914 streams 453 ca is	
 barred: The component is correctly working but is suspended from its task. unavailable: The component is not working correctly! 	MediaCenter 1 MediaCenter 2 FaxServer 1 FaxServer 2 CallAgent 1 CallAgent 2 CdrCollector RatingCenter 1 RatingCenter 2	active active active active active active passive passive	108 endpoints 102 endpoints	
In the remarks mostly the load of an active component is displayed. In an exceptional situation a short description is given.	AdminCenter 1 AdminCenter 2 ConfigCenter 1 ConfigCenter 2 Database 1 Database 2	 active active active active active active active 	28 sessions 6 sessions 209 connections 95 con <mark>n</mark> ections	Close

By clicking on the line of a component a dialog pops up, which provides more informations or enables to send messages or handle the work load of the component:

IP address of the component within the	ServiceCenter	X
VoIP Switch internal communication.	Name Servie Center State ad Te IP Address 192.168.32.12	
Installed software version of the component	Version 6.8.10542 Remark	Change Enables the possibility to generate a message with a certain severity
The Acceptance defines the work load that a component has	Test-Alarm Info •	Send and any text in the lo files of the component With a severity higher
to take over. A value of 0 puts the component in the "barred" state.		than "Info" an E-mail will be sent to the defined addressees i the Xymon alerting.

The ConfigCenter Channels

The ConfigCenter "Channels" is a live display of the current active connections and connection build-up. The administrator can filter an search the connections. If needed a connection can be forced to be released.



Navigate to "Channels"

ConfigCenter:

Interpretation of "Channels" Information

Display of "Channels":



The ConfigCenter System Utilization

The "System Utilization" gives a statistical overview of the VoIP Switch resource utilization:

- Number of accounts
- ◊ Number of addresses (telephone numbers)
- Number of registrations
- ◊ etc

Note On most VoIP Switches the "System Utilization" display is not available for the supporters and operators.

Navigate to "System Utilization"

ConfigCenter:

→ Menu "System"

→ Menu "Utilization"

Interpretation of the "System Utilization" Information

The "System Utilization" provides the numbers of used resources:



Manual for the Maintenance and Problem Solving of the Aarenet VoIP Switch

VoIP Switch Component Handling

Warning

All described actions can jeopardize the VoIP Switch's telephony service or server functionality!

If there are uncertainties the contact the "VoIP Switch Supplier Support"

Basic VoIP Switch Component Commands

The VoIP Switch Administrator finds here instruction for VoIP Switch Component handling on OS console level:

- Start the VoIP Switch Component
- ◊ Stop the VoIP Switch Component
- ♦ Check the VoIP Switch Component status
- Restart the VoIP Switch Component
- ◊ etc

The VoIP Switch Component command affects only the instance on this server and can be executed with root rights only!

Command syntax:

root# <AS_COMPONENT> <COMMAND_OPTION>

Example:

root# configcenter status

Warning

Do not use other VoIP Switch Component command options as they can produce heavy problems!

Command	Command Option	Remark
<as_component></as_component>		VoIP Switch Component command
e.g.:		
configcenter		
	version	Lists the VoIP Switch Component version
	status	Lists the VoIP Switch Component status and process ID
	stop	Stops the VoIP Switch Component
		The VoIP Switch Component stops immediately and any activity of the component will be interrupted!
	start	Starts the VoIP Switch Component
		The VoIP Switch Component becomes immediately active and operative!
	startpassive	Starts the VoIP Switch Component but it remains passive.

For becoming operative the VoIP Switch Component has to be started with the start option. Not all VoIP Switch Components offer this option.
Stops and starts the VoIP Switch Component
The VoIP Switch Component becomes immediately active and operative!
Stops and starts the VoIP Switch Component but it remains passive.
For becoming operative the VoIP Switch Component has to be started with the start option. Not all VoIP Switch Component offer this option.
Opens the error log file of the VoIP Switch Component
Opens the actual log file of the VoIP Switch Component

Put Out of / Back to Service a VoIP Switch Component in an Operative VoIP Switch

The VoIP Switch Administrator finds here instruction for putting out or back of a VoIP Switch Component.

Put Out of Service a VoIP Switch Component

There are two ways to put out of service a VoIP Switch Component:

Variant 1: "Stop it hard"

Action:

A) Stop and check the component via the shell:

```
root# <AS_COMPONENT> stop
root# <AS_COMPONENT> status
```

The consequences are that the component stops immediately its operative work and all its running tasks.

The following VoIP Switch components may be stopped this way without jeopardizing the telephony service:

ConfigCenter
 AdminCenter
 DataAccessCenter
 MediaCenter
 RatingCenter
 DataBase

	Make sure that:		
Note	 The second component is active The VoIP Switch administrators, operators and supporters are informed which ConfigCenter, AdminCenter are active The users are able to use the active AdminCenter The provider's CRM is able to use the active DataAccessCenter The active BatingCenter is producing the CDB 		

Variant 2: "Stop it gracefully"

Action:

A) Stop gracefully the component via the ConfigCenter.

For the following components do flip the "active ? passive" role:

•	HealthCenter
•	LoadBalance

CallBalancer

do:

ConfigCenter GUI Menu "System" Menu "Components"

Click the active component HealthCheck

Click the fat right arrow at "Make component passive"

Confirm by clicking Button [Yes]

For the following components do a "pre-bar":

ServiceCenter
 MediaServer
 FaxServer
 CallAgent

do:

ConfigCenter GUI Menu "System" Menu "Components" Click the desired VoIP Switch component Change the parameter "Acceptance" to **0**

C) Wait until the component displays no activity anymore.

ConfigCenter GUI Menu "System" Menu "Components"

D) Stop and check the component via the shell:

root# <AS_COMPONENT> stop
root# <AS COMPONENT> status

Put Back to Service a VoIP Switch Component

There are two ways to put back to service a VoIP Switch Component:

Variant 1: "Start it"

Action:

A) Start and check the component via the shell:

```
root# <AS_COMPONENT> start
root# <AS_COMPONENT> status
```

The consequence is that the component starts immediately its operative work.

Variant 2: "Start it gracefully"

© Aarenet AG 2017

This variant may make sense when the following VoIP Switch components shall become active but not operative immediately:

ServiceCenter
 MediaServer
 FaxServer
 CallAgent

Action:

A) Start "passive" the component via the ConfigCenter.

```
root# <AS_COMPONENT> startpassive
root# <AS_COMPONENT> status
```

B) Make the component operative at the appropriate time:

ConfigCenter GUI Menu "System" Menu "Components"

Click the desired VoIP Switch component

Change the parameter "Acceptance" to 100 The "Acceptance" may by any value >0 according. Choose according the load balancing scheme of the component.

C) Check if the component displays activity:

ConfigCenter GUI Menu "System" Menu "Components"

Work Flow for Analyzing VoIP Switch Problems

Note Not every red alarm jeopardizes the telephony service as a whole but a bulk of yellow warnings may endanger it!

The VoIP Switch Administrator and other service personnel find here a work flow for analyzing VoIP Switch problem indications and find out the appropriate action.

The main task is to find out if:

1. The situation jeopardizes the telephony service as a whole, e.g.:

- · IP network issues
- Several VoIP Switch servers failed or off line
- 2. The database replication is broken
 - IP network issues
 - · Server with running database failed
 - · Linux service MySQL failed
- 3. The situation hampers the operation of configuration of customer accounts, addresses etc.
 - Management server failed or off line
 - VoIP Šwitch component ConfigCenter, AdminCenter DataAccessCenter, RatingCenter stopped working correctly

The VoIP Switch Administrator finds here the work flow for analyzing VoIP Switch problems:

Work Flow for Analyzing VoIP Switch Problems

Analysis:

1. Check if it is a **single alarm** or a **bulk alarm** situation.

a) Connect to the VoIP Switch monitor Xymon "Main View"

As a rule of thumb: It is a single error if only one issue is displayed.

- 2. Analyze and treat a **single alarm** situation:
 - a) Check the contents of the error message.

b) Compare the error description against the **Indication "Xymon Event"** ones in chapter "VoIP Switch Maintenance"

- c) Check if the actual situation is equal or similar as described and the recommended actions suitable.
- d) Execute the suitable actions.

If you are not sure contact the "VoIP Switch Supplier Support"

3. Analyze the **bulk alarm** situation:

a) Get a first overview of the situation by analyzing the Xymon Monitor :

Check in the MS-01 Xymon monitor the server, component and IP status:

Xymon GUI Xymon "Main View"

- 1. Which type of server are affected?
 - At least one LoadBalancer LB server must be active that the telephony service can work!
 At least one Service Center SC server must be active that the telephony service
 - At least one ServiceCenter SC server must be active that the telephony service can work!
 - At least one server with the operative database must be active that the telephony service can work!
- 2. Check the CPE registration statistic :
 - Do drop the CPE registrations?
- 3. Check the call statistic:
 - Do drop the VoIP Switch number of calls?
 - Xymon GUI Management Server Column "calls_sys"
 Do drop the calls on one or more ServiceCenter?
 - Do drop the calls on one of more ServiceOenter?
 Xymon GUI ServiceCenter Server Column "calls_sc"
 Do drop the calls on one or more gateways?
 - Xymon GUI Gateway Column "calls_gw"
- 4. Do the same check as above on MS-02 Xymon Monitor
- 5. Does the comparison of the two Xymon Monitor point out that:
 - The same single component on the same server failed?
 - All components of one side failed?
 - The Xymon Monitor sees only the components on its side?
 - The telephony service is running at least on one side
- b) Extend the overview by analyzing the ConfigCenter "System Component" Overview :

Check in the MS-01 ConfigCenter the status of the VoIP Switch components: ConfigCenter GUI Menu "System" Menu "Components"

- 1. Are actually calls running and new calls can be established?
- 2. Make test calls:
 - To and from a telephone number in the PSTN
 - On-net test calls
 - Call a well known VoiceMail Box from on-net and from PSTN
- 3. Is the number of running calls fast dropping and no new calls are established?
- 4. Which type of VoIP Switch components are affected?
 - At least one LoadBalancer component must be active that the telephony service can work!
 - At least one ServiceCenter component must be active that the telephony service can work!
 - At least one operative database must be active that the telephony service can work!

- Does this picture correspond to the results of the first overview in the Xymon Monitor ?
- 5. Do the same check as above on MS-02 ConfigCenter
- 6. Does the comparison of the two ConfigCenter point out that:
 - The same single component on the same server failed?
 - All components of one side failed?
 - The ConfigCenter sees only the components on its side?
 - The telephony service is running at least on one side

4) Treat **bulk alarm** situations:

a) Is there a VoIP Switch server hardware, RAID or hard-disk problem?

Indications:

Indication: <HOST_NAME> "snmptrapd" "failure" <HOST_NAME> "snmptrapd" "degraded"

Actions:

For DELL server see: "Treating Problems of Servers from DELL Inc ®"

b) Is the IP connectivity affected to or between VoIP Switch servers?

Note	If VoIP Switch servers are affected then a lot of additional alarming messages of missing VoIP Switch components will pop up!			
	This can be one of the most annoying erroneous situations!			

Indications:

Indication:

<HOST_NAME> conn "Host does not respond to ping" <IP_ADDRESS> * Dropping CPE registrations ! • Dropping calls ! • No new calls!

Actions:

See: "Maintenance Due to IP Network Alarm"

c) If you are not sure what to do then contact the "VoIP Switch Supplier Support"

VoIP Switch Server Maintenance

Maintenance Due to VoIP Switch Components General Alarms

Maintenance Due to Messages from Java Framework

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "Jdbc"

Description:

Java internal exceptions. Mostly due to database accesses which are hopefully handled by the application.

Consequences:

For the VoIP Switch telephony service:

◊ Mostly none

For the operations:

◊ Mostly none

For the user:

◊ Mostly none

Solution: Observe the frequency of this event

Action:

1. Observe the frequency of this event

2. If the erroneous condition is to frequent then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from VoIP Switch Components Internals

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:						
<host_name></host_name>	msgs	"EventQueue"				
<host_name></host_name>	msqs	"SysCompDatabase	- Cannot	evalute	status"	

Description:

These events may happen on all VoIP Switch servers and are VoIP Switch component internal notes.

Consequences:

For the VoIP Switch telephony service:

Mostly none

For the operations:

◊ Mostly none

For the user:

◊ Mostly none

Solution:

Observe the frequency of this event

Action:

1. Observe the frequency of this event

2. If the erroneous condition is to frequent then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from LoadBalancer Server

Maintenance Due to HealthCheck Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "HealthCheck"

Description:

The HealthCheck supervises the status of virtual IP addresses and their associated physical IP addresses. If the HealthCheck on one server doesn't see the peer physical IP address it takes over the virtual IP address. It most probably points out an IP network problem in the "Public Voice Segment"

Consequences:



This erroneous condition must be checked within reasonable time!

For the VoIP Switch telephony service:

◊ None if concurrently no other IP network problems arise

For the operations:

◊ None

For the user:

◊ None

Solution:

Solve the IP network if needed.

Check status the VoIP Switch component with an active-passive scheme:

- ◊ LoadBalancer ◊ CallBalancer
- AatingCenter

Action:

- 1. Check if the IP network is OK
- 2. Check the status of the LoadBalancer components

Confirm if the active LoadBalancer swapped, e.g. from *-lb-01 to *-lb-02

3. Check the status of the CallBalancer components

Confirm if the active CallBalancer swapped, e.g. from *-lb-01 to *-lb-02

4. Check the status of the RatingCenter components

Confirm if the active CallBalancer swapped, e.g. from *-ms-01 to *-ms-02 Confirm if the active RatingCenter is processing the CDR's

5. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a LoadBalancer problem try to restart the component:

root# loadbalancer restart

c) If there is a CallBalancer problem try to restart the component:

root# callbalancer restart

d) If there is a RatingCenter problem try to restart the component:

root# ratingcenter restart

- e) If the RatingCenter swapped make sure that the CDR are processed:
 - 1. ConfigCenter GUI Menu "System" Menu "Components" Click line at "active" RatingCenter -> In dialog select "Process CDRs" Click button [Close]
 - 2. The CDR CSV-Files are processed:

root# cd /home/servicecenter/cdrs

Check if the CSV files have an actual time stamp which indicates that new CDRs where written:

root# ls -ltra

Open a CSV file and check for new entries, e.g.:

root# less monthly.csv

6. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to LoadBalancer Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "Balancer"

Description:

© Aarenet AG 2017

LoadBalancer internal problem that is treated internally by the component. The LoadBalancer has an "active-passive" redundancy scheme.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ None

Solution: Not defined yet

Action:

1. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to LoadBalancer Message "Missing ServiceCenter"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "BalancerSwitch" <SERVICECENTER> "not
available anymore"

Description:

The LoadBalancer indicates that it doesn't see a certain ServiceCenter.

