

Training anSwitch

AN SWITCH V7 SUPPORT TOOLS & DEBUGGING

Date: 18.9.2023
Author: D. Bochsler
Version: E1.3
© Aarenet Inc.

INTRODUCTION & MOTIVATION

This Training covers the topics:

- ▶ Which supporting tools the anSwitch offers
- ▶ What information the supporting tools delivers
- ▶ Analyzing and supporting different user problem types

After this training, the trainee is enabled:

- ▶ To understand which supporting tools the anSwitch offers
- ▶ How the supporting tools work
- ▶ To analyze user problems
- ▶ To start solving user problems



*IT'S NOT
MAGIC
IT'S "KNOW
HOW"*

TABLE OF CONTENTS

- 1 OVERVIEW OF INTEGRATED SUPPORTING TOOLS
- 2 CHECK THE SIP DEVICE REGISTRATION
- 3 CHECK CALL SIP TRACES
- 4 CHECK THE SUPPORT LOG
- 5 CHECK CALL STATISTICS
- 6 CHECK THE HISTORY LOG
- 7 CHECK COMPONENT LOGS
- 8 CHECK SYSTEM COMPONENT STATUS
- 9 CHECK SYSTEM MONITOR & ALARMING
- 10 CHECK PBX CALL ANALYTICS
- 11 EVALUATE THE PROBLEM TYPE
- 12 PROBLEM TYPE: "DEVICE / NETWORK"
- 13 PROBLEM TYPE: "CONNECTION"
- 14 PROBLEM TYPE: "AUDIO STREAM"
- 15 PROBLEM TYPE: "FAX TRANSMISSION"
- 16 LOGGING ANSWITCH V7 SYSTEM CONFIGURATION

1 OVERVIEW OF INTEGRATED SUPPORTING TOOLS

OVERVIEW OF THE INTEGRATED SUPPORT VIA PORTAL UI

- ▶ The anSwitch V7 provides a big number of integrated supporting tools which helps the support personnel to solve most problem. In most cases external tools are not needed.
- ▶ The PBX member has some basic tools at hand for a first aid or send logs to their support organization.
- ▶ The Operator has the most important tools at hand for providing support.
 - ▶ The support staff must have the Role of "Operator" to be able to provide adequate assistance.
- ▶ The Administrator has additional tools for supervising the VoIP system and checking component logs.

OVERVIEW SUPPORT TOOL: SIP DEVICE REGISTRATION PROBLEM

- ▶ Registration
 - ▶ The anSwitch provides registration information in a generalized manner at different places e.g., PBX Dashboard, phone list, extension features, phone related status, etc.
 - ▶ The "Phone Related Status" provides the detailed registration information of each SIP phone.
 - ▶ This tool is useful for analysing:
 - ▶ The registration status
 - ▶ IP network connection from the device to the VoIP switch
 - ▶ This tool is available for:
 - ▶ PBX Member → must have access to the Portal UI and an account
 - ▶ Operator → acting as supporter
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: TRACE

▶ SIP Traces

- ▶ The anSwitch records for each call (successful or not successful) the trace of the SIP messages.
- ▶ The SIP trace shows the external message flow between peers.
- ▶ It needs training to understand the information.
- ▶ The analyzing must be done in an external tool e.g.: Wireshark

- ▶ This tool is useful for analysing:
 - ▶ The SIP message flow between the peering devices
 - ▶ The reasons for call rejections, call fails, etc.
 - ▶ Dialed and displayed numbers
 - ▶ Codec negotiation

- ▶ This tool is available for:
 - ▶ PBX Member → must have access to the Portal UI and an account
 - ▶ Operator → acting as supporter
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: SUPPORT LOG

- ▶ Support Log
 - ▶ The Support log provides the information about the anSwitch internal activities during a call.
 - ▶ The information are good interpretable.
 - ▶ This tool is useful for analysing:
 - ▶ The executed internal activities of a call as dialed numbers, used Rules, Routes, Gateways
 - ▶ This tool is available for:
 - ▶ Operator → acting as supporter
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: HISTORY LOG

- ▶ History Log
 - ▶ The History log provides the information who made configurations via the Portal UI
 - ▶ This tools are useful for:
 - ▶ Finding out about misconfigurations
 - ▶ This tool is available for:
 - ▶ Operator → acting as supporter
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: CALL STATISTICS

- ▶ **Call Statistics**
 - ▶ The anSwitch provides for each call a Call Detail Record CDR which contains the calls basic information e.g., numbers, duration, charges, technical and quality information.
 - ▶ This tool is useful for analysing:
 - ▶ The call details
 - ▶ The call fail cause
 - ▶ The call quality QoS
 - ▶ Getting the call ID for filtering in the component logs
 - ▶ This tool is available for:
 - ▶ Operator → acting as supporter
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: COMPONENT LOGS

- ▶

Component Logs

 - ▶ Each anSwitch Component has its own deep logging
 - ▶ The logging is done in a round-robbing manner:
 - ▶ A log overflow is not possible.
 - ▶ The oldest information is overwritten by new ones.
 - ▶ A log buffer records approximately the last 3 days.
 - ▶ The Portal log menu collects the component logs on all servers/hosts and unifies them in a merged component log.
 - ▶ It needs training to understand the information.
 - ▶ This tool is useful for :
 - ▶ Analysing deep problems
 - ▶ Providing log information for the Aarenet support
 - ▶ This tool is available for:
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: SYSTEM COMPONENT STATUS

- ▶ **System Component Status Overview**
 - ▶ The anSwitch provides a component activity overview with information for each active component with its the status, utilization, version, etc.
 - ▶ This tool is useful for analysing:
 - ▶ The overall anSwitch status
 - ▶ This tool is available for:
 - ▶ Administrator

OVERVIEW SUPPORT TOOL: SYSTEM MONITORING & ALARMING

▶ System Monitor

- ▶ The System monitor is an independent supervision entity that is installed on every server or host. It supervises the server resources, defined IP connections and the anSwitch components and resources from the outside. It raises alarms if needed.
- ▶ This tool is useful for:
 - ▶ Supervising the VoIP system status and trends in graphs for e.g., incoming and outgoing calls, registrations, etc
 - ▶ Supervision of HW e.g., bar metal server, IT equipment of the VoIP system
- ▶ This tool is available for:
 - ▶ Administrator

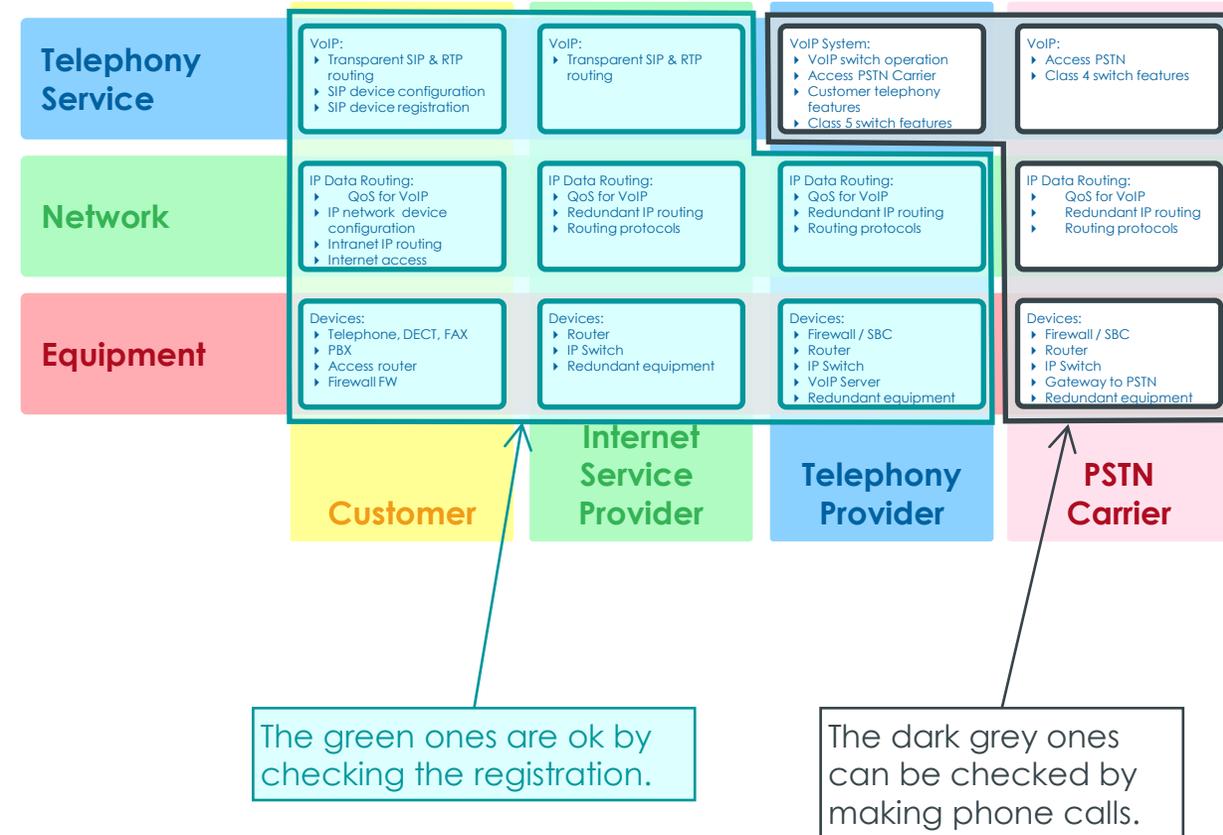
2 CHECK THE SIP DEVICE REGISTRATION

WHY CHECKING THE REGISTRATION IS IMPORTANT

► By checking the registration, we learn:

1. All equipment is running!
2. The IP network is working between the anSwitch and the phone
3. The phone is online and has the correct SIP credentials.

➔ For a safety of ~90% you know that the telephony service is ok!



