white paper

Deploying Sytel VoIP solution in hosted and standalone environments

A white paper that describes Sytel's VoIP solution, steps involved in fresh deployment or system migration and its suitability for different customers

white paper

Table of Contents:

white paper

1. Introduction

The purpose of this paper is to set out in practical terms the steps that customers need to take in implementing Sytel's VoIP solution. Reasons for going for a VoIP hosted solution for contact centers are various. For example

- A single site can be used to connect agents and customers on a world wide basis 24 hours a day, with significant cost savings.
- VoIP networks can be quickly deployed with QOS levels equivalent to traditional telephony systems
- And convergence of data and voice networks means a single point of management for both networks.

But new technologies have their challenges. So achieving the right QOS in VoIP systems, especially for contact center business, requires vigilance. For example an initial delay during set up of VoIP calls between colleagues in a company may just be acceptable. But the same delay on a commercial call will have a direct impact on the telemarketing and marketing research business. In hosted environment, this impact may increase exponentially if you are using public internet service.

Sytel understands the challenges of VoIP deployment and expects to take a proactive role with all customers making such investments. We will start by discussing basic concepts relevant to deploying our VoIP solution. This is important because in contrast to a traditional TDM environment, a VoIP solution may be deployed in a more dynamic network, where infrastructure, people and applications will be changing continuously. Hence we need to take extra care in order to avoid the problems that can arise within a state of constant change. The paper will describe deployment steps in detail and the necessary precautions that should be taken while actually undergoing these steps. This will also help in removing any basic misconceptions that people have regarding the feasibility of VoIP solutions for contact centers.

This paper is intended for a wide audience, including those with just a basic understanding of VoIP. More details, including definitions of technical terms used in the paper and a detailed callflow diagram, are given in the appendices.

2. When to go for VoIP

Reasons for going VoIP are sometimes lost in a cloud of slogans and soundbites. As a reader you may have already decided why you should go VoIP, and if so you can skip this section and move to the next one. If you are a user that is new to VoIP you may be grappling with what the benefits are for your business. These will clearly differ from one business to another but are likely to include some or all of the following:

- A converged network for telephony based activities and regular day-to-day data transmission means one-stop management.
- And this should always mean reduced investment in human resources
- It is easy and flexible to deploy since IP service is available almost everywhere,

infrastructure requirement is minimal and the technology is based on standardized protocols

- A VoIP network allows for continuous and immediate change in infrastructure and where people, resources and applications are deployed, allowing immediate response to changes in business needs.
- Infrastructure can be used more efficiently since all necessary communication facilities for an agent can be contained in a single workstation or terminal on the agent desktop.
- Hardware costs should always be lower than traditional setups by using soft phones (available free of cost) and regular switches/routers in contrast to using legacy hard phones and PBX
- Sytel's contact center solution will merge seamlessly with the other VoIP based day-to-day activities in the contact center since its communication model is based on standardized VoIP protocols

Customers may also want to consider VoIP deployment as an upgrade to a traditional telephony infrastructure. As well as the benefits above, others to consider are:

- It can provide the same QoS as traditional telephony
- Migration requires minimal configuration changes to software/hardware
- The regular network integration staff will require minimal training to support this solution

3. Before deployment

In any business setting there will usually be a choice of deployment strategies. For example there will be choices to be made as to which routers, where they will be sited and what software tools will be used to load balance the network(s). Sytel will be happy to get involved in the strategy development process so that we can help in determining bottlenecks and limitations with respect to system integration with our dialing and telephony architecture.

It is generally optimum strategy to have Sytel's telephony components located at a single site so that there is only one high bandwidth link between the telephony server and the external network.

This can be a factor in getting better rates from the network operator. Multiple agent and campaign layer applications (especially in a hosted environment) can connect in easily using dedicated IP links from multiple sites.

A centralized telephony architecture with high bandwidth will be easier to manage since security implementation will be local which means call admission control and denial of service attacks will be handled more efficiently. But if there are high concerns regarding system redundancy it is advised that a more distributed architecture is planned so that there are multiple sites capable of routing voice traffic to the network.

white paper

Planning at this stage should basically involve discussion about current and expected network topology so that the specific steps needed for the deployment can be understood both by Sytel and the customers. This also happens to be the right time to develop concrete plans for the immediate future to ensure easy scalability when going into production from pilot. A typical Sytel VoIP solution deployment is shown in Figure 1.