This happens when:

 the ServiceCenter has restarted the event will be transient
 the ServiceCenter is stopped the event will remain until the ServiceCenter is started again
 no IP connectivity the event will remain until the IP connectivity is reestablished

Consequences:

Warning This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

- None, the other ServiceCenter take over the work load
- \diamond If a ServiceCenter is missing then the VoIP Switch looses redundancy capability

For the operations:

◊ None

For the user:

◊ None

Solution:

Solve the IP network problems if needed:

Actions see: "Maintenance Due to IP Network Alarm"

Solve the server problem if needed

Actions see: "Treating Server Hardware Problems"

Action:

- 1. Check if the IP network is OK
- 2. Check the status of the ServiceCenter components

Confirm that the reported ServiceCenter server is affected

- 3. Check the reported ServiceCenter server with the "Server Administrator (OMSA)"
- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a ServiceCenter problem try to restart the component:

root# servicecenter restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to CallBalancer Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs

Description:

The CallAgent dispatches MGCP messages to the CallAgent components.

The CallAgent has an "active-passive" redundancy scheme.

Consequences:

Warning This erroneous condition must be checked within short time!

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

© Aarenet AG 2017

Our Users with MGCP MTA as telephone adapter may not be able to telephone

Solution:

Check status the CallBalancer active-passive scheme and if the MGCP messages are processed.

Action:

1. Check if the IP network is OK

2. Check the status of the CallBalancer components:

a) Confirm if the active CallBalancer swapped , e.g. from *-ms-01 to *-ms-02

b) Confirm if the active CallBalancer is processing the MGCP messages

Check if the CallAgent treat MGCP connections and that the total number of MGCP connections is not dropping.

3. Check if the MGCP audits are not dropping:

a) Connect to a Xymon monitor and check in Xymon Column "regs" the numbers of MGCP-Active and MGCP-Brocken

b) Check the questions:

Ob drop the number of MGCP-Active?
If yes => There may be a IP backbone problem or CallBalancer, CallAgent outage!

- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a CallBalancer problem try to restart the component:

root# callbalancer restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to MediaServer Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

```
Indication:
<HOST_NAME> msgs "MediaConnection (06) Cannot handle
outgoing message"
<HOST_NAME> msgs "MediaServerProvider (MS) refreshing
mediaserver mclms2 failed"
```

Description:

The MediaServer records or plays back announcements and VoiceMail messages. Occasionally it may not correctly record a message and transfer it to the MediaCenter or play back an announcement or message.

The MediaServer can act as media proxy for active connections and transcode media streams.

Consequences:



For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

A VoiceMail Box message or announcement couldn't correctly record or played back.
 User may not hear the other side or vica versa.

Solution:

Depends on the situation.

Action:

1. If the erroneous condition remains or happens to often then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from Management Server

Maintenance Due to AdminCenter Message "Missing FMC Application Server"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:



Description: The AdminCenter tried to configure the FMC application.

Consequences:



For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A configuration on a FMC server failed

For the user:

◊ A user "an MC-Phone" is not working

Solution:

Check the state of the FMC servers and their IP connectivity toward the VoIP Switch servers.

Action:

- 1. Check if the IP network is OK
- 2. Check the status of the FMC server
- 3. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a FMC server problem

Contact the "VoIP Switch Supplier Support"!

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to AdminCenter Message "Missing Redirection Server"

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "FmcProvider - could not provision user" <USER_TELEPHONE_NUMBER>

Description:

The mobile app "an MC-Phone" couldn't get the information from the associated redirection server (by default a Comdasys server located in Europe) where its responsible configuration server is located. Therefore the users "an MC-Phone" couldn't obtain its configuration and will not work.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ The mobile app "an MC-Phone" will not work

Solution:

Make sure to have good IP connectivity to the Internet

Action:

1. The user must find a reliable Internet connection and restart the app "an MC-Phone" until it gets its configuration

Maintenance Due to ConfigCenter Message "Wrong User Login"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "msgsAccessLogger - ADMIN:login; user" <USERNAME> "-> User Blocked"

Description:

A VoIP Switch Administrator, Operator, Supporter tried to login to the ConfigCenter with wrong credentials. The user will be blocked for several minutes.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ The user will be blocked from the ConfigCenter for several minutes.

For the user:

◊ None

Solution: Wait

vvan

Action:

1. Retry after a few minutes with the correct login credentials.

2. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ConfigCenter Message "DB Replication Check"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs JdbcReplicationMonitor "Replication"
'<BROKEN_REPLICATION_DIRECTION>' "is broken!"

Description:

The database replication check was not successful. This can happen from time to time when the database has to process heavy load.

In most cases the database replication recovers automatically even after several hours of failed replication. If it is not recovering then this is a severe problem and must be treated.

Consequences:

Warning If this erroneous condition remains then this is a SEVERE erroneous condition and must be treated within short time!

For the VoIP Switch telephony service:

♦ The database redundancy is endangered

For the operations:

◊ None

For the user:

◊ None

Solution:

Restore the MySQI DB replication if the erroneous condition remains.

Action:

- 1. Check periodically (ca. every half hour) the Xymon monitor for this error condition.
- 2. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to DataAccessCenter Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "Jdbc" "SQL-Exception during statement"

Description:

A configuration via the DataAccessCenter may have failed.

This may happen if the database is under heavy load.

Consequences:

Warning reasonable time!

This erroneous condition must be checked within

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A customer configuration may have failed (which is hopefully covered by the CRM application).

For the user:

◊ None

Solution:

Inter-working between the DataAccessCenter and database must be optimized.

Action:

1. If this Java event is logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to RatingCenter Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

© Aarenet AG 2017

Description:

The RatingCenter has an "active-passive" scheme. Every RatingCenter event has to be checked if the active RatingCenter is working correctly and is processing the CDRs.

Consequences:

Warning This erroneous condition must be checked within short time!

For the VoIP Switch telephony service:

◊ None

For the operations:

A CDR may be not written correctly into the CDR database and/or CSV files.
 The customer billing contains not all CDR

For the user:

◊ None

Solution:

Check status the RatingCenter active-passive scheme and if the CDR are processed.

Action:

1. Check the status of the RatingCenter component

Confirm if the active RatingCenter is processing the CDR's

2. Treat the problem:

a) If the RatingCenter swapped make sure that the CDR are processed:

Open the ConfigCenter Menu "Components"

Click line at "active" RatingCenter -> In dialog select "Process CDRs"

Click button [Close]

b) Check if the CDR CSV-Files are processed:

Open the CDR directory:

root# cd /home/ratingcenter/cdrs

Check if the CSV files have an actual time stamp which indicates that new CDRs where written:

root# ls -ltra

Open a CSV file and check for new entries, e.g.:

root# less monthly.csv

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from ServiceCenter Server

Maintenance Due to FaxServer Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs

Description:

Fax may not received correctly. The mailing of the PDF file may fail.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

A received Fax may not be correctly received and transferred to the user. This situation is usually handled by the Fax device either automatically or manually.

Solution:

Restart the FaxServer component.

Action:

1. Check if no Fax at all are received.

Send test fax.

2. Restart the FaxServer:

root# faxserver restart

3. If the FaxServer logs subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to MediaCenter Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

```
Indication:
<HOST_NAME> msgs MediaCenterCall
<HOST_NAME> msgs MediaServer
<HOST_NAME> msgs "file not found"
```

Description:

The MediaCenter handles the WAV files from announcements and VoiceMail messages. Occasionally it may not correctly record a message, loose a message file. Also an order to the MediaServer may fail to replay a message

or announcement.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ A VoiceMail Box message or announcement couldn't correctly recorded or played back

Solution:

Clean up the VioceMail message date base.

Optimize the inter-working of MediaCenter and MediaServer

Action:

1. If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs

Description:

The ServiceCenter is the main component of the VoIP Switch. It computes the connections signaling and telephony features.

The ServiceCenter has an all active redundancy scheme. If one ServiceCenter fails the remaining ServiceCenter take over the work load.

Consequences:

Warning This erroneous condition must be checked and treated within short time!

For the VoIP Switch telephony service:

◊ As long one ServiceCenter remains the VoIP Switch works!

For the operations:

◊ None

For the user:

◊ None

Solution:

Depends on the analyzed problem.

Action:

1. Check how acute the problem is:

b) Check the status of the ServiceCenter component

Are enough ServiceCenter active that the work load can be treated? If NO then there is a most SEVERE erroneous situation

c) Check in the ConfigCenter Menu "Components" if the active ServiceCenter is processing the connections:

 Do drop the total number of connections?
 If YES then there is a most SEVERE erroneous situation: There may be a IP backbone problem!

d) Check in the Xymon Column "regs" the number of registered SIP-Devices:

 O drop the number of SIP-Devices?
 If YES then there is a most SEVERE erroneous situation: There may be a IP backbone problem!

e) Check the reported ServiceCenter server with the "Server Administrator (OMSA)"

◊ Are problems signaled?

2. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a ServiceCenter problem try to restart the component:

root# servicecenter restart

c) If there is a hardware problem: Actions see: "Treating Server Hardware Problems"

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "License Violation"

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs License "License Violation" <HOST_NAME> msgs License "grace-period remaining:"

Description:

This ServiceCenter has a license problem and will work only for the remaining grace period.

Consequences:

© Aarenet AG 2017

For the VoIP Switch telephony service:

- ◊ As long one ServiceCenter remains the VOIP Switch works
- ♦ The telephony service will be stopped on this ServiceCenter after passing of the grace period

For the operations:

◊ None

For the user:

◊ None

Solution:

Get actual licenses from the VoIP Switch Supplier.

Action:

1. Check in the ConfigCenter Menu "Components" which ServiceCenter component has a license problem and how long the grace period is.

2. Contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "Failed Emergency Call"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs ServicePrioCallControl "Could not establish priority-call". Call from Connection/SIP_CALL_ID>/<CALLING_NUMBER> to <CALLED_EMERGENCY_NUMBER>

Description: A user's emergency call failed!

Consequences:

Warning Severe legal condition that must be handled! This case can have legal consequences for the provider!

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

Or The emergency call did not work

Solution:

Check if the call routing failed due to a VoIP Switch emergency call treating or routing. If yes fix them.

Check if the PSTN provider did reject the emergency call. If yes contact the PSTN provider.

Action:

1. Archive traces for legal responsibilities:

- ◊ Save the trace of this emergency call and all subsequent calls from this user toward emergency numbers
- 2. Check where the call was rejected.
 - If the call was rejected at the PSTN provider side contact the PSTN provider and let investigate into this case.
- 3. Check the VoIP Switch's emergency routing:
 - Emergency numbers
 - Emergency number rewriter
 - Or Routing Tables toward the PSTN
 - ORUMES Representation of the second state o
- 4. Check if any IP network devices may interfere with the SIP signaling:
 - If there are external Session Board Controller SBC or SIP-SS7 Gateway involved check their behavior concerning the emergency calls
 - If a firewall FW is involved check that no SIP ALG or "SIP Helpers" are active
- 5. Treat the problem:
 - a) Adjust the emergency routing of the VoIP Switch if needed
 - b) Fix the IP network devices if needed
- 6. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "TopStop"

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs ServiceRatingControl (01) <CALLING_NUMBER> "max available charges reached for account:" <HOST_NAME> msgs AlarmLogger "[TOPSTOP][ALARM] tenant" <TENANT> "topstop limit nearly reached for account"

Description:

A user's TopStop limit was reached!



Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A TopStop alarm early in the month indicates a possible fraud case

For the user:

◊ No outgoing calls except emergency call will work when the TopStop limit is reached

Solution:

If it is a regular TopStop then contact the user and enhance the monthly TopStop limit.

If it is a fraud situation handle according "Best Practice: Fraud"

Action:

1. Check if it is a regular TopStop situation.

2. Check if it is a possible fraud case:

- Reached TopStop limit early in the month?
 Concurrently a lot of TopStop limits reached?
- Ight call peak during the night or weekend? Check at Xymon Column " calls_sys ".
- 3. Treat according "Best Practice for "Fraud Situation"
- 4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Nimbus Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "NimbusLink (ue) Cannot subscribe"

Description:

The Nimbus component is a VoIP Switch internal bus that connects the various VoIP Switch components on the servers. If a Nimbus endpoint on one server is missing the other Nimbus endpoints start to complain.

If a Nimbus endpoint is missing then the component may be stopped, the server not on line or an IP network problem.

This error is often displayed during VoIP Switch software upgrades of the servers. In this situation just wait until the upgrade is finished.

Consequences:

This erroneous condition must be checked and treated Warning within reasonable time!

For the VoIP Switch telephony service:

Usually none

For the operations:

None

For the user:

None

Solution:

Solve the IP network problems or server problems if needed.

Action:

1. Check if the IP network is OK

2. Check the status of the VoIP Switch components located on the server where the Nimbus is missing:

Is only Nimbus missing or other components to on this server?

3. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is not a planned outage then try to solve the server problem

c) If there is not a planned outage then try to restart the Nimbus on this server:

root# nimbus restart

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from CallAgent Server

Maintenance Due to CallAgent Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs

Description:

The CallAgent treats the message exchange with the MGCP MTA. The CallAgent has an all active redundancy scheme. If one CallAgent fails the remaining CallAgent take over the work load.

Consequences:



This erroneous condition must be checked within short

For the VoIP Switch telephony service:

◊ As long one CallAgent remains the VOIP Switch works

For the operations:

◊ None

For the user:

Single MGCP MTA at the user's premises is not working correctly. The telephone service may not always work for this users.

Solution:

Depends on the analyzed problem.

Action:

1. Check if the IP network is OK

2. Check the status of the CallAgent components

Confirm that the reported CallAgent server is affected

- 3. Check the reported CallAgent server with the "Server Administrator (OMSA)"
- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a CallAgent problem try to restart the component:

root# callagent restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from CPECenter Server

Maintenance Due to CpeCenterMessage

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:



Description:

During the preparation of a device configuration file two device configuration templates were found. If a CPE loads a device configuration file which was produced under these conditions it may not work correctly.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

O The CPE may not work with the produced configuration file

Solution:

One device configuration template has to be deleted.