HOW TO CHECK THE REGISTRATION STATUS

- ▶ There are several locations in the Portal where a general overview of the registration situation is given:

- Green: At least one phone has registered
- Red: No active registration currently, but there were registered phone already
- Black: No phone registered ever

- ▶ Overview in the PBX Dashboard:

Phone Information		
Phone Name	Internal Number	Registration Status
Sales 1-Yealink T21P E2	315 (Sales 1)	●
Agent 1-snom D735	21 (Agent 1)	●
Front Desk-Yealink T48G	311 (Front Desk)	●
Sales 2-Yealink T40G	316 (Sales 2)	●
Agent 2-snom D785	22 (Agent 2)	●
Boss Office -Yealink T21P E2	300 (Boss), 311 (Front Desk)	●
Boss-an IP-Phone	300 (Boss)	●
Warehouse 1-Yealink W53H	330 (Warehouse 1)	●
Boss Office - GRANDSTREAM GRP2613	300 (Boss)	●
Warehouse 2 - Polycom		●

- ▶ Overview in the Phone List:

+ New × Delete					
<input type="checkbox"/>	Phone/Device Name	Extension Name	Extension	Phone/Device Type	State
<input type="checkbox"/>	Agent 1-snom D735	Agent 1	21 (Agent 1)	snom D735	●
<input type="checkbox"/>	Agent 2-snom D785	Agent 2	22 (Agent 2)	snom D785	●
<input type="checkbox"/>	Boss - an IP-Phone Desktop	Boss	300 (Boss)	an IP-Phone desktop	●
<input type="checkbox"/>	Boss Office - GRANDSTREAM GRP2613	Boss	300 (Boss)	Grandstream GRP2613	●

- ▶ Overview in the extension:

Assigned Phones		
<input type="checkbox"/>	Phone Name	Registration Status
<input type="checkbox"/>	Boss Office -Yealink T21P E2	●
<input type="checkbox"/>	Boss-an IP-Phone	●
<input type="checkbox"/>	Boss Office - GRANDSTREAM GRP2613	●
<input type="checkbox"/>	The Boss's anConnect	●
<input type="checkbox"/>	Boss-Yealink T53W	●
<input type="checkbox"/>	Boss - an IP-Phone Desktop	●

HOW TO CHECK THE REGISTRATION DETAILS

- ▶ Detailed information about the SIP registration and presence/message subscriptions can be found in the phone status.

1. Access the Portal with sufficient rights, usually: PBX Administrator

- > Menu: PBX Administrator
- > Sub-Menu: Phones
- > Click the row of the phone that must be checked
- > Click link: Phone Related Status

2. Analyze the SIP registration and subscription details

Phone Related Status - Boss Office -Yealink T21P E2

Extension Related Features Phone Setup Phone Related Features

Synchronize

Last Synchronization 19.10.2021 19:38

ACD Membership Boss - 300

Registrations

Deactivate

Status	Expires	IP Address	Extension	Endpoint	UserAgent	Contact
●	5:05	185.150.4.193:60844	300	Public	Yealink SIP-T21P_E2 52.84.0.125	sip:300@10.10.0.95:5060
●	5:04	185.150.4.193:60844	311	Public	Yealink SIP-T21P_E2 52.84.0.125	sip:311@10.10.0.95:5060

Subscriptions

Status	Expires	IP Address	Endpoint	From Number	To Number	Event
●	45:03	185.150.4.193	Public	300	300	message-summary
●	45:03	185.150.4.193	Public	300	300	as-feature-event
●	45:03	185.150.4.193	Public	311	311	message-summary
●	45:03	185.150.4.193	Public	311	311	as-feature-event

Subscriptions for signaling:

- ▶ New VoiceMail Box messages
- ▶ Team key status changes
- ▶ Line key status changes

Phones and other SIP devices that have registered to the extension.

Note:
The registrations of Line keys are also displayed.

Information when the configurations were the last time synchronized to the phone.

Note

Information about debugging registration problems, see the training presentation:

- ▶ training_answitch_301_support_debugging

3 CHECK CALL SIP TRACES

CHECK CALL SIP TRACES

- ▶ The anSwitch provides for each call (successful or not successful) the trace of the SIP messages in the PBX Calls list.

- > Menu: Operator
- > Sub-Menu: Calls
 - > Search and select the desired call
 - > Click button: Download SIP Trace

	Start	From	To	Duration	Call State
<input type="radio"/>	31.12.2021 10:13	300	*86	00:05:09	410- Gone
<input type="radio"/>	31.12.2021 10:13	300	311	00:05:09	410- Gone
<input checked="" type="radio"/>	27.12.2021 13:05	300	0012xxxx	00:00:00	487- Request Terminated
<input type="radio"/>	26.12.2021 15:26	316	300	00:00:00	487- Request Terminated
<input type="radio"/>	16.12.2021 11:51	0319802818	*86	00:00:12	200- Calling Party Released

- ▶ A PBX Administrator may send the trace as file to the support.

- ▶ With an appropriately configured Web browser, the SIP trace is opened in an analyse application e.g., Wireshark.

- ▶ Check the SIP messages between the peers:

- ▶ SIP message flow regular or irregular
- ▶ SIP header content
- ▶ SDP: IP address, IP port and codec negotiation

trace (6).pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1	14:24:20.012000	185. . .216	185. . .210	SIP/SDP	6293	Request: INVITE sip:45@185. . .210
2	14:24:20.015000	185. . .210	185. . .216	SIP	499	Status: 401 Unauthorized
3	14:24:20.017000	185. . .216	185. . .210	SIP	411	Request: ACK sip:45@185. . .210
4	14:24:20.019000	185. . .216	185. . .210	SIP/SDP	6499	Request: INVITE sip:45@185. . .210
5	14:24:20.026000	185. . .210	185. . .216	SIP	409	Status: 100 Trying
6	14:24:20.082000	185. . .210	213. .85.50	SIP/SDP	985	Request: INVITE sip:0792536035@213. .85.50
7	14:24:20.096000	213. .85.50	185. . .210	SIP	386	Status: 100 Trvine

```

> Frame 1: 6293 bytes on wire (50344 bits), 6293 bytes captured (50344 bits)
> Ethernet II, Src: 00:00:00_00:ca:00 (00:00:00:00:ca:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 185. . .216, Dst: 185. . .210
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (INVITE)
  > Request-line: INVITE sip:45@185. . .210 SIP/2.0
  > Message Header
    > Route: <sip:185. . .210>;lr>
    > Via: SIP/2.0/UDP 192.168.5.32:5060;branch=z9hG4bK.OT1BFZFu5a7s11pdR8xpuxnWVOPh1qaF;rport
    > CSeq: 1 INVITE
    > From: <sip:24@185. . .210>;tag=WI96aF19vmi8ICfiquGuxjrX0W6wkbw
    > To: <sip:45@185. . .210>
    > Call-ID: 162142705856603b125H3VbjZaYA
    [Generated Call-ID: 162142705856603b125H3VbjZaYA]
    > Contact: <sip:24@185. . .210>
    Max-Forwards: 70
    Content-Type: application/sdp
    User-Agent: GoSIP
    Content-Length: 5959
    Allow: INVITE, ACK, CANCEL, NOTIFY, BYE
  > Message Body
  
```

4 CHECK THE SUPPORT LOG

CHECK THE SUPPORT LOG

- ▶ The Support log provides the information about the anSwitch internal activities during a call.

- > Menu: Operations
 - > Sub-Menu: Logs
 - > Select Log Type: Support Log
 - > Set Filters: Regex Pattern, From-Until date/time

Logs

Show log Download log

Log type Support Contains Regex Pattern From Until

2021-12-27-13:05:19.524 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 terminal=Boss-an IP-Phone call routing from address '300' to '00123456'

2021-12-27-13:05:19.530 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 address="Boss" 300 routing to gateway, tags are:

2021-12-27-13:05:19.533 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 address="Boss" 300 routing to gateway found 1 routes

2021-12-27-13:05:19.551 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 address="Boss" 300 using route Route to PSTN

2021-12-27-13:05:19.564 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 address="Boss" 300 route to terminals [GW: an-training-rs]

2021-12-27-13:05:30.158 [INFO] SupportLog (cc1/CC08) ou=39 call=cc1anloctrain-dc69bd5c2729e4b0 terminal=Boss-an IP-Phone releasing with reason CANCELED

- ▶ The log information can be interpreted well.

- ▶ Predefined search options as "Regex Pattern":

- ▶ Beside applying a regex pattern the supporter can select from a list often used search pattern.

- ▶ Hint:

- ▶ Use the unique call ID of a call or call attempt to filter the events of this call.
 - ▶ The unique call ID of a call can be found in the [call statistics \(see below\)](#)

Logs

Show log Download log

Log type Support Contains Regex Pattern Registration From 18.09.2023 10:55 Until

remove filter

Registration	shows all entries related with Registration
call	shows all entries related to calls
channels	show all entries with channel information
charge	shows all messages related with TopStop
acd	shows calls to acd
ivr	shows calls to IVR

2023-09-18-10:56:11.292 [INFO] er A.PA-PBX-0AX89001.Warehouse 1 Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:56:11.299 [INFO] Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:56:11.299 [INFO] Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:56:11.936 [INFO] Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:56:11.936 [INFO] Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:56:11.938 [INFO] Registration to sip:185.150.4.203 has invalid username for au

2023-09-18-10:58:00.602 [INFO] er A.PA-PBX-0AX89001.Support Department.Agent 2 Registration

2023-09-18-10:58:09.306 [INFO] er A.PA-PBX-0AX89001.Front Desk Registration to sip:185.150.4

5 CHECK CALL STATISTICS

CHECK CALL STATISTICS

- ▶ The anSwitch provides for each call a Call Detail Record CDR which contains the calls basic information e.g., numbers, duration, charges, technical and quality information.

