VoIP Operators

From a Carrier Point of View

CHRISTINA SIDIROPOULOU

KTH Information and
Communication Technology

Degree project in
Communication Systems
Second level, 30.0 HEC
Stockholm, Sweden

VoIP Operators: From a Carrier Point of View

Christina Sidiropoulou
csid@kth.se

Supervisor and Examiner: Gerald Q. Maguire Jr.

School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden

Abstract

Voice over Internet Protocol (VoIP) is a service that has recently gained a lot of attention from the telecommunications (telecom) world since both Internet service providers (ISPs) and telecommunications operators have realized the important advantages that it can offer. Although traditional telephony is well established both in the telecom world and in our daily lives, VoIP is now competing with it by offering cost savings, simplicity, and introducing new ways of communicating. Internet service providers have already started deploying efficient VoIP services for their customers and carriers are transforming their network infrastructures in order to be able to accommodate the requirements of VoIP traffic.

There are a lot of essential factors that both providers and carriers have to take into consideration in order to efficiently build and operate VoIP technologies. Proper service planning and well-established monitoring and troubleshooting procedures are vital for successful VoIP service. This thesis focuses on commercial VoIP implementation at the carrier's side and investigates how a carrier can efficiently maintain and troubleshoot their VoIP infrastructure so as to comply with the Service Level Agreements (SLAs) they have signed with their customers (ISP providers), as well as analyses proactive actions that can be taken for minimizing the resources required for customer support. As an outcome, this thesis presents efficient ways of network planning and monitoring, as well as it provides conclusions regarding what are the efficient methods for troubleshooting the carrier's VoIP products in both technical and organizational level.

Keywords: VoIP, fault management, SBC, SIP, carrier, troubleshooting, telecom

Sammanfattning

Röst över Internet Protokoll (VoIP) är en tjänst som nyligen har fått ökad uppmärksamhet inom telekommunikations (telecom) branschen eftersom att både Internetleverantörer (ISPs) och telecom operatörer har insett vilka fördelar som tjänsten erbjuder. Även om traditionell telefoni är väl etablerad i både telecombranschen och vår vardag, så kan VoIP konkurrera genom att erbjuda kostnadsbesparingar, förenkling, och introducera nya sätt att kommunicera på. IP leverantörer har redan påbörjat lansering av effektiva VoIP tjänster till sina kunder och telecom carriers bygger om sin nätverksstruktur för att möta kraven av VoIP traffik.

Det finns många faktorer att bejaka för både IP leverantörer och telecom carriers för att effektivt bygga och driva VoIP nätverk. Noggrann produktplanering och väletablerad övervakning samt felsökningsprocedurer är en vital del i en framgångsrik VoIP tjänst. Denna avhandling fokuserar på VoIP implementering hos en telecom carrier och hur en telecom carrier effektivt kan underhålla och felsöka VoIP infrastruktur för att möta de servicenivåavtal de har skrivit med sina kunder (IP leverantörer), samt analysera det förebyggande åtgärder som kan tas för att minimera de resurser som behövs till kundtjänst. Denna avhandling presenteras effektiva tillvägagångssätt för planering och övervakning samt erbjuder effektiva, teknisk och organisationella metoder för felsökning av en telecom carriers VoIP produkter.

Nyckelord: VoIP, felhantering SBC, SIP, carrier, felsökning, telecom

Acknowledgements

I would like to thank my supervisor Prof. Gerald Q. Maguire Jr. for guiding and assisting me from the beginning of my thesis till its completion, as well as for being always available and willing to help me. His valuable feedback, guidelines, and ideas were vital for the continuation and completion of this project.

Furthermore, I would like to thank my industrial advisor Tommy Hjälm for his help and guidance during the whole duration of the thesis work. His useful inputs and advices were a major contribution in this project.

In addition, I would like to thank Anna Demchenko for being the initiator of this project, as well as for her co-operation and continuous interest on my thesis work and progress.

Finally, I would like to thank all the people who supported me and encouraged me all the way along this entire project.

Christina Sidiropoulou,

Stockholm, 2011-07-29

Table of Contents

Abstract i
Sammanfattning ii
Acknowledgements iii
Table of Contents iv
List of Figures vi
List of Tables vii
List of Acronyms and Abbreviations viii
1. Introduction 1
2. Background 3
   2.1. VoIP overview 3
   2.2. VoIP signalling and media functions 3
      2.2.1. Signalling protocols 3
      2.2.2. Media protocols 7
      2.2.3. Voice encoding 9
   2.3. PSTN overview 9
      2.3.1. PSTN network infrastructure 10
      2.3.2. Signalling and voice functions in PSTN 10
   2.4. Interworking between IP and PSTN networks 11
   2.5. VoIP network components 12
   2.6. VoIP routing and traffic engineering 13
   2.7. Fault management in the telecom industry 14
3. VoIP Planning 16
   3.1. Example VoIP product description 16
      3.1.1. Customer is directly connected to the access network (product A) 16
      3.1.2. Customer is connected through public Internet to the access network (product B)17
   3.2. VoIP monitoring and maintenance recommendations 18
      3.2.1. Role of the SBC 18
      3.2.2. Call Admission Control (CAC) in VoIP 20
      3.2.3. Monitoring techniques in VoIP 23
4. VoIP troubleshooting analysis 27
   4.1. VoIP technical troubleshooting 28
      4.1.1. Packet loss 28
      4.1.2. Delay 29
      4.1.3. Jitter 30
      4.1.4. Sequence errors 31
      4.1.5. CODEC distortion 32
      4.1.6. Echo 32
      4.1.7. Connectivity loss 32
      4.1.8. Protocol error 33
      4.1.9. One-way or no-way audio 35
      4.1.10. End-points problems 37
      4.1.11. Voice related problems 38
      4.1.12. VoIP technical cause analysis diagrams 39
   4.2. VoIP organizational troubleshooting procedures within the company 44
      4.2.1. Organizational problem definition 44
      4.2.2. Improvement recommendations 45
   4.3. Problem information collection 47

5. Conclusions and future work 51
5.1. Efficient VoIP technical troubleshooting 51
5.1.1. Troubleshooting product A 51
5.1.2. Troubleshooting product B 52
5.2. Efficient VoIP organizational troubleshooting 52
5.3. General conclusion 54
5.4. Future work 54
Bibliography 56
Appendix 59

List of Figures

Figure 1: VoIP end-to-end network implementation example [3] 1
Figure 2: SIP session establishment [18] 7
Figure 3: RTP packet format [26] 8
Figure 4: Packetization of audio stream [7] 9
Figure 5: ISUP call flow [40] 11
Figure 6: Gateway architecture [22] 11
Figure 7: ISUP-SIP call flow [22] 12
Figure 8: Fault handling procedures within telecom industry 14
Figure 9: Customer is directly connected to the access network (product A) 17
Figure 10: Customer is connected through public Internet to the access network (product B) 18
Figure 11: The function of the SBC [25] 19
Figure 12: VoIP G.711 frame [35] 22
Figure 13: VoIP G.729 frame [35] 22
Figure 14: Wireshark VoIP capture filter example 26
Figure 15: Jitter description [17] 31
Figure 16: Jitter buffering and packet loss compensation [1] 31
Figure 17: Firewall problem in VoIP [20] 37
Figure 18: NAT implementation in a VoIP session [20] 37
Figure 19: "Call not established" diagram [Spread sheet template: http://www.vertex42.com/] 41
Figure 20: "One-way or no-way audio" diagram [Spread sheet template: http://www.vertex42.com/] 42
Figure 21: "Call quality degradation" diagram [Spread sheet template: http://www.vertex42.com/] 43
Figure 22: Diagram of escalations and resources 45
Figure 23: Improved diagram of escalations and resources 47

List of Tables

Table 1: SIP requests examples 4
Table 2: SIP responses categories 5
Table 3: SIP/SDP sample request message format 5
Table 4: CODECs [35] 9
Table 5: SBC alarms 23
Table 6: Recommendation G.114 Delay Specifications [17] 29
Table 7: SIP error response codes [18] 34
Table 8: VoIP symptom categories 39
Table 9: VoIP cause categories 40

List of Acronyms and Abbreviations

Acronym	**Description**
ACM	Address Complete Message
ANM	Answer Message
ARP	Address Resolution Protocol
B2BUA	Back To Back User Agent
BGP	Border Gateway Protocol
CAC	Call Admission Control
CC	Customer Care
CIC	Circuit Identification Code
CoS	Class of Service
cRTP	compressed RTP
CSRC	Contributing Source identifier
DiffServ	Differentiated services
DoS	Denial of Service
DPC	Destination Point Code
FCS	Frame Check Sequence
IAM	Initial Address Message
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IntServ	Integrated Services
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MCU	Multipoint Control Units
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MTP	Message Transfer Part
NAT	Network Adress Translation
NOC	Network Operation Centre
NUP	National User Part
OPC	Originating Point Code
OSI	Open Systems Interconnection
PLC	Packet Loss Concealment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Registration, Admission, and Status
REL	Release
RLC	Release complete
RTCP	Real-time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controllers
SCCP	Signalling Connection Control Part
SDP	Session Description Protocol
SG	Signalling Gateway

SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SS7	Signalling System No. 7
SSRC	Synchronization Source identifier
TDM	Time Division Multiplexing
TT	Trouble Ticket
TUP	Telephone User Part
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

1. Introduction

Voice over IP (VoIP) emerged many years ago. However, it recently has become an alternative to the traditional Public Switched Telephony Network systems (PSTN). In addition to basic conversational voice, VoIP also allows the development of value-added applications, as well as differentiation of the services offered to users. Service providers are now realizing the importance of the new opportunities that VoIP can offer: reduced expenditures, increased revenue, and the ability to offer a wide range of new services to their customers. Traditional voice and IP wholesale carriers are also a part of this development, since they are starting to offer access network and backbone solutions specifically prepared and designed for carrying VoIP traffic, by taking advantage of their existing infrastructures and network capabilities.

When it comes to wholesale carriers, VoIP has become an interconnection solution for their customers (who are IP and service providers) by means of network infrastructure provisioning and connection solutions to a VoIP platform. This interconnection can have a variety of forms, such as IP-to-PSTN, PSTN-to-IP, and IP-to-IP. In order to achieve this, carriers must develop and design a network platform that includes the necessary VoIP network components and is suitable for carrying prioritised voice traffic. This requires implementing appropriate routing policies, selecting suitable protocol implementations, ensuring the required Quality of Service (QoS), network reliability, and security.

Figure 1 depicts an example of a VoIP end-to-end network deployment between multiple providers. In this figure, the IP core (backbone) network is a fully managed carrier network that has VoIP capabilities and offers interconnection to both IP & PSTN providers and to its own PSTN infrastructure. The access network is usually provided by a service or network provider that offers VoIP services to end customers (in the figure this is labelled as the subscriber network). Each party in such an implementation has separate requirements and responsibilities towards both their own infrastructure and the neighbouring parties (which can be either customers or peers - the later are indicated in the figure as "Peering Network").

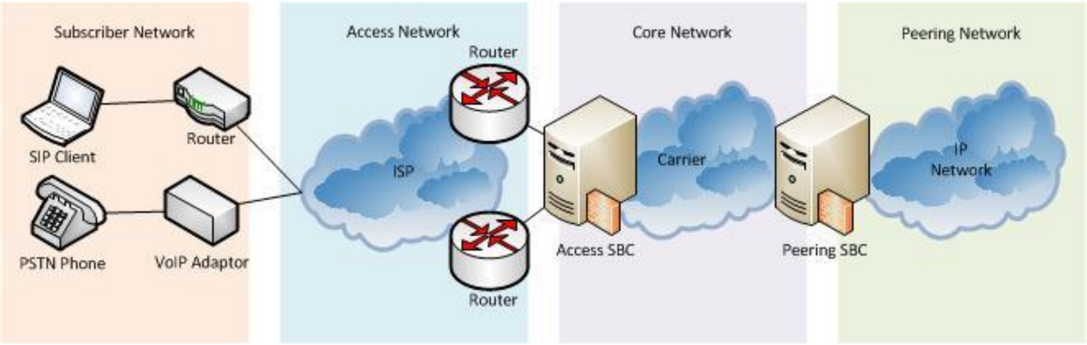


Figure 1: VoIP end-to-end network implementation example [3]

Apart from product planning, carriers must maintain their network infrastructure and increase their productivity by using appropriate monitoring and troubleshooting methods and procedures. Monitoring properly and troubleshooting efficiently a VoIP network infrastructure are difficult and demanding tasks. There are several steps in this procedure which need to be analysed in depth and followed carefully. This thesis analyses those steps and investigates VoIP planning, monitoring, and troubleshooting possibilities of wholesale carriers. Specifically, the case study of this thesis regards a carrier company that provides wholesale VoIP interconnection products to Internet Service Providers (ISPs). In this way, the providers can send voice traffic to the PSTN destinations offered by the carrier. The analysis has been divided into three main parts.

The first part of the investigation describes VoIP planning guidelines for a wholesale carrier regarding monitoring and alarm procedures. This includes an overview of VoIP implementation planning for a carrier’s network taking into consideration alarm and monitoring procedures in order to facilitate proper maintenance of the service and efficient ways of troubleshooting. As an example, a case study of a wholesale carrier is described and planning recommendations are made.

The second part is a detailed analysis of VoIP technical troubleshooting based on existing literature and market research, as well as real experiences in the industry. The analysis is technically-oriented and describes the potential problems and faults that can appear in a VoIP service and network implementation. This part includes a cause analysis of common and potential problems in VoIP, in the form of cause and effect diagrams [24], which can be used as a guide for support personnel in the company when troubleshooting a VoIP issue reported by a customer.

The third part concerns a survey and review of how to efficiently troubleshoot a VoIP issue internally in the carrier. Specifically, it analyses which parties should be responsible for fault resolution according to specific problem cases and how to handle trouble tickets internally. Additionally, this part investigates possible service models and fault management procedures that the company should use in order to properly provide customer support and comply with the Service Level Agreements (SLAs). Finally, as a last step, the interaction between the company and the customer is investigated. For efficient and rapid troubleshooting, it is of great importance to collect as much knowledge about the problem reported as possible. Therefore, this final part investigates the questions that the company should ask the customer in order to obtain all the information necessary for efficient troubleshooting.

2. Background

This chapter provides an overview of the VoIP technologies, concepts, and other industry information that are considered as important background for the understanding of this thesis. Sections 2.1, 2.2, 2.3 describe the VoIP network components, protocols and functions. Section 2.4 and 2.5 describes the PSTN network infrastructure and its interconnection with the IP network. Section 2.6 presents VoIP routing and traffic engineering procedures. Finally section 2.7 outlines fault management procedures within the telecom industry.

2.1. VoIP overview

VoIP is a technology which allows voice services to be transmitted over IP networks, for example telephony, conferencing, voice instant messaging, fax, etc. The voice data can travel through different networks by being converted from analogue signals to digital packets and vice versa. For the call establishment, maintenance, and termination, signalling protocols are used and translation between the different types of protocols is needed. After a call is established, media protocols are used in order to transport the actual voice data in the network between the end-users via the connection established by the signalling protocols.

The users' devices can be either IP devices or traditional PSTN devices depending on the access network they are connected to. There are different models of VoIP implementation, for example PSTN-IP-PSTN or IP-PSTN-IP. Due to the VoIP technology nature, different kinds of equipment and network devices are needed in order to successfully implement a VoIP solution: IP devices, PSTN devices, PSTN-IP & IP-PSTN interconnection devices, and network border devices.

For example, if a PSTN user wants initiate a call to an IP user, the call establishment starts by the use of a PSTN signalling protocol which is transformed to an IP signalling protocol in the network's border. In this way the IP signalling for the call establishment reaches the other party. After the signalling session is established, the two users can start exchanging media traffic which passes through the network's border where the voice data from the PSTN format is converted to the IP format (and vice versa for the traffic in the other direction). The following sections provide details and explanations of the VoIP implementation.

2.2. VoIP signalling and media functions

In VoIP technology, certain protocols have been introduced and developed in order to perform the signalling functions, the media transportation, as well as certain formats have been proposed for the media encoding. The following sections describe the most common signalling protocols, media protocols and formats used today in VoIP implementations.

2.2.1. Signalling protocols

The two most common signalling protocols used today for VoIP in the industry are H.323 and Session Initiation Protocol (SIP). This thesis focuses only on the SIP protocol; however this section will include a short description of the H.323 protocol.

2.2.1.1. SIP

SIP is a multimedia signalling protocol defined by the Internet Engineering Task Force (IETF) that establishes, controls, and terminates sessions between session end-points through exchanging messages in an ASCII-text-based format over packet networks.

SIP contains the following five logical entities [33]:

- **User Agent (UA)**. A User Agent constitutes the endpoint of the session and has two separate functionalities; it can act as User Agent Client (UAC) or User Agent Server (UAS). The UAC is responsible for initiating or terminating sessions through the exchange of request and response messages. The UAS functions as a server which serves requests and generates responses via contacting the user.
- **Proxy server**. A Proxy server acts as a representative of the clients by making requests and processing responses by acting as both a client and a server.
- **Registrar server**. A Registrar server is responsible for processing user REGISTER requests and updating its database regarding the location and contact information of the users.
- **Redirect server**. A Redirect server is responsible for returning SIP requests back to the calling users including information about the location of the called party (new SIP address if there is one or no address at all).
- **Back-To-Back User Agent (B2BUA)**. A B2BUA is an entity that acts as an intermediary in a SIP session. It is able to receive requests and process them as an UAS, alter the messages and regenerate the requests. It actively controls the session and processes requests and responses of the call endpoints.

SIP has two types of messages: requests (sent from the UAC to the UAS) and responses (sent from the UAS to the UAC). There are different kinds of requests depending on the call signalling function that needs to be implemented (for example initiate a session, release a session, cancel the process, register a user etc.) and there are also different types of responses depending on the reply that the recipient SIP device needs to provide back to the caller (for example if the request is successful, if there is an error in the process etc.). Table 1 and table 2 present request and response message types of SIP.

Table 1: SIP requests examples

Method	Description
INVITE	Initiates the session and requests the establishment of the call.
ACK	Confirms the final response of SIP INVITE.
BYE	Terminates the session.
CANCEL	Cancels the current signalling process, e.g. ringing.
OPTIONS	Negotiates the capabilities of the other session endpoint.
REGISTER	Requests the registration of the user’s location in the Registrar’s database.
INFO	Requests session information without modifying the current status.

Table 2: SIP responses categories

Classes	Description
1xx Provisional	Request is received and processing is ongoing.
2xx Success	The request was successfully received and accepted.
3xx Redirection	Further process is needed for this request.
4xx Client Error	Bad syntax request or inability to process it.
5xx Server Error	Server cannot process the request.
6xx Global Failure	Request cannot be processed by any server.

A SIP message consists of the following three parts:

- **Start line**. Every SIP message starts with a start line which contains the message type and protocol version. The message type indicates the method type in requests and the response code in responses. There are two types of start line: the request-line and the status-line. The request-line contains the Request-URI (SIP address of the called party) of the recipient of the call and the status-line contains a numerical status code and its corresponding textual description.
- **Header (one or more)**. The headers in a SIP message contain information regarding the message characteristics, such as the Via, Contact and Route fields. They always appear in the format <name>:<value>.
- **Message body (optional)**. The message body includes information regarding the session, for example sampling rates, codec, transport protocol, media type, etc. The protocol that is used for building the message body is the Session Description Protocol (SDP). SDP is used to define media sessions and describe their parameters. In VoIP, SDP is responsible for exchanging negotiation information between the endpoints, such as which CODEC to be used for the media stream (encoded voice), timings, and other capabilities [37]. This exchange of information is based on the Offer/Answer Model of SDP defined in RFC 3264 [39]. The SDP protocol is defined in RFC 4566 [38].

Table 3 depicts a sample SIP/SDP request message format including field descriptions [18] [33] [39]. This message is a SIP INVITE request from Bob to Alice including the SDP message body where the caller agent is negotiating the CODECs that it can support. The recipient agent should then send back a SIP 200 OK response message including the corresponding SIP headers and indicating the CODECs that is willing to accept.

Table 3: SIP/SDP sample request message format

Request Message Lines	Description
INVITE sip:bob@sweden.com SIP/2.0	Method type, the Request-URI, and the SIP version.
Via: SIP/2.0/UDP pc.usa.com; branch=z9hG4bK-5f874	Address for receiving responses.
Max-Forwards: 70	Threshold of the number of hops till the message reaches its destination.
To: Bob <sip:bob@sweden.com>	Message destination.
From: Alice <sip:alice@usa.com>;tag=1955498675	Message source (user that initiates the request) and a unique tag.