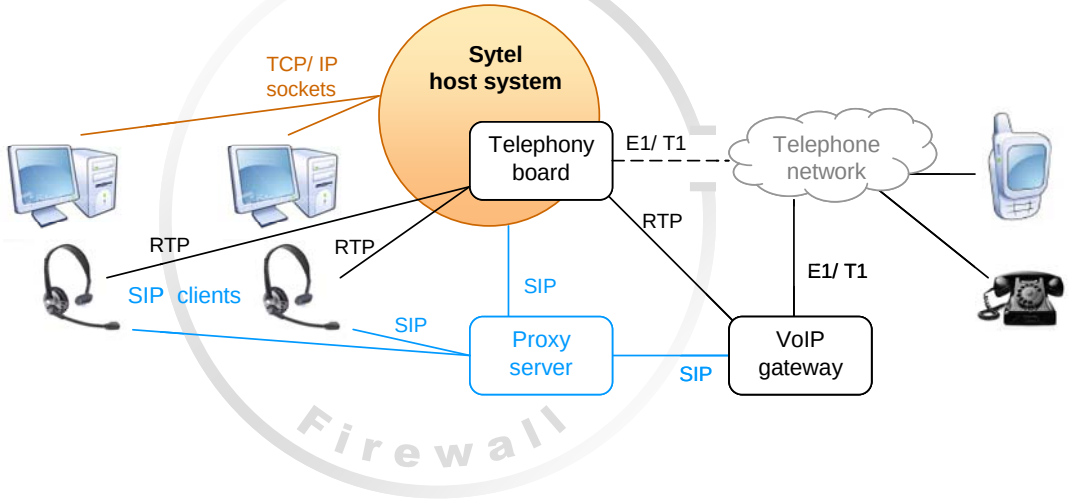


Figure 1. Basic network architecture in a VoIP deployment

A basic understanding of the hardware components at this stage will help in realizing the effect of hardware configuration changes on the system capacity. If you would like to go for the cheapest possible solution using the G.729 codec (to save transmission costs) this will mean a comparative increase in DSP resource utilization for every call because of additional transcoding that will take place due to conversion of G.729 to G.711 over the CTI bus in the Sytel server. The good news is that the hardware requirements for Sytel's VoIP solution will remain the same irrespective of the selection of codec.

It is important at this stage to set an appropriate expectation of the system's performance to avoid surprises later. Tone detection, AMD and fax machine detection with VoIP systems will not be as accurate as in the case of TDM lines since G.729 codec strips off a lot of important information from the voice packets thereby decreasing detection capability. Human speech quality will be acceptable using this low bit rate codec but input signals, such as music (used in various call center activities like inbound campaigns, customer/agent hold, IVR, etc.) may not sound very well if using G.729 since this codec was designed for speech applications in the first place. Having said that, the technology is good enough to meet most business needs because the level of voice degradation will not be noticed by the end user. If you are interested in

using other codecs, please contact us since our architecture is capable of supporting most of the codecs available in market.

We will be able to handle even the upcoming Speex, an open source patent-free audio compression format. Since this codec would be free (unlike the most popular G.729 codec) and could handle voice sampling of 8, 16 or 32 kHz, supporting this codec is important to have a robust and acceptable solution for future VoIP installations.

A recovery and redundancy plan should also be considered at this stage since it is vital to keep the system running from the user's perspective (agents in this case) once you go into production. Whether there is a system failure or call overflow, recovery is required. How this is managed may depend on whether this is a new VoIP installation or a phased migration from a traditional telephony system.

In the case of a fresh installation (especially for hosting), a redundant Sytel system containing one or more telephony boards may be required. We encourage all new users to do risk assessments with us, so that an appropriate redundancy strategy can be determined. In the case of a phased migration from a traditional system, care should be taken during the system setup such that any temporary bursts of call overflow are successfully handled by the traditional telephony system. Cutover from the traditional components should be planned as soon as the old service and voice quality levels are met with the new VoIP architecture.

To successfully install the Sytel VoIP solution, especially if the agents are located outside the LAN where the telephony boards reside, a proxy server will be required (e.g.: Brekeke Ondo) for both Sytel's Telephony Gateway (STG) and also the SIP agent registration. This will enable the STG and the agents to communicate with each other via SIP messages using the ethernet port on the NIC of the host system. Any signaling between the STG and the network end will also be via the NIC on the host system. The ethernet port on the telephony card will be used only to transmit or receive the RTP packets associated with voice, DTMF and other tones. Other basic software/hardware requirements are a VoIP gateway(s) (to terminate calls via PSTN), testing tools (to perform tests during the pilot and production phase to monitor system health) and firewalls (for network security).

Customers need to understand their key responsibilities during this phase so that system rollout can be done efficiently. Basic steps that should be taken regardless of network topology are:

- **Ensure** that the service provider is providing echo cancellation support for any one-way transmission time of greater than 10 ms.
- **Confirm** that G.711 and/or G.729a/b speech codecs are supported over the IP link according to the requirement. If there are other codecs that are in use, contact us to figure out the best approach
- **Understand** any limitations of the VoIP gateway, say conformance to RFC2833 which means DTMF or other tones (busy,

alerting, ringback) received from the PSTN can be propagated to the telephony gateway as signaling messages or as modified RTP packets. Any other constraints on this gateway service (like RTP port restriction to a certain range, call admission control thresholds, etc.) should be discussed with Sytel.