- > Menu: PBX Administrator
 - > Sub-Menu: Calls
 - > Search and select the desired call
 - > Click button: Show Call Stats

- ▶ Check for the desired information e.g.:
 - ▶ Call ID → Use this as a reach criterion in the Support Log and Component Log for this call
 - ▶ Call released or failed reasons → SIP Status
 - ▶ Audio problems → Due to packet loss or heavy jitter

PBX Calls -

Download SIP Trace Show Call Stats

	Start	From	To	Duration	Call State
<input type="radio"/>	31.12.2021 10:13	300	*86	00:05:09	410- Gone
<input type="radio"/>	31.12.2021 10:13	300	311	00:05:09	410- Gone
<input checked="" type="radio"/>	27.12.2021 13:05	300	0012xxxx	00:00:00	487- Request Terminated
<input type="radio"/>	26.12.2021 15:26	316	300	00:00:00	487- Request Terminated
<input type="radio"/>	16.12.2021 11:51	0319802818	*86	00:00:12	200- Calling Party Released

Call Stats

Basic Info

Calling Number : 300
 Display Number : 300
 Called Number : 00123456
 Time Start : 27.12.2021 13:05
 Time Connect :
 Duration : 00:00:00
 Charges Tenant : 0.0
 Charges Account : 0.0
 Destination : International Unknown - PBX: User
 Destination Type : OffNet

Technical Info

Call ID : cc1anloctrain-dc69bd5c2729e4b0
 SIP Call ID : 6BC603E6D1CD3B7174980074C1F6D45C47892A5D
 Originating IP : 83.77.4.169
 Destination IP : 185.150.4.200
 SIP Status : 487- Request Terminated
 Cause of Release(Q850) : 0- Valid cause code not yet received

Quality Info

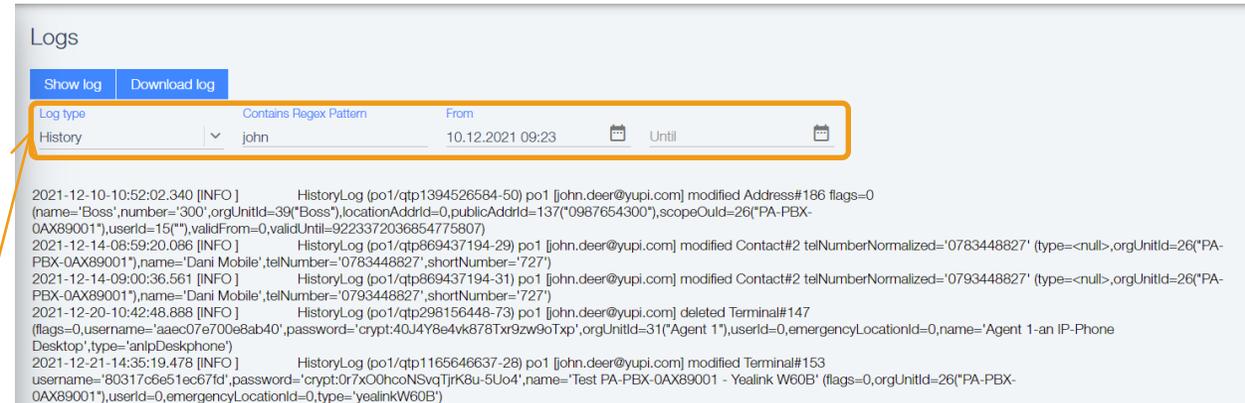
	Leg	Codec	Average Jitter RX	Average Jitter TX	Packet Loss RX	Packet Loss TX	Average Latency
<input type="radio"/>	A	opusFb	21 ms	15 ms	0 %	2 %	12 ms
<input type="radio"/>	B	opusFb	0 ms	0 ms	0 %	0 %	0 ms

6 CHECK THE HISTORY LOG

CHECK THE HISTORY LOG

- ▶ The History log provides the information who made configurations via the Portal UI.

- > Menu: Operations
 - > Sub-Menu: Logs
 - > Select Log Type: History
 - > Set Filters: Regex Pattern, From-Until date/time



The screenshot shows the 'Logs' interface with a filter applied. The filter is set to 'History' log type, with a 'Contains Regex Pattern' of 'john' and a date range from '10.12.2021 09:23' to 'Until'. Below the filter, a list of log entries is displayed, including details such as timestamp, log type, and user information.

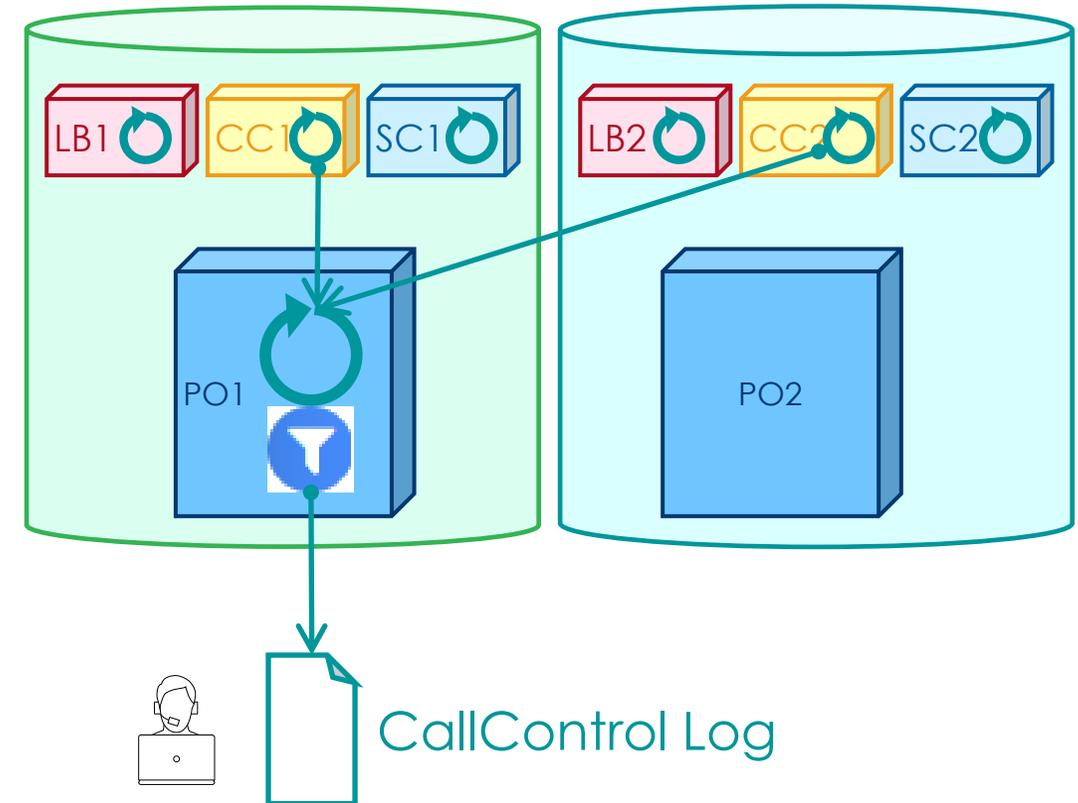
```

2021-12-10-10:52:02.340 [INFO] HistoryLog (po1/qtp1394526584-50) po1 [john.deer@yupi.com] modified Address#186 flags=0
(name='Boss',number='300',orgUnitId=39('Boss'),locationAddrId=0,publicAddrId=137('0987654300'),scopeOuld=26('PA-PBX-
0AX89001'),userId=15(''),validFrom=0,validUntil=9223372036854775807)
2021-12-14-08:59:20.086 [INFO] HistoryLog (po1/qtp869437194-29) po1 [john.deer@yupi.com] modified Contact#2 telNumberNormalized='0783448827' (type=<null>,orgUnitId=26('PA-
PBX-0AX89001'),name='Dani Mobile',telNumber='0783448827',shortNumber='727')
2021-12-14-09:00:36.561 [INFO] HistoryLog (po1/qtp869437194-31) po1 [john.deer@yupi.com] modified Contact#2 telNumberNormalized='0793448827' (type=<null>,orgUnitId=26('PA-
PBX-0AX89001'),name='Dani Mobile',telNumber='0793448827',shortNumber='727')
2021-12-20-10:42:48.888 [INFO] HistoryLog (po1/qtp298156448-73) po1 [john.deer@yupi.com] deleted Terminal#147
(flags=0,username='aaec07e700e8ab40',password='crypt:40J4Y8e4vk878Txr9zW9oTxp',orgUnitId=31('Agent 1'),userId=0,emergencyLocationId=0,name='Agent 1-an IP-Phone
Desktop',type='anipDeskphone')
2021-12-21-14:35:19.478 [INFO] HistoryLog (po1/qtp1165646637-28) po1 [john.deer@yupi.com] modified Terminal#153
username='80317c6e51ec67fd',password='crypt:0r7xOOhcoNSvqTjrK8u-5Uo4',name='Test PA-PBX-0AX89001 - Yealink W60B' (flags=0,orgUnitId=26('PA-PBX-
0AX89001'),userId=0,emergencyLocationId=0,type='yealinkW60B')
  
```

7 CHECK COMPONENT LOGS

OVERVIEW OF COMPONENT LOGS

- ▶ Each anSwitch Component has its own round-robbing log.
 - ▶ The size of the round-robbing log is configurable on system level.
 - ▶ By default, the Aarenet system engineers configure the round-robbing log mechanism of the log so that approximately 3 days of logging is possible.
- ▶ The Log collects each single component log and unifies them in a merged component log and delivers a log file where the filters were applied according:
 - ▶ Log type
 - ▶ Start – End date/time
 - ▶ Regex



Note

Component logs are complicated to be understand and interpreted.

➔ In most cases, the user is prompted to send the downloaded logs to Aarenet Support for evaluation.

OVERVIEW OF PROVIDED CONTENTS OF COMPONENT LOGS

▶ Log Type: CallControl

- ▶ SIP message exchange
- ▶ Call routing
- ▶ Telephony features
- ▶ DB accesses by the CallControl component
- ▶ Host resources usage by the CallControl component

▶ Log Type: MediaControl

- ▶ Codec negotiation
- ▶ Socket & endpoint management for media streams
- ▶ RTCP QoS information

▶ Log Type: LoadBalancer

- ▶ SIP message distribution to CallControl components according SIP dialogs
- ▶ DB accesses by the LoadBalancer component
- ▶ Host resources usage by the LoadBalancer component

▶ Log Type: Portal

- ▶ Phone configuration file download
- ▶ Activities of the REST API
- ▶ DB accesses by the Portal component
- ▶ Host resources usage by the Portal component

▶ Log Type: SystemControl

- ▶ The generation of CDR
- ▶ DB accesses by the SystemControl component
- ▶ Host resources usage by the SystemControl component

CHECK COMPONENT LOGS

- ▶ The Portal provides merged component logs for display in the Web browser or download file:

- > Menu: Operations
 - > Sub-Menu: Logs
 - > Select Log Type of the desired component
 - > Set Filters: Regex Pattern, From-Until date/time

- ▶ Check the log file for deep and detailed researches about the internal component activities.