Call-ID: a244bc22d77432@pc.usa.com	Globally unique identification for this call.
CSeq: 366889 INVITE	Command sequence that identifies the message transaction.
Contact: <sip:alice@pc.usa.com>	Route towards the call originator.
Content-Type: application/sdp	Type of message body (SDP).
Content-Length: 182	Number of bytes in the message body.
	Blank line that indicates end of the SIP header and beginning of the message body.
v=0	Version of the SDP.
o=Bob 76655432789 766522981783 IN IP4 20.3.2.1	Owner (originator), session identifier, session version, address type (IP), and address (IP).
s=Call from Alice to Bob	Subject of the session.
t=0 0	Time of the session.
c=IN IP4 pc.usa.com	Connection information.
m=audio 3466 RTP/AVP 0 1 3	Media description: type (audio), port (3466), possible media formats that the caller agent can support.
a=rtpmap:0 PCMU/8000	First supported audio CODEC.
a=rtpmap:1 1016/8000	Second supported audio CODEC.
a=rtpmap:3 GSM/8000	Third supported audio CODEC.
m=video 5233 RTP/AVP 31 34	Media description: type (video), port (5233), possible media formats that the caller agent can support.
a=rtpmap:31 H261/90000	First supported video CODEC.
a=rtpmap:34 H263/90000	Second supported video CODEC.

Figure 2 depicts a simple SIP session establishment [18]. In this example, the two user agents establish and terminate a call. The caller sends a SIP INVITE to initiate the session and receives as a response 100/Trying which means that the request was accepted and is currently being processed. Subsequently, the caller receives the response 180/Ringing which indicates that the caller’s device is ringing. If the caller answers the call, then a response 200/OK will be received by the caller, who will in turn reply with an ACK confirming the call establishment action. Finally, when one call party wants to terminate the call, a SIP BYE will be generated and sent to the other party, who in turn will reply with an ACK confirming the call termination.

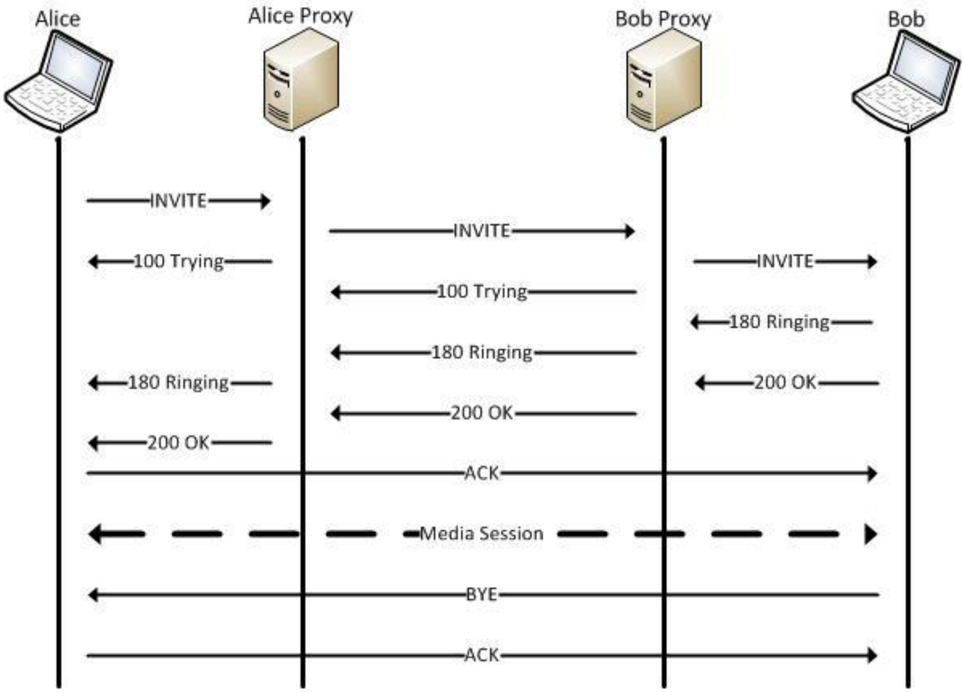


Figure 2: SIP session establishment [18]

2.2.1.2. H.323

H.323 is a family of protocols specified by the International Telecommunication Union (ITU) for multimedia conferencing services over packet networks. H.323 includes the following entities [31]:

- **Gateways**. They are responsible for the translation between the IP and the traditional PSTN network.
- **Gatekeepers**. They are responsible for providing call control services to the endpoints. Some of the functions that they perform are address translation, admission and bandwidth control.
- **Multipoint Control Units (MCU)**. They are the endpoints of the multimedia conference.

Protocols included in this family are [30]:

- **H.225 Call Signalling**. It is responsible for establishing connection between two H.323 endpoints or one H.323 endpoint and a H.323 gatekeeper through exchanging H.225 messages.
- **H.225 Registration, Admission, and Status (RAS)**. It is responsible for the establishment of a signalling channel between the H.323 endpoints and gatekeepers and performs functions such as admission control, bandwidth limitations, and registrations.
- **H.245 Control Signalling**. It is responsible for the operation of the H.323 endpoints by exchanging end-to-end control messages regarding endpoints' capabilities, channel of media streams.

2.2.2. Media protocols

The protocol that is used for the media traffic transport is the Real-time Transport Protocol (RTP). RTP defines a transport packet format for voice and video delivering over IP networks and is used for multimedia applications, such as VoIP, video conferencing, and media streaming.

RTP does not guarantee timely delivery and correct sequence of the packets and it does not recover for lost packets. These functions are the responsibility of the multimedia application; therefore depending on the application different packet handling procedures are used. The functions though that the RTP provides are: payload type identification, source identification, sequence numbering, and time stamping [36]. RFC 3550 [26] defines the RTP protocol functionality. Figure 3 shows the packet format of RTP.

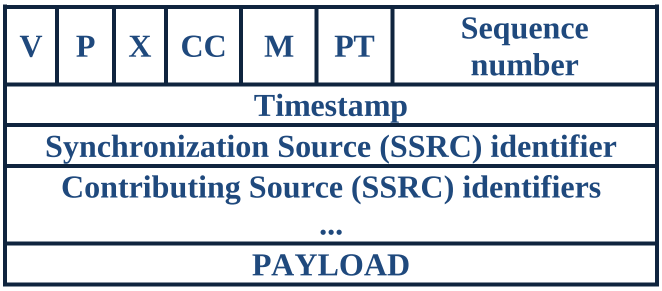

V
P
X
CC
M
PT
Sequence number
Timestamp
Synchronization Source (SSRC) identifier
Contributing Source (SSRC) identifiers
...
PAYLOAD

Figure 3: RTP packet format [26]

The RTP packet format contains the following fields [26]:

- **Version (V)**. This field contains the version of the RTP. Currently the latest version is 2.
- **Padding (P)**. If this bit is set, it means that the last one or two bytes of the payload are padding bits, used to fill in the payload. This can be used when the application wants to generate a specific payload length.
- **Extension (X)**. Indicates if there must be an extended header after the fixed RTP header.
- **CSRC count (CC)**: This field contains the number of the Contributing Source identifiers (CSRC) that follow the header.
- **Marker (M)**. This bit can be used as a general marker, for example indicating audio frame boundaries.
- **Payload Type (PT)**. This field indicates the payload format.
- **Sequence number**. This field increments by one with each new RTP packet and it is used by the receiver in order to identify non-sequential or missing packets (in the case of packet loss).
- **Timestamp**. The timestamp indicates the time instant of the first byte of the RTP packet sent.
- **Synchronization Source identifier (SSRC)**. The SSRC field is a random value that is generated in order to uniquely identify the source within a session.
- **Payload**. This is the payload of the packet carrying the actual voice data.

RTP generally works in conjunction with the Real-time Control Protocol (RTCP). RTCP provides monitoring and Quality of Service (QoS) statistics among other functions. It uses the same dynamic port range as RTP and it is usually assigned a port number one port number higher that the RTP port. The functions that RTCP offers are the following: QoS monitoring, congestion control, multiple streams synchronization, identification, and session scaling [36].

2.2.3. Voice encoding

Encoding is the process of transforming the analogue signals to digital packets and decoding is the process of transforming the packets back to their original analog form. In VoIP, the voice data are encoded and decoded in order to travel over IP networks. Figure 4 illustrates the encoding and encapsulation process for the audio stream in order to become a VoIP packet.

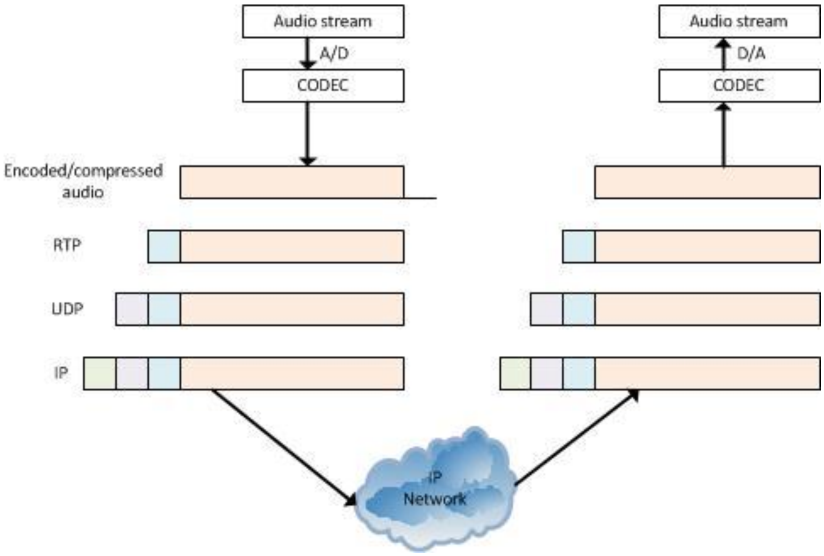


Figure 4: Packetization of audio stream [7]

CODECs are used to make a trade-off between bandwidth requirements and compression. Different CODECs provide different voice qualities and incur different delays. There are several standard voice CODECs, but the most common voice CODECs used are G.711 and G.729. G.711 provides good voice quality, but consumes more bandwidth than G.729. . While G.729 requires less bandwidth it provides lower voice quality. Some CODECs offer extra capabilities, such as silence suppression methods and packet loss concealment. Table 4 lists several CODECs that are in use today together with their descriptions.

Table 4: CODECs [35]

CODEC	Bandwidth (Kbps)	Sample period (ms)	Frame size (Bytes)
G.711 (PCM)	64	20	160
G.723.1A (ACELP)	5.3	30	20
G.723.1A (MP-MLQ)	6.4	30	24
G.726 (ADPCM)	32	20	80
G.728 (LD-CELP)	16	2.5	5
G.729A (CS-CELP)	8	10	10

2.3. PSTN overview

The PSTN has been the dominant network technology for wide area telephony services. The PSTN infrastructure uses different protocols, network components, and technologies than IP. VoIP requires the interconnection of these two different networks and therefore, it is important to develop appropriate and efficient methods in order to achieve this interconnection. Sections 2.3.1 and 2.3.2 provide an overview of the PSTN network and its protocols.

2.3.1. PSTN network infrastructure

The PSTN infrastructure is a circuit switched network that consists of 64Kbps digital channel circuits. The PSTN end devices are connected to the analogue access network through local subscriber loops. The voice is transmitted from the end device as a 3 kHz bandwidth analog signal and it is converted to a digital signal in the access switch to which the subscriber is connected. ISDN technology allows the end devices to connect through digital access lines to an ISDN switch in the PSTN network.

Time Division Multiplexing (TDM) technology is used for the voice traffic between switches in the PSTN. In TDM the time domain is divided into fixed length timeslots, where one timeslot is devoted to one call from the time the call is established until it is terminated.

For call routing in a PSTN network, telephony switches perform routing and call handling functions. These switches are identified uniquely by their signalling codes, which are used for the message exchange. . The Originating Point Code (OPC) is the call originator switch and the Destination Point Code (DPC) is the destination switch. The protocol suite defined for PSTN signalling is called Signalling System No. 7 (SS7) and it is described in the following section ((further details can be found in [15] [40]).

2.3.2. Signalling and voice functions in PSTN

SS7 is a protocol stack that is used in PSTN networks and it defines a protocol suite organised in a layered stack, responsible for telephony signalling functions. The lower layer is called the Message Transfer Part (MTP) and it contains three sub layers that function in a similar way to the first three layers of the International Standard Organization Open Systems Interconnection (OSI) protocol stack. Above the 3rd layer of MTP, the Signalling Connection Control Part (SCCP) provides additional routing functions by handling virtual circuits and connectionless services.

The SS7 protocol used for the voice signalling is called ISDN User Part (ISUP) and operates on top of MTP/SCCP. There are also signalling protocols older than ISUP included in the SS7 suite, these include: Telephone User Part (TUP) which can only be used for analog circuits and performs basic call set-up and tear-down, and National User Part (NUP) which allows variations of messages within a nation. ISUP is responsible for establishing, controlling, and terminating calls and can be used for both ISDN and non-ISDN calls. However, calls that are initiated and terminated in the same switch do not use ISUP signalling [40] [41].

Figure 5 depicts a simple ISUP call flow between two subscribers. When subscriber A wants to initiate a call, an Initial Address Message (IAM) is sent in order to reserve a circuit between switch A and the destination switch B. The IAM message includes the OPC, DPC, Circuit Identification Code (CIC) which uniquely identifies the timeslot reserved for the call, the dialled destination number, and other optional information. After receiving the IAM and determining that it serves the called party, switch B initiates ringing on the access line of subscriber B and sends back to A an Address Complete Message (ACM) notifying the caller that the called party has received the call. When subscriber B picks up their phone, switch B sends back to A an Answer Message (ANM). When subscriber A hangs up the phone, a Release (REL) message is sent in order to release the reserved circuit. Upon receiving the

REL, switch B releases the circuit, sets the status of the timeslot that it has been using to an idle state and replies back to switch A with a Release complete (RLC) message [40].

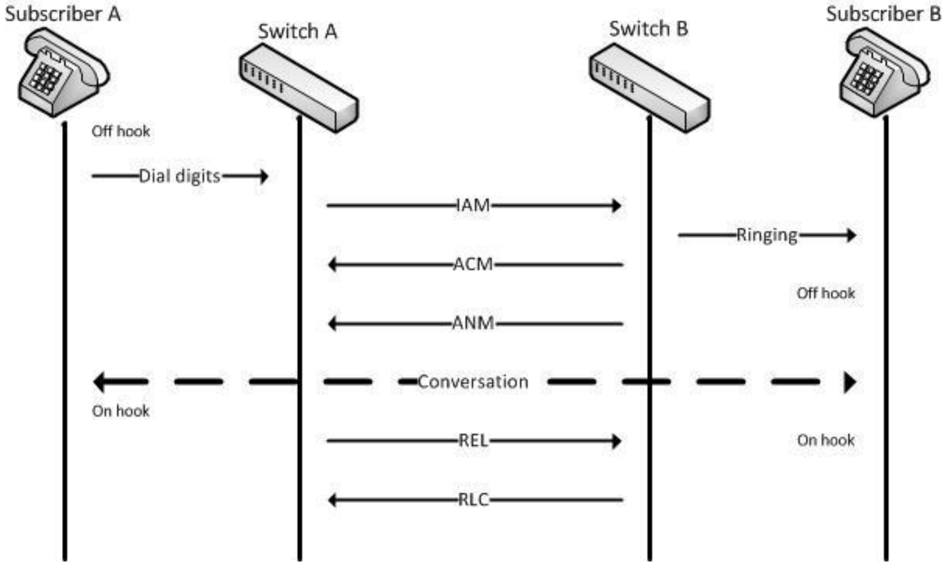


Figure 5: ISUP call flow [40]

2.4. **Interworking between IP and PSTN networks**

In PSTN networks, the signalling and media traffic is carried separately. In the case of ISDN networks signalling uses the D-channel and media uses the B-channel. In VoIP networks, the signalling and media traffic are handled by different protocols. For the transparent conversion between these two technologies, gateways are used that provide signalling translation of the D-channel data to the corresponding VoIP signalling protocols such as SIP and a media gateway provides media translation functions of the B-channel data to RTP media streams [23].

The architecture of a PSTN-IP gateway is shown in Figure 6. Such a gateway consists of three separate components: the Signalling Gateway (SG) which performs routing of ISUP messages and translation of the dialled numbers to IP addresses, the Media Gateway (MG) which transcodes the media from the PSTN to RTP media streams in the IP network, and the Media Gateway Controller (MGC) which converts the format of PSTN signalling to an appropriate IP format in order to bridge the ISUP with the SIP networks [22] [29].

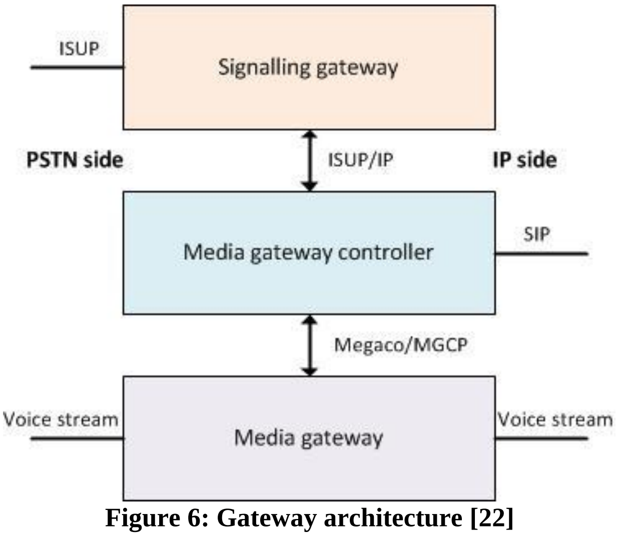


Figure 6: Gateway architecture [22]

Figure 7 depicts a sample ISUP-SIP call flow between a PSTN and a SIP end-point. The PSTN end-point initiates a call by sending an ISUP IAM message to the MGC. The MGC translates the ISUP IAM message to a SIP INVITE through appropriate translation and encapsulation procedures, and sends the message to the SIP Proxy which is responsible to forwarding it to the destination SIP end-point. In the same way, the other messages are exchanged between the two end-points by translating them from ISUP to SIP and vice versa. In the end, the call is terminated from the PSTN end-point by sending an ISUP REL message which is translated to a SIP BYE message [22].

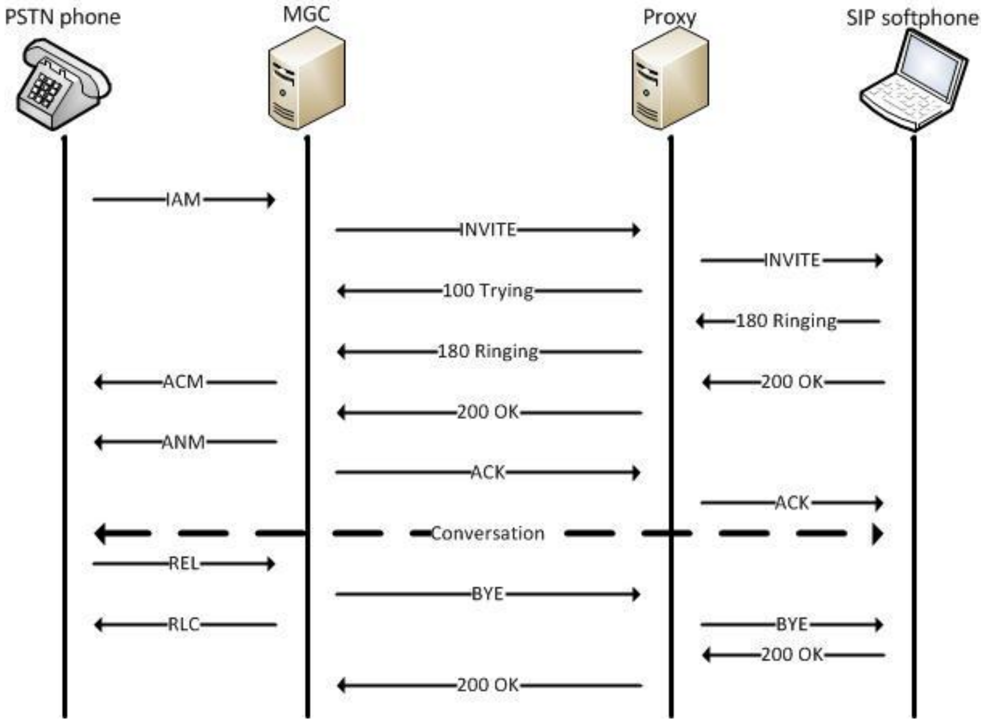


Figure 7: ISUP-SIP call flow [22]

2.5. **VoIP network components**

A VoIP network infrastructure consists of several different network components and each of them contributes to the VoIP implementation in different ways and provides different functions and processes. The VoIP network components are outlined below [7] [30].