Action:

1. Contact the "VoIP Switch Supplier Support"!

Maintenance Due to IP Network Alarms

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> conn "Host does not respond to ping" <IP_ADDRESS>

Description:

This test performs a "ping" toward the IP address of the host. If the "ping" is not answered then there is a problem with the IP network, e.g.

- Inged host defect or off line
- Layer2 IP Switch defect or off line
 Brocken IP backbone network

Consequences:

MOST SEVERE condition if several VoIP Switch server Warning are affected for a longer duration (ca 15min)!

For the VoIP Switch telephony service:

Or The telephone service may be interrupted

For the operations:

O The MySQL databases may loose their replication

For the user:

◊ The telephone service may be interrupted for the users!

Solution:

Solve the IP network problems!

Check the IP network devices:

- Index Print Pri
- ◊ Layer 2 IP switches
- IP Routes ◊ Firewalls

Check the VoIP Switch server IP connectivity.

Action:

1. Evaluate the severity of the IP network outage:

a) Check if it is a occasional ping failure:

- Only one host doesn't respond
- Only 1 or 2 poll cycle fail Type "Occasional Failure":
- In this situation the erroneous situation may be neglected.

b) Check if it is only a single host:

- One host doesn't respond anymore

 - Type "Host Failure": ◊ Check the hardware condition and IP connectivity of this device
 - Ocheck with the VoIP Switch Administrator in the ConfigCenter Menu
 - "Components" how the VoIP Switch is affected

c) Check if more than one VoIP Switch server is affected:

- More than one VoIP Switch server don't respond anymore
 - Type "VoIP Switch Failure": 1. Check with the VoIP Switch Administrator how the VoIP Switch is affected: a) Connect to both (*-ms-01, *-ms-02) ConfigCenter Menu "Components" and check the component status
 - b) Check the questions:
 - ◊ Which VoIP Switch servers are not visible?
 - ◊ Are they the same on both ConfigCenter?
 - Object to Does one ConfigCenter see only the servers on its side? E.g.: Side A components complain that they doesn't see their peers on Side B?

Side B components complain that they doesn't see their peers on Side A?

If yes => There is a heavy IP backbone problem

c) Check in the ConfigCenter Menu Channles if new connections were established since the IP outage

If yes => Some users still can make phone calls

2. Check with the VoIP Switch Administrator how the users are affected:

a) Connect to both (*-ms-01, *-ms-02) Xymon Column "regs" and check the CPE and MTA registrations status.

b) Check the questions:

Oreclambda Check: Do drop the user's CPE registration? If yes => There is a heavy IP backbone problem some users cannot use the telephony service anymore!

- 3. Treat the Type "VoIP Switch Failure":
 - a) VoIP Switch Administrator:

In this situation the erroneous situation may be neglected. Observe if the situation remains.

- 2. Treat the Type " Occasional Failure ":
 - a) VoIP Switch Administrator:

If possible pre-bar the VoIP Switch component on this server

- b) Solve the IP or hardware issue with the failed host
- 3. Treat the Type "VoIP Switch Failure":
 - a) VoIP Switch Administrator:

Contact the "VoIP Switch Supplier Support"

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!
Maintenance Due to Operating System Alarms

The VoIP Switch Administrator and/or server service personnel find here instructions for managing problems indicated by the operating system supervision.

Maintenance Due to Supervised Processes Missing

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<host_NAME> procs "Processes not OK" <MISSING_PROCESS>

Description:

One or more supervised process of a Linux service or VoIP Switch component is missing.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

- ◊ Depends If a VoIP Switch component is missing then the VoIP Switch looses redundancy
- capability
- If a Linux service is missing the VoIP Switch may be hampered or the server is not working correctly

For the operations:

Object to Depends on the VoIP Switch components or Linux service

For the user:

Opends on the VoIP Switch components or Linux service

Solution:

Restart the VoIP Switch component or Linux service.

Action:

1. Check with the VoIP Switch Administrator if it is possible to restart the component or service without endangering the VoIP Switch telephony service.

If possible pre-bar the VoIP Switch component via the ConfigCenter!

- 2. Restart the VoIP Switch component or Linux service:
 - a) Restart the VoIP Switch component

root# <COMPONENT> restart

◊ Example:

root# servicecenter restart





◊ Example:

root# monit restart

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised IP Ports

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> ports "Ports not OK" <MISSING_PROCESS_PORTS>

Description:

One or more supervised IP port of a Linux service or VoIP Switch component is missing.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

- Obepends If a VoIP Switch component is missing then the VoIP Switch looses redundancy
- capability
 If a Linux service is missing the VoIP Switch may be hampered or the server is not working correctly

For the operations:

Obepends on the VoIP Switch components or Linux service

For the user:

Obepends on the VoIP Switch components or Linux service

Solution:

Restart the VoIP Switch component or Linux service.

Action:

1. Check with the VoIP Switch Administrator if it is possible to restart the component or service without endangering the VoIP Switch telephony service.

If possible pre-bar the VoIP Switch component via the ConfigCenter!

- 2. Restart the VoIP Switch component or Linux service:
 - a) Restart the VoIP Switch component

root# <COMPONENT> restart

◊ Example:

root# servicecenter restart



3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Hard-Disk Usage

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:



Description:

A hard-disk or hard-disk partition is full. If a hard-disk is full then the Linux operating system behaves unpredictable and the server will most probably crash.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

Observed by Depends on the VoIP Switch components running on the server

For the operations:

Observed by Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

Identify big files or directories. Delete or archive files externally.

Action:

1. Check hard-disk usage:

root# df -h

2. Find fat files:

root# ls -lahS \$(find / -type f -size +100k)

♦ Example find file sizes >60MByte:

Ob not touch big files in: /var/lib/mysql/

3. Find big directories:

root# du -hs

Example of a more specific search find directory sizes >1GByte:

```
root# du -hs /home/ratingcenter/* | grep G
root# du -hs /home/*/* | grep G
```

Or Check the following suspicious directories:



4. Prior of deleting files or directories check with the VoIP Switch Administrator if they are not needed anymore!

If you are suspicious but not sure if it is wise to delete a certain file or directory then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Memory Usage

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> memory "Memory low"

Description:

One or more processes consume a lot of memory space. If the memory becomes low the operating system Linux start to swap memory to and from hard-disk. This reduces the performance of the server.

Consequences:



This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

Observe the Order Switch Components running on the server

For the operations:

◊ None

For the user:

◊ None

Solution:

Identify which process or consumes the memory. Restart the process in order to free memory. Stop and restart the swapping on the server.

Action:

1. If a LoadBalancer *-lb-* or ServiceCenter *-sc-* server is affected:

Contact the "VoIP Switch Supplier Support"!

2. Find which processes use the memory:

◊ This is a difficult task!

root# top

3. Stop and restart the swapping:

Preconditions:

- Ohoose a day time where the server is not in high load.
- If possible pre-bar the VoIP Switch components on this server via the ConfigCenter
 Make sure that the redundant VoIP Switch component is running

a) Restart the responsible process:

root# /etc/init.d/<PROCESS_NAME> restart

b) Stop the swapping:

Oon't do this during high load! It will take some time until accomplished!

root# swapoff -a

c) Restart the swapping:

root# swapon -a

d) Check if the swap is working regularly:

root# swapon -s

Maintenance Due to Supervised CPU Load

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> cpu "Load is High"

Description:

One or more processes consume extensively CPU power. This may reduce the performance of the server.

Consequences:

Warning This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

Or Reduced performance on the affected server and VoIP Switch component

For the operations:

◊ None

For the user:

◊ None

Solution:

The CPU consuming process has to be identified. If a process is identified it has to be checked if it is a regular or erroneous situation.

If it is a regular situation then it has to be investigated if the servers computing power is still sufficient for this VoIP Switch. If the server hosts a VoIP Switch component which offers an configurable load acceptance via the ConfigCenter then it is worth a try to reduce the components workload.

An erroneous situation can mostly be solved by restarting the process.

Action:

1. Identify the responsible process:

a) Check the process situation with:

```
root# top
root# ps aux
```

b) If a process is suspicious check for multiple processes of the same name:

root# ps -aef

c) If a process is suspicious check for zombie processes (lists the zombie process id):

root# ps aux

d) Evaluate with the VoIP Switch Administrator if the suspicious process is in a regular or erroneous state.

2. Handle an erroneous Linux process state.

a)* Restart a Linux process:

root# /etc/init.d/<PROCESS_NAME> restart

```
b) Kill a process, e.g. double started process, zombie:
```

```
root# kill -9 <PROCESS_ID>
```

3. Handle a VoIP Switch component :

a) Restart an erroneous VoIP Switch component:

root# <COMPONENT_NAME> restart

b) If the VoIP components ServiceCenter or MediaServer produces high load then the VoIP Switch Administrator may reduce their accepted work load via the ConfigCenter.

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Files Missing or to Big

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:	
<host_name></host_name>	????

Description:

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ None

Solution:

Action:

1. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

VoIP System Maintenance

Best Practice for Handling a "Fraud" Situation

The Aarenet VoIP Switch Administrator finds here instructions for managing fraud problems.

1. Immediate action:

 \diamond Block call routing to the destination (usually somewhere in the Caribbean, west or central Africa) \diamond If only from one source IP address then block this IP address on the FW

2. Investigate if the fraud is due to "Direct Registrations" with correct SIP credentials on the VoIP Switch:

Ocheck if the calling number has multiple SIP registrations of a suspicious source IP range or user agent! If YES then:

The SIP credentials were not kept secret or hacked from the users CPE

Action:

- Block this user account for outgoing calls (blocking international calls is usually sufficient)
- Change the SIP credential in the user account and the user's CPE.
- Change the CPE administration login credentials
- 3. Investigate if the fraud is due to "Hacked Users CPE":
 - a) Analyze the traces of some fraud connections.

Check if the source IP remain the one of a registered user CPE! If YES then:

If yes block this user account for outgoing calls

Action:

- Block this user account for outgoing calls (blocking international calls is usually sufficient)
- Inform the user about the fraud and its reason
- Change the SIP credential in the user account and the user's CPE.
 Change the CPE administration login credentials

4. Post Work:

Output Undo the "immediate action"

In Enable the customer account when the SIP credentials and CPE administration login credentials are changed

ar:both" />

Put Back to Service a VoIP Switch Component

There are two ways to put back to service a VoIP Switch Component:

Variant 1: "Start it"

Action:

A) Start and check the component via the shell:

root# <AS_COMPONENT> start root# <AS COMPONENT> status

The consequence is that the component starts immediately its operative work.

Variant 2: "Start it gracefully"

This variant may make sense when the following VoIP Switch components shall become active but not operative immediately:

> ServiceCenter ◊ MediaServer



Action:

A) Start "passive" the component via the ConfigCenter.

```
root# <AS_COMPONENT> startpassive
root# <AS_COMPONENT> status
```

B) Make the component operative at the appropriate time:

ConfigCenter GUI Menu "System" Menu "Components"

Click the desired VoIP Switch component

Change the parameter "Acceptance" to 100 The "Acceptance" may by any value >0 according. Choose according the load balancing scheme of the component.

C) Check if the component displays activity:

ConfigCenter GUI Menu "System" Menu "Components"

Work Flow for Analyzing VoIP Switch Problems

Note Not every red alarm jeopardizes the telephony service as a whole but a bulk of yellow warnings may endanger it!

The VoIP Switch Administrator and other service personnel find here a work flow for analyzing VoIP Switch problem indications and find out the appropriate action.

The main task is to find out if:

1. The situation jeopardizes the telephony service as a whole, e.g.:

- · IP network issues
- · Several VoIP Switch servers failed or off line
- 2. The database replication is broken
 - IP network issues
 - · Server with running database failed
 - · Linux service MySQL failed
- 3. The situation hampers the operation of configuration of customer accounts, addresses etc.
 - Management server failed or off line
 VoIP Switch component ConfigCenter, AdminCenter DataAccessCenter, RatingCenter stopped working correctly

The VoIP Switch Administrator finds here the work flow for analyzing VoIP Switch problems:

Work Flow for Analyzing VoIP Switch Problems

Analysis:

1. Check if it is a **single alarm** or a **bulk alarm** situation.

a) Connect to the VoIP Switch monitor Xymon "Main View"

As a rule of thumb: It is a single error if only one issue is displayed.

2. Analyze and treat a **single alarm** situation:

a) Check the contents of the error message.

b) Compare the error description against the **Indication "Xymon Event"** ones in chapter "VoIP Switch Maintenance"

- c) Check if the actual situation is equal or similar as described and the recommended actions suitable.
- d) Execute the suitable actions.

If you are not sure contact the "VoIP Switch Supplier Support"

- 3. Analyze the **bulk alarm** situation:
 - a) Get a first overview of the situation by analyzing the Xymon Monitor :

Check in the MS-01 Xymon monitor the server, component and IP status: Xymon GUI Xymon "Main View"

xymon GUI Xymon "Main View"

- 1. Which type of server are affected?
 - At least one LoadBalancer LB server must be active that the telephony service can work!
 - At least one ServiceCenter SC server must be active that the telephony service can work!
 - At least one server with the operative database must be active that the telephony service can work!
- 2. Check the CPE registration statistic :
 - Do drop the CPE registrations?
- 3. Check the call statistic:
 - Do drop the VoIP Switch number of calls?
 - . Xymon GUI Management Server Column "calls_sys"
 - Do drop the calls on one or more ServiceCenter?
 - Xymon GUI ServiceCenter Server Column "calls_sc"
 - Do drop the calls on one or more gateways?
 - Xymon GUI Gateway Column "calls_gw"
- 4. Do the same check as above on MS-02 Xymon Monitor
- 5. Does the comparison of the two Xymon Monitor point out that:
 - The same single component on the same server failed?
 - All components of one side failed?
 - The Xymon Monitor sees only the components on its side?
 - The telephony service is running at least on one side
- b) Extend the overview by analyzing the ConfigCenter "System Component" Overview :

Check in the MS-01 ConfigCenter the status of the VoIP Switch components: ConfigCenter GUI Menu "System" Menu "Components"

- 1. Are actually calls running and new calls can be established?
- 2. Make test calls:
 - To and from a telephone number in the PSTN
 - On-net test calls
 - Call a well known VoiceMail Box from on-net and from PSTN
- 3. Is the number of running calls fast dropping and no new calls are established?
- 4. Which type of VoIP Switch components are affected?
 - At least one LoadBalancer component must be active that the telephony service can work!
 - At least one ServiceCenter component must be active that the telephony service can work!
 - At least one operative database must be active that the telephony service can work!
 - Does this picture correspond to the results of the first overview in the Xymon Monitor ?
- 5. Do the same check as above on MS-02 ConfigCenter

6. Does the comparison of the two ConfigCenter point out that:

- The same single component on the same server failed?
- ♦ All components of one side failed?
- The ConfigCenter sees only the components on its side?
- The telephony service is running at least on one side

4) Treat **bulk alarm** situations:

a) Is there a VoIP Switch server hardware, RAID or hard-disk problem?