- ▶ If needed or requested download and send the log file to the Aarenet Support.

The screenshot shows a web interface for viewing logs. At the top, there are two buttons: 'Show log' and 'Download log'. Below them is a table with columns: 'Log type', 'Contains Regex Pattern', 'From', and 'Until'. The first row shows 'CallControl' as the log type, 'INVITE' as the regex pattern, '19.05.2021 15:19' as the start time, and '19.05.2021 16:00' as the end time. Below the table, the log content is displayed in a light blue box. It starts with a timestamp and level: '2021-05-19-15:19:13.989 [DEBUG]'. The log content includes SIP headers and a registration message: 'REGISTER sip:185.210.5060 SIP/2.0', 'Via: SIP/2.0/UDP 10.1.3.33:33184;branch=z9hG4bK-eranqywtahoo;rport', 'From: "Norbert Toth" <sip:42@185.210.5060>;tag=te693rricr', 'To: "Norbert Toth" <sip:42@185.210.5060>', 'Call-ID: 313631383538363239393233373339-d6cg95tjpf06', 'CSeq: 18473 REGISTER', 'Max-Forwards: 70', 'User-Agent: snomD717/10.1.54.13', 'Contact: <sip:42@10.1.3.33:33184;line=8l0ap04c>;reg-ld=1;q=1.0;+sip.instance="<urn:uuid:704963ac-ee3f-4b41-854c-000413A618AD>;audio;mobility="fixed";duplex="full";description="snomD717";actor="principal";events="dialog";methods="INVITE,ACK,CANCEL,BYE,REFER,OPTIO', 'NS,NOTIFY,SUBSCRIBE,PRACK,MESSAGE,INFO"', 'Allow-Events: dialog, talk, hold, check-sync', 'X-Real-IP: 10.1.3.33', 'Supported: path, gruu', 'Authorization: Digest', 'username="a8942f5f2ae6347e", realm="185.210", nonce="60a51047d44177d69e948f0b1b9ad26a03b0019", uri="sip:185.210:5060", response="4651de56d13cf23199eb6bb6d185396e", algorithm=MD5', 'Expires: 600', 'Content-Length: 0'. Below this, another log entry is partially visible: '2021-05-19-15:19:14.101 [DEBUG] Endpoint (cc1/LbListeningPointlb) ----- received ----- [185.150.4.209:30994] -> [185.150.4.210:5060] REGISTER sip:185.150.4.210:5060 SIP/2.0'. Orange arrows point from the 'Download log' button and the first log entry to the text in the first bullet point.

8 CHECK SYSTEM COMPONENT STATUS

CHECK SYSTEM COMPONENT STATUS

- ▶ For the Administrator, the anSwitch provides a Component activity overview with information of the status, utilization, version, etc.

> Menu: System
> Sub-Menu: Components

- ▶ Check System Components status:
 - The component is active
 - The component is not operational working. It is in passive mode or set manually to barred.
 - The component is in failed status

- ▶ By clicking  additional information are available about the component.

Components		
AareSwitch Components		
	CallControl 1	1 call ● Active
	CallControl 2	1 call ● Active
	MediaControl 1	6 streams ● Active
	MediaControl 2	● Active
	SystemControl 1	● Active
	SystemControl 2	● Passive
	Portal 1	● Active
	Portal 2	● Active
	LoadBalancer 1	● Active
	LoadBalancer 2	● Passive
	DataBase 1	● Active
	DataBase 2	● Active

CallControl 2		● Active
Version	7.3.1	
Host	172.31.253.11	
Memory	0.22 GB of 0.50 GB used	
CPU Load	0%	
Barred	<input type="button" value="No"/>	

9 SYSTEM MONITORING & ALARMING

OVERVIEW BUILT IN MONITORING AND ALARMING

- ▶ The anSwitch has a built-in system monitoring and alarming based on the open source "Xymon Project".
- ▶ The system monitoring and alarming basic features are:
 - ▶ Web based user interface
 - ▶ Supervises:
 - ▶ the anSwitch V7 server/host internal states
 - ▶ the anSwitch V7 component states
 - ▶ the anSwitch V7 component log entries
 - ▶ the IP connectivity between the anSwitch V7 servers/hosts and important external devices of the VoIP system
 - ▶ Provides graphical trend overviews of the telephony service:
 - ▶ Call load
 - ▶ Device registration
 - ▶ Incoming SIP message flow
- ▶ Alarms by email if one of the defined alarm or error conditions is met.

OVERVIEW INTEGRATED SYSTEM MONITOR

- ▶ Access the system monitor main view:
http://IP_ADDRESS:6320/xymon/

Note

No login and authentication is needed.
→ Make sure that only authorized personnel is allowed to access this URL.

- ▶ What do the little red/yellow/green icons mean?

Color	Recently changed	Last change > 24 hours
Green: Status is OK		
Yellow: Warning		
Red: Critical		
Clear: No data		
Purple: No report		
Blue: Disabled		



OVERVIEW INTEGRATED SYSTEM MONITOR MAIN VIEW

- ▶ Which information is delivered by clicking a red/yellow/green icon?

VoIP telephony graphs

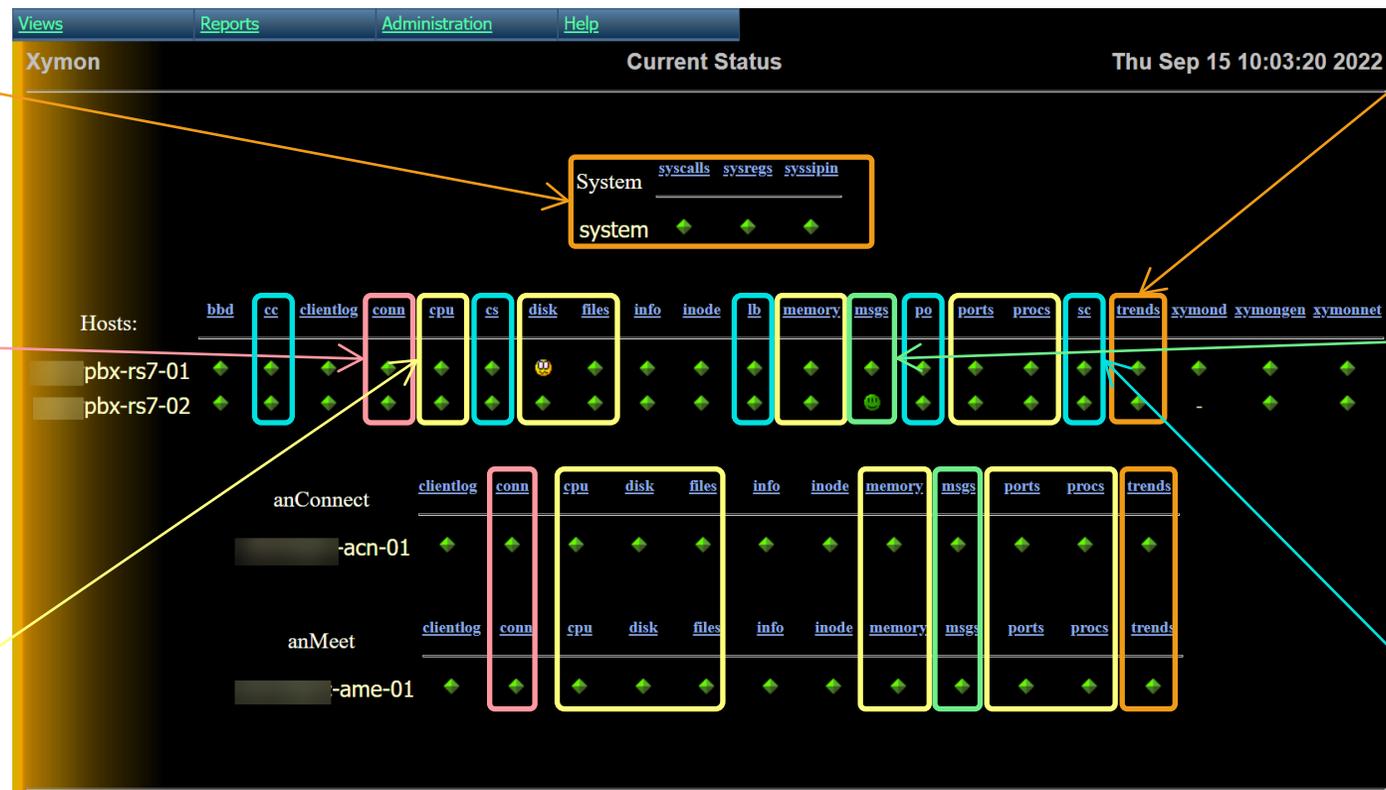
- ▶ syscalls Call load
- ▶ sysregs Device registration
- ▶ syssipin Incoming SIP messages

IP connectivity to devices

- ▶ conn Ping the device IP

Server/host

- ▶ cpu CPU load
- ▶ disk Disk usage
- ▶ files Usage of the file system
- ▶ memory Usage of memory
- ▶ ports Usage of the IP ports
- ▶ procs Status or OS processes



Collection of graphs

- ▶ trends A collection of graphs that show trends

Critical errors

- ▶ msgs Monitors the log-files for critical errors of:
 - ▶ System logs
 - ▶ anSwitch V7 component logs