- **End-systems.** The end-systems of the VoIP service can be IP-based devices, such as IP phones or PC software programs (also called soft clients) that are used for voice communication. The communication between the end-points is established through signalling protocols which allow the end-points to contact their corresponding call agents, SIP servers, or gateways.
- **Gateways.** The gateways provide interconnection and translation between VoIP and non-VoIP networks, such as TDM-based PSTN networks. They perform transcoding functions (conversions from one voice CODEC to another), transformations of signalling protocols from one type to another (for example ISUP-to-SIP and SIP-to-ISUP), and they are the main point of physical access for both analog and digital network devices.
- **Call agents.** The call agents are responsible for the connection of the end-points, maintenance and control of the call, address translation, bandwidth management functions, control of media streams in a session, collection of call statistics etc. In a

SIP-based environment, the User Agent Client (UAC) and User Agent Server (UAS) play a role similar to call agents.

- **Session Border Controllers (SBC).** The SBCs devices are usually located at the network borders of providers and carriers and offer functions such as Call Admission Control (CAC), security, transcoding, session control and maintenance, signalling message manipulation, QoS provisioning for different media streams, etc.
- **Routers.** Routers in a VoIP environment are configured to treat the VoIP traffic in an appropriate way by providing priority to the voice data in order to achieve the required voice QoS.

2.6. **VoIP routing and traffic engineering**

Voice and video streaming, telephony, and conferencing services are very time-sensitive, and therefore the media packets should be treated differently than normal traffic in an IP network. The access and core routers within a provider's or carrier's network should be configured to separate the traffic and prioritize voice and video media packets, so as to meet the QoS requirements of the VoIP traffic. Several different methods for VoIP traffic prioritization and handling have been introduced and are described in the following sections [3].

- **Class of Service (CoS)**. CoS is specified in the IEEE 802.1p standard and provides QoS mechanisms in IP networks. CoS is a 3-bit field in Ethernet frames that carries a priority value. Packets with higher priority are treated differently than packets with lower priority value. In the VoIP network, the voice packets have higher priority than other traffic, and in case of network congestion the packets with lower priority will be discarded first.
- **Virtual LAN (VLAN)**. VLAN are defined in IEEE 802.1q standard and they are used to logically separate the VoIP traffic from the normal traffic. VLANs are usually used in conjunction with the CoS mechanism in order to allow more efficient voice prioritization, as one VLAN is typically mapped to a single CoS value.
- **Differentiated services (DiffServ)**. DiffServ is a QoS provisioning mechanism that is used for traffic classification and prioritization. It uses a 6-bit field in the IP header which is called a DiffServ Code Point (DSCP) in order to classify the packets and define the Per-Hop Behaviour (PHB) of the routers so as to decrease the latency along the routing path.
- **Integrated Services (IntServ)**. IntServ is a flow-based QoS provisioning technique which reserves bandwidth in the same way PSTN reserves circuits. IntServ uses as an underlying mechanism - the Resource Reservation Protocol (RSVP) - in order to establish flow-based capacity reservations.
- **Multi-Protocol Label Switching (MPLS)**. MPLS is a routing protocol that uses labels in order to route packets to their destinations. For routing packets, virtual Label Switched Paths (LSPs) are established, which enable the router to separate and prioritize the traffic by sending different traffic over different LSPs. Moreover, MPLS contains a 3-bit QoS field which can be used in order to apply further QoS features to the VoIP traffic (e.g. in order to minimize the latency along the path).

2.7. Fault management in the telecom industry

The telecom industry is a very competitive area and it takes a lot of attention and careful planning in order to provide a new service to customers. However, a very essential factor in service development and success is the maintenance of this service and consequently providing appropriate customer support is essential. A telecom company can gain the trust of their customers by providing high quality fault management, troubleshooting, and service support.

The interaction between a telecom company and a customer is performed through the use of a Service Level Agreement (SLA). A SLA specifies the terms under which a service is provided to the customer from the company and it covers technical and organizational agreements and thresholds that both the customer and the company should follow and comply with. If one of them violates the SLA, then corresponding fees specified in the SLA may be applied. For example, the SLA can specify service QoS thresholds, network availability guarantees, fault resolution times, security policies, bandwidth agreements, etc. For example, an SLA might specify no more than 35ms added delay, jitter below 10ms, 99.99% availability, a maximum of 4 hour response time (time limit for providing feedback to the customer regarding the problem they have reported), etc. Missing one of these requirements might cost the operator one or more days of service for every defined period that the requirements are not met.

The general model of the organizational fault management procedure is depicted in Figure 8. The first point of contact with customers is the Customer Care department (CC). The CC is responsible for direct communication with customers, problem registration by opening a Trouble Ticket (TT) in the company's trouble ticketing system, customer update provisioning, ticket follow-up and escalation, ticket closure, etc. Usually the CC incorporates first-line support responsibilities, i.e., provides a first investigation and analysis of the problem and corresponding troubleshooting and resolution; if they are not able to resolve the problem they hand the problem over to the second-line support department (first-level escalation).

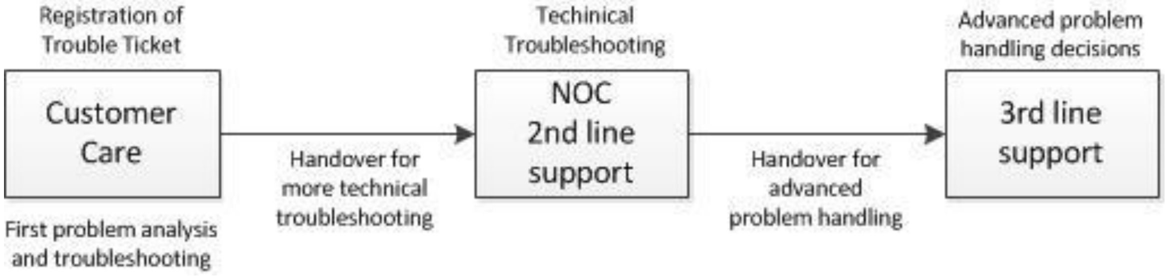

Registration of Trouble Ticket
Customer Care
First problem analysis and troubleshooting
Handover for more technical troubleshooting
Techinical Troubleshooting
NOC 2nd line support
Handover for advanced problem handling
Advanced problem handling decisions
3rd line support

Figure 8: Fault handling procedures within telecom industry

In a telecom company, the second-line support department is the Network Operation Centre (NOC) which consists of network and service engineers. The NOC is responsible for deeper analysis and technical troubleshooting of the first-level escalated tickets. When a fault case becomes difficult to troubleshoot and more advanced means are needed, then the NOC escalates the ticket to the third-line support which consists of more specialized core engineers who have full access to the network infrastructure and services, as well as full awareness of the network and services deployments.

The higher the escalation is, the more expensive it becomes for the company to dedicate the resources required for the ticket resolution. For this reason, it is necessary for the company to establish efficient organizational and technical fault management procedures and routines in order to reduce the time and resources spent for the ticket resolution. Additionally, one important aspect of improving fault management is proactive monitoring and problem discovery by the company themselves. Proactive monitoring and problem discovery means the implementation of alarm mechanisms within the company’s network (e.g. network devices, transmission links, etc. are enabled to generate alarms) in order for the company to be aware of problem appearance and possibly resolve the issue before the customers report the fault themselves. Careful proactive monitoring in conjunction with efficient troubleshooting procedures can minimize of the number of trouble tickets and reduce the number of tickets that have to be escalated. Furthermore, proactive monitoring and problem resolution can reduce operating costs for the operator, as well as provide input into planning future network upgrades. In this way, the carrier’s network availability increases and the customers’ trust of the company also increases.

3. VoIP Planning

Planning properly and efficiently maintaining a VoIP network infrastructure is a difficult task. After a product has been implemented and is made available as a service, then network administrators have some specific responsibilities. Some questions that arise for a wholesale carrier are:

- What are the VoIP planning and troubleshooting guidelines for a wholesale carrier?
- What kind of network designs should be used and how should the product be realized?
- What are the focal areas for monitoring and troubleshooting such a service in order to ensure compliance with the SLAs with the customers?

As an example case study, this thesis analyses the VoIP product of a wholesale carrier. This analysis of real world product planning will help identify some key points in commercial VoIP development and deployment. Section 3.1 describes the main VoIP products that the company offers, as well as the technical implementation of this product and main conclusions. Section 3.2 provides recommendations on what should be further implemented technically in the VoIP network in order to perform efficient service monitoring and maintenance.

3.1. **Example VoIP product description**

The company that has been studied in this thesis project maintains an international voice and IP carrier network. The VoIP product of the company provides interconnection between customers' VoIP traffic and the carrier's international PSTN network. The company's customers are other IP operators or telephony providers who offer voice and other services to end users.

The basic setup of this interconnection service includes a SBC connected to two different networks. On one side, the SBC is connected to the company's private internal network which connects to the company's media gateways - which in turn provide access to PSTN equipment, while on the other side the SBC is connected through public IP addresses to the customer's equipment. The carrier provides to the customer as a destination IP address the SBC's public interface that has been configured for this particular customer.

This VoIP interconnection product offers two different technical implementation types. The first type of implementation (product A) applies to customers who are connected through the public Internet to the carrier's VoIP infrastructure, and the second type of implementation (product B) is a direct IP connection of the customer to the carrier's VoIP network. Both of these solutions eventually connect to a border SBC which routes the traffic towards the media gateways in the carrier's internal network. Below each type of implementation is described in detail.

3.1.1. Customer is directly connected to the access network (product A)

The customer's VoIP equipment is connected directly to one of the company's access routers though a pre-configured interface. This VoIP solution utilizes a Virtual Private Network (VPN) tunnel all the way from the customer's equipment to the border SBC. This tunnel is implemented by configuring Virtual Routing and Forwarding (VRF) tables in the access router to include the customer's route and the customer's destination interface. MPLS routing is used to carry the voice traffic through the carrier's network from the customer's equipment to the SBC. Figure 9 illustrates this type of implementation.

The advantage of this implementation is that the customer is provided with a MPLS/VPN tunnel connection to the border SBC along with configured QoS prioritization ensuring a certain level of voice traffic privacy and quality. The disadvantage of this implementation is that this is not a flexible solution, since there is a need to establish a physical connection between the company's access router and the customer. Additionally, the customer can only connect via a specific access location (the location of the origin of the MPLS tunnel) to the company's VoIP infrastructure.

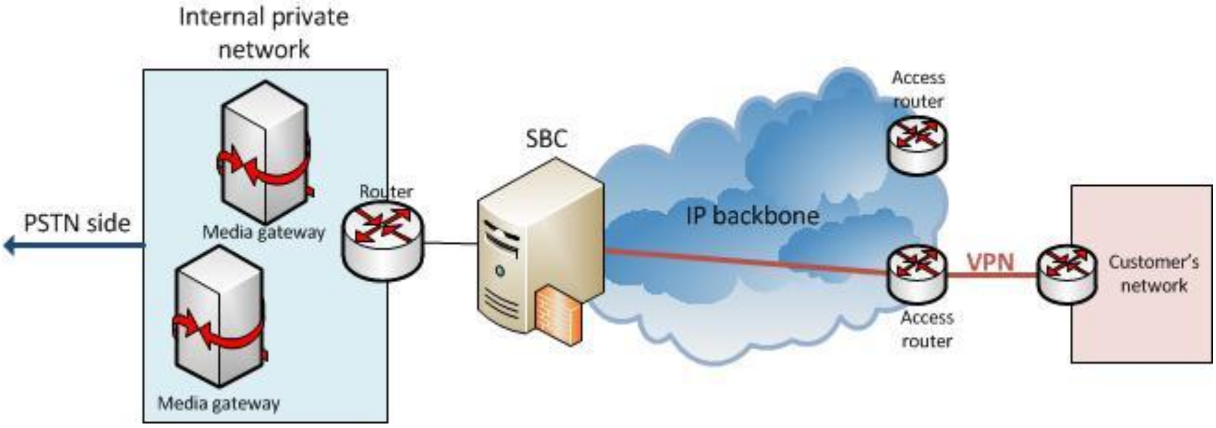


Figure 9: Customer is directly connected to the access network (product A)

3.1.2. Customer is connected through public Internet to the access network (product B)

The customer's VoIP equipment is indirectly connected to the carrier's network, using the public Internet (thus traffic can pass through multiple providers before entering the carrier's network) to reach the company's SBC. From the customer's equipment, the route towards the SBC is determined on a packet by packet basis through a traditional best effort service. The routers that provide this connectivity are most often configured using Border Gateway Protocol (BGP) routing and the set of policies that have been configured by all of the network operators along the path. This means that the customer's traffic can enter the access network from any access router and will be forwarded via the network until it reaches the SBC. However, since the SBC is configured to apply prioritization policies to the packets passing through it, the voice traffic from the SBC to the customer's equipment can be prioritized (at least over the portion of the path that the company and the customer control). Figure 10 represents this product implementation.

The advantage of this implementation is that this is a very flexible solution for the customer since they can connect from any location they want, without having to establish and maintain a physical connection to the carrier's network. The disadvantages of this solution are that from the access router where the customer's traffic enters the carrier's network until the actual SBC, the public Internet is used and routes are determined according to routing tables. Since traffic travels through the public Internet, best effort service is used to route the traffic from the customer's equipment to the SBC, hence there is limited guaranty of a specific voice quality while prioritization is applied to only a part of the path. However, in some settings end-to-end priority may be possible if all of the operators along the path have agreed to SLAs that are at least as stringent as the SLA between the company and the customer. Another problem with this solution is that the actual route from the customer's equipment to the SBC is not known, which makes monitoring of the service status more difficult. This also makes the troubleshooting procedure more complicated.

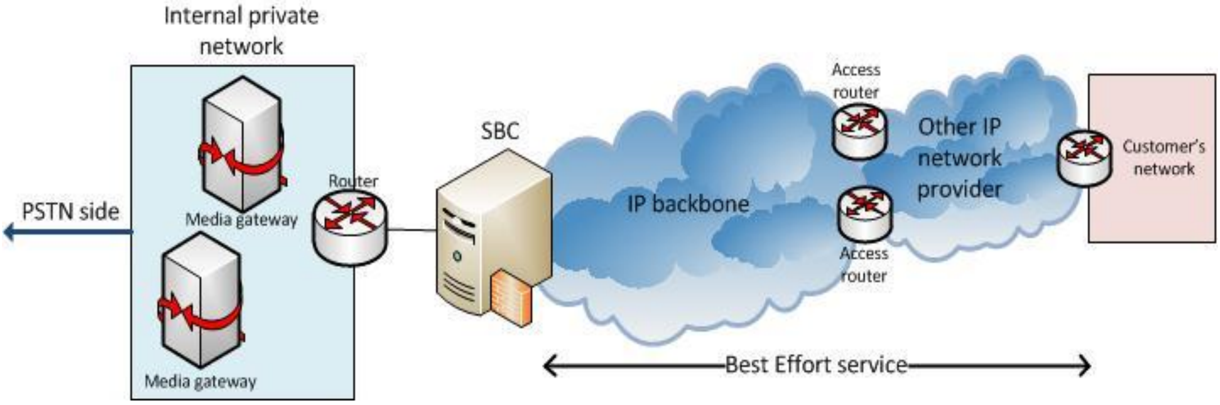


Figure 10: Customer is connected through the public Internet to the access network (product B)

3.2. VoIP monitoring and maintenance recommendations

The two types of VoIP implementation that were described in the previous section use the SBC. All the VoIP traffic to and from the customer passes through the SBC and therefore, it is vitally important to configure the SBC appropriately so that it is possible to perform proper monitoring and efficient troubleshooting of the service. Section 3.3.1 describes the role of the SBC in the VoIP implementation and presents aspects of its configuration, as well as further deployment recommendations.

In order to be able to efficient troubleshoot problems, monitoring functions should be implemented. Since the SBC is the central point of all VoIP traffic from the company's point of view, it is important to analyse the monitoring and alarm capabilities that the SBC can offer and find the most efficient and appropriate way to implement them.

Two important options that should be considered for the SBC configuration are:

- Call Admission Control (CAC) (i.e., how can the company efficiently manage the available bandwidth in the outside and inside interfaces of the SBC according to customers' requests)
- Packet tracing implementation and alarm configurations (for monitoring purposes and troubleshooting procedures)

The following sections describe and analyse these two options and propose specific implementations based on the needs of the VoIP carrier's implementation.

3.2.1. Role of the SBC

The SBC is used for session control, admission control, topology hiding, and firewall service; as well as acting as a central point of communication between the carrier and its customers. Both the SIP signalling traffic and the RTP media traffic pass through this device. The SBC operates as a SIP B2BUA. This means that the SBC receives requests and processes them as a UAS and then regenerates those requests as a UAC, creating and maintaining, in this way, VoIP sessions. Therefore, the SBC terminates SIP sessions and re-originates them, controlling in this way all the signalling and media traffic that passes through it. Figure 11 depicts the function of the SBC. As noted earlier, the SBC is placed at the border between the carrier's private network and a public network (or direct link to the customer - as was described in section 3.1.2).

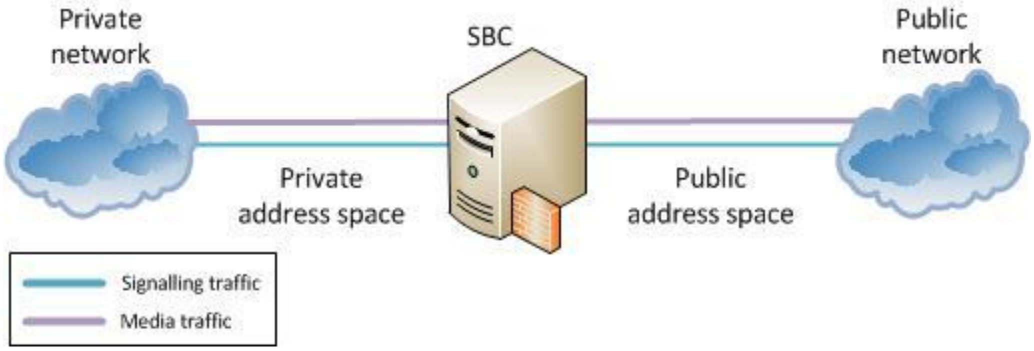


Figure 11: The function of the SBC [25]

According to [14], there are two main logical functions of a SBC:

Signalling function Controls access and determines routing of the signalling traffic into the destination network by manipulating the (SIP) message headers.

Media function Controls access of the media traffic into the destination network by implementing QoS and differentiated traffic policies for the (RTP) media packets.

The questions that arise regarding the SBC are: How should the SBC be implemented for a carrier's VoIP solution? What options, settings, and configurations should be set in order to efficiently plan for and deliver the service for a given customer?

There are two SBC interfaces: the public interface (towards customers) and the private interface (towards internal voice equipment). These interfaces will be referred as the outside (public) and the inside (private) interface for the remainder of this section. The current implementation includes configuration of a VLAN for each customer and configuration of local policies of the SBC in order to route certain traffic on a per customer basis to specific outgoing interfaces. This means that the SBC allocates resources on a per customer basis and assigns specific SIP interfaces (with TCP and UDP port 5060) and dynamic RTP ports per call. Access lists are also implemented in order to allow only the customer's traffic to enter the SBC and to ensure that this traffic originates from the customer's equipment (this equipment can include SIP user agents). The main configuration details of the SBC are:

- VLAN interfaces are assigned per customer on the SBC
- SIP interfaces are assigned per customer and the SIP UDP or TCP port 5060 are used
- RTP UDP or TCP ports are dynamically assigned per customer from a specified range corresponding to the customer's user agent(s)
- Pre-defined routing policies are configured to connect the outside interface of the customer to a specific inside interface
- Certain manipulation rules are applied to the SIP headers (as the SBC works as B2BUA)
- A customer specific QoS policy is applied to all voice packets by the SBC
- Access lists are implemented per protocol in order to allow only traffic coming from valid sources, where the only permitted protocols are: SIP, RTP, and Internet Control Message Protocol (ICMP). The SIP access list contains the addresses of the customers

SIP User Agents and SBC attached interfaces and the ICMP list allows an ICMP ping only to certain IP addresses

- Simple Network Management Protocol (SNMP) traps are implemented in order to create notifications of certain problems or failures. These SNMP traps are explained in detail in section 3.3.4.1.