Indications:

Indication:		
<host_name></host_name>	"snmptrapd"	"failure"
<host name=""></host>	"snmptrapd"	"degraded"

Actions:

For DELL server see: "Treating Problems of Servers from DELL Inc ®"

b) Is the IP connectivity affected to or between VoIP Switch servers?

Note	If VoIP Switch servers are affected then a lot of additional alarming messages of missing VoIP Switch components will pop up!! This can be one of the most annoying erroneous
NOLE	This can be one of the most annoying erroneous situations!

Indications:

```
Indication:
<HOST_NAME> conn "Host does not respond to ping"
<IP_ADDRESS>
* Dropping CPE registrations !
```

- Dropping calls !
- No new calls!

Actions:

See: "Maintenance Due to IP Network Alarm"

c) If you are not sure what to do then contact the "VoIP Switch Supplier Support"

VoIP Switch Server Maintenance

Maintenance Due to VoIP Switch Components General Alarms

Maintenance Due to Messages from Java Framework

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "Jdbc"

Description:

Java internal exceptions. Mostly due to database accesses which are hopefully handled by the application.

Consequences:

For the VoIP Switch telephony service:

Mostly none

For the operations:

◊ Mostly none

For the user:

◊ Mostly none

Solution:

Observe the frequency of this event

Action:

1. Observe the frequency of this event

2. If the erroneous condition is to frequent then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from VoIP Switch Components Internals

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "EventQueue" <HOST_NAME> msgs "SysCompDatabase - Cannot evalute status"

Description:

These events may happen on all VoIP Switch servers and are VoIP Switch component internal notes.

Consequences:

For the VoIP Switch telephony service:

◊ Mostly none

For the operations:

◊ Mostly none

For the user:

◊ Mostly none

Solution:

Observe the frequency of this event

Action:

1. Observe the frequency of this event

2. If the erroneous condition is to frequent then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from LoadBalancer Server

Maintenance Due to HealthCheck Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "HealthCheck"

Description:

The HealthCheck supervises the status of virtual IP addresses and their associated physical IP addresses. If the HealthCheck on one server doesn't see the peer physical IP address it takes over the virtual IP address. It most probably points out an IP network problem in the "Public Voice Segment"

Consequences:

Warning

This erroneous condition must be checked within reasonable time!

For the VoIP Switch telephony service:

◊ None if concurrently no other IP network problems arise

For the operations:

◊ None

For the user:

◊ None

Solution:

Solve the IP network if needed.

Check status the VoIP Switch component with an active-passive scheme:

◊ LoadBalancer

◊ CallBalancer
 ◊ RatingCenter

Action:

1. Check if the IP network is OK

2. Check the status of the LoadBalancer components

Confirm if the active LoadBalancer swapped, e.g. from *-lb-01 to *-lb-02

3. Check the status of the CallBalancer components

Confirm if the active CallBalancer swapped, e.g. from *-lb-01 to *-lb-02

- 4. Check the status of the RatingCenter components
- © Aarenet AG 2017

Confirm if the active CallBalancer swapped, e.g. from *-ms-01 to *-ms-02 Confirm if the active RatingCenter is processing the CDR's

5. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a LoadBalancer problem try to restart the component:

root# loadbalancer restart

c) If there is a CallBalancer problem try to restart the component:

root# callbalancer restart

d) If there is a RatingCenter problem try to restart the component:

root# ratingcenter restart

e) If the RatingCenter swapped make sure that the CDR are processed:

- ConfigCenter GUI Menu "System" Menu "Components" Click line at "active" RatingCenter -> In dialog select "Process CDRs" Click button [Close]
 The CDR CSV-Files are processed:
- 2. The CDR CSV-Files are processed:

root# cd /home/servicecenter/cdrs

Check if the CSV files have an actual time stamp which indicates that new CDRs where written:

root# ls -ltra

Open a CSV file and check for new entries, e.g.:

root# less monthly.csv

6. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to LoadBalancer Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "Balancer"

Description:

LoadBalancer internal problem that is treated internally by the component. The LoadBalancer has an "active-passive" redundancy scheme.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ None

Solution:

Not defined yet

Action:

1. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to LoadBalancer Message "Missing ServiceCenter"

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs "BalancerSwitch" <SERVICECENTER> "not available anymore"

Description:

The LoadBalancer indicates that it doesn't see a certain ServiceCenter.

This happens when:

the ServiceCenter has restarted

- the event will be transient
- the ServiceCenter is stopped
- the event will remain until the ServiceCenter is started again on IP connectivity
 - the event will remain until the IP connectivity is reestablished

Consequences:



This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

None, the other ServiceCenter take over the work load
 If a ServiceCenter is missing then the VoIP Switch looses redundancy capability

For the operations:

◊ None

For the user:

◊ None

Solution:

Solve the IP network problems if needed:

Actions see: "Maintenance Due to IP Network Alarm"

Solve the server problem if needed

Actions see: "Treating Server Hardware Problems"

Action:

1. Check if the IP network is OK

2. Check the status of the ServiceCenter components

Confirm that the reported ServiceCenter server is affected

- 3. Check the reported ServiceCenter server with the "Server Administrator (OMSA)"
- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a ServiceCenter problem try to restart the component:

root# servicecenter restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to CallBalancer Message

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs

Description:

The CallAgent dispatches MGCP messages to the CallAgent components.

The CallAgent has an "active-passive" redundancy scheme.

Consequences:

This erroneous condition must be checked within short Warning time!

For the VoIP Switch telephony service:

None

For the operations:

◊ None

For the user:

Our Users with MGCP MTA as telephone adapter may not be able to telephone

Solution:

Check status the CallBalancer active-passive scheme and if the MGCP messages are processed.

Action:

1. Check if the IP network is OK

2. Check the status of the CallBalancer components:

a) Confirm if the active CallBalancer swapped , e.g. from *-ms-01 to *-ms-02

b) Confirm if the active CallBalancer is processing the MGCP messages

Check if the CallAgent treat MGCP connections and that the total number of MGCP connections is not dropping.

3. Check if the MGCP audits are not dropping:

a) Connect to a Xymon monitor and check in Xymon Column "regs" the numbers of MGCP-Active and MGCP-Brocken

b) Check the questions:

Ob drop the number of MGCP-Active?
If yes => There may be a IP backbone problem or CallBalancer, CallAgent outage!

- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a CallBalancer problem try to restart the component:

root# callbalancer restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to MediaServer Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:



Description:

The MediaServer records or plays back announcements and VoiceMail messages. Occasionally it may not correctly record a message and transfer it to the MediaCenter or play back an announcement or message.

The MediaServer can act as media proxy for active connections and transcode media streams.

Consequences:



For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

A VoiceMail Box message or announcement couldn't correctly record or played back.
 User may not hear the other side or vica versa.

Solution:

Depends on the situation.

Action:

1. If the erroneous condition remains or happens to often then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from Management Server

Maintenance Due to AdminCenter Message "Missing FMC Application Server"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Description:

The AdminCenter tried to configure the FMC application.

Consequences:

Warning

This erroneous condition is sporadic or must be handled within reasonable time!

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A configuration on a FMC server failed

For the user:

◊ A user "an MC-Phone" is not working

Solution:

Check the state of the FMC servers and their IP connectivity toward the VoIP Switch servers.

Action:

1. Check if the IP network is OK

2. Check the status of the FMC server

3. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a FMC server problem

Contact the "VoIP Switch Supplier Support"!

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to AdminCenter Message "Missing Redirection Server"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:									
<host_< td=""><td>_NAME></td><td>msgs</td><td>"FmcProvider</td><td>_</td><td>could</td><td>not</td><td>provision</td><td>user"</td><td></td></host_<>	_NAME>	msgs	"FmcProvider	_	could	not	provision	user"	
<user< td=""><td>TELEPH</td><td>HONE N</td><td>IUMBER></td><td></td><td></td><td></td><td></td><td></td><td></td></user<>	TELEPH	HONE N	IUMBER>						

Description:

The mobile app "an MC-Phone" couldn't get the information from the associated redirection server (by default a Comdasys server located in Europe) where its responsible configuration server is located. Therefore the users "an MC-Phone" couldn't obtain its configuration and will not work.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ The mobile app "an MC-Phone" will not work

Solution:

Make sure to have good IP connectivity to the Internet

Action:

1. The user must find a reliable Internet connection and restart the app "an MC-Phone" until it gets its configuration

Maintenance Due to ConfigCenter Message "Wrong User Login"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Description:

A VoIP Switch Administrator, Operator, Supporter tried to login to the ConfigCenter with wrong credentials. The user will be blocked for several minutes.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

Or The user will be blocked from the ConfigCenter for several minutes.

For the user:

◊ None

Solution: Wait

Action:

1. Retry after a few minutes with the correct login credentials.

2. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ConfigCenter Message "DB Replication Check"

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs JdbcReplicationMonitor "Replication" '<BROKEN_REPLICATION_DIRECTION>' "is broken!"

Description:

The database replication check was not successful. This can happen from time to time when the database has to process heavy load.

In most cases the database replication recovers automatically even after several hours of failed replication. If it is not recovering then this is a severe problem and must be treated.

Consequences:

If this erroneous condition remains then this is a SEVERE erroneous condition and must be treated within Warning short time!

For the VoIP Switch telephony service:

The database redundancy is endangered

For the operations:

◊ None

For the user:

◊ None

Solution:

© Aarenet AG 2017

Restore the MySQI DB replication if the erroneous condition remains.

Action:

- 1. Check periodically (ca. every half hour) the Xymon monitor for this error condition.
- 2. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to DataAccessCenter Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "Jdbc" "SQL-Exception during statement"

Description:

A configuration via the DataAccessCenter may have failed.

This may happen if the database is under heavy load.

Consequences:

Warning

This erroneous condition must be checked within reasonable time!

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A customer configuration may have failed (which is hopefully covered by the CRM application).

For the user:

◊ None

Solution:

Inter-working between the DataAccessCenter and database must be optimized.

Action:

1. If this Java event is logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to RatingCenter Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs

Description:

The RatingCenter has an "active-passive" scheme. Every RatingCenter event has to be checked if the active RatingCenter is working correctly and is processing the CDRs.

Consequences:



For the VoIP Switch telephony service:

◊ None

For the operations:

A CDR may be not written correctly into the CDR database and/or CSV files.
 The customer billing contains not all CDR

For the user:

◊ None

Solution:

Check status the RatingCenter active-passive scheme and if the CDR are processed.

Action:

1. Check the status of the RatingCenter component

Confirm if the active RatingCenter is processing the CDR's

2. Treat the problem:

a) If the RatingCenter swapped make sure that the CDR are processed:

Open the ConfigCenter Menu "Components"

Click line at "active" RatingCenter -> In dialog select "Process CDRs"

Click button [Close]

b) Check if the CDR CSV-Files are processed:

Open the CDR directory:

root# cd /home/ratingcenter/cdrs

Check if the CSV files have an actual time stamp which indicates that new CDRs where written:

root# ls -ltra

Open a CSV file and check for new entries, e.g.:

root# less monthly.csv

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from ServiceCenter Server

Maintenance Due to FaxServer Message

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs

Description:

Fax may not received correctly. The mailing of the PDF file may fail.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

A received Fax may not be correctly received and transferred to the user. This situation is usually handled by the Fax device either automatically or manually.

Solution:

Restart the FaxServer component.

Action:

1. Check if no Fax at all are received.

Send test fax.

2. Restart the FaxServer:

root# faxserver restart

3. If the FaxServer logs subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to MediaCenter Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs MediaCenterCall <HOST_NAME> msgs MediaServer <HOST_NAME> msgs "file not found"

Description:

The MediaCenter handles the WAV files from announcements and VoiceMail messages. Occasionally it may not correctly record a message, loose a message file. Also an order to the MediaServer may fail to replay a message or announcement.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ A VoiceMail Box message or announcement couldn't correctly recorded or played back

Solution:

Clean up the VioceMail message date base.

Optimize the inter-working of MediaCenter and MediaServer

Action:

1. If those events are logged subsequently then rapport it to the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msgs

Description:

The ServiceCenter is the main component of the VoIP Switch. It computes the connections signaling and telephony features.

The ServiceCenter has an all active redundancy scheme. If one ServiceCenter fails the remaining ServiceCenter take over the work load.

Consequences:

Warning This erroneous condition must be checked and treated within short time!

For the VoIP Switch telephony service:

◊ As long one ServiceCenter remains the VoIP Switch works!

For the operations:

◊ None

For the user:

◊ None

Solution:

Depends on the analyzed problem.

Action:

1. Check how acute the problem is:

- a) Check if the IP network is OK
- b) Check the status of the ServiceCenter component

Are enough ServiceCenter active that the work load can be treated? If NO then there is a most SEVERE erroneous situation

c) Check in the ConfigCenter Menu "Components" if the active ServiceCenter is processing the connections:

 Do drop the total number of connections?
 If YES then there is a most SEVERE erroneous situation: There may be a IP backbone problem!

d) Check in the Xymon Column "regs" the number of registered SIP-Devices:

 O drop the number of SIP-Devices?
 If YES then there is a most SEVERE erroneous situation: There may be a IP backbone problem!

e) Check the reported ServiceCenter server with the "Server Administrator (OMSA)"

◊ Are problems signaled?

2. Treat the problem:

a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a ServiceCenter problem try to restart the component:

root# servicecenter restart

c) If there is a hardware problem: Actions see: "Treating Server Hardware Problems"

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "License Violation"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:



Description:

This ServiceCenter has a license problem and will work only for the remaining grace period.

Consequences:

Warning This erroneous condition must be checked and treated within the remaining grace period!