Monitor anSwitch V7 containers

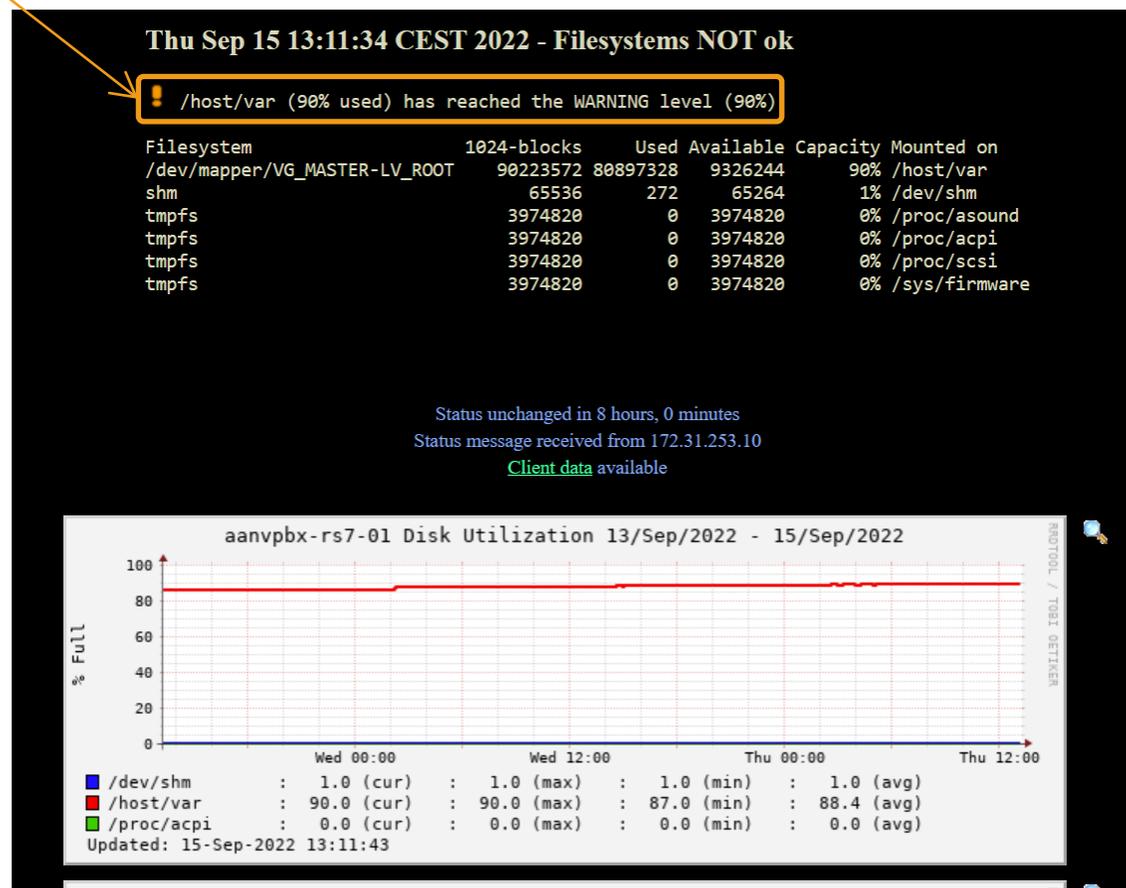
- ▶ cc, cs, lb, po, sc Monitor the containers of the anSwitch V7 components

ACCESSING THE ERROR INFORMATION

▶ Accessing the error information

> Click the icon of interest that indicates a problem

▶ Study the information and act



ACCESSING THE HISTORY LOG OF A SUPERVISED ENTITY

▶ Accessing the history log of a supervised entity

> Click the icon of interest

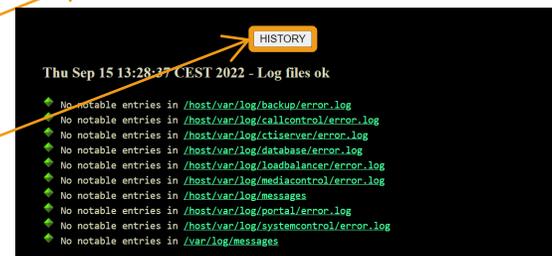
▶ The messages page of the entity pops up

> Click the button: History

▶ The history page of the entity pops up

> Click the row of the error of interest

▶ Study the information



INTERPRETATION OF ERROR MESSAGES

- ▶ Most error descriptions are easy to understand.
- ▶ **The following** system alert or error reports must be considered as VoIP system threatening issues
→ Address them immediately:
 - ▶ Server issues e.g., hard disk full, stopped processes
 - ▶ Linux service issues e.g., DB replication broken
 - ▶ IP connections lost
 - ▶ Fraud
 - ▶ Traffic shaper
- ▶ In order to estimate the extent of a problem for the VoIP system, it can be useful to examine the **trends in the VoIP telephony graphs**.
 - ▶ Collapsed registrations or connection numbers indicate large-scale failures
→ These must be addressed immediately.

VoIP telephony graphs

- ▶ syscalls Call load
- ▶ sysregs Device registration
- ▶ syssipin Incoming SIP messages



DISPLAY DURATION OF AN ERROR INDICATION

- ▶ A problem is repeatedly re-reported **every hour** (default) until it is solved or disappears.
 - ▶ The system monitor refreshes the error indication every 5 minutes. Then it removes the oldest solved error indication. So, it may last until all error indications are removed.

- ▶ Some server problems are reported via SNMP trap to the system monitor.

➔ A problem reported via SNMP traps is signaled **only 1 time!**

Note If you miss this 1 time, then the server may be in danger.

- ▶ System monitor Log, email or SMTP trap may contain the following information

```
"snmptrapd" "failure" "degraded"
```

CONFIGURATION OF SYSTEM ALARMING

- ▶ The system alarming configuration is done during the system provisioning:
 - ▶ It defines the email addresses to be informed
 - ▶ It defines the repetition of the email until the issue is over
 - ▶ It defines the severity which shall be informed:
 - ▶ **red**
 - ▶ Defined thresholds
 - ▶ Logging severity: FATAL, ERROR
 - ▶ **yellow**
 - ▶ Defined thresholds
 - ▶ Logging severity: WARN
 - ▶ **purple** No report from the supervised entity

- ▶ Example of an alarming configuration:

```
1 HOST=%.* EXGROUP=%.+
2 MAIL noc@customer.com REPEAT=60 COLOR=red,yellow,purple
3 MAIL supporter1@customer.com REPEAT=15 COLOR=red
```

Note

Depending on a maintenance contract between the customer and Aarenet the alarm is included in the Aarenet call duty organization.

10 CHECK PBX CALL ANALYTICS

CHECK PBX CALL ANALYTICS

- ▶ The anSwitch provides for each PBX a call analytics summary with information of e.g., number of calls, number of answered and declined, number of erroneous calls, average conversation time, etc.

> Menu: PBX Administrator
> Sub-Menu: Call Analytics

- ▶ Check for the desired information e.g.:
 - ▶ Abnormally low number of answered calls
 - ▶ High number of calls with errors
 - ▶ Abnormally short call durations
 - ▶ etc.