3.2.2. Call Admission Control (CAC) in VoIP

Call Admission Control (CAC) implements capacity limiting procedures that have been defined to shape the traffic passing through a device and to allow only a certain amount of traffic by using bandwidth thresholds or other policies. CAC is implemented as an industrial solution in order to allow the carrier to control and limit the traffic passing though their network in order to avoid congestion and to meet equipment limitations. Another purpose of implementing CAC implementation is to keep track of the traffic that the customers send, and to ensure that they do not violate the bandwidth specification in their SLA. There are two main ways in the SBC to configure CAC: CAC based on the number of total active sessions and CAC based on the total bandwidth consumed at any time. The following sections describe each of these ways, as well as the effects they will have if implemented. It should be noted that the following CAC analysis regards the IP side of the implementation since in the PSTN side the link bandwidth is fixed to 64Kbps.

3.2.2.1. CAC based on the number of total sessions

If CAC based on the number of total active sessions is configured, then the SBC keeps track of the number of total active sessions that it is handling at the time and ensures that this number will not exceed a the pre-defined threshold. This configuration can be implemented on a per customer basis, so that the maximum number of sessions that the customer is allowed to establish is as specified in their SLA.

The advantage of this type of CAC implementation is that it is very easy to configure and control. However, when the CAC is based simply on the number of active sessions, this does not correspond to the actual traffic that is passing through the SBC, since the actual bandwidth per session can differ due to the use of different media parameters such as different CODECs, silence suppression, etc. For example, G.711 offers good quality of encoded voice, but consumes a lot of bandwidth in contrast to G.729 which consumes much less bandwidth but offers lower voice quality. This means that unless the carrier is aware of the CODECs that their customer is using for their VoIP solutions, then the carrier cannot pre-calculate the total bandwidth that each customer sends and as a result there is a possibility for congestion or traffic overload in the SBC or other gateways.

3.2.2.2. CAC based on the total bandwidth consumed

If CAC based on the total bandwidth consumed is configured, then the traffic that the customers are allowed to send will be limited to a pre-defined bandwidth threshold. This CAC policy can be implemented on a per customer basis so as to police the amount of bandwidth that each customer can send to the carrier’s VoIP network.

The advantage of this solution is that the carrier can have full knowledge of the maximum actual traffic that the customer sends and as a result, they can avoid congestion or traffic overload events since they can ensure that the pre-defined bandwidth thresholds are kept. For the customers, this type of CAC means that after they have agreed upon a certain SLA with the carrier including specified bandwidth limitations, while the number of active sessions that they can have depends on the CODECs that they are currently using. Using a CODEC that needs a lot of bandwidth such as G.711 leads to a certain maximum number of active sessions. On the other hand, if they use a CODEC that consumes less bandwidth (such as G.729), then they can increase the number of active sessions that they can have.

However, this type of CAC implementation requires careful calculations from the carrier's side about the bandwidth threshold that they should apply. These calculations should be based on the VoIP protocols used, equipment capabilities and bandwidth availabilities, and this calculation is a difficult task since miscalculation can lead to VoIP traffic being dropped. The next section provides an analysis of the bandwidth calculation formula that should be used in order to properly design CAC solutions for VoIP.

3.2.2.3. VoIP bandwidth calculation analysis

According to [34] the bandwidth calculation should be based on the protocol headers, the voice payload, and the CODEC used. The formula is the following:

i. *PPS = (codec bit rate) / (voice payload size)*

ii. *Total packet size = (L2 header) + (IP/UDP/RTP header) + (voice payload size)*

iii. *Bandwidth per call = total packet size * PPS*

These terms are defined below:

- PPS means packets per second and it represents the number of packets that need to be processed per second based on the CODEC used. The standard PPS value for the G.711 is 50 pps (with 64Kbps bit rate and 160 bytes voice payload size). The standard PPS value for the G.729 is also 50 pps (with 8Kbps bit rate and 20 bytes voice payload size) [34].
- The total packet size is calculated as the sum of all the protocol headers attached to the packet plus the actual voice payload. The IP/UDP/RTP headers have a fixed overhead of 40 bytes (12 bytes for RTP, 8 bytes for UDP, and 20 bytes for IP header). However this can be reduced to 2-4 bytes by using point-to-point compressed RTP (cRTP). The transmission medium used (usually Ethernet frames) adds additional 38 bytes for the header and trailer. If silence suppression methods are implemented, the required bandwidth can be reduced up to 50% [35]. Finally, transmission media such as Frame Relay, ATM, and VPN links consume extra bandwidth due to the additional overhead of the transport protocols [5].
- The bandwidth per call is calculated by multiplying the total packet size by the PPS, to compute the total number of bits per seconds needed for one call.

The two following examples present the bandwidth calculation of VoIP using Ethernet as a transmission medium for the CODECs G.711 and G.729 respectively [35]. It should be noted that for the Ethernet frame, 12 bytes for the Ethernet Inter-Frame Gap are used in the calculations. The Inter-Frame Gap size can be different according to the speed and duplex mode (minimum value is 96 bit times according to the IEEE Ethernet specifications). Therefore the calculations can be different depending on the Inter-Frame Gap size being used. These examples are applied to the carrier case study in order to implement CAC based on the total bandwidth for a customer X that needs to support 150 active calls via the SBC. The choice of 150 calls applies to a small scale customer case, since there are customers using much higher number of active calls. It should also be noted that this sample calculations apply to an example case for product B where open Internet is used and not to the case of VPN tunnel (product A), since the packets' format differs in this case. Figure 12 and Figure 13 depict the G.711 and G.729 frames used from the bandwidth calculations respectively.

- **Example A: Bandwidth calculation for VoIP using G.711**

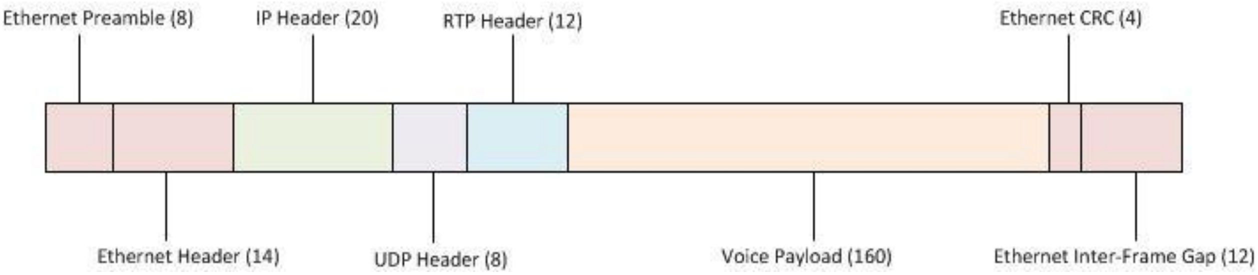


Figure 12: VoIP G.711 frame [35]

The standard bit rate from the G.711 CODEC is 64 Kbps with a voice payload size 160 bytes; therefore the PPS for G.711 is 50 pps. The total packet size is: 40 bytes (IP/UDP/RTP header) + 38 bytes (Ethernet frame header) + 160 bytes (standard G.711 voice payload size) = 238 bytes. Finally, the total bandwidth per call is: (238 bytes/packet) * (50 packets/second) * (8 bits/byte) = 95200 bps = 95.2 Kbps. Since customer X requires support for 150 active simultaneous calls, the total bandwidth that is needed is: (95.2 Kbps/call) * (150 calls) = 14280 Kbps = 14.28 Mbps.

If the cRTP is used, then the total packet size will be: 2 bytes (compressed IP/UDP/RTP header) + 38 bytes (Ethernet frame header) + 160 bytes (standard G.711 voice payload size) = 200 bytes. The total bandwidth per call will be: (200 bytes/packet) * (50 packets/second) * (8 bits/byte) = 80000 bps = 80 Kbps. Since customer X requires support for 150 active simultaneous calls, the total bandwidth needed will be: (80 Kbps/call) * (150 calls) = 12000 Kbps = 12 Mbps.

- **Example B: Bandwidth calculation for VoIP using G.729**

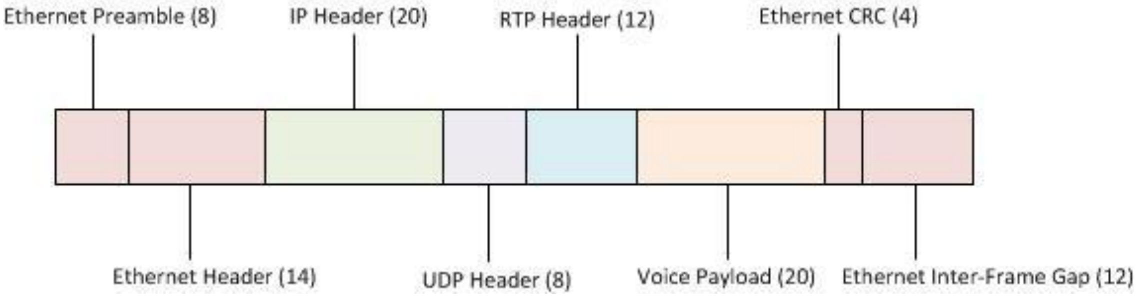


Figure 13: VoIP G.729 frame [35]

The standard bit rate from the G.729 CODEC is 8 Kbps with voice payload size 20 bytes; therefore the PPS for G.729 is 50 pps. The total packet size is: 40 bytes (IP/UDP/RTP header) + 38 bytes (Ethernet frame header) + 20 bytes (standard G.729 voice payload size) = 98 bytes. Finally, the total bandwidth per call is: (98 bytes/packet) * (50 packets/second) * (8 bits/byte) = 39200 bps = 39.2 Kbps. Since customer X requires support for 150 active simultaneous calls, the total bandwidth that is needed is: (39.2 Kbps/call) * (150 calls) = 5880 Kbps = 5.88 Mbps.

If the cRTP is going to be used, then the total packet size will be: 2 bytes (compressed IP/UDP/RTP header) + 38 bytes (Ethernet frame header) + 20 bytes (standard G.729 voice payload size) = 60 bytes. The total bandwidth per call will be: (60 bytes/packet) * (50 packets/second) * (8 bits/byte) = 24000 bps = 24 Kbps. Since customer X requires support for 150 active simultaneous calls, the total bandwidth needed will be: (24 Kbps/call) * (150 calls) = 3600 Kbps = 3.6 Mbps.

Based on the above example methods, capacity planning procedures can be efficiently performed by the carrier and their customers in order to agree upon a CAC SLA according to the VoIP solution needs and requirements.

3.2.3. Monitoring techniques in VoIP

Monitoring techniques in an industrial environment require proactive alarm configurations and implementation of network and service monitoring tools. In this way, problems can be identified in real-time, as well as making troubleshooting is easier since networking information and traces are registered in history logs. The following sections describe and provide monitoring recommendations for VoIP.

3.2.3.1. SBC alarm configurations

The SBC provides the possibility of alarm configurations from both hardware and software. For some SBC hardware and software faults or failures, alarms are generated providing information about the problem, the time that the fault/failure occurred, and its severity level. Table 5 describes the alarm categories that the SBC supports.

Table 5: SBC alarms

Alarms	Description
Hardware alarms	Generated when an internal problem in the SBC system chassis occurs
System alarms	Generated when a problem occurs regarding the system resources, such as high CPU utilization, low memory availability, suspended task events, etc.
Network alarms	Generated when the software is unable to communicate with the hardware
Application alarms	Generated when a problem occurs in the protocol level such as in the SIP implementations. For example, security violations, session failures, accounting problems, etc.

There are several different ways for the SBC to provide alarm notifications. For example, the alarm can be displayed in a display on the chassis, an external alarm can be transmitted to another physical location or a SNMP trap can be generated to signal the alarm to the network management system(s).

The SBC can also generate other kinds of alarms that are related to IP connectivity and reachability of certain VoIP network devices. These alarms are based upon a continuous background pinging function which pings IP addresses of specific gateways in the carrier's internal network, as well as IP addresses of the customer's UAs. In order to enable this function, the SBC has to be provided with a list of IP addresses that need to be monitored. In this way, a connectivity failure with the customer's UAs or the company's internal gateways can easily be detected in real time.

3.2.3.2. Implementation of SNMP traps

SNMP traps are a very common way of providing failure notifications. These notifications provide extra monitoring assistance by using Management Information Bases (MIBs) related to specific SBC alarms. When an event occurs, the SBC sends a SNMP trap to the management station reporting this fault. There are many different kinds of traps supported by the SBC. These traps can be used as a proactive method of troubleshooting VoIP issues. In this way, the company can identify and solve certain VoIP problems *before* customers report them.

SNMP traps are implemented both in the outside and inside interfaces of the SBC. When a trap is triggered, the notification is sent to a central management system through the SBC's management interface. In this way, the NOC is notified whenever an alarm has been triggered in the SBC. The SNMP traps that are recommended to be implemented in the SBC in order to facilitate proper monitoring and troubleshooting are:

- **Link down trap**: Generated when an interface transitions from the up state to the down state
- **Threshold exceeded trap**: Generated when the threshold (such as 90% utilization) of a system resource use has been exceeded; examples of system resources are: Network Address Translation (NAT) table entries, Address Resolution Protocol (ARP) table entries, memory usage or CPU, etc.
- **Licensed capacity reached trap**: Generated when the total number of active sessions of all protocols has reached the licensed capacity
- **Power trap**: Generated when there is a problem with the power supply
- **Temperature trap**: Generated when there is a temperature problem
- **Fan unit speed trap**: Generated when there is a problem with the fan speed
- **Suspended task trap:** Generated when a task running on the system has transferred to a suspended state
- **Media ports trap**: Generated when certain number of failures has occurred in the port allocation according to the system's default threshold rate
- **Media bandwidth trap**: Generated when certain number of failures has occurred in the bandwidth allocation according to the system's default threshold rate
- **Media out of memory trap**: Generated when there is a problem with the media allocation process
- **Unknown media trap**: Generated when the media process cannot identify the media flow
- **Gateway unreachable trap**: Generated when the specified gateway has become unreachable by the system
- **Hardware error trap**: Generated when a hardware error occurs in the system
- **Denial of Service (DoS) trap**: Generated when the IP address and other packet information indicates a denial of service attack

3.2.3.3. Packet tracer implementation

A very good configuration option for monitoring purposes is the packet tracer function of the SBC. The SBC is able to mirror traffic to/from specific interfaces and/or IP addresses. The mirrored traffic can be forwarded to a specific interface as configured by the administrator and input to a trace server.

The first step in implementing packet tracing is to enable and configure the tracer option in the SBC. The information needed for this implementation is the interface of the SBC that is going to be mirrored and the IP address. In order to start a trace, a command must be entered which specifies the SBC interface and the IP address that is going to be monitored. There is also the possibility of applying multiple traces at the same time, in order to get more complete monitoring results by monitoring multiple components that correspond to a VoIP session, a particular customer, or end-to-end calls.

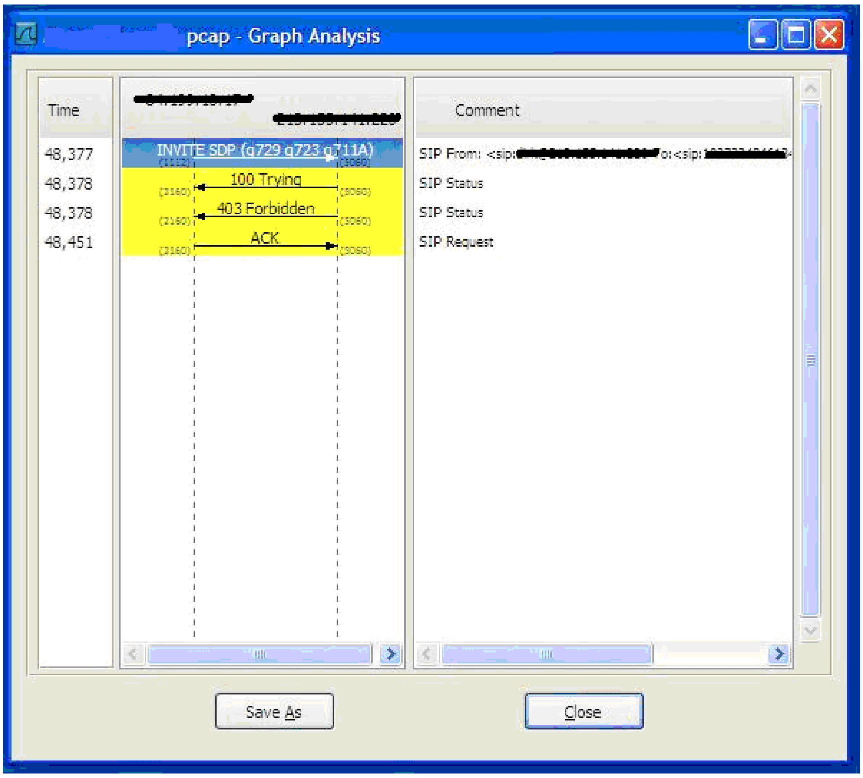
The second step is the implementation of the trace server which will receive the mirrored traffic from the SBC. The trace server must support a tracing tool, such as Wireshark [42]. Wireshark analyses and presents the captured packets. Filtering rules can be applied in order to extract only the packet information that is needed, for example only SIP messages. Moreover, Wireshark supports VoIP telephony monitoring functions and can provide representations of the calls established or attempted during tracing. Specifically, we can press the “Telephony” button in the menu bar, then choose “VoIP calls” and see all the calls collected in the trace. If we choose a particular call and press “Flows”, the SIP and media message flows for this call are shown.

There are many different scenarios that we can use depending on the troubleshooting case. For example, if we want to monitor end-to-end calls, we should initiate two different packet traces in the SBC mirroring the traffic between the UA of the customer (sent to or received from the outside interface of the SBC) and the carrier’s internal gateways on the other side (sent to or received from the inside interface of the SBC). Another scenario is to monitor only the interfaces/IP addresses attached to the SBC for a particular customer. An example troubleshooting case is illustrated in Figure 14.

In this troubleshooting case a customer has reported that they cannot send traffic from a particular UA, where they are receiving SIP error response code 403 FORBIDDEN. Since there is a SIP error produced, it means that the problem probably can be found by examining the SIP message exchange. To do this, the packet tracer in the SBC can be used to monitor the customer’s outside interface to the SBC. In this case, we can see that there are no packets containing the source IP address of the customer’s problematic UA. However, we can see then that we are actually receiving SIP messages from an unknown address. Checking the VoIP calls and flows in Wireshark, we can see that the SBC replies to the packets from this unknown address with message 403 FORBIDDEN since it does not recognize and consequently does not allow messages from this address (eligible source IP addresses are considered to be only well-defined, pre-registered customers’ UAs). The conclusion is that for some reason, the customer’s UA produces SIP INVITE messages with an incorrect source IP address which is not eligible and is consequently not allowed due to the SBC security policies. This may indicate that the customer has added a new UA, replaced one UA with another, mis-configured their UA, a proxy along the path to the SBC has incorrectly re-written the source address, or some other reason exists for this problem.

The Wireshark capture file shown in Figure 14 shows the problem. The first column of the diagram represents the customer’s UA and the second column represents the SBC. The actual IP addresses have been redacted for confidentiality reasons. The customer’s UA initiates a session with a SIP INVITE containing SDP call negotiation information (CODECs to be used in the call). After the usual 100 Trying response, the SBC replies with the SIP error response code 403 FORBIDDEN. The IP address of the UA in the diagram (which is redacted) is not registered in the SBC configuration as the customer's UA, and this is why this INVITE request is rejected.

Using similar means and the functionalities of the tracer, many other problems reported by the customers can be isolated. The packet capture mechanism provides the ability to identify several problem causes related to protocol and configuration errors. However, it should be noted that this tool only helps identify the cause for the reported problem, then remains the issue of resolving the problem which may require action by the customer, the company, an intermediate network provider, or all parties. Further details of troubleshooting are described in the next chapter.