For the VoIP Switch telephony service:

◊ As long one ServiceCenter remains the VOIP Switch works

◊ The telephony service will be stopped on this ServiceCenter after passing of the grace period

For the operations:

◊ None

For the user:

◊ None

Solution:

Get actual licenses from the VoIP Switch Supplier.

Action:

1. Check in the ConfigCenter Menu "Components" which ServiceCenter component has a license problem and how long the grace period is.

2. Contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "Failed Emergency Call"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

```
Indication:
<HOST_NAME> msgs ServicePrioCallControl "Could not establish
priority-call". Call from
Connection/SIP_CALL_ID>/<CALLING_NUMBER> to
<CALLED_EMERGENCY_NUMBER>
```

Description:

A user's emergency call failed!

Consequences:

WarningSevere legal condition that must be handled!This case can have legal consequences for the provider!

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

The emergency call did not work

Solution:

Check if the call routing failed due to a VoIP Switch emergency call treating or routing. If yes fix them.

Check if the PSTN provider did reject the emergency call. If yes contact the PSTN provider.

Action:

1. Archive traces for legal responsibilities:

Save the trace of this emergency call and all subsequent calls from this user toward emergency numbers

- 2. Check where the call was rejected.
 - If the call was rejected at the PSTN provider side contact the PSTN provider and let investigate into this case.
- 3. Check the VoIP Switch's emergency routing:
 - Emergency numbers
 - Emergency number rewriter
 - Routing Tables toward the PSTN
 - RuleSet that may tag outgoing calls toward emergency numbers
- 4. Check if any IP network devices may interfere with the SIP signaling:
 - ◊ If there are external Session Board Controller SBC or SIP-SS7 Gateway involved check their
 - behavior concerning the emergency calls
 - If a firewall FW is involved check that no SIP ALG or "SIP Helpers" are active
- 5. Treat the problem:
 - a) Adjust the emergency routing of the VoIP Switch if needed
 - b) Fix the IP network devices if needed
- 6. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to ServiceCenter Message "TopStop"

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

```
Indication:
<HOST_NAME> msgs ServiceRatingControl (01) <CALLING_NUMBER>
"max available charges reached for account:"
<HOST_NAME> msgs AlarmLogger "[TOPSTOP][ALARM] tenant"
<TENANT> "topstop limit nearly reached for account"
```

Description: A user's TopStop limit was reached!



Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ A TopStop alarm early in the month indicates a possible fraud case

For the user:

◊ No outgoing calls except emergency call will work when the TopStop limit is reached

Solution:

If it is a regular TopStop then contact the user and enhance the monthly TopStop limit.

If it is a fraud situation handle according "Best Practice: Fraud"

Action:

1. Check if it is a regular TopStop situation.

2. Check if it is a possible fraud case:

- ◊ Reached TopStop limit early in the month?
- ◊ Concurrently a lot of TopStop limits reached?
 ◊ High call peak during the night or weekend? Check at Xymon Column " calls_sys " .
- 3. Treat according "Best Practice for "Fraud Situation"

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Nimbus Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> msgs "NimbusLink (ue) Cannot subscribe"

Description:

The Nimbus component is a VoIP Switch internal bus that connects the various VoIP Switch components on the servers. If a Nimbus endpoint on one server is missing the other Nimbus endpoints start to complain.

If a Nimbus endpoint is missing then the component may be stopped, the server not on line or an IP network problem.

This error is often displayed during VoIP Switch software upgrades of the servers. In this situation just wait until the upgrade is finished.

Consequences:



For the VoIP Switch telephony service:

◊ Usually none

For the operations:

◊ None

For the user:

◊ None

Solution:

Solve the IP network problems or server problems if needed.

Action:

1. Check if the IP network is OK

- 2. Check the status of the VoIP Switch components located on the server where the Nimbus is missing: Is only Nimbus missing or other components to on this server?
- 3. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is not a planned outage then try to solve the server problem

c) If there is not a planned outage then try to restart the Nimbus on this server:

root# nimbus restart

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from CallAgent Server

Maintenance Due to CallAgent Message

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> msqs

Description:

The CallAgent treats the message exchange with the MGCP MTA. The CallAgent has an all active redundancy scheme. If one CallAgent fails the remaining CallAgent take over the work load.

Consequences:

Warning This erroneous condition must be checked within short time!

For the VoIP Switch telephony service:

Ore As long one CallAgent remains the VOIP Switch works

For the operations:

◊ None

For the user:

Single MGCP MTA at the user's premises is not working correctly. The telephone service may not always work for this users.

Solution:

Depends on the analyzed problem.

Action:

- 1. Check if the IP network is OK
- 2. Check the status of the CallAgent components

Confirm that the reported CallAgent server is affected

- 3. Check the reported CallAgent server with the "Server Administrator (OMSA)"
- 4. Treat the problem:
 - a) If there are IP network problems

Actions see: "Maintenance Due to IP Network Alarm"

b) If there is a CallAgent problem try to restart the component:

root# callagent restart

5. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Messages from CPECenter Server

Maintenance Due to CpeCenterMessage

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:



Description:

During the preparation of a device configuration file two device configuration templates were found. If a CPE loads a device configuration file which was produced under these conditions it may not work correctly.

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

Or The CPE may not work with the produced configuration file

Solution:

One device configuration template has to be deleted.

Action:

1. Contact the "VoIP Switch Supplier Support"!

Maintenance Due to IP Network Alarms

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> conn "Host does not respond to ping" <IP_ADDRESS>

Description:

This test performs a "ping" toward the IP address of the host. If the "ping" is not answered then there is a problem with the IP network, e.g.:

- Index Pinged host defect or off line
- Layer2 IP Switch defect or off line
 Brocken IP backbone network

Consequences:

MOST SEVERE condition if several VoIP Switch server Warning are affected for a longer duration (ca 15min)!

For the VoIP Switch telephony service:

Or The telephone service may be interrupted

For the operations:

O The MySQL databases may loose their replication

For the user:

◊ The telephone service may be interrupted for the users!

Solution:

Solve the IP network problems!

Check the IP network devices:

- Index Pinded host
- ◊ Layer 2 IP switches
- ◊ IP Routes
- ◊ Firewalls

Check the VoIP Switch server IP connectivity.

Action:

1. Evaluate the severity of the IP network outage:

a) Check if it is a occasional ping failure:

- Only one host doesn't respond
- Only 1 or 2 poll cycle fail
 - Type "Occasional Failure":
- In this situation the erroneous situation may be neglected.

b) Check if it is only a single host:

- One host doesn't respond anymore
 - Type "Host Failure":

 - Check the hardware condition and IP connectivity of this device
 Check with the VoIP Switch Administrator in the ConfigCenter Menu "Components" how the VoIP Switch is affected

- c) Check if more than one VoIP Switch server is affected:
 - More than one VoIP Switch server don't respond anymore
 - Type "VoIP Switch Failure": 1. Check with the VoIP Switch Administrator how the VoIP Switch is affected:
 - a) Connect to both (*-ms-01, *-ms-02) ConfigCenter Menu "Components" and check the component status
 - b) Check the questions:
 - ◊ Which VoIP Switch servers are not visible?
 - ◊ Are they the same on both ConfigCenter?
 - Object to Does one ConfigCenter see only the servers on its side? E.g.: Side A components complain that they doesn't see their peers on Side B?
 - Side B components complain that they doesn't see their peers on Side A?
 - If yes => There is a heavy IP backbone problem

c) Check in the ConfigCenter Menu Channles if new connections were established since the IP outage

If yes => Some users still can make phone calls

2. Check with the VoIP Switch Administrator how the users are affected:

a) Connect to both (*-ms-01, *-ms-02) Xymon Column "regs" and check the CPE and MTA registrations status.

b) Check the questions:

Output Check: Do drop the user's CPE registration? If yes => There is a heavy IP backbone problem some users cannot use the telephony service anymore!

- 3. Treat the Type "VoIP Switch Failure":
 - a) VoIP Switch Administrator:

In this situation the erroneous situation may be neglected. Observe if the situation remains.

- 2. Treat the Type " Occasional Failure ":
 - a) VoIP Switch Administrator:

If possible pre-bar the VoIP Switch component on this server

- b) Solve the IP or hardware issue with the failed host
- 3. Treat the Type "VoIP Switch Failure":
 - a) VoIP Switch Administrator:

Contact the "VoIP Switch Supplier Support"

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Operating System Alarms

The VoIP Switch Administrator and/or server service personnel find here instructions for managing problems indicated by the operating system supervision.

Maintenance Due to Supervised Processes Missing

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<host_NAME> procs "Processes not OK" <MISSING_PROCESS>

Description:

One or more supervised process of a Linux service or VoIP Switch component is missing.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

- ◊ Depends If a VoIP Switch component is missing then the VoIP Switch looses redundancy
- capability
 If a Linux service is missing the VoIP Switch may be hampered or the server is not working correctly

For the operations:

Opends on the VoIP Switch components or Linux service

For the user:

Object to Depends on the VoIP Switch components or Linux service

Solution:

Restart the VoIP Switch component or Linux service.

Action:

1. Check with the VoIP Switch Administrator if it is possible to restart the component or service without endangering the VoIP Switch telephony service.

If possible pre-bar the VoIP Switch component via the ConfigCenter!

- 2. Restart the VoIP Switch component or Linux service:
 - a) Restart the VoIP Switch component

root# <COMPONENT> restart

◊ Example:

root# servicecenter restart

b) Restart the service:

root# /etc/init.d/<SERVICE> restart

◊ Example:

```
root# monit restart
```

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised IP Ports

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> ports "Ports not OK" <MISSING_PROCESS_PORTS>

Description:

One or more supervised IP port of a Linux service or VoIP Switch component is missing.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

- Object Depends If a VoIP Switch component is missing then the VoIP Switch looses redundancy capability
- If a Linux service is missing the VoIP Switch may be hampered or the server is not working correctly

For the operations:

Object to Depends on the VoIP Switch components or Linux service

For the user:

Obepends on the VoIP Switch components or Linux service

Solution:

Restart the VoIP Switch component or Linux service.

Action:

1. Check with the VoIP Switch Administrator if it is possible to restart the component or service without endangering the VoIP Switch telephony service.

If possible pre-bar the VoIP Switch component via the ConfigCenter!

2. Restart the VoIP Switch component or Linux service:

a) Restart the VoIP Switch component

root# <COMPONENT> restart

◊ Example:

root# servicecenter restart

b) Restart the service:

```
root# /etc/init.d/<SERVICE> restart
```

◊ Example:

3. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Hard-Disk Usage

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> disk "File systems not OK"

Description:

A hard-disk or hard-disk partition is full. If a hard-disk is full then the Linux operating system behaves unpredictable and the server will most probably crash.

Consequences:

Warning SEVERE erroneous condition that must be handled!

For the VoIP Switch telephony service:

Observed by Depends on the VoIP Switch components running on the server

For the operations:

Observed by Depends on the VoIP Switch components running on the server

For the user:

Object to Depends on the VoIP Switch components running on the server

Solution:

Identify big files or directories. Delete or archive files externally.

Action:

1. Check hard-disk usage:

root# df -h

2. Find fat files:

root# ls -lahS \$(find / -type f -size +100k)

◊ Example find file sizes >60MByte:

root# ls -lahS \$(find /opt/backup/ -type f -size +60000k)

On not touch big files in: /var/lib/mysql/

3. Find big directories:

root# du -hs

Example of a more specific search find directory sizes >1GByte:

```
root# du -hs /home/ratingcenter/* | grep G
root# du -hs /home/*/* | grep G
```

Or Check the following suspicious directories:

/opt/backup/ /home/mediacenter/messages //home/ratingcenter/cdrs

4. Prior of deleting files or directories check with the VoIP Switch Administrator if they are not needed anymore!

If you are suspicious but not sure if it is wise to delete a certain file or directory then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Memory Usage

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> memory "Memory low"

Description:

One or more processes consume a lot of memory space. If the memory becomes low the operating system Linux start to swap memory to and from hard-disk. This reduces the performance of the server.

Consequences:

Warning This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

Observed by Depends on the VoIP Switch components running on the server

For the operations:

◊ None

For the user:

◊ None

Solution:

Identify which process or consumes the memory. Restart the process in order to free memory. Stop and restart the swapping on the server.

Action:

1. If a LoadBalancer *-lb-* or ServiceCenter *-sc-* server is affected:
2. Find which processes use the memory:

♦ This is a difficult task!

root# top

3. Stop and restart the swapping:

Preconditions:

- O Choose a day time where the server is not in high load.
- If possible pre-bar the VoIP Switch components on this server via the ConfigCenter
- O Make sure that the redundant VoIP Switch component is running

a) Restart the responsible process:

root# /etc/init.d/<PROCESS_NAME> restart

b) Stop the swapping:

Oon't do this during high load!
 It will take some time until accomplished!

root# swapoff -a

c) Restart the swapping:

root# swapon -a

d) Check if the swap is working regularly:

root# swapon -s

Maintenance Due to Supervised CPU Load

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> cpu "Load is High"

Description:

One or more processes consume extensively CPU power. This may reduce the performance of the server.

Consequences:

Warning This erroneous condition must be handled within reasonable time!

For the VoIP Switch telephony service:

◊ Reduced performance on the affected server and VoIP Switch component

For the operations:

◊ None

For the user:

◊ None

Solution:

The CPU consuming process has to be identified. If a process is identified it has to be checked if it is a regular or erroneous situation.

If it is a regular situation then it has to be investigated if the servers computing power is still sufficient for this VoIP Switch. If the server hosts a VoIP Switch component which offers an configurable load acceptance via the ConfigCenter then it is worth a try to reduce the components workload.

An erroneous situation can mostly be solved by restarting the process.

Action:

1. Identify the responsible process:

a) Check the process situation with:

root# top root# ps aux

b) If a process is suspicious check for multiple processes of the same name:

root# ps -aef

c) If a process is suspicious check for zombie processes (lists the zombie process id):

root# ps aux

d) Evaluate with the VoIP Switch Administrator if the suspicious process is in a regular or erroneous state.

2. Handle an erroneous Linux process state.

a)* Restart a Linux process:

root# /etc/init.d/<PROCESS_NAME> restart

b) Kill a process, e.g. double started process, zombie:

root# kill -9 <PROCESS_ID>

3. Handle a VoIP Switch component :

a) Restart an erroneous VoIP Switch component:

root# <COMPONENT_NAME> restart

b) If the VoIP components ServiceCenter or MediaServer produces high load then the VoIP Switch Administrator may reduce their accepted work load via the ConfigCenter.

4. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

Maintenance Due to Supervised Files Missing or to Big

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> ????

Description:

Consequences:

For the VoIP Switch telephony service:

◊ None

For the operations:

◊ None

For the user:

◊ None

Solution:

Action:

1. If the erroneous condition remains then contact the "VoIP Switch Supplier Support"!

VoIP System Maintenance

Best Practice for Handling a "Fraud" Situation

The Aarenet VoIP Switch Administrator finds here instructions for managing fraud problems.

1. Immediate action:

Block call routing to the destination (usually somewhere in the Caribbean, west or central Africa)
 If only from one source IP address then block this IP address on the FW

- 2. Investigate if the fraud is due to "Direct Registrations" with correct SIP credentials on the VoIP Switch:
 - Ocheck if the calling number has multiple SIP registrations of a suspicious source IP range or user agent! If YES then:
 - The SIP credentials were not kept secret or hacked from the users CPE

Action:

- Block this user account for outgoing calls (blocking international calls is usually sufficient)
- Change the SIP credential in the user account and the user's CPE.
 Change the CPE administration login credentials
- 3. Investigate if the fraud is due to "Hacked Users CPE":
 - a) Analyze the traces of some fraud connections.

Check if the source IP remain the one of a registered user CPE!

If YES then:

If yes block this user account for outgoing calls

Action:

- Block this user account for outgoing calls (blocking international calls is usually sufficient)
- Inform the user about the fraud and its reason
 Change the SIP credential in the user account and the user's CPE.
 Change the CPE administration login credentials

4. Post Work:

Output Undo the "immediate action"

In Enable the customer account when the SIP credentials and CPE administration login credentials are changed

-->

Guide for the Maintenance and Problem Solving for Servers from DELL Inc $\ensuremath{\mathbb{B}}$

Best Practice When a Hardware HW Problem is Indicated

It is assumed that from any source a hardware problem of a server is indicated, e.g.:

- ♦ Monitor Log
- ♦ Alerting email
 ♦ SMTP trap
- ♦ system engineer observation
- ♦ etc

	 Access the server's "OpenManage Server Administrator (OMSA)" GUI → Show me how Check the server's hardware problem → Show me how 	
Best Practice	 3. Prepare documentation for a ticket at the DELL support: Description of the problem Get the servers Service Tag → Show me how Get the server log → Show me how 	
	 4. Organize the hardware part replacement if needed → Show me how 5. Treat the hardware problem: Replace the defect hardware part → Show me how Replace the defect hard-disk → Show me how 	
	Show me how	

Server Monitoring

Manual Server Monitoring With DELL's "Server Administrator (OMSA)"

DELL OpenManage Server Administrator (OMSA) is a software agent that provides a comprehensive, one-to-one systems management solution in two ways: from an integrated, Web browser-based graphical user interface (GUI) and from a command line interface (CLI) through the operating system.

Note In this chapter enough information is given for being dangerous! If there are uncertainties contact the "DELL Support" or the "VoIP Switch Supplier Support".

Access the "OpenManage Server Administrator (OMSA)"

Connect with any Web browser to the server's "OpenManage Server Administrator (OMSA)" GUI:

- 1. Insert the following URI: https://<IP_ADDRESS>:1311 Example: https://172_100_100_100:13
- https://172.100.100.100:1311 2. Insert the user "root" login credentials:
 - ♦ Username: root
 - Password: the server root password

Check the Type of Server and Service Tags

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Check the server type:

or

In the OMSA home page menu bar at the top the server type is listed, e.g.: "PowerEdge620"

◊ Menu "System" Tab "Properties" Tab "Summary"

Check the Service Tag:

Menu "System" Tab "Properties" Tab "Summary"
 In frame "Main System Chassis" the Service Tag is displayed, e.g.: 47x....
 In frame "Main System Chassis" the "Express Service Code" is displayed, e.g.: 9187....

Check the Server's Hardware Status

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Check the Server's Hardware Status:

Menu "System" Tab "Properties" Tab "Health"

◊ Click "Main System Chassis"

The status of all server hardware components is displayed and can be checked in detail.

Check the Server's and RAID and Hard-Disk HD Status

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Check the RAID Controller Type:

Menu "System" Tab "Properties" Tab "Health"
 Click "Storage"
 In frame "RAID Controller(s)" the RAID controller type is displayed, e.g. : "PERC 6/i integrated"

Check the RAID Controller Status:

 Menu "System" Tab "Properties" Tab "Health"
 Click "Storage" In frame "RAID Controller(s)" the name and status of the RAID is displayed: "Virtual Disk 0 RAID-1"

Check the Hard-Disk HD Replication Status

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Check the Hard-Disk HD Status: You have to dig in via the left navigation tree:

```
◊ Menu "Storage" Menu "PERC ... " Menu "Connector ... " Menu "Enclosure ... "
                                                                                 Menu
 "Physical Disks ..."
 Check the disk state: Column "State"
```

States:

♦ Online:

• The disk is online and productive working in the RAID. The replication is working.

◊ Ready:

• The disk is ready for integration into a RAID. The replication is not active.

◊ Rebuilding:

• The disc is currently integrated into the RAID. The progress is displayed in %.

If there is an indication of a hard-disk replication problematic then check in chapter "Treating RAID and Hard-Disk Problems" about further maintenance actions.

Get the Server's Log Data

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Get the OMSA log:

- Menu "System" Tab "Logs"
- Save the "Embedded System Management (ESM) Log" on the server: Click "Save AS" and follow the instructions
 Copy the saved EMS Log file to the support directory of the case

Server Monitoring by Xymon

The VoIP Switch default monitor Xymon is described in "VoIP Switch Monitoring"

Indication of a Server Hardware Defect

Indication "Xymon Event":

Monitor Log, Émail or SMTP Trap may contain the following information:

Indication: <HOST_NAME> "snmptrapd" "failure"

Description:

© Aarenet AG 2017

The server indicates any hardware failure:

- ◊ Failed power module
- ◊ Failed main board
- ♦ Failed RAID controller
- Failed hard-disk
 Any other hardware problem

Consequences:

Warning It may be a SEVERE server condition that must be immediately investigated and treated!

For the VoIP Switch telephony service:

Observed by Depends on the VoIP Switch components running on the server

For the operations:

Observed by Depends on the VoIP Switch components running on the server

For the user:

◊ Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" Direct at DELL support
 - Contact the "VolP Switch Supplier Support"
- 3. Repair the server:

or

- · Default processing of hardware problems that forces to shutdown the server, e.g.:
 - ♦ Fix main board
 - Fix RAID controller
 - Fix or wear out batteries
 - ♦ Fix fan
 - Fix RAM modules
- · Processing of hardware problems that can be done hot, e.g.:
 - Fix power module
 - Fix hard-disk

Indication of a Server Hard-Disk or RAID Controller Problem

Indication "Xymon Event":

Monitor Log, Email or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> "snmptrapd" "degraded"

Description:

The server indicates a problem with the virtual disk:

- ◊ Failed RAID controller
- ◊ Failed hard-disk
- Failed hard-disk replication

Consequences:

For the VoIP Switch telephony service:

Observe Depends on the VoIP Switch components running on the server

For the operations:

Observed by Depends on the VoIP Switch components running on the server

For the user:

Observe Depends on the VoIP Switch components running on the server

Solution: The RAID controller must be repaired or a hard-disk exchanged.

Action:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" · Direct at DELL support
 - Contact the "VolP Switch Supplier Support"
- Repair the server:
 - · Default processing of hardware problems that forces to shutdown the server, e.g.: Fix RAID controller

or

- Processing of hardware problems that can be done hot, e.g.:
 - Fix hard-disk
 - Fix hard-disk replication

Procedure for Replacing Defect HW Parts with DELL

The procedure for exchanging defect hardware HW of DELL servers' is different from country to country and may also change from time to time.

The following basic procedure for HW exchange seems more or less stable:

- 1. Detect the HW problem
- 2. Make sure to have ready the DELL server details:
- Server Type
 Service-Tag number or the "ExpressService Code"
 - Check the guaranty time of the server
- 3. Report DELL support
- DELL will analyze the case and order more information if needed
 DELL will organize and send the exchange part
- 5. The VoIP Switch Administrator has to organize the replacing of the part
 - Usually this has to be done within 1 3 working days
- 6. The VoIP Switch Administrator has to make ready the defect part for returning it to DELL
 - Do not dispose the defect part!
 - Either the defect part will be picked up at the location or it has to be send back to DELL.

Treating Server Hardware Problems

The VoIP Switch Administrator and/or server service personnel find here instructions for managing HW defects.

Default Process for Fixing Hardware Problems

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
 - RAID degraded
 - Host does not respond to ping
 - Ports not OK
 - Processes not OK

O The provider's system monitoring indicates no access to the server

- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition
- ◊ Server Console: The server doesn't respond to console input

Description: Any hardware problem. Most probably:

- Oefect main board
- Of Defect RAID controller
- Of Defect or wear out batteries
- Oefect fan
- Of Defect power module

Note	The telephony service for the customers is not endangered as long only one server fails! It becomes disastrous if the two LoadBalancer servers or all ServiceCenter servers are not working anymore.
------	---

Consequences:

It may be a SEVERE server condition that must be Warning immediately investigated and treated!

For the VoIP Switch telephony service:

- Object to Depends on the VoIP Switch components running on the server
- ◊ If a ServiceCenter server fails the capability of concurrent connection handling may decline.

For the operations:

Observed Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier"

 - Direct at DELL support
 Contact the "VoIP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- Stop provider alarming
- 3. Graceful pre-bar the VoIP Switch component

Repair the server:

If the main board or RAID controller had to be replaced then follow these special instructions:

Fix main board ◊ Fix RAID controller

If the power-module or hard-disk have to be replaced, see:

◊ Fix power module
 ◊ Fix hard-disk

	For the following actions the server casing has to be opened!	
Warning	The effects of EMC must be considered and the appropriate precautions must be taken to prevent further hard ware damage.	

- 1. Shut down and power off the server if the part has to be replaced on the main board
- 2. Repair the server Follow the server manufacturer's instructions!

Put back the server to normal working state:

- 1. Start the server (if needed):
 - This automatically starts the VoIP Switch components!
- 2. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check in the ConfigCenter if all VoIP Switch components on the sever are ok: ConfigCenter GUI Menu "System" Menu "Components"

 - 3. Check if the Xymon monitor doesn't show any error

If the VoIP Switch doesn't get back to normal telephony service operation:

- Investigate what is wrong and solve it
 Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Fix Defect Main Board or RAID Controller

See section "Default Process for Fixing Hardware Problems" for the general description of the problem.

Actions:

Repair the server:

- 1. Shut down and power off the server if the part has to be replaced on the main board
- 2. Repair the server hardware Follow the server manufacturer's instructions
- 3. Connect a VGA monitor to the console port of the server

If the RAID controller was repaired then there will be still a RAID problem continue at "Default Process for Fixing RAID Problems", Case 2

If the main board was repaired continue here:

1. Insert the original hard-disk 1 in bay 0 (do not insert the hard-disk 2 yet)

Put back the server to normal working state:

- 1. Power on and start the server
 - This automatically starts the VoIP Switch components!
- 2. Checks:
 - 1. Check the console output on the VGA monitor if any exceptions are displayed during the BIOS booting

If the booting stucks during virtual hard disk initialization (RAID controller) then check the replication issues . 2. Check the server status with "Server Administrator (OMSA)"

- 3. Check in the ConfigCenter if all VoIP Switch components on the sever are ok:
- Menu "System" ConfigCenter GUI Menu "Components"
- 4. Check if the Xymon monitor doesn't show any error:
 - After a certain time all supervised objects should get green except the missing hard-disk 2

If the VoIP Switch doesn't get back to normal telephony service operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

When the server and the telephony service are working correctly again then:

- Insert the original hard-disk 2 in bay 1
 - Check with "Server Administrator (OMSA)" if the RAID controller started automatically the hard disk replication if not then restart the replication manually

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Fix Defect Power Module

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition

Description:

Defect power module

Consequences:

This erroneous condition must be checked and treated Note within reasonable time!

For the VoIP Switch telephony service:

- No immediate consequences
- O The server is running just with one power module

For the operations:

For the user:

No immediate consequences

Solution:

The power module must be replaced

Actions:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" Direct at DELL support
 - · Contact the "VolP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- 2. Stop provider alarming

Replace the power module:

- 1. Remove the defect power module (hot plug out possible)
- 2. Insert the new power module (hot plug in possible)
- 3. Connect the power cord

Put back the server to normal working state:

- 1. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check if the Xymon monitor doesn't show any error

If the server doesn't go back to normal operation:

- Investigate what is wrong and solve it
 Contact the "VoIP Switch Supplier Support" for helping recovering the server

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Treating RAID and Hard-Disk Problems

All servers of the VoIP Switch run a RAID type 1 which mirrors the contents of the two installed hard-disks. The "RAID controller" manages the replication between the two hard-disks.

Several conditions may interrupt the hard-disk replication and/or degrade the RAID virtual disk:

- Main board defect
- AID controller defect
- Ard-disk defect

The consequences are that the server is not running at all or only with one hard-disk. The good news is as long one hard-disk is running the server will work as expected.

Fix Defect Hard Disk

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
 - RAID degraded
- Server Administrator (OMSA): Displays the error condition
- ◊ Server Display: The server front display is yellow and indicates the error condition

Description:

Defect hard-disk

Consequences:

Note This erroneous condition must be checked and treated within reasonable time!

For the VoIP Switch telephony service:

No immediate consequences
 The server is running just with one hard-disk

For the operations:

No immediate consequences

For the user:

◊ No immediate consequences

Solution: The hard-disk must be replaced

Actions:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" Direct at DELL support
 - Contact the "VoIP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- 2. Stop provider alarming

Replace the hard-disk:

- 1. Remove the defect hard-disk (hot plug out possible)
- 2. Insert the new hard-disk (hot plug in possible):
 - If the hard-disk is brand-new the replication starts immediately

If the hard-disk was already used then the replication may not start automatically then check the instructions at " Default Process for Fixing RAID Problems", Case 1.