PBX Call Analytics PbxAarenet

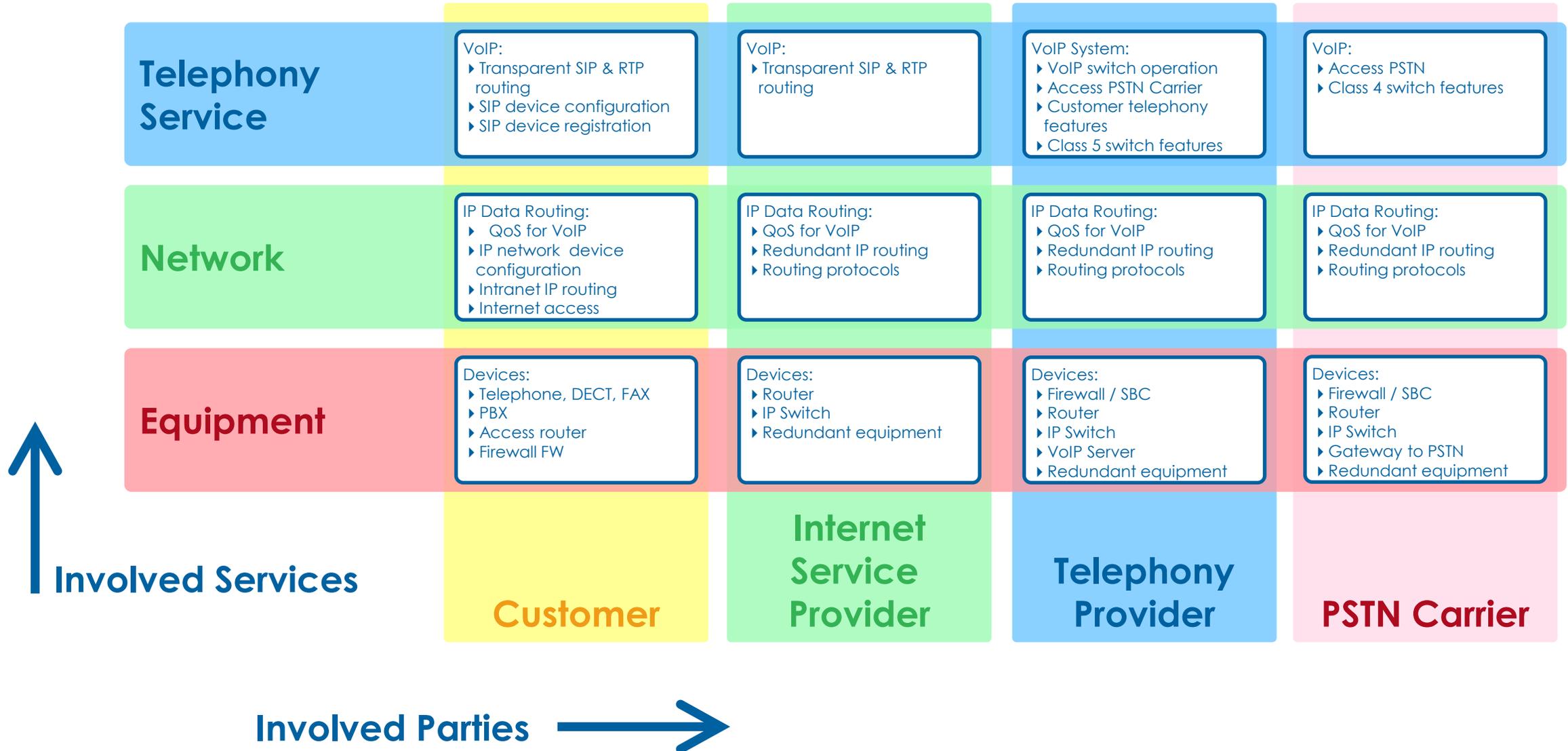
From 01.05.2021 To 19.05.2021

✓ Apply

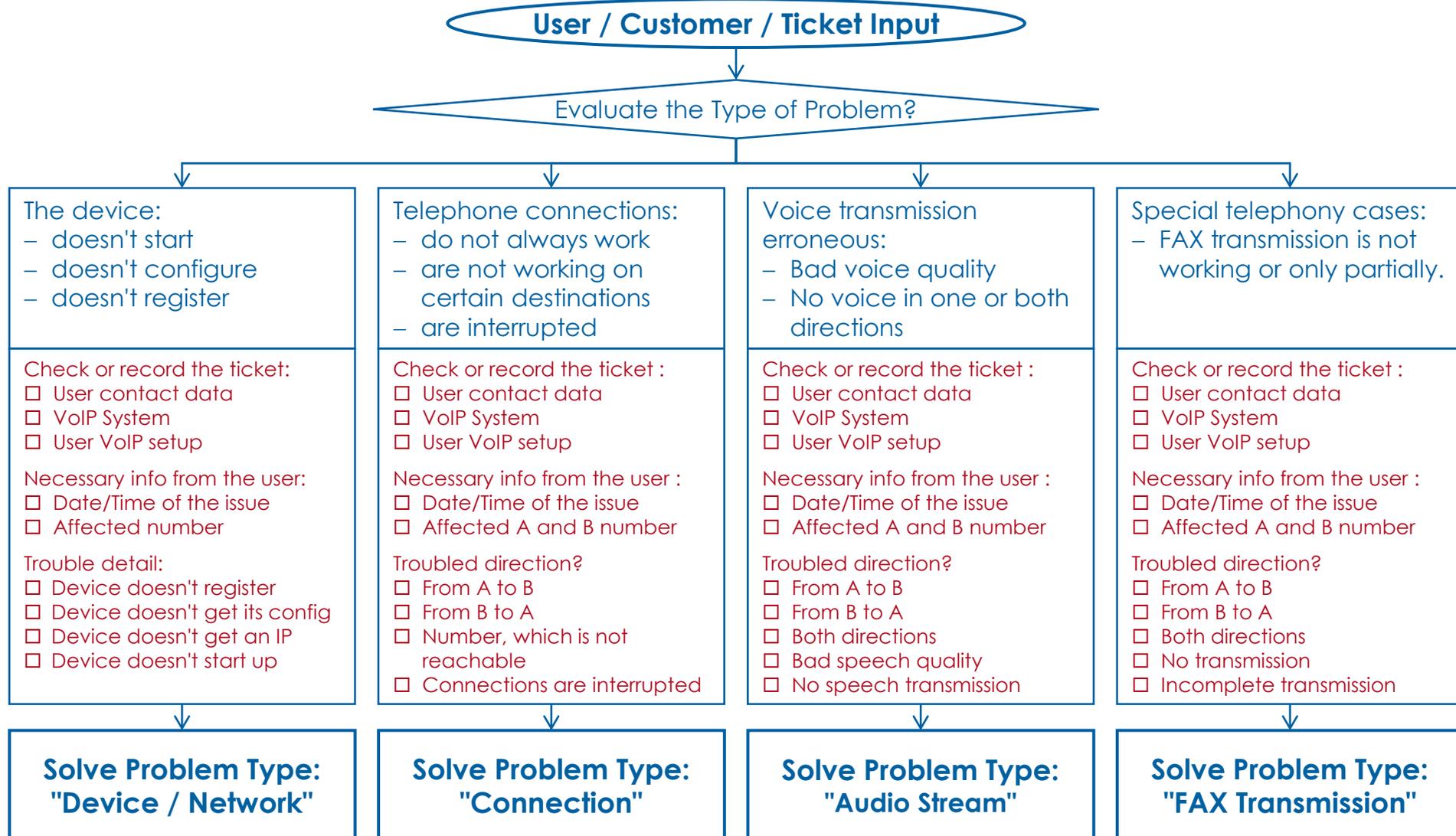
Incoming calls		Outgoing calls	
Number of calls	794	Number of calls	1031
Number of answered calls	643	Number of answered calls	750
Number of calls with a busy line	0	Number of calls with a busy line	82
Number of calls with no reply	130	Number of calls with no reply	162
Number of declined calls	14	Number of declined calls	24
Number of calls with errors	7	Number of calls with errors	13
Average conversation time	00:07:14	Average conversation time	00:06:07

11 EVALUATE THE PROBLEM TYPE

SOMEWHERE IN THE "SUPPORT MATRIX" LIES THE PROBLEM



EVALUATE THE PROBLEM TYPE



12 PROBLEM TYPE: "DEVICE / NETWORK"

PROBLEM TYPE: "DEVICE / NETWORK" CHECK THE REGISTRATION

- ▶ Check the registration of the phone number in the Portal!
 - ▶ If the registration exists, it can be assumed that:
 - ▶ The terminal is working
 - ▶ The IP transmission works

- ➔ Continue with "Problem Type: Connection"

PROBLEM TYPE: "DEVICE / NETWORK" CHECK THE REGISTRATION

2. Use the Portal menu "Log" for finding any hint about erroneous registrations from this SIP phone in the Log types:
 - ▶ CallControl
 - ▶ Support

- a. Set reasonable "From" date/time values
- b. Set the filter "Contains Regex Pattern":
 - ▶ REGISTRATION
 - ▶ Phone number of the SIP Phone

PROBLEM TYPE: "DEVICE / NETWORK" CHECK THE SIP PHONE

3. Investigate whether the SIP phone at the user's premises is functional:

- Check if the power cable is connected and ok?
 - ➔ Replace the power cable if necessary!

- Check if the phones Ethernet patch cable is connected and ok?
 - Connected and plugged into the correct socket?
 - ➔ Replace the Ethernet patch if necessary!

- Check if the SIP phone works?
 - Are LEDs and/or the display "alive"?
 - Light the LED? Do they flash an "error code"?
 - Is there an error text displayed on the display?
 - ➔ If necessary, replace the SIP phone for testing!

PROBLEM TYPE: "DEVICE / NETWORK"

CHECK IP CONNECTIVITY

4. Investigate whether the Intranet and Internet access works at the user's premises:
 - Check if the user has Internet access e.g., from a PC next to the SIP phone. For a reliable statement, both should be connected to the same IP switch.
 - ➔ If not, do the next checks.
 - Check if the Intranet LAN devices e.g., access router, firewall, IP switches work?
 - Are LEDs and/or the display "alive"?
 - Light the LED? Do they flash an "error code"?
 - Is there an error text displayed on the display?
 - Check the FW configuration for unnecessary SIP ALG or helpers, blocking policies
 - ➔ If necessary, replace the devices for testing!
 - Check if the Internet access device works?
 - Internet connection device (DSL, cable modem, FTTH, etc.)
 - ➔ If not, contact the support of the Internet provider, the equipment supplier, etc.

13 PROBLEM TYPE: "CONNECTION"

PROBLEM TYPE: "CONNECTION"

The main objective of this problem type is to determine why:

- I. Incoming calls are not working
- II. Outgoing calls are not working
- III. Calls are interrupted after a certain time

PROBLEM TYPE: GENERAL "CONNECTION PROBLEM" CHECKS

- ▶ Check the operational configuration in the Portal:
 - a. Check the PBX OrgUnit:
 - Is there a blocking Public Call Permission responsible?
 - b. Check the PBX Dashboard:
 - Is there the limit of external calls reached?
 - c. Check the PBX Settings:
 - Is the PBX still active (date valid)?
 - d. Check the number:
 - Is the number available?

PROBLEM TYPE: "NO INCOMING CONNECTION"

Search for the claimed connection(s) in the Portal UI "Support Log" and/or "Trace".

- If the connection can no longer be found, the user must be asked to re-do the connection attempt. Then these logs can be examined.
1. Find the connection in the Portal UI menu "Calls" the requested call:
 - a. Extract the connections log entries in the "Support Log" with the "Call-ID" as text filter.
 - b. Extract the SIP trace of this call directly out of the CDR by clicking the [Download SIP Trace] button.

PROBLEM TYPE: "NO INCOMING CONNECTION"

2. What was received from the PSTN concerning this failed call?
 - ▶ Check if there was an incoming call from the PSTN?
 - Was there an incoming INVITE from the PSTN with the B number?
 - ➔ If no INVITE was received:
 - Check with the PSTN provider, why this number is not routed to this anSwitch.
 - ▶ Check if the dialed B number is known on the anSwitch V7?
 - Is the dialed B number correct and active on this anSwitch V7?

PROBLEM TYPE: "NO INCOMING CONNECTION"

3. Are there entries in the logs that indicate a problem with a Ruleset, TopStop, call forward, etc.?
 - ▶ Check the "Support Log":
 - a. Is the phone correctly registered?
 - b. The called B number cannot be found on the Aarenet VoIP Switch?
 - c. A blocking Ruleset active?
 - d. The B number is rewritten incorrectly by a Ruleset and therefore no longer routable.

 - ▶ Check the "SIP Trace":
 - a. Is the INVITE sent toward the phone?
 - b. Did the phone send back any SIP message?

PROBLEM TYPE: "NO OUTGOING CONNECTION"

- ▶ Check in the Call List if the call was routed in the anSwitch to the PSTN or OnNet destination:
 - a. Check the dialed B number:
 - Is the dialed B number correct public PSTN number?
 - Is the dialed B number a OnNet public PSTN number?
 - b. Check the PBX Settings of A:
 - Is the TopStop of the PBX reached?
 - c. Check in the Extension Settings of A:
 - Is there a blocking Public Call Permission responsible?
 - d. If B is a OnNet destination, check in its Extension Features:
 - Are the assigned phones registered?

PROBLEM TYPE: "NO OUTGOING CONNECTION"

e. Check the Trace:

- Was there an incoming INVITE with the B number from the A user?
 - ➔ If no INVITE was received:
 - ▶ Check with the A user, why this call did not work:
 - ▶ Phone defect?
 - ▶ Phone not correct connected?
 - ▶ Phone not registered → is it correct configured?
 - ▶ No internet access?