Time	[redacted] [redacted]	Comment
48,377	INVITE SDP (g729 g723 g711A) (1112) (5060)	SIP From: <sip:[redacted]o:<sip:[redacted]
48,378	100 Trying (2160) (5060)	SIP Status
48,378	403 Forbidden (2160) (5060)	SIP Status
48,451	ACK (2160) (5060)	SIP Request

Figure 14: Wireshark VoIP capture filter example

4. VoIP troubleshooting analysis

After the VoIP product has been defined and implemented, the company needs to be able to provide the customer with technical support in case of service failures or other problems. The normal troubleshooting procedures begin when a customer reports a service fault to the Customer Care department (first-line support) who opens a Trouble Ticket (TT) for this issue. The TT has a reference number that is used for tracking the troubleshooting progress of the reported fault. The Customer Care (CC) department should collect all the necessary information from the customer in order to be able to proceed with problem analysis, investigation, and resolution. If the CC department is unable to resolve the problem, then the problem is handed over to the Network Operation Centre (NOC) -the second-line support department- for troubleshooting and resolution. At this point, the troubleshooting procedure can become complicated from both a technical and organizational point of view.

From a technical point of view, troubleshooting VoIP is a difficult task, since there are a lot of different technologies involved. Each of these technologies uses its own protocols and service designs. Therefore, when a problem occurs in a VoIP service, there are numerous potential causes. From an organizational point of view, VoIP combines two traditionally very different technologies: voice and IP. Within the company these two technologies are traditionally handled by different NOCs: a Voice NOC and an IP NOC. Thus confusion is often caused when a VoIP fault is reported since it is not clear which NOC should handle it or where the line separating the handover from one NOC to the other is, especially when the cause of the fault is difficult to identify. Moreover, the customer does not always provide the information necessary in order for the NOCs to have sufficient information to properly investigate and resolve the problem. Therefore, there is a need for an efficient troubleshooting procedure which guides the CC department and the NOCs enabling them to handle problems in an appropriate way.

This chapter analyses VoIP troubleshooting from both the technical and organizational points of view. This analysis is based on a root cause analysis method proposed in [16]. According to [16], there are four major steps in a root cause analysis procedure:

1. Data collection
2. Casual factor charting
3. Root cause identification
4. Recommendation generation and implementation

In the case study in this thesis project, data collection will be done by getting a complete description of the problem and all the necessary information from the customer when they report the problem (this is the responsibility of the CC department). Casual factor charting is the analysis of possible causes of VoIP problems and categorization of them according to the symptoms that the customers can experience. Root cause identification is the procedure that should be followed by the NOC in order to troubleshoot and resolve the reported problem based on casual factor charting. Finally, recommendation generation and implementation are the actions that should be taken by management teams in order to prevent a reoccurrence of this particular problem. This last step is outside of the scope of this thesis and is proposed as future work.

This chapter is structured as follows: section 4.2 presents a detailed analysis of potential problems in a VoIP implementation, as well as a mapping the symptoms that VoIP users can experience to potential causes. This section corresponds to the second step of the root cause analysis mentioned above. Section 4.3 presents an investigation inside the company of efficient troubleshooting procedures for the carrier's VoIP product. This corresponds to the third step of the root cause analysis. Finally, section 4.4 presents an investigation of the questions that the company needs to ask the customer in order to collect all the information necessary for troubleshooting. This section corresponds to the first step of the troubleshooting procedure. This step is presented last, since it depends upon knowing the information that is required for steps 2 and 3.

4.1. **VoIP technical troubleshooting**

In this section, a theoretical analysis of potential problems in a VoIP service are presented, as well as how the cause analysis method can be used in order to categorise the causes and the corresponding symptoms of VoIP problems.

4.1.1. Packet loss

Packet loss occurs when IP packets are dropped in the network and do not reach their destination. There are two kinds of packet losses: random packet losses and burst packet loss (massive packet loss that happens for some period of time). Many UAs can tolerate packet loss to some extend by using compensating techniques for the lost packets. Most UAs using common COCDECs can tolerate up to five percent random packet drops without causing serious degradation in the voice quality [17].

One class of techniques used to compensate for packet loss is Packet Loss Concealment (PLC), of which there are several different variations. For example, "zero substitution" is the simplest method and requires the least computational power, but provides very low quality; "waveform substitution" replaces lost voice packets with artificial sound; and other advanced algorithms using increasing amounts of computational resources can compensate for up to 20 percent random packet loss [4].

Congestion due to competing traffic and limited link capacity is a common reason for packet loss. In order to properly perform traffic engineering in a network, the number of calls that should be admitted that must traverse a limited-bandwidth link should be carefully selected to avoid overloading the link. Additionally, priority policies should be utilized to prioritise time-sensitive data such as voice [17]. Non-optimal routing can cause packet drops if packets are lost on their way to their destination [9]. Routing flapping, due to missing or invalid routes are two common network problems that cause packet loss and therefore, proper monitoring systems are needed in order to keep track of route changes, along with routing and IP configuration problems [10].

In an Ethernet environment, a very common issue that causes packet drops is duplex mismatch of the interfaces. Duplex mismatch is caused when the one side of the connection is set to full duplex, while the other side is set to half duplex. When this mismatch occurs, Frame Check Sequence (FCS) or non-alignment errors appear on the interfaces of the switches or routers along the traffic path causing packet drops [17]. This problem can be identified by SNMP queries in order to retrieve the interface configurations. Poor cabling and connectors are another reason for packet loss, since they cause transmission errors in the switches or routers and can be also identified via SNMP queries. [17].

Play-out (de-jitter) buffers used in the end-devices to provide steady voice play-out can also be a reason in certain cases for packet loss. When the size of the buffer is too small, late packets will not have been received in sufficient time to be played out leading to the sound having gaps. This problem can be identified from the RTCP statistics (especially the VoIP

QoS metrics). However, this means that the VoIP operators have to implement and enable RTCP in their solution.

4.1.2. Delay

Delay is the amount of time that it takes for a packet to travel from the source to the destination. Voice applications are time-sensitive and therefore, the ITU has defined bounds for the one-way delay for VoIP in their Recommendation G.114 [17]. See Table 1.

Table 6: Recommendation G.114 Delay Specifications [17]

ITU Recommendation - Range in Milliseconds	Private Network Recommendation - Range in Milliseconds	Description
0 to 150	0 to 200	Acceptable for most user applications.
150 to 400	200 to 250	Acceptable provided that administrators are aware of the transmission time and its impact on the transmission quality of user applications.
Above 400	Above 250	Unacceptable for general network planning purposes. However, it is recognized that in some exceptional cases, this limit will be exceeded (for example, satellite connections)

There are two types of delay in a VoIP network: fixed delay and variable delay. Fixed delay is the constant latency component in every voice session and does not depend on the network conditions. Variable delay is the latency component that changes based on network conditions and processor utilization (at the SBC and the source and destination). The variable latency can also depend upon which CODEC is used and which software and/or hardware is used. Fixed delay includes the following types of delay [17]:

- Processing delay is the amount of time spent by the Digital Signal Processor to encode and decode the voice samples. This delay is different for different CODECs used and may also depend on the local processor’s speed. Thus, CODECs such as G.711, that do not use compression have minimal processing delay. CODECs that need multiple voice samples to encode the voice need to have these additional samples before they can do the encoding. This delay is called algorithmic delay. For example, G.729 adds 5 ms and G.723.1 adds 7.5 ms of algorithmic delay.

- Packetization delay is the amount of time required to fill the outgoing packet with the voice payload and to add all of the necessary headers. In order to reduce packetization delay, smaller packets can be used. However, this solution increases both packet rate and overhead (due to the fixed overhead per packet).

- Serialization delay is the amount of time needed to send the packet out through a network interface (this occurs on the receiving and sending interfaces of each router along the path, unless cut-through routing is used).

- Propagation delay is the amount of time taken for a bit to travel from the one side of a link to the other. This delay depends on the type of link being used, for example the link could be a copper cable, optic fibre, microwave link, etc.

Variable delay includes the following types of delay:

- Queuing delay is the amount of time that a packet has to wait in a router's or switch's buffer queue in order to be forwarded. Usually, in a VoIP network, voice packets are prioritized over other IP traffic since they are time-sensitive. However, only one packet can be sent by each interface at a time, hence the packet may have to be queued for the serialization delay of a packet in front of it and for existing RTP packets that are ahead of it in the queue for an outgoing interface.
- Delay due the play-out buffer, which can cause latency if its depth gets too large, since the samples have to wait until they are played -out. This play-out buffer is used to hide jitter due to packets arriving somewhat late [11].
- Delay due to network congestion is the latency caused by overloaded links in the network. This problem can be avoided by avoiding overloaded links - either by proper network dimensioning or by routing around heavily loaded links. Usually, this is caused in the low-speed links where even a single packet has to wait a significant amount of time before being transmitted.
- Unexpected network outages, which can cause sudden increases in latency of the network. For example, if a link or a device goes down, this can cause backup links or devices to take its place which may necessitate routing packets over different paths. Under these circumstances, backup links can become overloaded or routes can be mis-configured.

4.1.3. Jitter

Jitter is the variance in delay of the packets arriving at the destination. Ideally a voice stream should be such that the VoIP packets arrive with the same time intervals between packets at the end device. However, due to the varying network conditions, packets may arrive at the destination with different inter-packet time intervals, for example some packets arrive later than others. Jitter can be caused by queuing or buffering, network congestion, and non-optimal bandwidth utilization.

Figure 15 describes how jitter appears in the network. Packets A and B arrive at times D1=D2 ms at the destination. However, packet C is delayed and it arrives following a different time interval D3. The time difference between the expected arrival time and the actual arrival time of packet C is called jitter.

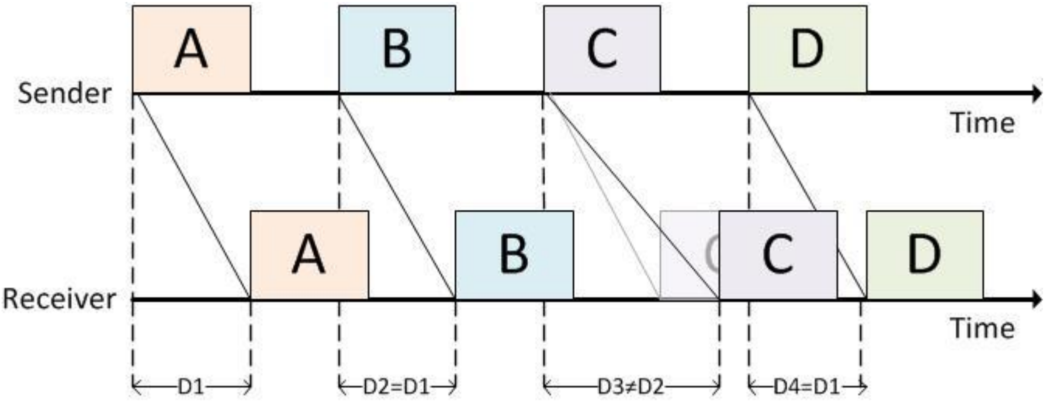


Figure 15: Jitter description [17]

In order to minimize the effects of jitter, play-out (de-jitter) buffers are used. These play-out buffers are used in the VoIP end-devices to control the variation in packet delays so that packets are forwarded to the CODEC in an orderly manner [1]. However, determining an appropriate buffer depth requires trade-offs between packet loss and delay [11]. If the depth of the buffer is set too small, then the packets arriving late will cause problems with the output audio since they will not be processed in time. On the other hand, if the buffer depth is set too big, then this will cause additional delay in the voice playback [9]. Figure 16 below depicts how the de-jitter buffering works.

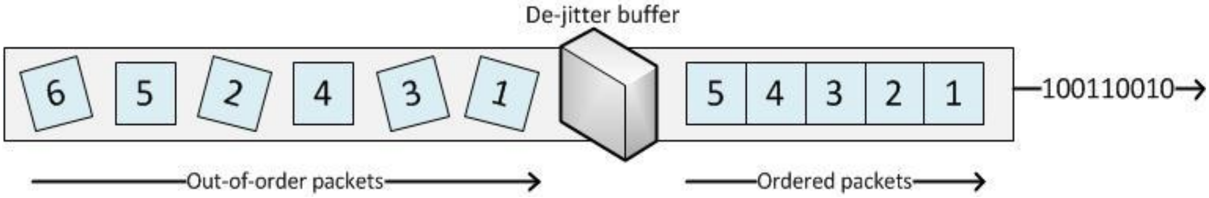


Figure 16: Jitter buffering and packet loss compensation [1]

Another way to reduce jitter is to prioritize the VoIP traffic so that voice packets will be less affected by problematic network conditions. Another method to perform traffic shaping is to control in a more optimal way the VoIP traffic. Reducing the actual delay will not help reduce jitter, but it will help reduce the effect of jitter (as there is more time to hide the effects of jitter) so as the problem of jitter will be less noticeable to the end-users [4].

4.1.4. Sequence errors

Packets travel towards their destination through different paths and when they reach the end-point they may be out-of-order. RTP provides the information necessary to re-order the packets. However, when it comes to time-sensitive services such as VoIP, out-of-order packets can cause problems since the end devices will either discard them immediately or the de-jitter buffer will drop them if the buffer reaches its buffering limit, thus causing packet loss. Sequence errors cause serious degradation in voice quality and one way to limit the problem is to implement consistent routes for the voice packets and optimal routing policies [4].

Each RTP packet contains in the RTP header a sequence number field, which increments by one for each RTP packet sent and helps the receiver to reconstruct the voice stream, as well as to estimate the number of packet drops in the stream. This information can be used then in order to identify possible network outages or other problems in the voice path [26].

4.1.5. CODEC distortion

Depending on the CODEC used, the voice quality can be reduced or increased. When there is limited available bandwidth, a suitable CODEC must be used that generates outgoing traffic at a lower rate, however this generally provides lower quality voice or requires increased resources (such as increased processing). A good CODEC choice matches the quality with available bandwidth. Moreover, when the voice traffic travels through the different network providers and carriers (especially in long-distance calls), transcoding might be needed in certain borders (when voice data are transformed from one CODEC to another) which can deteriorate the voice quality [3].

4.1.6. Echo

Echo is one of the most common problems in voice services and one of the most difficult to troubleshoot. Traditional voice services (PSTN) always suffered from echo problems; while in VoIP services echo effects can be both greater since the IP network (for example due to delays in the IP network) or lesser when appropriate signal processing is done in the UAs. There are two sources of echo [17] [21]:

- Hybrid echo is caused in analog voice circuits using two-wire connections for the transmitting and receiving signals over the same two wires. However, when the voice moves to digital circuits, then four wires are needed since the transmitting and receiving signals must be separated. This conversion from two-wire to four-wire connections can cause echo problems when it is unbalanced.
- Acoustic echo is caused by voice equipment interaction, usually between a headset or speaker with the microphone of the same device. Echo is caused because the microphone picks up audio signals from the speaker(s) and retransmits them. However, newer devices include acoustic echo cancellation via digital signal processing in order to avoid this problem.

Echo is influenced by latency and loudness. The more delayed the echo is, the quieter it should be in order not to be noticeable by the end users. The IP packet network does not cause additional echo, however it makes the problem greater since it adds additional latency due to CODEC processing and IP network delays as the voice packets travel from source to destination. When the round trip delay is less than 50 ms then, then echo is not very noticeable, while for round trip delays beyond 50 ms the echo will start being more and more distinguishable by the user unless it is very low in volume [5]. Echo is reduced with the use of special devices called echo cancellers. They are responsible for dynamically detecting, controlling, and removing echo from the voice channels and they are recommended to be used when the one-way delay in the network exceeds the 25 ms [17].

4.1.7. Connectivity loss

There are many reasons that can lead to call setup problems and dropped sessions. The most usual case is the loss of connectivity somewhere in the path between the voice endpoints. This connectivity can be lost due to different factors, as described below:

- Network outage, due to physical damage to the equipment or the transmission links (for example a cable being cut). If there is a transmission problem or a network component goes down, then physical connectivity will be lost and the session might not be established or might be abnormally terminated.

- Interface duplex mismatch is a very common problem in networking. It happens when the two sides of the connection have different duplex settings (one side half duplex and the other full duplex) and this can cause broken speech or a call to eventually be dropped due to multiple packet drops [19].

- Missing routes, which can be caused either by a physical outage somewhere in the network and consequently loss of the ability to advertise certain route prefixes or by mis-configuration where a route is missing in the routing configuration of some equipment. A missing route can lead to dropped sessions, as RTP packets cannot be delivered or the call setup might not be successful due to SIP messages not being successfully exchanged. Another cause for a missing route is when the limit in routing tables has been reached in the router's configuration causing some received routes to be dropped from the routing table (for example, in a VPN/VRF table where only the routes needed for the call setup are included in the table).
- Router access control list blocking, where a router denies access to packets for some reason, i.e., they do not fulfil the configured access policies. In this case, packets reaching the router will be dropped and the session will not be able to be established or an existing session will not be able to continue to exchange media. This problem can be caused by mis-configuration, i.e., where the wrong policies are configured in the router. This could also be caused by errors at the source (for example, incorrect source address configuration).
- Problems with the VoIP equipment, such as the SBC. Mis-configuration or access control policies can lead to connectivity loss since the signalling or voice packets are not processed by the device. For example, an incorrect source address in the SIP Invite message will lead to the SBC declining the INVITE and responding with a 403 Forbidden code error message (as shown in the example in sections 3.2.3.3). CAC is usually implemented in the SBC, thus if the call originator exceeds the configured maximum number of simultaneous session limit or the maximum configured bandwidth, then the SBC will start rejecting new calls (although the existing calls will continue).

4.1.8. Protocol error

In VoIP, problems often occur due to errors in the protocol's implementation. Very common problems are an incorrect description in a SIP packet of the source address or the destination address. If the call initiator places the wrong source IP address in the SIP packet, then a SIP error response may be generated by a network or VoIP device in the path as access control policies implemented may reject this packet (this can occur when the equipment has been configured so that only packets with a certain source IP address are allowed).

Moreover, if the destination IP address is an error, then the session will not be able to be established since the VoIP devices cannot process the destination IP address correctly. For example, a typical issue faced in the industry is when the destination number has been included by the call initiator without the "plus (+)" sign, which indicates that this is a national call while the actual destination should have been an international number. In this case, the initiator may receive an error message that the destination is unreachable or might reach the wrong party. Another problem occurs when the SDP message has an incorrect format and cannot be processed by the VoIP devices, leading to a SIP error message being generated and sent back to the source in order to notify it of the error.

When a session is in the process of being setup, the CODEC type to be used is decided through the exchange of SDP messages. This procedure is called CODEC negotiation and there is a possibility that the endpoints will not manage to decide upon any CODEC, then the session cannot be established. This case does not happen often (as nearly all implementations implement a G.711 CODEC), however it is a potential problem.

There are certain SIP error responses generated during an ongoing session setup, if a problem is encountered. The error code responses are generated and sent back to the source indicating that an error has occurred and to provide relevant information in order to identify this error. RFC 3261 [18], which defines the SIP protocol, analyses in detail the possible SIP error responses. Table 5 contains an overview of the SIP error responses that can be generated when an unexpected problem occurs in the VoIP call setup which needs troubleshooting.

Table 7: SIP error response codes [18]

SIP Response Codes	Description	Possible Causes
400 Bad Request	The request could not be understood due to malformed syntax.	The session initiator has sent the SDP message in a format which the end-device is not able to process.
403 Forbidden	The server understood the request, but is refusing to fulfil it.	The request received cannot be processed due to restriction policies. For example, the source IP address of the SIP Invite request is not allowed or is not valid.
404 Not Found	The server has definitive information that the user does not exist at the domain specified in the Request-URI or the domain does not match any of the domains handled by the recipient of the request.	The destination phone number is not valid or the user (recipient) is not registered with the incoming proxy server.
408 Request Timeout	The server could not produce a response within a suitable amount of time.	The server is not able to find the user's location in time or there is a network problem with the remote subnet (such as a physical outage), causing delay.
415 Unsupported Media Type	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.	The request received contains media types that are not supported by the server.
482 Loop Detected	The server has detected a loop.	The server detects a loop of the received request based upon examining the Via field of the SIP message.