Put back the server to normal working state:

- 1. Checks:
 - 1. Check if the hard-disk replication is in progress
 - Check the server status with "Server Administrator (OMSA)"
 Check if the Xymon monitor doesn't show any error

If the server doesn't go back to normal operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the hard-disk replication

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Default Process for Fixing RAID Problems

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
 - RAID degraded
- O The provider's system monitoring may indicate no access to the server
- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition
- ◊ Server Console: The server may not respond to console input

Description:

Any hardware problem. Most probably:

> Of Defect RAID controller Oefect hard-disk

Consequences:

It may be a SEVERE server condition that must be Warning immediately investigated and treated!

For the VoIP Switch telephony service:

- Observe Depends on the VoIP Switch components running on the server
- ◊ If a ServiceCenter server fails the capability of concurrent connection handling may decline.

For the operations:

Observed Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

A) Analyze the degrade situation and organize spare parts:

© Aarenet AG 2017

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Check the VoIP Switch documentation for the server type and used RAID controller
- 3. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier"
 - Direct at DELL support
 - · Contact the "VoIP Switch Supplier Support"
- B) Treat the VoIP Switch operation if the defect stops the proper server functionality :
 - 1. Disable Xymon Alarming
 - Stop provider alarming
 - support_switch#supportSwitchPreBar Graceful pre-bar the VoIP Switch component

C) Evaluate the repair case for DELL RAID controller type: PERC5 / PERC 6 / H310 Mini / H320 Mini / H330 Mini:

Case 1: "One Hard-Disk Defect"

Precondition:

- · Main board is ok
- RAID controller is ok
- 1 operative hard-disk is ok
- Server is still operative within the VoIP Switch
- The replacement hard-disk has the same form factor and size of bytes

To-Do:

- 1. Remove the defect hard-disk (hot plug-out is no problem)
- 2. Insert the new hard-disk (hot plug-in is no problem) either:
 - a brand-new hard-disk
 - an already used spare hard-disk
- 3. Check the hard-disk replication status
 - If the replication did not start automatically then start the replication manually !

Case 2: "Main Board or RAID Controller Defect:

Precondition:

- The main board RAID controller are repaired according description above
- 2 operative hard-disks are ok
- Server is shut down
- Disconnect all Ethernet patch cables from the server GB ports.
- Connect a VGA monitor and USB keyboard and mouse tot the console port of the server

To-Do:

- 1. Insert the original hard-disk 1 in bay 0 (do not insert the hard-disk 2 yet)
- 2. Power up the server
- 3. Check the console output on the VGA monitor:

During the BIOS startup the following message may be displayed:

Foreign configuration(n) found on adapter. Press any key ? or 'F' to import foreign configuration and continue.

- 4. If requested press key F on the keyboard!
 - Note:

If you miss to press F then restart the BIOS booting by pressing the keys [Ctrl Alt Delete] else the server booting stops after the BIOS start up.

Check the console output on the VGA monitor: A security question may be displayed which enables you to stop the procedure:

All of the disk from your previous configuration are gone. If this is an unexpected message ...

- 6. Do not press any key!
 - Note:

If no key is pressed then the RAID controller takes over the hard-disk as part of its new virtual disk.

Wait until the server has booted!

7. Insert the original hard-disk 2 in bay 1

8. Check the hard-disk replication status

Note:

It is very probable that the replication did not start automatically! Then:

At Menu "Storage" a yellow warning triangle is displayed Upon click on "Storage" the status is displayed: Virtual Disk 0: degraded

If the replication did not start automatically then start the replication manually !

For all other cases:

- Ocontact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality
- C) Put back the server to normal working state:
 - 1. If needed connect all Ethernet patch cables to the correct server GB ports
 - 2. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check in the ConfigCenter if all VoIP Switch components on the sever are ok: ConfigCenter GUI Menu "System" Menu "Components"
 - Menu "Components'
 - 3. Check if the Xymon monitor doesn't show any error

D) If the VoIP Switch doesn't get back to normal telephony service operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

E) Enable the alarming again:

1. Enable Xymon Alarming

2. Start provider alarming

Manually Restart the Hard-Disk Replication

In this situation the RAID's virtual disk is in state degraded (only one hard-disk is operative, but two are expected). The RAID controller will automatically grab a free "hot spare" hard-disk and associate it with its degraded virtual disk and start the replication.

Restart the hard-disk replication manually:

- 1. Connect with any Web browser to the server's "Server Administrator (OMSA)" GUI: Login as user "root"
- 2. From the inserted 2nd hard-disk the foreign RAID configuration has to be deleted:

Select at [Available Task]: "Clear Foreign Configuration" Menu "Storage" Click button [Execute] <tt> <tt> Confirm the security check click button [Clear] 3. The inserted 2nd hard-disk has to be declared as "hot spare": <tt> Menu "Storage" Menu "PERC xxxxx" Menu "Physical Disks" "Connector 0" Menu "Enclosure (Backplane)" Select at [Available Task]: "Assign Global Hot Spare" <tt> Click button [Execute]

4. Check the virtual disk replication state: <tt> Column "State"

If the hard-disk replication is not starting then contact the appropriate DELL Support or the "VoIP Switch Supplier Support".

k_the_Hard-Disk_HD_Replication_Status_2">Check the Hard-Disk HD Replication Status

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Check the Hard-Disk HD Status: You have to dig in via the left navigation tree:

> Menu "Storage" Menu "PERC ..." Menu "Connector ..." Menu "Enclosure ..." Menu
> "Physical Disks ..." Check the disk state: Column "State"

States:

♦ Online:

The disk is online and productive working in the RAID. The replication is working.

Ready:
 The disk is ready for integration into a RAID. The replication is not active.

◊ Rebuilding:

• The disc is currently integrated into the RAID. The progress is displayed in %.

If there is an indication of a hard-disk replication problematic then check in chapter "Treating RAID and Hard-Disk Problems" about further maintenance actions.

Get the Server's Log Data

Access the server's "OpenManage Server Administrator (OMSA)" GUI.

Get the OMSA log:

- ◊ Menu "System" Tab "Logs"
- Save the "Embedded System Management (ESM) Log" on the server:
- Click "Save AS" and follow the instructions
- Ocopy the saved EMS Log file to the support directory of the case

Server Monitoring by Xymon

The VoIP Switch default monitor Xymon is described in "VoIP Switch Monitoring"

Indication of a Server Hardware Defect

Indication "Xymon Event": Monitor Log, Émail or SMTP Trap may contain the following information:

Indication:

<HOST_NAME> "snmptrapd" "failure"

Description:

The server indicates any hardware failure:

- Failed power module
- ♦ Failed main board
- Failed RAID controller ◊ Failed hard-disk
- Any other hardware problem

Consequences:

It may be a SEVERE server condition that must be Warning immediately investigated and treated!

For the VoIP Switch telephony service:

Observed by Depends on the VoIP Switch components running on the server

For the operations:

Observed Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" · Direct at DELL support
 - Contact the "VoIP Switch Supplier Support"
- 3. Repair the server:
- · Default processing of hardware problems that forces to shutdown the server, e.g.:
 - Fix main board
 - Fix RAID controller
 - Fix or wear out batteries
 - Fix fan
 - Fix RAM modules

or

- · Processing of hardware problems that can be done hot, e.g.:
 - Fix power module
 - Fix hard-disk

Indication of a Server Hard-Disk or RAID Controller Problem

Indication "Xymon Event": Monitor Log, Email or SMTP Trap may contain the following information:

Indication: <HOST_NAME> "snmptrapd" "degraded"

Description:

The server indicates a problem with the virtual disk:

- Failed RAID controller
- Failed hard-disk
- ◊ Failed hard-disk replication

Consequences:



SEVERE server condition that must be immediately investigated and treated!

For the VoIP Switch telephony service:

Observed Depends on the VoIP Switch components running on the server

For the operations:

Observe Depends on the VoIP Switch components running on the server

For the user:

Observe the VolP Switch components running on the server

Solution:

The RAID controller must be repaired or a hard-disk exchanged.

Action:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" · Direct at DELL support
 - · Contact the "VolP Switch Supplier Support"
- 3. Repair the server:
 - · Default processing of hardware problems that forces to shutdown the server, e.g.: Fix RAID controller
 - or
- · Processing of hardware problems that can be done hot, e.g.:
 - Fix hard-disk
 - Fix hard-disk replication

Procedure for Replacing Defect HW Parts with DELL

The procedure for exchanging defect hardware HW of DELL servers' is different from country to country and may also change from time to time.

The following basic procedure for HW exchange seems more or less stable:

- 1. Detect the HW problem
- 2. Make sure to have ready the DELL server details:
 - Server Type
 - Service-Tag number or the "ExpressService Code"
 Check the guaranty time of the server
- 3. Report DELL support
 - DELL will analyze the case and order more information if needed
- 4. DELL will organize and send the exchange part
- 5. The VoIP Switch Administrator has to organize the replacing of the part
 - Usually this has to be done within 1 3 working days
- 6. The VoIP Switch Administrator has to make ready the defect part for returning it to DELL
 - Do not dispose the defect part! Either the defect part will be picked up at the location or it has to be send back to DELL.

Treating Server Hardware Problems

The VoIP Switch Administrator and/or server service personnel find here instructions for managing HW defects.

Default Process for Fixing Hardware Problems

Indication:

◊ Xymon Event either email and/or SNMP trap: Hardware failed

- RAID degraded
- Host does not respond to ping
- Ports not OK
- Processes not OK

O The provider's system monitoring indicates no access to the server

- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition
- Server Console: The server doesn't respond to console input

Description:

Any hardware problem. Most probably:

- Of Defect main board
- Of Defect RAID controller
- Of Defect or wear out batteries
- Oefect fan
- Of Defect power module

Note	The telephony service for the customers is not endangered as long only one server fails!
Note	It becomes disastrous if the two LoadBalancer servers or all ServiceCenter servers are not working anymore.

Consequences:

Warning	It may be a SEVERE server condition that must be
warning	immediately investigated and treated!

For the VoIP Switch telephony service:

- Object to Depends on the VoIP Switch components running on the server
- ◊ If a ServiceCenter server fails the capability of concurrent connection handling may decline.

For the operations:

Observed by Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier"
- Direct at DELL support
 Contact the "VoIP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- 2. Stop provider alarming
- 3. Graceful pre-bar the VoIP Switch component

Repair the server:

If the main board or RAID controller had to be replaced then follow these special instructions:

◊ Fix main board

◊ Fix RAID controller

If the power-module or hard-disk have to be replaced, see:

◊ Fix power module◊ Fix hard-disk

	For the following actions the server casing has to be opened!
Warning	The effects of EMC must be considered and the appropriate precautions must be taken to prevent further hard ware damage.

- 1. Shut down and power off the server if the part has to be replaced on the main board
- 2. Repair the server Follow the server manufacturer's instructions!

Put back the server to normal working state:

- 1. Start the server (if needed):
 - This automatically starts the VoIP Switch components!
- 2. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check in the ConfigCenter if all VoIP Switch components on the sever are ok:
 - ConfigCenter GUI Menu "System" Menu "Components"
 - 3. Check if the Xymon monitor doesn't show any error

If the VoIP Switch doesn't get back to normal telephony service operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Fix Defect Main Board or RAID Controller

See section "Default Process for Fixing Hardware Problems" for the general description of the problem.

Actions:

Repair the server:

- 1. Shut down and power off the server if the part has to be replaced on the main board
- 2. Repair the server hardware Follow the server manufacturer's instructions
- 3. Connect a VGA monitor to the console port of the server

If the RAID controller was repaired then there will be still a RAID problem continue at "Default Process for Fixing RAID Problems", Case 2

If the main board was repaired continue here:

1. Insert the original hard-disk 1 in bay 0 (do not insert the hard-disk 2 yet)

Put back the server to normal working state:

- 1. Power on and start the server
 - This automatically starts the VoIP Switch components!
- 2. Checks:
 - 1. Check the console output on the VGA monitor if any exceptions are displayed during the BIOS booting
 - If the booting stucks during virtual hard disk initialization (RAID controller) then check the replication issues .
 2. Check the server status with "Server Administrator (OMSA)"
 3. Check in the ConfigCenter if all VoIP Switch components on the sever are ok:

 - Menu "System" ConfigCenter GUI Menu "Components"
 - 4. Check if the Xymon monitor doesn't show any error: After a certain time all supervised objects should get green except the missing hard-disk
 - 2

If the VoIP Switch doesn't get back to normal telephony service operation:

- Investigate what is wrong and solve it
 Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

When the server and the telephony service are working correctly again then:

- 1. Insert the original hard-disk 2 in bay 1
 - Check with "Server Administrator (OMSA)" if the RAID controller started automatically the hard disk replication if not then restart the replication manually

Enable the alarming again:

- 1. Enable Xymon Alarming
- Start provider alarming

Fix Defect Power Module

Indication:

- ◊ Xymon Event either email and/or SNMP trap: Hardware failed
- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition

Description:

Defect power module

Consequences:

This erroneous condition must be checked and treated Note within reasonable time!

For the VoIP Switch telephony service:

No immediate consequences Or The server is running just with one power module

For the operations:

No immediate consequences

For the user:

No immediate consequences

Solution:

The power module must be replaced

Actions:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier"

 - Direct at DELL support Contact the "VoIP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- 2. Stop provider alarming

Replace the power module:

- 1. Remove the defect power module (hot plug out possible)
- 2. Insert the new power module (hot plug in possible)
- 3. Connect the power cord

Put back the server to normal working state:

- 1. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check if the Xymon monitor doesn't show any error

If the server doesn't go back to normal operation:

- Investigate what is wrong and solve it
 Contact the "VoIP Switch Supplier Support" for helping recovering the server

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Treating RAID and Hard-Disk Problems

All servers of the VoIP Switch run a RAID type 1 which mirrors the contents of the two installed hard-disks. The "RAID controller" manages the replication between the two hard-disks.

Several conditions may interrupt the hard-disk replication and/or degrade the RAID virtual disk:

- Main board defect
- ♦ RAID controller defect
- Ard-disk defect

The consequences are that the server is not running at all or only with one hard-disk. The good news is as long one hard-disk is running the server will work as expected.

These types of defect have to be solved as fast as Note possible!

Fix Defect Hard Disk

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
 - RAID degraded
- Server Administrator (OMSA): Displays the error condition
- ◊ Server Display: The server front display is yellow and indicates the error condition

Description:

Defect hard-disk

Consequences:

This erroneous condition must be checked and treated Note within reasonable time!