- Was there an INVITE from the anSwitch to the PSTN or OnNet destination?
 - ▶ Is in this INVITE the B number still correct?
 - ▶ Was there any SIP cause response from the PSTN provider like:
 - ▶ 4xx: Failure responses from the B side
 - ▶ 6xx: No route was found in the routing table
- ➔ If no INVITE was sent:
 - ▶ Check the SIP cause response of the anSwitch
 - ▶ Check the Support Log with the call-ID of this call and search for any hints

OVERVIEW "INTERRUPTED CONNECTION"

Interrupted connections can have multiple reasons:

- I. Charge limitation by a TopStop
- II. Unintentional "hooking on" of the phone by a user
- III. Connection supervision by the phones (Session Timer)
- IV. Media stream supervision by any device in the telephone system e.g., no RTP packets during 30sec
- V. Phone defect

➔ I. - II. are the most common reasons.

PROBLEM TYPE: "INTERRUPTED CONNECTION"

- I. Check interruption by TopStop:
 - a. Check the PBX Settings of A:
 - Is the TopStop of the PBX reached?
- II. Check for unintended "hook on" of a user:
 - a. Search the call in the PBX Calls list > Select Show Call Stats
 - b. Check in the Technical Info:
 - ▶ SIP Status
 - ▶ Cause of Release(Q850)

For details on the SIP response codes, see:

http://en.wikipedia.org/wiki/List_of_SIP_response_codes

PROBLEM TYPE: "INTERRUPTED CONNECTION"

- III. Check the call supervision by the SIP Session Timer:
 - a. Search the call in the PBX Calls list > Select Show Call Stats
 - b. Check in the Technical Info:
 - ▶ SIP Status
 - ▶ Cause of Release(Q850)
 - c. Search the call in the PBX Calls list > Select Download SIP Trace
 - d. Analyze the trace for timed out "Session timers"
 - ▶ "Session Timer" within the dialog is expired without renewal.
 - ▶ It is typically renewed every 180 - 300sec via RE-INVITE
 - ▶ The renegotiated is initiated by the pre-negotiated side (refresher)

PROBLEM TYPE: "INTERRUPTED CONNECTION"

- IV. Check for RTP media problems if the release reason of the SIP trace points to the PSTN:
 - a. Search the call in the PBX Calls list > Select Show Call Stats
 - b. Check in the Quality Info for:
 - ▶ High packet loss

14 PROBLEM TYPE: "AUDIO STREAM"

AUDIO STREAM INTRODUCTION

Note

- ▶ In most cases, "Audio Stream" problems can only be found and solved by means of an exclusion procedure.
- ▶ It is paramount that the customer/user knows that audio stream problems are difficult to track down and to solve.
- ▶ It's nerve-wracking and it is time consuming.
- ▶ Solving audio stream 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.

AUDIO STREAM INTRODUCTION

The audio stream 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 of audio stream problems:

- ▶ **One-Way/No-Way Connection:**
There is no speech transmission in one or both directions from beginning of the connection.
- ▶ **Glitch Connection:**
There is speech transmission, but it is disturbed.

AUDIO STREAM PROBLEM CHARACTERISTICS

Characteristics of audio stream problems:

▶ One-Way/No-Way Connection:

- ▶ Silence in both directions
- ▶ Silence from A → B
- ▶ Silence from B → A

➔ Possible reason:

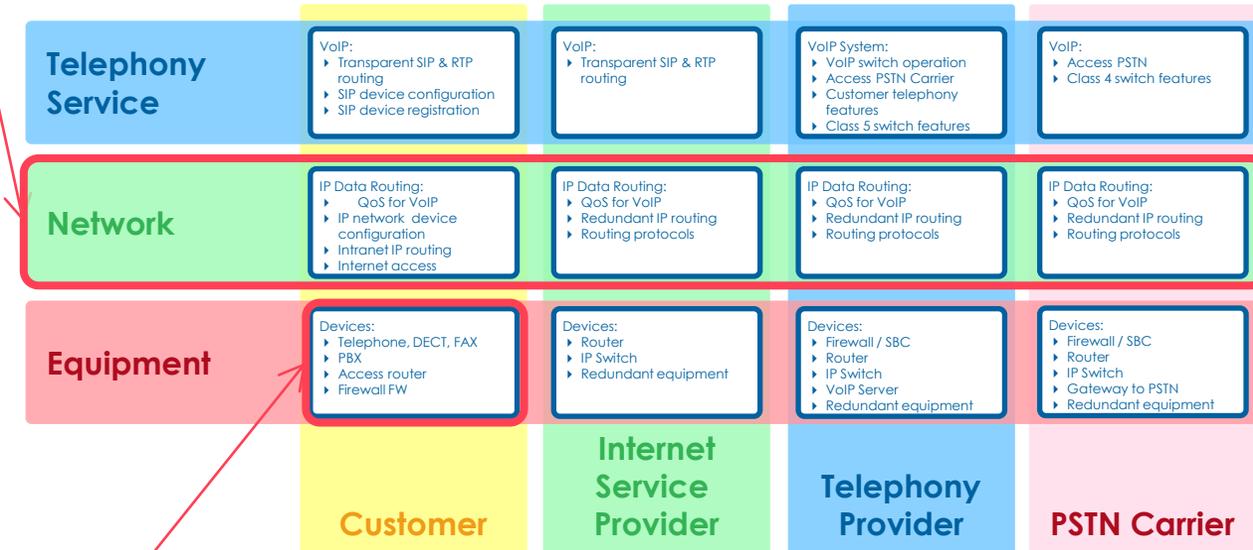
Mostly due to no or blocked RTP data transmission

▶ Glitch Connection:

- ▶ 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

AUDIO STREAM PROBLEM ZONES

The source of the audio stream problems are all too often somewhere in the data transmission "Data Transfer D" layer.



But sometimes they are surprisingly simple:

- ▶ The microphone or loudspeaker in the telephone handset defect
- ▶ Volume configuration in the telephone set wrong
- ▶ Telephone defect
- ▶ The company Intranet is not made ready for VoIP

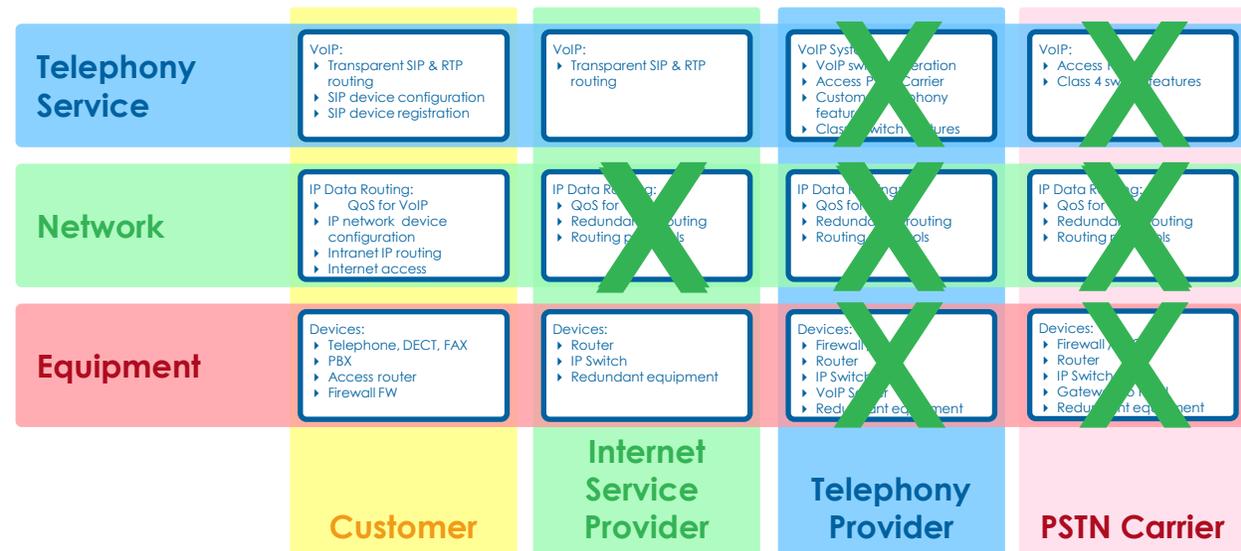
EXCLUSION OF AUDIO STREAM PROBLEM SOURCES

1. Make sure that only the complaining user is affected!

a. Check the "Big Picture"

→ See next page!

- ▶ If only this user is affected, then the crossings with the **X** are no longer suspicious.



Note

Consider that there could be a problem on the B side either:

- ▶ B PSTN provider
- ▶ B user

"CHECK THE BIG PICTURE"

2. Are a lot of users affected?

- ▶ Lot of user complains?
- ▶ Check the System "trends":
 - ▶ Is there a remarkable drop of calls/registrations?

→ If yes, then wake up the System Administrator!

3. Check where the affected calls are:

a. Are all calls affected?

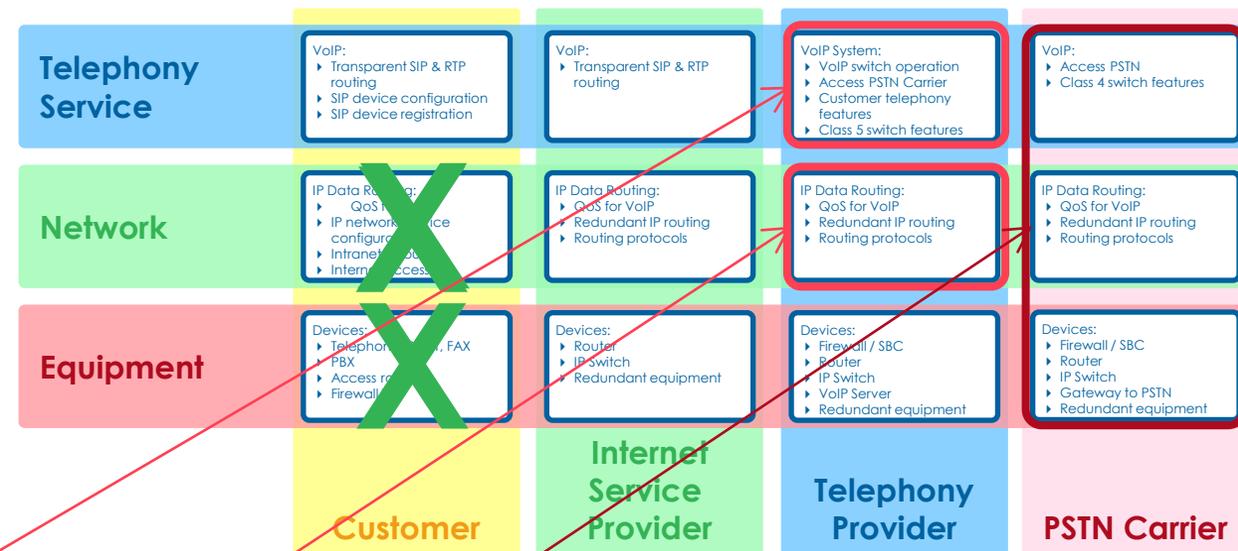
- ▶ Are the FW, L2 IP switch, ok?
- ▶ Are the anSwitch servers, ok?
- ▶ Are all anSwitch components, ok?

b. Are only OnNet calls affected?