483 Too Many Hops	The server received a request that contains a Max-Forwards header field with the value zero.	Non-optimal routing or manually break the line mis-routing of the SIP packet has leaded the packet's forwarding to exceed the maximum hops allowed.
484 Address Incomplete	The server received a request with a Request-URI that was incomplete.	The destination number is incomplete, a special prefix is required by the provider or calls are only allowed to specified destinations
488 Not Acceptable Here	The response has the same meaning as 606 (Not Acceptable), but only applies to the specific resource addressed by the Request-URI and the request might succeed elsewhere.	The SDP negotiation between the endpoints has been unsuccessful due to media, lack of bandwidth, or addressing mismatch.
503 Service Unavailable	The server is temporarily unable to process the request due to a temporary overload or scheduled maintenance of the server.	The server (for example the SBC) has an internal problem and cannot process the request. This problem can be overload, internal scheduled maintenance, or a hardware malfunction.
513 Message Too Large	The server was unable to process the request because the message length exceeded its capabilities.	The call initiator is sending messages than the server cannot handle.
606 Not Acceptable	The user's agent was contacted successfully, but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable.	The SDP negotiation between the endpoints has been unsuccessful due to media, bandwidth, or addressing mismatch.

4.1.9. One-way or no-way audio

One-way or no-way audio means that the session has been established and the call has been setup, however either both users are not able to hear each other (no-way audio) or one of the users is not able to hear the other one (one-way audio). This problem usually stems from connectivity issues, mis-configuration, NAT/PAT, or a firewall.

Connectivity issues and mis-configurations are common problems in IP networks and can cause connectivity loss in some parts of the network or mis-routing (as has already been discussed in a previous section). When connectivity loss or mis-routing occurs while media traffic is being exchanged between two or more end-points, then the users can experience audio problems (one user cannot hear the other or both users cannot hear each other). When one-way or no-way audio is the symptom experienced by the end users, then the IP connectivity as well as all the relevant device configurations should be checked in order to find out the actual cause of this problem.

Unfortunately, one-way or no-way audio is usually the result of a firewall or NAT/PAT along the path. Firewalls are frequently used as a border security component for a subnet. The firewall provides traffic access control by allowing only certain packets to pass. This decision of which packets to forward is based on a variety of policies that may include specific protocols, ports, source and destination IP addresses, etc. NATs/PATs provide topology hiding for private networks. They are frequently located at the border of a private network and are responsible for mapping private addresses of the outgoing packets into public addresses, as this is necessary in order to forward the packets to public networks. They also map the public destination IP address of the incoming packets back to their corresponding internal private addresses and forward the packet internally to the actual destination.

Firewalls and NATs/PATs are a big challenge for VoIP, especially for the media traffic. For the signalling traffic, these devices are not usually a problem since SIP uses a single port number for message exchange (port 5060) hence firewalls can be configured to allow traffic originated from or destined to port 5060. Unfortunately, the SIP messages include source and destination IP addresses in the SIP headers and/or in the SDP, hence the NATs/PATs need to be aware of the SIP signalling - especially which end-points are setting up a session.

For the media traffic (voice traffic in the case of VoIP) firewalls and NATs/PATs have serious negative effects. First of all, when a SIP session is being setup, the end points exchange SDP messages in order to negotiate the resources needed for the VoIP call such as the desired RTP source/destination IP addresses and ports for the voice traffic and which CODEC to be used for the voice data encoding (along with other parameters). Unfortunately all of this information is embedded in the SDP in the body of the SIP messages, hence unless the firewall/NAT/PAT is SIP aware it will not open holes in the firewall for this traffic and the network address translation and port mapping will not be set up correctly.

Unlike the SIP signalling, RTP does not use a single fixed port number, as the RTP port allocation is dynamic. The port number to be used is embedded in a SDP message. This can be a problem for firewalls since unless they are SIP aware they will not know which UDP port will be used by the RTP of this session, hence they will probably block the RTP traffic. Figure 6 depicts this problem with a firewall. Moreover, the RTP source and destination IP address information is also specified inside the SDP messages, if these IP addresses are private (for example if the negotiation was originated by a device within a private network and hence behind a NAT/PAT) then these address will not be reachable from outside this private network [6] [20]. Figure 7 shows an example of NAT that can cause a problem due to the RTP packet's private source IP address. Due to all of these issues, firewalls and NATs/PATs can cause one-way or no-way media if one side of the connection or both sides are located behind firewalls and NATs/PATs that are not SIP aware.

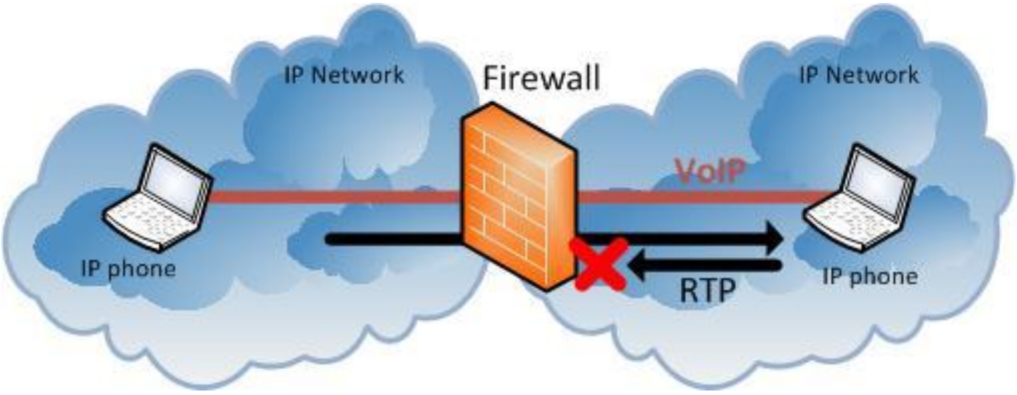


Figure 17: Firewall problem in VoIP [20]

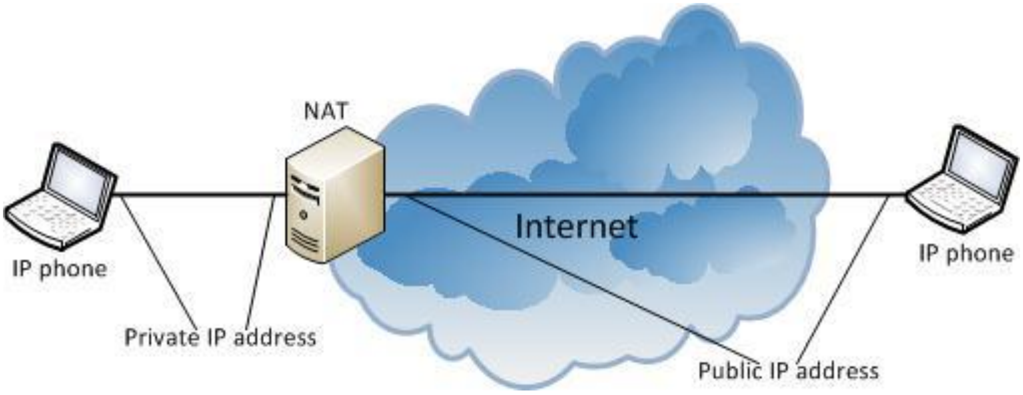


Figure 18: NAT implementation in a VoIP session [20]

4.1.10. End-points problems

Background noise is a usual problem that can negatively affect voice quality as experienced by users. Noise exists everywhere around a user and it is always incorporated into the voice packets along with the actual user's voice. There are ways to eliminate this noise; however these methods can lead to the other party's perception of a "dead line" (i.e., that there is absolute silence when the party is not speaking). For this reason some UAs include a feature called "Comfort Noise Generation" which generates suitable background noise to avoid the listener experiencing a dead line perception [3]. Comfort noise can also be generated when there is no packet to play-out due to a dropped or late RTP packet.

Audio level mismatch is another common issue that occurs where the two users' phones have different volume levels. This decreases the perceived call quality. This can be caused due to the parties using different vendor equipment or because the equipment differs in sound sensitivity. Users should try to adjust the volume level of their phone in order to eliminate this problem [3].

Different vendors have developed different phone and VoIP equipment. This may lead to endpoint incompatibility. For example, different end user devices may have different constraints causing the call setup procedure to be complicated or even unable to be completed due to unsupported functions for the party to the desired call.

A common compatibility problem is CODEC mismatch. When a call is being setup, a negotiation between the endpoints is performed in order to agree upon a CODEC to use for the voice encoding. This negotiation takes place within the exchanged SDP messages. However, there is a possibility that this negotiation is unsuccessful; hence the call setup cannot be completed, if the two endpoints do not support at least one common CODEC [17].

4.1.11.Voice related problems

In today's commercial VoIP environment two different types of networks have to co-exist: IP and PSTN. Calls are established and traffic travels between several network providers, hence the signalling and media have to be translated from one type of voice network to the other (IP-to-PSTN or PSTN-to-IP). This interconnection between IP and PSTN can often cause problems in call setup or lead to poor voice quality.

For this interconnection, special signalling gateways are used that translate one signalling protocol to the other (SIP-to-ISUP or ISUP-to-SIP), as well as media gateways that interconnect the media traffic from one network to the other (IP-to-PSTN and PSTN-to-IP). These translation procedures have to follow certain rules, however since the protocols are based on fundamentally different designs, the translation does not direct cause faults in translation from one protocol message to the other. However, the interconnection between IP and PSTN can lead to problems since they are very different network designs and use different state machines, timers, etc. Some of the problems that can appear are [22]:

- There are several types of ISUP implementations that have different message flows, thus when an IP network interconnects two PSTN networks, the egress signalling gateway must address this issue when translating from one ISUP message to another ISUP message.
- When a call is initiated in the PSTN, the signalling messages utilize ISUP. However, certain servers transform the SIP headers according to transformation rules that do not always comply with the ISUP message encapsulation leading to a protocol violation.
- European phone numbers do not have a fixed length; therefore the ingress signalling gateway is unable to recognize if a number is incomplete. The number format is also translation-problematic, since national and international numbers are not always easily distinguishable.
- The Multipurpose Internet Mail Extensions (MIME) multipart format can be used by certain gateways in order to include both SDP and ISUP elements into the same SIP message. This can cause an interoperability problem when not all the gateways have this feature enabled.
- The transformation and translation between the different signalling protocols is also a security risk since there is opportunity for fraud during the translation procedures.

In addition to the interconnection problems, other faults can occur in the PSTN/TDM network. A summary of the most common problems in PSTN networks is presented according to [27]:

- Physical/hardware failures in the voice switches or cabling can cause connectivity loss or service quality degradation.
- Network overloads due to exceeding the system’s design capacity can lead to service quality degradation and dropped calls.
- Software errors and mis-configurations in the voice network components can cause signalling and traffic routing problems.
- Clock synchronization problems can affect the voice quality.

4.1.12.VoIP technical cause analysis diagrams

There are many different methods for root cause analysis that can be used for troubleshooting analysis. These methods are described and compared in [24]. For the cause analysis in this thesis's case study, the Ishikawa Fishbone method will be used (this is also called the Cause and Effect diagram). This method has been selected because it seems to best match the requirements for troubleshooting analysis in a carrier's implementation of a VoIP system.

The Fishbone diagram presents the main causes and sub-causes that lead to a specific effect (symptom). The diagram resembles a fish's skeleton, where the fish head illustrates the problem that needs to be resolved (symptom/effect) and the fish bones indicate the potential causes of the problem and are placed and categorized in different types along the branches. The Fishbone method is actually a brainstorming tool used for cause and process analysis and it helps recognize the actual causes of certain problems by following the fish branches (cause categories and sub-categories). Since this method allows the separation and the categorization of possible causes leading to specific symptoms, it is appropriate and suitable for this particular case study's troubleshooting analysis [28] [24].

In this analysis, only the technical side of the service troubleshooting has been considered. The VoIP problems are categorized into three major symptom types based on the fact that each type belongs to a different family of effects on the user's experience. Table 3 describes each of these types.

Table 8: VoIP symptom categories

Symptom Categories	Description
Call not established	The signalling session cannot be completed and the call cannot be established between the endpoints.
One-way or no-way audio	The call has been established between the end-points, however one or both of the users are not able to hear each other.
Call quality degradation	The call has been established between the end-points, however the audio quality is low.

Moreover, the potential causes of VoIP problems have been categorized into six types (i.e., families) based on the source of the problem(s). Each problem source can contain various types of fault causes and the categorization is based on the type of fault or failure that can occur in the VoIP implementation. Table 4 lists and describes these categories.

Table 9: VoIP cause categories

Cause Categories	Description
Connectivity loss	Connectivity has been lost somewhere along the path between the endpoints.
Protocol error	There is a problem with the protocol implementation, for example incorrect message formatting.
Network performance degradation	There is poor connectivity between the endpoints which degrades the service, such as packet loss, delay, or jitter.
SBC related	The SBC is causing a problem to the voice connection.
Voice related	The voice side (PSTN/TDM) of the VoIP implementation has a fault which is translated into the IP side as well.
External factors	Other external factors are causing a problem in the VoIP connection.

This section presents three Fishbones - one for each symptom category - where every fishbone contains the six cause categories (see Figures 8, 9, and 10). Some of the main cause categories also contain sub-categories leading to additional possible fault causes. This analysis focuses only on the technical aspects of VoIP troubleshooting and categorizes the possible causes of each symptom based on literature sources, research work, and actual experiences in the company's environment.

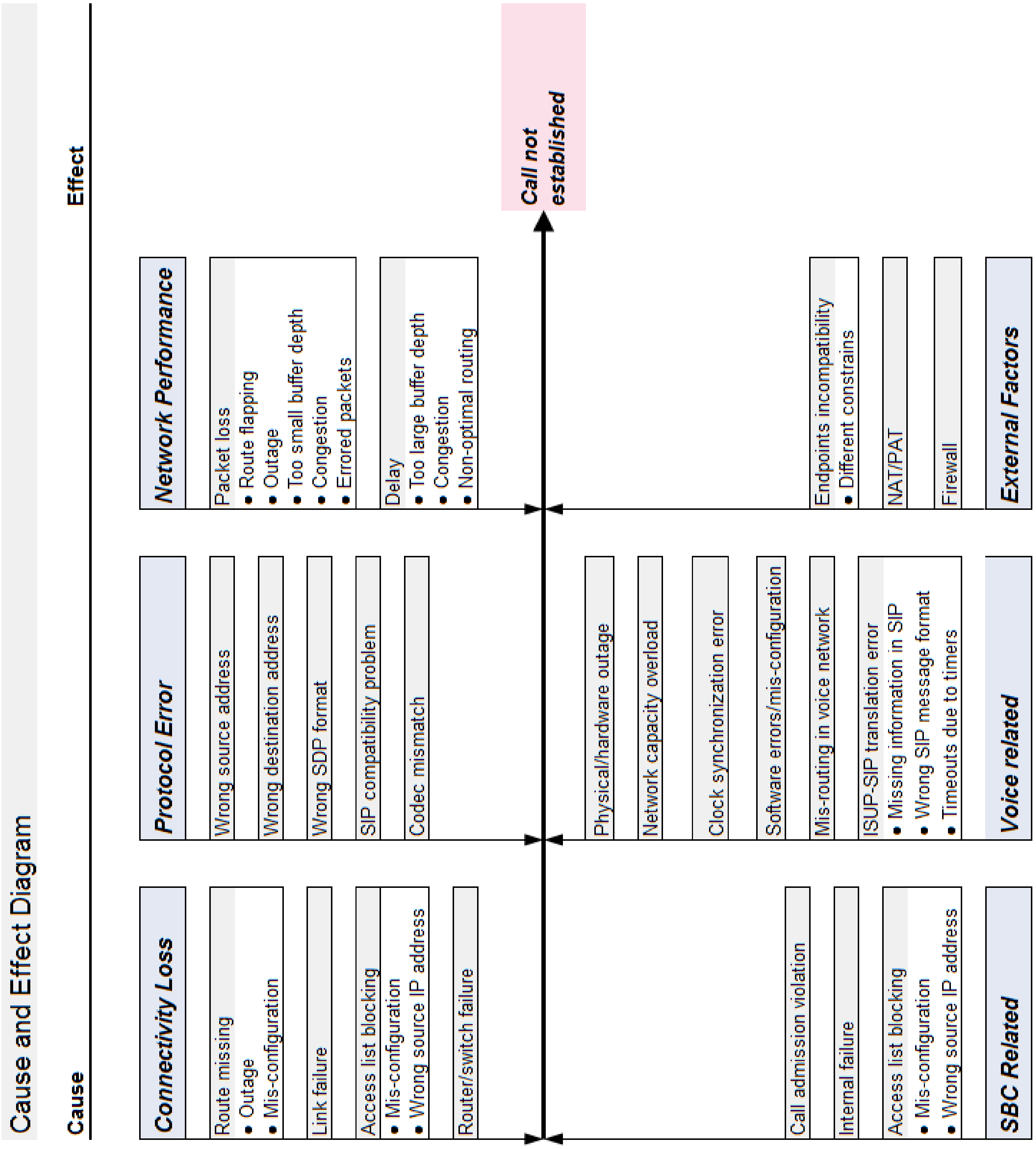


Figure 19: "Call not established" diagram [Spread sheet template: http://www.vertex42.com/]

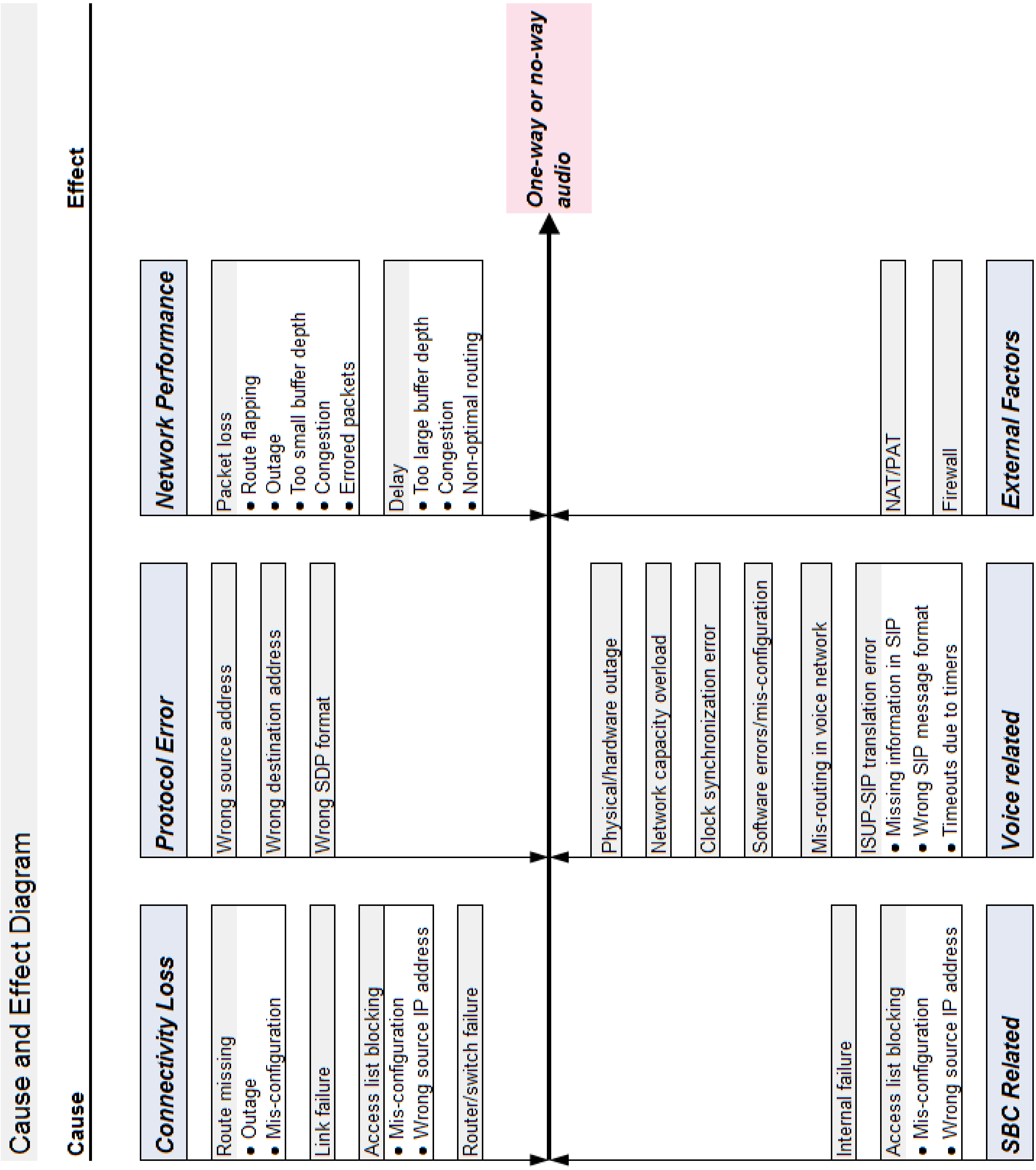


Figure 20: "One-way or no-way audio" diagram [Spread sheet template: http://www.vertex42.com/]