For the VoIP Switch telephony service:

No immediate consequences O The server is running just with one hard-disk

For the operations:

No immediate consequences

For the user:

No immediate consequences

Solution: The hard-disk must be replaced

Actions:

Analyze the situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier"
 - · Direct at DELL support
 - Contact the "VoIP Switch Supplier Support"

Treat the VoIP Switch operation if the defect stops the proper server functionality :

- 1. Disable Xymon Alarming
- 2. Stop provider alarming

Replace the hard-disk:

- 1. Remove the defect hard-disk (hot plug out possible)
- 2. Insert the new hard-disk (hot plug in possible):

 - If the hard-disk is brand-new the replication starts immediately If the hard-disk was already used then the replication may not start automatically then check the instructions at "Default Process for Fixing RAID Problems", Case 1 .

Put back the server to normal working state:

- 1. Checks:
 - 1. Check if the hard-disk replication is in progress
 - Check the server status with "Server Administrator (OMSA)"
 Check if the Xymon monitor doesn't show any error

If the server doesn't go back to normal operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the hard-disk replication

Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Default Process for Fixing RAID Problems

Indication:

- ◊ Xymon Event either email and/or SNMP trap:
 - Hardware failed
 - RAID degraded
- O The provider's system monitoring may indicate no access to the server
- Server Administrator (OMSA): Displays the error condition
- Server Display: The server front display is yellow and indicates the error condition
 Server Console: The server may not respond to console input

Description:

Any hardware problem. Most probably:

> Of Defect RAID controller Oefect hard-disk

Consequences:

It may be a SEVERE server condition that must be Warning immediately investigated and treated!

For the VoIP Switch telephony service:

- Object to Depends on the VoIP Switch components running on the server
- ◊ If a ServiceCenter server fails the capability of concurrent connection handling may decline.

For the operations:

Observe Depends on the VoIP Switch components running on the server

For the user:

Observed by Depends on the VoIP Switch components running on the server

Solution:

The server must be repaired or exchanged.

Action:

A) Analyze the degrade situation and organize spare parts:

- 1. Check the details on the server with the "Server Administrator (OMSA)"
- 2. Check the VoIP Switch documentation for the server type and used RAID controller
- 3. Organize DELL repair parts according the maintenance agreement with your "VoIP Switch Supplier" · Direct at DELL support
 - · Contact the "VoIP Switch Supplier Support"

B) Treat the VoIP Switch operation if the defect stops the proper server functionality :

© Aarenet AG 2017

- 1. Disable Xymon Alarming
- Stop provider alarming
- 3. :support switch#supportSwitchPreBar Graceful pre-bar the VoIP Switch component
- C) Evaluate the repair case for DELL RAID controller type: PERC5 / PERC 6 / H310 Mini / H320 Mini / H330 Mini:

Case 1: "One Hard-Disk Defect"

Precondition:

- Main board is ok
- RAID controller is ok
- 1 operative hard-disk is ok
- Server is still operative within the VoIP Switch
- The replacement hard-disk has the same form factor and size of bytes

To-Do:

- 1. Remove the defect hard-disk (hot plug-out is no problem)
- Insert the new hard-disk (hot plug-in is no problem) either:
 ♦ a brand-new hard-disk

 - an already used spare hard-disk
- 3. Check the hard-disk replication status
 - If the replication did not start automatically then start the replication manually !

Case 2: "Main Board or RAID Controller Defect:

Precondition:

- The main board RAID controller are repaired according description above
- 2 operative hard-disks are ok
- Server is shut down
- Disconnect all Ethernet patch cables from the server GB ports.
- Connect a VGA monitor and USB keyboard and mouse tot the console port of the server

To-Do:

- 1. Insert the original hard-disk 1 in bay 0 (do not insert the hard-disk 2 yet)
- 2. Power up the server
- 3. Check the console output on the VGA monitor:
 - During the BIOS startup the following message may be displayed:

Foreign configuration(n) found on adapter. Press any key ? or 'F' to import foreign configuration and

- continue.
- 4. If requested press key F on the keyboard!
 - Note:

If you miss to press F then restart the BIOS booting by pressing the keys [Ctrl Alt Delete] else the server booting stops after the BIOS start up.

5. Check the console output on the VGA monitor:

A security question may be displayed which enables you to stop the procedure: All of the disk from your previous configuration are gone. If this is an

unexpected message ...

6. Do not press any key!

Note:

If no key is pressed then the RAID controller takes over the hard-disk as part of its new virtual disk.

Wait until the server has booted!

- Insert the original hard-disk 2 in bay 1
- 8. Check the hard-disk replication status
 - Note:

It is very probable that the replication did not start automatically! Then:

At Menu "Storage" a yellow warning triangle is displayed

Upon click on "Storage" the status is displayed: Virtual Disk 0: degraded

If the replication did not start automatically then start the replication manually !

For all other cases:

- Ocontact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality
- C) Put back the server to normal working state:
 - 1. If needed connect all Ethernet patch cables to the correct server GB ports
 - 2. Checks:
 - 1. Check the server status with "Server Administrator (OMSA)"
 - 2. Check in the ConfigCenter if all VoIP Switch components on the sever are ok: ConfigCenter GUI Menu "System" Menu "Components"

 - 3. Check if the Xymon monitor doesn't show any error

D) If the VoIP Switch doesn't get back to normal telephony service operation:

- 1. Investigate what is wrong and solve it
- 2. Contact the "VoIP Switch Supplier Support" for helping setting up the server and recovering the missing VoIP Switch functionality

E) Enable the alarming again:

- 1. Enable Xymon Alarming
- 2. Start provider alarming

Manually Restart the Hard-Disk Replication

In this situation the RAID's virtual disk is in state degraded (only one hard-disk is operative, but two are expected). The RAID controller will automatically grab a free "hot spare" hard-disk and associate it with its degraded virtual disk and start the replication.

Restart the hard-disk replication manually:

- 1. Connect with any Web browser to the server's "Server Administrator (OMSA)" GUI: Login as user "root"

2. From the inserted 2nd hard-disk the foreign RAID configuration has to be deleted: Menu "Storage" Menu "PERC xxxxx" Select at [Available Task]: "Clear Foreign Configuration" <tt> Click button [Execute] <tt> Confirm the security check click button [Clear] 3. The inserted 2nd hard-disk has to be declared as "hot spare": <tt> Menu "Storage" Menu "PERC xxxxx" "Connector 0" Menu "Enclosure (Backplane)" Menu "Physical Disks" Select at [Available Task]: "Assign Global Hot Spare" <tt> Click button [Execute]

4. Check the virtual disk replication state: <tt> Column "State"

If the hard-disk replication is not starting then contact the appropriate DELL Support or the "VoIP Switch Supplier Support".

-->

Brief Tutorial of the SIP Signaling and SDP Media Protocols

Knowhow Connection Signaling with "Session Initiation Protocol SIP"

The **Session Initiation Protocol SIP** is a communications protocol for signaling and controlling multimedia communication sessions. One of the most common applications of SIP is in Internet telephony for voice and video calls.

For an extended overview of the SIP protocol visit:

```
Wikipedia: Session Initiation Protocol SIP
```

Basics: Session Session Protocol SIP

Example of a "SIP dialog" with the minimal needed messages for a connection setup or connection renegotiation:



Example of a "SIP dialog" with the minimal needed messages for a connection release:



Examples: SIP Signaling Flows

Example of a regular outgoing call into the PSTN:



Example of a regular incoming call from the PSTN:



Example of an outgoing call into the PSTN with three exceptional signaling situations:

- The PSTN Gateway 1 doesn't respond so the VoIP Switch has to re-route to the PSTN Gateway 2
 The telephone on side A offers an invalid "Session Time" value which is refused by the PSTN Gateway 2. The telephone on side A has to do a reINVITE with an acceptable "Session Time"
- value.
- 3. End point B is busy.



Example of a connection where the VoIP Switch checks the presence of the end points with OPTION messages. The VoIP Switch would release the connection if one end point doesn't respond with "200 OK":



SIP Response Codes

A list of SIP response codes and their meaning can be found here:

Wikipedia: List of SIP Response Codes

Most Important 1xx?Provisional Responses

100 Trying

Extended search being performed may take a significant time so a forking proxy must send a 100 Trying response.

180 Ringing

Destination user agent received INVITE, and is alerting user of call.

183 Session in Progress

This response may be used to send extra information for a call which is still being set up.

Most Important 2xx?Successful Responses

200 OK

Indicates the request was successful.

Most Important 3xx?Redirection Responses

302 Moved Temporarily

The client should try at the address in the Contact field. If an Expires field is present, the client may cache the result for that period of time.

Most Important 4xx?Client Failure Responses

400 Bad Request

The request could not be understood due to malformed syntax.

401 Unauthorized

The request requires user authentication. This response is issued by UASs and registrars.

403 Forbidden

The server understood the request, but is refusing to fulfil it.

404 Not Found

The server has definitive information that the user does not exist at the domain specified in the Request-URI. This status is also returned if the domain in the Request-URI does not match any of the domains handled by the recipient of the request.

406 Not Acceptable

The resource identified by the request is only capable of generating response entities that have content characteristics but not acceptable according to the Accept header field sent in the request.

408 Request Timeout

Couldn't find the user in time. The server could not produce a response within a suitable amount of time, for example, if it could not determine the location of the user in time. The client MAY repeat the request without modifications at any later time.

410 Gone

The user existed once, but is not available here any more.

480 Temporarily Unavailable

Callee currently unavailable.

486 Busy Here

Callee is busy.

487 Request Terminated

Request has terminated by bye or cancel.

488 Not Acceptable Here

Some aspect of the session description or the Request-URI is not acceptable.

Most Important 5xx?Server Failure Responses

503 Service Unavailable

The server is undergoing maintenance or is temporarily overloaded and so cannot process the request. A "Retry-After" header field may specify when the client may reattempt its request.

Most Important 6xx?Global Failure Responses

603 Decline

The destination does not wish to participate in the call, or cannot do so, and additionally the destination knows there are no alternative destinations (such as a voicemail server) willing to accept the call.

Knowhow Media Stream Signaling with "Session Description Protocol SDP"

The **Session Description Protocol SDP** describes how during a connection setup the end points negotiate the parameters of this exchange as session announcement, session invitation, and parameter. SDP does not deliver media itself but is used between end points for negotiation of media type, format, and all associated properties for voice, Fax, DTMF, bit transparent data etc..

For an extended overview of the SDP protocol visit Wikipedia.



Basics: Session Description Protocol SDP

The SDP is embedded in the SIP messages during connection setup or connection renegotiation:



The following SDP properties and parameters are important for supporting customer problems:



Example of a SDP offer from the calling side A:



Example of a SDP offer for a Fax transfer with T.38 from the calling side A:



Interpretation of the "Media Attributes":

Index	Туре	Attribute	Remark
0	PCMU	ISDN G.711µlaw	Very good quality VoIP codec
8	PCMA	ISDN G.711alaw	Very good quality VoIP codec
2	G.726-32		Good quality VoIP codec
18	G.729		Low quality VoIP codec

125	x-clear-channel	data service bit transparent	Echo canceling will be switched off and the data bit by bit transferred
101	telephone-event	DTMF, RFC 2833	DTMF will not be transferred inband but as RTP event according RFC 2833
18	annexb=0	Special information for codec with index 18	Special directive for codec G.729
101	0-16	Special information for for telephone-event with index	0-15 : DTMF character 0-9, *,#, A,B,C,D
		101	0-16 : DTMF character 0-9, *,#, A,B,C,D, Flash

Basics: RTP/RTCP

The Real Time Protocol RTP is used to transfer media data, e.g. speech in VoIP based telephony.

The Real Time Control Protocol RTPC transfers periodically statistical media data between the peers of a connection.

If RTP packets are lost, delayed or jitter then we speak of a Quality of Service QoS problem. For the support it is of interest to know if the number of transferred packets between the peers of a connection and if the numbers in the receive and send paths are reasonable equal, if packets were lost on call leg etc. With these statistical media information it can be possible to identify a path or transfer direction were QoS problems occure.

The media stream must be proxied via the MediaServer of the VoIP Switch in order to compute statistical Note numbers of a connection.

The Aarenet VoIP Switch supports RTP/RTCP statistic data collection of a connection. How they can be obtained is described in article "Manual of the Aarenet VoIP Switch Support Tools", chapter "The ConfigCenter Call Data"

Overview of "RTP/RTCP" information collection:



Details of "RTP/RTCP" information collection:



or="#f4cc35">

Basics: Session Description Protocol SDP

The SDP is embedded in the SIP messages during connection setup or connection renegotiation:



The following SDP properties and parameters are important for supporting customer problems:


Example of a SDP offer from the calling side A:



Example of a SDP offer for a Fax transfer with T.38 from the calling side A:



Interpretation of the "Media Attributes":

Index	Туре	Attribute	Remark
0	PCMU	ISDN G.711µlaw	Very good quality VoIP codec
8	PCMA	ISDN G.711alaw	Very good quality VoIP codec
2	G.726-32		Good quality VoIP codec
18	G.729		Low quality VoIP codec

125	x-clear-channel	data service bit transparent	Echo canceling will be switched off and the data bit by bit transferred
101	telephone-event	DTMF, RFC 2833	DTMF will not be transferred inband but as RTP event according RFC 2833
18	annexb=0	Special information for codec with index 18	Special directive for codec G.729
101	0-16	Special information for for telephone-event with index 101	0-15 : DTMF character 0-9, *,#, A,B,C,D 0-16 : DTME character 0-9, * # A B C D, Elash

Basics: RTP/RTCP

The Real Time Protocol RTP is used to transfer media data, e.g. speech in VoIP based telephony.

The Real Time Control Protocol RTPC transfers periodically statistical media data between the peers of a connection.

If RTP packets are lost, delayed or jitter then we speak of a Quality of Service QoS problem. For the support it is of interest to know if the number of transferred packets between the peers of a connection and if the numbers in the receive and send paths are reasonable equal, if packets were lost on call leg etc. With these statistical media information it can be possible to identify a path or transfer direction were QoS problems occure.

The Aarenet VoIP Switch supports RTP/RTCP statistic data collection of a connection. How they can be obtained is described in article "Manual of the Aarenet VoIP Switch Support Tools", chapter "The ConfigCenter Call Data"

Overview of "RTP/RTCP" information collection:



Details of "RTP/RTCP" information collection:



-->