- ▶ If only OnNet, then all or just out of a certain IP subnet?

c. Are only PSTN calls affected?

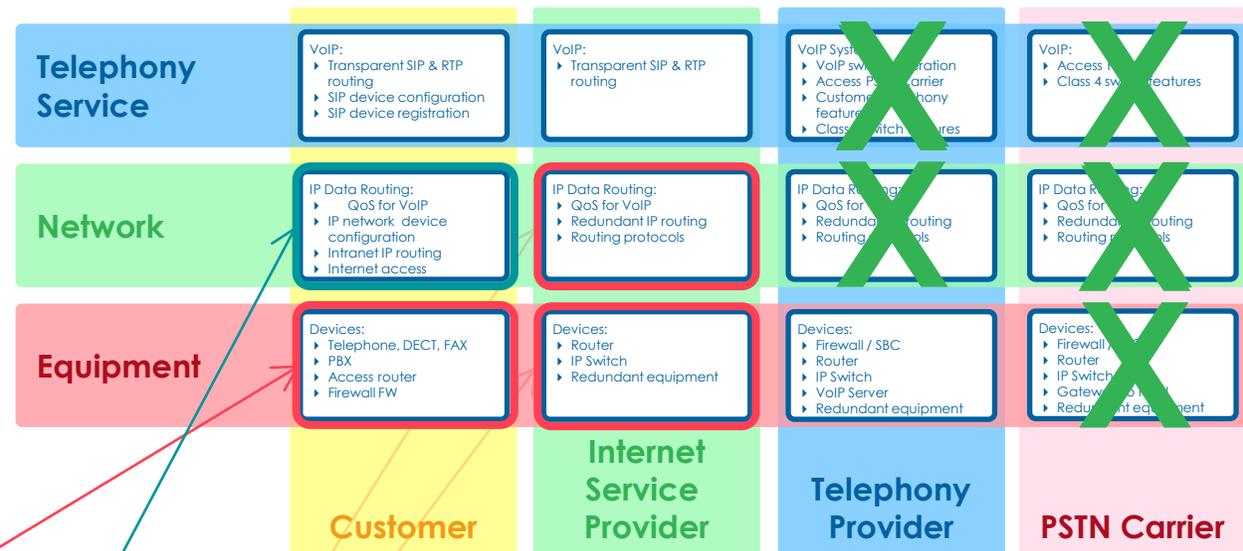
- ▶ Is the IT connectivity to the PSTN Gateway, ok?
- ▶ Is the PSTN Gateway/SIP-trunk, ok?
- ▶ Is the PSTN carrier, ok?



INTERVIEW THE COMPLAINING USER

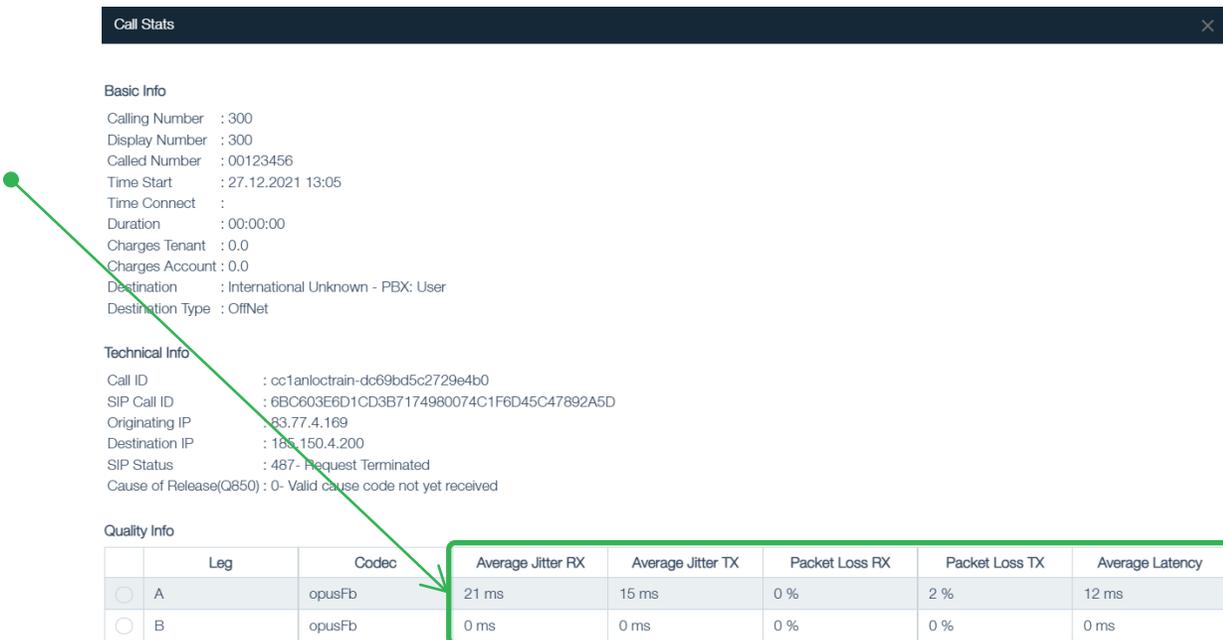
Interview the user:

- Which type of audio stream problem?
 - No/One-Way
 - Glitch
 - Affected side
- Problem with all B peers or just with one?
 - ➔ If only one, then the B side could cause the problem!
- Check if there could be a problem with the A SIP phone.
- Check if there were any changes in the user's Intranet access:
 - FW: policies, SIP ALG, SIP Helper active?
 - NAT timeout?
- Check if there were any changes in the user's Internet access.
 - Is the Internet access running?



CHECK THE CALL STATISTICS OF THE CALL

- ▶ Check the call statistic for suspicious values:
 - ▶ Heavy packet loss
 - ▶ Heavy packet jitter
- ▶ Check whether a connection leg is specifically eye-catching
 - ➔ Go on with your search in this direction!



Call Stats

Basic Info

Calling Number : 300
Display Number : 300
Called Number : 00123456
Time Start : 27.12.2021 13:05
Time Connect :
Duration : 00:00:00
Charges Tenant : 0.0
Charges Account : 0.0
Destination : International Unknown - PBX: User
Destination Type : OffNet

Technical Info

Call ID : cc1anloctrain-dc69bd5c2729e4b0
SIP Call ID : 6BC603E6D1CD3B7174980074C1F6D45C47892A5D
Originating IP : 83.77.4.169
Destination IP : 185.150.4.200
SIP Status : 487- Request Terminated
Cause of Release(Q850) : 0- Valid cause code not yet received

Quality Info

	Leg	Codec	Average Jitter RX	Average Jitter TX	Packet Loss RX	Packet Loss TX	Average Latency
<input type="radio"/>	A	opusFb	21 ms	15 ms	0 %	2 %	12 ms
<input type="radio"/>	B	opusFb	0 ms	0 ms	0 %	0 %	0 ms

15 PROBLEM TYPE: "FAX TRANSMISSION"

PROBLEM TYPE: "FAX TRANSMISSION"

- ▶ The reason of the most Fax transmission problems lie in the "analogue" versus "packetized" transfer of the data.
- ▶ Fax bases on analogue modem technology and relies on precise and continuous modulated frequency transmission.
- ▶ And just the SIP based packetized transmission technology breaks the required "precise and continuous modulated frequency transmission" of the Fax service.

SOLUTION ATTEMPTS FOR "FAX TRANSMISSION" PROBLEMS

- ▶ With Fax problems you have the following possibilities to solve it:
 1. Change the FAX device configuration:
 - ▶ Reduce transmission rate to 14400 Baud or lower
 - ▶ Switch off ECM
 - ▶ Activate any existing VoIP transmission mechanism
 - ▶ If necessary, replace the FAX machine to test it.
 2. Change the codec type in the upstream SIP device usually an analogue terminal adapter ATA:
 - ▶ G.711: for in-band Fax transmission
 - ▶ T.38: for packetized out-band Fax transmission

Note

Every transcoding hampers the Fax transmission!

The experience shows that more than two transcoding points enhances the probability of erroneous Fax transmissions.

16 LOGGING ANSWITCH V7 SYSTEM CONFIGURATION

CONFIGURE THE LOGGING LEVEL PER COMPONENT TYPE

▶ Logging levels:

- ▶ All components have different logging levels by default.
- ▶ trace : Is the most verbose level
- ▶ debug :
- ▶ info :
- ▶ warn :
- ▶ error :
- ▶ fatal : Is the most silent level

1. Configure the valid logging level in file: /etc/aareswitch/*system.yaml

- ▶ Valid for a single component type, e.g. CallControl

```
1 components:  
2   cc*:  
3     logging:  
4       baseLogLevel: trace
```

2. Restart the component on all server/hosts

Warning

High logging levels produce heavy system load!

➔ After finishing logging on an enhanced logging level switch back to the default level.

LAST PAGE

Date	Doc-ID	Description	Changes
21.9.2021	training_as7_304_support_debugging_e05	New document published	
18.9.2023	training_as7_304_support_debugging_e13	V7.13: Support log offers default filters	Page: 22