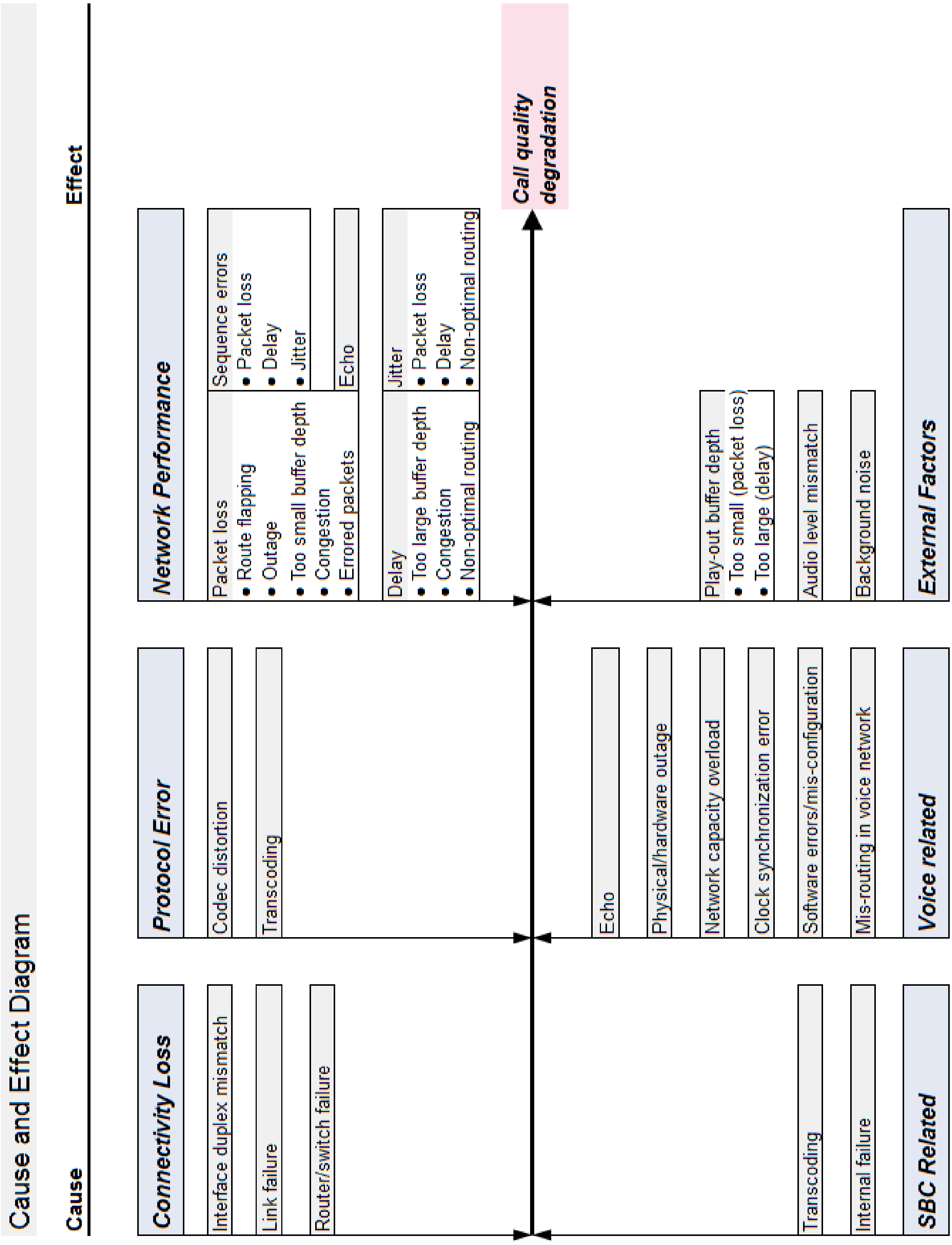


Figure 21: "Call quality degradation" diagram [Spread sheet template: http://www.vertex42.com/]

4.2. **VoIP organizational troubleshooting procedures within the company**

Apart from the technical aspects of the troubleshooting procedures within the company, it is very important to build efficient organizational procedures internally, in order to properly provide customer support and comply with the SLAs. Sections 4.2.1 and 4.2.2 analyse the organizational difficulties in VoIP fault handling and recommend improvement steps and additional procedures that can assist in order to achieve efficient VoIP fault management.

4.2.1. Organizational problem definition

As first step in the internal fault handling procedure, the Customer Care (CC) department is the main contact between the company and the customer. The CC is responsible for contacting the customers, opening and handling Trouble Tickets (TTs). After the TT is opened, the CC can perform a first analysis of the issue according to the provided information and decide upon possible problem causes.

As a next step, if the problem needs further technical investigation, the CC will hand over the case to the second-line support teams. For the fault handling procedures within the second-line teams (NOCs), a survey within the company has been conducted addressed to the NOCs' personnel responsible for the VoIP fault troubleshooting. This survey includes questions regarding the troubleshooting methods followed and improvement suggestions and comments.

This survey resulted in the following considerations:

- There is lack of information and necessary details regarding the reported problem from the customer. The NOCs would perform investigation faster and easier if the correct information is collected from the beginning.
- There is a certain difficulty during the initial problem investigation in identifying if the issue is PSTN or IP related. This difficulty stems from the lack of specialized VoIP knowledge, such as protocol functions, product technical planning details, VoIP device configurations, etc.
- The VoIP technical troubleshooting is not very efficient, since, due to the lack of specialized VoIP knowledge, the cause analysis performed is mostly based on the most common faults in PSTN or IP networks than on the most possible VoIP faults.
- The escalations to the third-level can be often, due to the facts that the NOCs need assistance in troubleshooting a VoIP issue and the third-line support has the VoIP knowledge needed and the technical resources to resolve the problem.

Regarding the considerations resulted from the survey, the main concern appears to be the lack of VoIP specialists among the NOC personnel. The Voice NOC is a team of specialized engineers in PSTN networks and POTS telephony systems who have the knowledge and expertise to troubleshoot traditional voice issues. On the other hand, the IP NOC is a team of specialized engineers in IP networks who have the knowledge and expertise to troubleshoot IP-related faults. Therefore, when a VoIP problem is reported, each NOC has their own part of expertise in the area, where the Voice NOC is checking the PSTN side and the IP NOC the IP side. However, that implies that there is a certain difficulty during the problem investigation procedure to identify the cause of the problem, especially when it is not related to normal PSTN or IP issues. For example, when a problem is IP related and it is handed-over to the Voice NOC, it is not clear from the beginning for the engineers to identify if the problem is indeed PSTN-related, and therefore they are checking this side for any common PSTN problems according to the usual routines and after the investigation does not show any faults there, they hand-over the case to the IP NOC, so they can check their side. However, this way of fault handling is not very efficient since valuable time can be lost if the investigation begins from the wrong point.

In addition, after the investigation from the NOCs is completed, if the problem causes cannot be identified (for example due to the fact that the problem is VoIP technology-specific), the TT is handed over to the third-line support team, which has the VoIP specialized knowledge needed for the troubleshooting. For example, if the problem is related to a protocol error, then the third-line support has the resources and knowledge to perform the necessary tracing or investigate the SBC configuration, analyse the results and identify the cause of the problem or error.

Figure 22 depicts a diagram of the escalations and resources needed according to the organizational procedures.

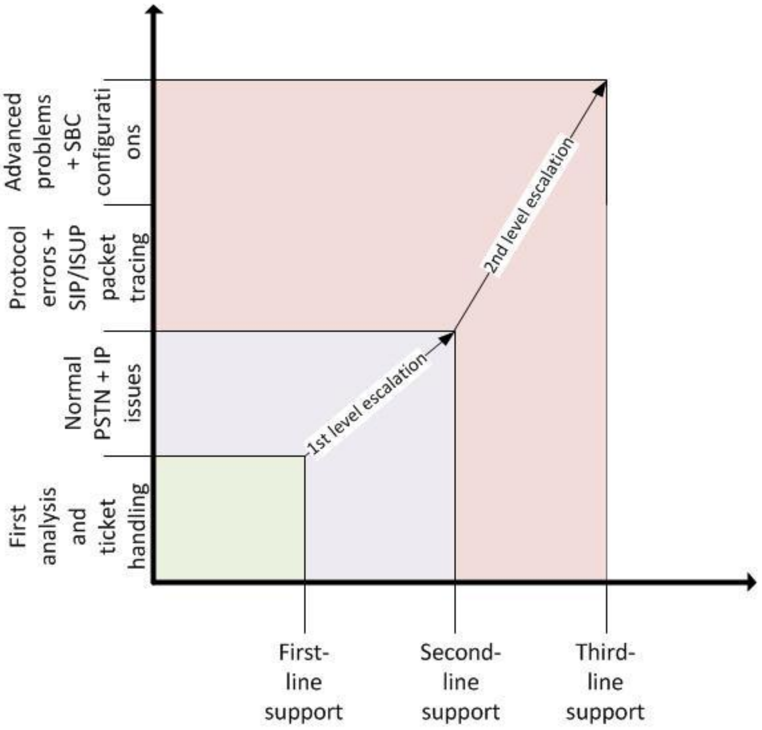


Figure 22: Diagram of escalations and resources

4.2.2. Improvement recommendations

The main goal of any improvement suggestions is to minimize the escalations and resources spent in the company in order to provide customer support and fault handling in VoIP issues. In order to achieve this goal, certain improvement steps can be implemented in each level of the internal fault management procedure.

First of all, it can be very useful for the CC and NOCs to have proper documentation for each VoIP customer and their technical solution. This information should include technical implementation details, for example product description, IP source and destination addresses, protocols and CODECs used, any unique configuration parameters, bandwidth and access limitations, etc. This information is useful since the CC and the NOCs can have all the details regarding the technical implementation and solution of each customer available at any time when they need to initiate troubleshooting.

Since the CC is the first and main point of contact with the customer, it is essential to gather all the necessary information from the customer regarding the problem that they are reporting. This is analysed in detail in section 4.3 and a questions-template is suggested which can improve the fault handling and investigation. Therefore, the CC should first provide the questions-template suggested in section 4.3 to the customer in order to collect the necessary problem details and accordingly open a TT to follow up the case. Continuously, the CC can perform a first analysis of the issue according to the provided information in the template and decide upon possible cause categories.

Since the network is monitored, any outages or faults will be detected by the NOCs. In this case, the NOCs should send out notifications to the CC regarding any known problems in the network, so the CC can be prepared and immediately inform the customer if the problem they are reporting is related to any outage. This can be decided upon looking in the answers of the customer in the questions-template where one can see if the problem description and the information provided are matching the current outage. For example, if a customer reports connectivity issue to the SBC and their access router equipment has been down, the CC can inform the customer of the reason of their problem without the need for escalating the TT to the second-line support. In this sense, certain escalations to the second-line support can be avoided.

Additionally, the CC can receive necessary training in an entry level regarding VoIP issues in order to be able to perform a first analysis of the problem reported. This training can include information useful on how to analyse a problem based on the information that the customer provides (see section 4.3) and identify possible cause categories. For example, if there is an IP connectivity issue reported, the CC can investigate where the problem is based on a traceroute that the customer provides (e.g. if the problem exists in another provider’s network, etc.).

When a case is escalated to the second-line support, with the introduction of the questions-template, the NOCs will have all the information needed to initiate the problem investigation. In this way, the time spent for problem investigation and resolution can be significantly reduced. It is also clear from the survey outcome that VoIP-specific training is needed for the NOCs in order to understand the nature of VoIP faults and investigate efficiently the problem. For example, a lot of time spent in the investigation can be saved if the NOCs are able to recognize easily the PSTN or IP origin of the fault without the need to check first all the common problems in each side, but instead to evaluate the most possible problem causes and start the investigation from that angle. A recommended technical troubleshooting routine for the company’s products A and B is presented in section 5.1 as a part of the conclusions.

Additionally, one further step that can benefit the fault handling procedure and reduce the number of escalations to the third-line support would be to create a specialized VoIP NOC that belongs to the second-line support and consists of VoIP specialists. This can be achieved by selecting an adequate number of engineers from Voice and IP NOC (for example two engineers from each NOC) and train them to become specialized in VoIP services and VoIP troubleshooting. The training should include protocol functions (SIP, RTP), VoIP product descriptions, SBC functions, SIP packet tracing, VoIP fault handling etc. In this way, the second-line support will always have VoIP specialists that can troubleshooting in depth VoIP issues without the need to escalate these cases to the third-level. The third-level can be involved only in advanced problem cases where special treatment is needed or certain configuration changes and orders.

Figure 23 depicts a diagram of the escalation and resources needed if the recommended organizational improvements take place and can be compared with Figure 22. As Figure 23 shows, if the recommended organizational procedures are applied, more problem cases can be handled without the need to escalate to the second-line support and a large amount of cases can be resolved without escalation to the third-line support. In this way, the company can reduce the number of tickets that are escalated.

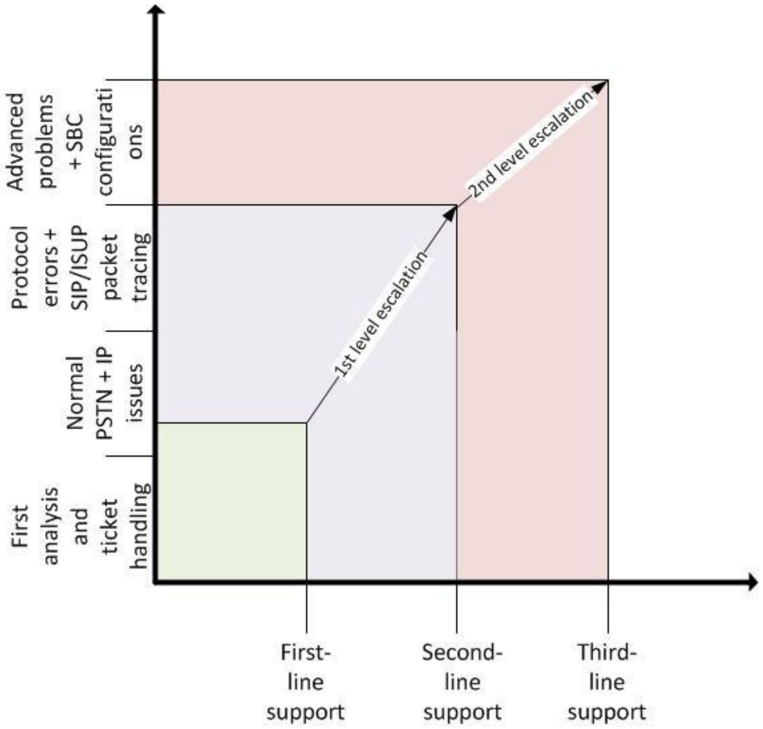


Figure 23: Improved diagram of escalations and resources

4.3. **Problem information collection**

According to telecom companies' procedures, when a customer wants to report a fault they have to contact the Customer Care department, who in turn have to open a Trouble Ticket for this case. When the ticket is opened, the analysis and investigation of the problem begins based on the data registered in the ticket. However, when the data describing the problematic issue are not adequate, the effort and time needed to resolve the case increase significantly. Therefore, it is very important to receive and register all the necessary information from the customer when they report the fault. In this way, it is easier to analyse the problem based on the registered information, such as specific problem impacts, timing, alarms created, service history and lots of other details. A good way to handle this problem information collection is to define and distinguish what the actual information needed is in order to assist the problem investigation for specific problems. This section presents an analysis and recommendation of the information the Customer Care needs to collect from the customer in order to accommodate the investigation of a VoIP fault in the company.

According to the troubleshooting analysis performed in section 4.1, there are three different categories of user experience impact in VoIP. Therefore, the first information that the customer should provide is the actual impact of the problem they are experiencing, that is:

1. Call not established
2. One-way or no-way audio
3. Call quality degradation (including the type of quality issues they are experiencing)

The next step is to acquire a better understanding of the problem by gathering additional information of the impact. According to the source of the problem, the failure symptoms can differ. Therefore, a good plan is to separate possible additional symptoms that can accommodate the problem cause identification. For VoIP cases, the following need to be considered –in conjunction to the cause analysis in section 4.1-:

- If all calls are dropped, then it could be a connectivity issue that doesn't allow the customer to connect to their SBC interface. The connectivity issue could be for example due to a route missing, link failure, device failure, SBC internal failure, congestion, etc. In this case it is useful to receive a traceroute from the customer including the source and destination IP address, in order to locate the connectivity fault.
- If only some calls are dropped, then one thing to check is if these calls have something in common, such as source address of a specific User Agent. In this case, the cause of the problem could be that the IP address of the source is not allowed due to access list rules. Another possible cause could be call admission violation. If the customer exceeds the bandwidth or session number thresholds, then the SBC will start dropping the new calls while maintaining the ones in progress. Network performance issues can also lead to some calls dropped, for example in case of packet loss, congestion, etc. In this case it is useful to know if the problem that the customer reports has impact in all the calls or only in certain calls.
- For both cases (all calls or some calls dropped), it is very useful to know if the customer receives any SIP error responses from the SBC, for example 403 FORBIDDEN or 400 BAD SYNTAX. In this way, a lot of other causes can be eliminated and resolution can be focused on protocol errors and mis-configurations.
- If the customer reports that the voice quality is degraded, then it is good to know if there is any network performance issue in the network, where a traceroute can be useful in order to show if there is, for example, latency or a connectivity issue (in product B this can show problem within a different provider along the trace path as well).
- Even though the carrier has the possibility to perform packet tracing in the SBC, it is useful if the customer can provide a SIP trace themselves when they report a fault, which can speed up the troubleshooting process and minimize resources needed in the company.
- It is important to know the IP source address that the customer is using, in case it is needed for the problem investigation). The destination IP address that the customer uses is the SBC's outside interface which is already known, however it is useful if the customer provides the destination address in case they have multiple interfaces in the SBC (this can be avoided if proper documentation per customer is provided to the CC and NOCs, as mentioned earlier in section 4.2.2).

According to the above, the following questions-template is recommended to be used by the Customer Care in order to get all the necessary information from the customer:

1. *What is the impact of the problem, date/time and time zone observed?*
2. *Are all or only certain calls dropped (i.e. international, national, specific destinations/sources)?*
3. *Do you receive any SIP error responses and if yes, which type?*
4. *Is the connectivity problematic? Please provide traceroute with source/destination.*
5. *Please provide a SIP trace.*
6. *Please provide your source IP address and destination IP address.*

The following real-case problem reporting and resolution examples show the importance of the above information collection.

- **Example A**

A customer that uses Product A reports a problem. The description of the problem according to the questions-template should be registered as follows:

1. *What is the impact of the problem and date/time observed?*

   Calls are not established. Date/time: dd:mm:yy xx:xx.

2. *Are all or only certain calls dropped (i.e. international, national, specific destinations/sources)?*

   All calls are dropped.

3. *Do you receive any SIP error responses and if yes, which type?*

   No.

4. *Is the connectivity problematic? Please provide traceroute with source/destination.*

   No, the destination address is not reachable, the trace stops in the access router.

5. *Please provide a SIP trace (preferably an Ethereal trace).*

   No possibility for trace since connectivity is lost.

6. *Please provide your source IP address and destination IP address.*

   The source address is s.s.s.s and the destination address is d.d.d.d.

Resolution:

The customer uses the Product A, which means that they are provided with a physical port connection to one of the company's access routers and a VPN tunnel from their access port to the SBC. Since the customer reports that there is no connectivity to their outside SBC interface, it is clear that the company needs to check this connection. Since the ping stops in the access router, it seems that either there is a physical problem (e.g. the router interface is down) or the router does not know how to route the traffic to the destination.

Since there have been no alarms so far regarding physical network status, it is possible that the problem exists in the route configuration. After checking this configuration in the access router of the customer, it appears that the destination route has been disappeared from the VRF table of the customer's VPN connection, which is the reason why the connectivity to the SBC has been lost.

- **Example B**

A customer that uses Product B reports a problem. The description of the problem according to the questions-template should be registered as follows:

1. *What is the impact of the problem and date/time observed?*

   Calls are not established. Date/time: dd:mm:yy xx:xx.

2. *Are all or only certain calls dropped (i.e. international, national, specific destinations/sources)?*

   Only the international calls are dropped.

3. *Do you receive any SIP error responses and if yes, which type?*

   Yes, SIP 404 NOT FOUND.

4. *Is the connectivity problematic? Please provide traceroute with source/destination.*

   Yes.

5. *Please provide a SIP trace (preferably an Ethereal trace).*

   Provided.

6. *Please provide your source IP address and destination IP address.*

   The source address is s.s.s.s and the destination address is d.d.d.d.

Resolution:

The customer uses the Product B, which means that they are reaching the SBC via public Internet. Since the connectivity is established, this cause category can be eliminated. The investigation can begin with the fact that only the international calls are not established and additionally the customer receives from the SBC the SIP error response SIP 404 NOT FOUND. This information leads to the conclusion that there should be something wrong with the format of the international destination numbers registered in the SIP INVITE, and therefore they cannot be identified.

In this situation, it is useful to look at the trace provided by the customer or -in case the customer does not have the possibility for a trace- to perform a packet tracing by using the packet tracer implementation described in section 3.2.5. After performing the trace, the SIP INVITE message analysis shows that the international destination numbers are registered in the message without the use of the "+" sign (which is an indicator of country code number). Because the destination number does not include that sign, the system in the carrier's voice equipment assumes that this is a national call (call within Sweden) and adds "+46" in front of the number (which is Sweden's country code) which results in an unknown number. This is the reason why the international calls are dropped and in return the SIP 404 NOT FOUND is generated.

These two examples show the importance of the right collection of information from the customer when they report a problem. First of all, these questions cover a great extent of possible VoIP issues and they make easier the localization of the starting point of the investigation or even the identification of the problem. Secondly, when some of this information is missing, it can result in spending more time resolving the issue, since it is more difficult to eliminate cause categories from the beginning of the investigation and furthermore clues are might missing which are important for the cause identification.

5. Conclusions and future work

This thesis has investigated and analysed the planning and monitoring techniques and methods that are recommended to be applied to the commercial development of a VoIP product in a carrier's network, as well as has proposed troubleshooting and fault management procedures that can be introduced and followed within the company in both technical and organizational level. Chapter 5 provides conclusions regarding the above thesis work and recommended future work.

5.1. **Efficient VoIP technical troubleshooting**

The VoIP technical troubleshooting regards investigation and resolution techniques of VoIP problems reported by customers to their carrier. It is essential for a telecom company to develop the right technical troubleshooting procedures and routines that lead to fast and efficient Trouble Ticket handling and resolution. According to the previous chapters of this thesis, it is clear that efficient technical troubleshooting is actually a combination of suitable service planning & monitoring and VoIP problem cause analysis knowledge. Sections 5.1.1 and 5.2.2 provide conclusions regarding how the carrier can efficiently troubleshoot in a technical level their two different products.

5.1.1. Troubleshooting product A

Product A regards a direct connection of the customer to the company's access network and a VPN tunnel from the customer's access router to the carrier's SBC. When a customer reports a problem, the first step as mentioned in section 4.3 is that the Customer Care should collect the correct information by using the recommended questions-template. The problem investigation will be based on this information.

If the problem is reported by the customer as a connectivity issue (without any SIP error response generated from the SBC), a lot of time can be saved if monitoring and alarm functions are implemented as suggested in section 3.2. The alarms should show already if there is any problem with the physical connections, devices and transmission links, so the company will be already informed. Moreover, SNMP queries is a very useful way in order to check for poor cabling connections and the router interface configurations in order to identify potential transmission errors or problems with the interfaces' implementation.

In this case, if there are no alarms generated related to the customer's service, the investigation can begin with checking the routing/VRF/VPN/MPLS configurations. For example, in order to identify a connectivity issue, if traces/pings are unsuccessful, the routing table of the problematic router should be checked in order to assure that all the necessary routes are configured.

However, if the connectivity is lost in the SBC end, then the SBC configuration should be validated, as well as the access lists, call admission control settings (to check if the customer is blocked by the access control list or if they violate the session or bandwidth thresholds).

If the customer reports that they are receiving a SIP error response from the SBC, the investigation should start by checking the protocol functions. In this case, the SBC packet tracer –described in section 3.2.5- should be used in order to trace the traffic passing through the SBC between the customer's equipment and the carrier's internal gateways. The tracing results can show all the messages exchanged and further analysis of the messages can reveal what is the cause that generates the SIP error response. For example, the destination numbers may have the wrong format, the SDP text format may be incorrect, the source IP address may be blocked, etc.

There is also the possibility that the SIP error message is generated due to a fault in the PSTN side, where in this case an ISUP error message is generated and translated into a SIP error response. Therefore, if the tracing does not show any issue in the IP side, the PSTN side should be checked by performing ISUP traffic tracing. However, the troubleshooting analysis is out of the scope of this thesis and it is suggested as future work.

5.1.2. Troubleshooting product B

Product B regards connection of the customer to the carrier's SBC via public Internet. When a customer reports a problem, the first step as mentioned in section 4.3 is that the Customer Care should collect the correct information by using the recommended questions-template. The problem investigation will be based on this information.

If the problem is reported by the customer as a connectivity issue (without any SIP error response generated from the SBC), the first thing to check is the traceroute provided by the customer in order to identify the routing path used to reach the SBC, as well as the access router used for the customer to enter the carrier's IP network. In that case, after discovering this routing information, a lot of time can be saved if monitoring and alarm functions are implemented as suggested in section 3.2. The alarms should show already if there is any problem with the physical connections, devices and transmission links along the routing path, so the company will be already informed. SNMP queries should also be used in order to check for poor cabling connections and the router interface configurations in order to identify potential transmission errors or problems with the interfaces' implementation.

In this case, if there are no alarms generated related to the customer's service, there is the possibility that the problem exists within one of the other providers' network in the routing path (since it is via public Internet), which can also be identified from the customer's traceroute.

However, if the connectivity is lost in the SBC end, then the SBC configuration should be validated, as well as the access lists, and call admission control settings (to check if the customer is blocked by the access control list or if they violate the session or bandwidth thresholds).

If the customer reports that they are receiving a SIP error response from the SBC, the investigation should start by checking the protocol functions. In this case, the SBC packet tracer –described in section 3.2.5- should be used in order to trace the traffic passing through the SBC between the customer's equipment and the carrier's internal gateways. The tracing results can show all the messages exchanged and further analysis of the messages can reveal what is the cause that generates the SIP error response. For example, the destination numbers may have the wrong format, the SDP text format may be incorrect, the source IP address may be blocked, etc.

There is also the possibility that the SIP error message is generated due to a fault in the PSTN side, where is this case an ISUP error message is generated and translated into a SIP error response. Therefore, if the tracing does not show any issue in the IP side, the PSTN side should be checked by performing ISUP traffic tracing. However, the troubleshooting analysis is out of the scope of this thesis and it is suggested as future work.

5.2. **Efficient VoIP organizational troubleshooting**

Apart from the technical troubleshooting analysis and investigation within the company, the organizational troubleshooting procedures were also described and analysed in this thesis. This section provides the conclusions regarding this analysis and further considerations.

- Proper documentation regarding the VoIP customers and VoIP implementation or solutions per customer should be available for the CC and NOCs. The documentation should include information regarding the product that the customer uses, the implementation parameters (numbering, IP addresses, access router –for product A-, bandwidth, protocols, and CODECs), and description of any special or unique implementation features. This documentation can lead to easier and faster identification and understanding of the customer's solution in problem cases.
- By introducing a template of questions for the customers when they first report a problem, the troubleshooting procedure will be simplified, since the CC can collect important information regarding the current fault which will use in order to efficiently start the problem investigation. In this way, the CC will have all the necessary problem details for a first problem analysis, as well as the NOCs will have all the necessary information to identify the most possible causes of the problem and perform troubleshooting in an efficient way.
- The CC department can further develop their contribution to the customer support service by getting further training in certain issues of the VoIP products, being notified about the outages, failures or other alarms in the network, and performing first analysis of the problem reported. In this way, the number of tickets escalated to the second-line support can be reduced, since the CC will have the possibility to handle cases themselves without the need for escalation. Additionally, the CC will be able to faster analyse a problem when first reported and hand it over to the corresponding support team, reducing in this way the time needed to resolve a fault.
- The NOCs can also receive further training regarding specific VoIP knowledge. An efficient solution is to actually build a "VoIP NOC" by selecting and training certain engineers from each of the NOCs (PSTN and IP) in order to become VoIP-specialized engineers. In this way, these engineers will constitute the VoIP personnel which can handle VoIP specific problems (apart from only the traditional PSTN and IP issues) without the need to escalate in many occasions the TT to the third-line support. Thus more tickets can be resolved by the second-line support teams and fewer resources will be needed by the company for fault handling and customer support.
- One of the purposes of this thesis is to serve as training material for the company's personnel. The training recommended for the CC includes description and understanding of the VoIP questions-template, and the purpose that each question serves. VoIP product description and description of problem impacts and related causes. The training recommended for the "VoIP NOC" should include VoIP technology description, signalling protocol functions (especially SIP), media functions (RTP and CODECs)l, voice quality features and configuration parameters, description of products A & B, SBC basic functions and tracing, and finally VoIP technical troubleshooting details.

The above recommendations can improve the organizational troubleshooting procedures within the company, and serve for efficient ticket handing and fault management having as a main goal the minimization of the number of the tickets that are escalated to next levels, as well as a well-organized and strong customer support base.

5.3. **General conclusion**

The combination of proper planning of the VoIP product implementation, applied monitoring and alarm methods and the efficient troubleshooting procedures, both in technical and organizational level, can increase the competitiveness of the VoIP product that the company offers as well as make the customer support service stronger and accordingly the trust and confidence of the company.

5.4. **Future work**

This thesis has been focused to a great extent on the analysis and improvement of the VoIP technical and organizational procedures and routines within a telecom carrier. In this analysis there have been some aspects that are not in the scope of this thesis and are recommended as future work. This further work can continue the investigation of VoIP efficient planning and troubleshooting procedures within the telecom industry introduced in this thesis and cover further aspects and considerations, so as to be used by telecom companies as a vital source in the commercial development of a VoIP-oriented product.

According to chapter 4, there are four major steps in a root cause analysis procedure: Data collection, casual factor charting, root cause identification and finally, recommendation generation and implementation. In chapter 4, the three first steps have been analysed and presented. The fourth step “Recommendation generation and implementation” is the last step of the root cause analysis and is recommended for future work. The generation implementation and recommendation analysis regards a further step to improve the troubleshooting internal procedures in a telecom company, conducted by the management teams. After the root cause identification (third step of root cause analysis), the management teams should investigate and decide upon the measures that should be applied in order to prevent a reoccurrence of this root cause that led to this particular problem, minimizing in this way the occurrences of VoIP faults and the number of tickets opened by the customers. As future work, one can investigate how this last step can be efficiently and successfully introduced and function internally in the company, as well as analyse the methods of how this procedure can be improved.

Furthermore, this thesis provided an extended technical analysis of VoIP problems and faults that can be experienced in the telecom area; however this analysis has been mainly focused on the IP side of the VoIP infrastructure and little information has been provided regarding the technical troubleshooting and faults that can occur in the PSTN side. In chapter 4, the cause analysis presents a voice side category of possible problem causes, without describing though in detail the technical aspects and features of this category. This PSTN technical troubleshooting analysis is recommended as future work, where one can investigate the potential faults and problems that a telecom company can experience in the PSTN side, as well as analyse technical troubleshooting methods that can be followed for these cases.

Additionally, this thesis has investigated the case where the carrier provides VoIP interconnection to ISPs where the ISPs are sending IP traffic destined to PSTN destinations provided by the carrier. A further step in this investigation would be that one can investigate the case where the carrier provides IP-to-IP interconnection to their customers, for example voice traffic sent from one customer to another (one ISP to another ISP).

The survey performed in the organizational troubleshooting analysis was based on the opinion and feedback of the 2nd-line support personnel. One could also investigate this part based on a survey destined to the customer’s input and feedback in order to acquire a more complete overview of the customer support service level and lead to further improvements in the internal organization.

Finally, this thesis has based its results in a case study of a carrier network, and therefore the analysis has been mostly focused in the planning and troubleshooting of a VoIP carrier infrastructure. As completion of this work, from the general commercial VoIP implementation point of view, one can perform a case study for a VoIP provider instead regarding their planning and troubleshooting procedures, as well as their interconnection and relation to their corresponding carrier.

Bibliography

1. **Network Instruments.** *Your Guide to Troubleshooting VoIP.* **Network Instruments.** USA : October 2007, White Paper.

2. *Services, Managing Next Generation Networks: Service Assurance for new IP Services.* EMC Corporation, February 2008, White Paper. Part Number S0066.1.

3. **Ditech Networks.** *Voice Quality beyond IP QoS.* January 2007, White Paper.

4. *Monitoring and Troubleshooting VoIP Networks with a Network Analyzer.* **TamoSoft.** New Zealand : 2008.

5. **Jeffrey Szczepanski.** *VoIP White Paper.* Allworx, February 2009, White Paper.

6. **Nortel Networks.** *Elimitating Boundaries.* North America : 2004, White Paper.

7. **Brocade Communications Systems** *Technical Brief: Voice over IP (VoIP) Solutions.***.** 2009.

8. **JDS Uniphase Corporation.** *Testing VoIP on MPLS Networks.* June 2010, Application Note.

9. **Instruments, SAGE.** *Testing Voice Service for Next Generation Packet Voice Networks.***.** 2007.

10. **Packet Design, Inc.** *Routing & Traffic Analysis for Converged Networks.* 2010, White Paper.

11. **Miroslaw Narbutt and Liam Murphy.** *VoIP Playout Buffer Adjustment using Adaptive Estimation of Network Delays.* Proceedings of the 18th International Teletraffic Congress ITC18 Berlin Germany, September 2003, pages: 1171-1180.

12. **Alina M. Ionescu-Graff, Cheryl F. Newman, Chi-Hung Kelvin Chu,Bhadrayu J. Trivedi, Benjamin Tang, and Alexander Y. Zhu.** *Quantifying the Value Proposition of Advanced Fault Management Systems in MPLS Core Networks.* Lucent Technologies Inc. : Wiley Periodicals, Inc., Bell Labs Technical Journal, Vol. 10, pages 157–167.

13. **Richard Lau and Ram Khare.** *Service Model and Its Application to Impact Analysis* . USA : Telcordia Technologies, Inc., 2004.

14. **Huihong Chen and Zhigang Chen.** *The Role of Session Border Controllers in the DMZ of Voice over IP(VoIP) Networks.* 3, August 2008, Computer and Information Science, Vol. 1.

15. **M. Hamdi, O. Verscheure, and J.-P. Hubaux.***Voice Service Interworking for PSTN and IP Networks.* Lausanne, Switzerland : Institute for Computer Communications and Applicatins - ICA (EPFL).

16. **James J. Rooney and Lee N. Vanden Heuvel.** *Root Cause Analysis for Beginners.* July 2004, Quality Basics Article,www.asq.org.

17. **Paul Giralt, Addis Hallmark, and Anne Smith.** *Troubleshooting Cisco IP Telephony.* Cisco Press, December 2002. ISBN-10: 9781587050756.

18. **J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler.** *SIP: Session Initiation Protocol.* Network Working Group, June 2002, Request for Comments: 3261.

19. **Fluke Networks.** *Using the ClearSight Analyzer to troubleshoot the top five VoIP problems and troubleshoot Streaming Video.* USA : Fluke Corporation, 2010, Application Note.

20. **Cisco.** *VoIP Traversal of NAT and Firewall.* Cisco Systems, Inc., 2003.

21. **Ditech Networks.** *Echo Cancellation for VoIP Service Providers.* USA : 2007, Application Note.

22. **Yuan, Zhang.** *SIP-Based VoIP Network And Its Interworking With The PSTN.* China.

23. **Radvision.** *Implementing Media Gateway Control Protocols.* RADVision Confidential., den 27 January 2002, White Paper.

24. **Deal L. Gano.** Comparison of Common Root Cause Analysis Tools and Methods. *Apollo Root Cause Analysis - A new way of thinking.* 2007.

25. **MetaSwitch Networks.** *Session border controllers - Enabling the VoIP Revolution.* February 2005.

26. **H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson.** *RTP: A Transport Protocol for Real-Time Applications.* Network Working Group, July 2003, Request for Comments: 3550.

27. **D. Richard Kuhn.** *Sources of Failure in the Public Switched Telephone Network.* Computing Practices, IEEE, April 1997, pages 31-36, 0018-9162.

28. **Factory Improvement Program.** *Using Fishbone Diagram as Problem Solving Tool.* International Labour Organization. March 2008.

29. **ChenXin Zhang.** *SIP and Application Internetworking.* Helsinki : Helsinki University of Technology, 2003, T-110.551 Seminar on Internetworking.

30. **Kevin Wallace.** Cisco Voice over IP (CVOICE). Indianapolis : Cisco Systems, Inc, 2009.

31. **Realsoft Corporation.** *H.323 Tutorial.* Realsoft Corporation, January 2000.

32. **Henning Schulzrinne and Jonathan Rosenberg.** *A Comparison of SIP and H.323 for Internet Telephony.* June 1998.

33. **Radvision.** *Session Initiation Protocol (SIP).* RADVision Ltd., April 2005, Technical Overview.

34. **Cisco.** *Voice Over IP − Per Call Bandwidth Consumption.* Cisco Systems, Inc., 2009-2010. ID: 7934.

35. **Newport Networks.** *VoIP Bandwidth Calculation.* Newport Networks Ltd., 2005.

36. **Tommi. Koistinen.** *Protocol overview: RTP and RTCP.* Course paper for S-38.130 Licentiate course on Telecommunications Technology, Helsinki University of Technology, December 1999, http:www.netlab.tkk.fi/opetus/s38130/k99/presentations/4.pdf.

37. **James Wright.** *Session Description Protocol.* Konnetic Ltd., July 2010, Technical Overview, http://www.konnetic.com/Documents/KonneticSDPTechnicalOverview.pdf.

38. **M. Handley, V. Jacobson, and C. Perkins.** *SDP: Session Description Protocol.* Network Working Group, July 2006, Request for Comments: 4566.

39. **J. Rosenberg and H. Schulzrinne.** *SDP: Session Description Protocol.* Network Working Group, June 2002, Request for Comments: 3264.

40. **Ion Pirsan.** *SS7 Overview*. Industrial Computer Group, Ltd., May 2003.

41. **Nokia Networks.** *Introduction to SS7 Signalling.* Nokia Networks Oy, January 2002, Training Document.

42. Wireshark. Available at http://www.wireshark.org/.

Appendix

This appendix presents the questionnaire that was used for conducting the survey described to the Voice and IP NOC.

VoIP Questionnaire for the Voice NOC

1. What are the most common VoIP problems, caused by the voice part that you experience?
2. When do you recognize, most of the times, that a VoIP problem is IP related and not voice?
3. Can you easily understand if a VoIP problem is IP or voice related?
4. How do you troubleshoot a VoIP fault (what steps do you follow)?
5. Do you meet any kind of problems or difficulties (technical or organizational) when troubleshooting VoIP issues? Please clarify your answer.
6. According to your opinion, what information is important to receive from the customer when they report the VoIP issue, in order to make the troubleshooting easier and faster?
7. Do you have any improvement or change suggestions for the VoIP fault handling routines in the company?

VoIP Questionnaire for the IP NOC

1. What are the most common VoIP problems, caused by the IP part that you experience?
2. When do you recognize, most of the times, that a VoIP problem is voice related and not IP?
3. Can you easily understand if a VoIP problem is IP or voice related?
4. How do you troubleshoot a VoIP fault (what steps do you follow)?
5. Do you meet any kind of problems or difficulties (technical or organizational) when troubleshooting VoIP issues? Please clarify your answer.
6. According to your opinion, what information is important to receive from the customer when they report the VoIP issue, in order to make the troubleshooting easier and faster?
7. Do you have any improvement or change suggestions for the VoIP faults handling routines in the company?

TRITA-ICT-EX-2011:166

www.kth.se