- **Ensure** that the network meets 150 ms one way transmission time limit set by ITU-T G.114 specification. If G.729 is used at least once between the Sytel server and the external user endpoint, avoid using G.711 anywhere else in the network (which will reduce transmission costs) since speech bits lost during G.729 compression cannot be recovered accurately even after adding synthetic bits during the decompression process.
- **Confirm** from the provider that you are getting correct IP bandwidth according to the codec used – normally it is 80kbps per G.711 audio stream and 24 kbps per G.729 audio stream.

And you will need to prepare carefully for the arrival of the physical server from Sytel containing telephony boards. Sytel provides a separate deployment paper detailing preparation. For example the server should be mounted in a rack with proper support under the base to avoid hardware failure due to excessive vibration. Air conditioning and the room temperature should be checked regularly to avoid a critical telephony board failure or other hardware fault from over-heating.

4. During deployment

It is now time to arrange for the basic ethernet connections, one for the host system's NIC and others for ethernet ports on the telephony boards. If the E1/T1 ports on the boards are also enabled, additional PRI cabling connections are required. For TDM connections, normally a crossover cable is required to connect to PBX and a straight through cable is required to connect to the PSTN. The connection status for each of these ports can be verified using tools which will be supplied as part of the complete Softdial Contact Center installation. Although training at the Sytel offices would have provided the necessary knowledge and skills to customers to deploy and configure the system, it is advised that they provide regular updates to Sytel throughout the deployment process.

This system will have call control connections between dialer and the agent scripting applications and these connections may not have any flow of data traffic for a certain period of time. The representative scenario may be when agent is engaged in a long conversation and making a probable sale or may be it's a market research call which is going on for 20-30 minutes. Firewalls should be configured such that these connections are not closed since this will result in call termination.

Other things that need to be deployed and initiated now are the firewall, the proxy server (or SIP server) and VoIP gateways. Tuning of these components will basically determine the performance of the system after everything is setup as with a given IP bandwidth.

If you are planning to use a proxy server for registrations from multiple dialer locations, installing it on a separate standalone machine may be a better option to rule out the possibility of this being a bottleneck during high data traffic. Setting up an efficient dial plan will be a key factor since this will consist of routing rules that will decide the actual movement of IP packets throughout the VoIP network. If the Sytel server is installed in an existing data network, priority should be given to voice

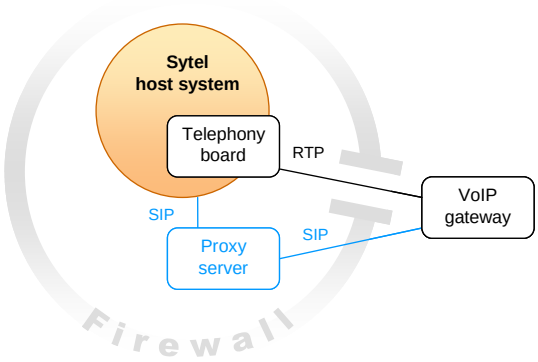


Figure 2. Alternative deployment strategy for VoIP gateway

packets over other traffic because real-time communication between an agent and an external party is highly delay sensitive and traffic peaks in the network may quickly undermine the customer experience. This can be handled by setting up a QOS check at the routers or using VLAN capable switches.

VoIP gateways can be deployed in multiple ways depending on the business requirement. A gateway can be deployed behind a firewall so that all kinds of data/voice traffic flow through that firewall which means additional CPU resource utilization but more protection against denial of service attacks. Alternatively, the gateway can be set up such that only signaling information goes through the firewall and the RTP connection is established directly between Sytel server and the VoIP gateway (as shown in Figure 2). This will reduce the transmission times and help in meeting the ITU-T quality standards but will result in a less secure system. In the case of a hosted environment where there will be a lot of localised RTP stream processing, it is better to follow the second approach and keep the firewall away from RTP streams. This is reasonable because the enterprise VoIP (VoIP setup within an organization) and the carrier VoIP (provided by Telco/ITSP) should be secure. Customers should expect that any additional actions required for safe and effective management of RTP packets will be provided in one or other of these contexts.

To have a system which is manageable and also allows for ease of trouble-shooting in the future, relevant information regarding the network topology should be documented at this stage so that the upgrade/migration process (due to network modifications, which nowadays happen regularly) can be done efficiently. Once these deployment activities have been completed, it is time to install some basic tools on the Sytel server besides the ones that are provided with the installation kit. Install Wireshark (formerly known as Ethereal) to capture IP packets send/received at the host system's NIC and also a SIP software client (e.g.: X-Lite) for initiating VoIP calls.

5. After deployment

Begin pilot testing: this involves using SIP phones (which should have in-build echo cancellation), landlines and mobile phones. SIP phones need to be registered at the proxy server as agent or external user end. In real life, most of the calls will terminate on landlines or mobile phones so using this setup in the basic test is mandatory. A dial plan needs to be configured in the proxy server to handle inbound and outbound calls, if the calls launched for user end are also via IP link. This basically means that a call initiated from the telephony server should route via the proxy server to the VoIP gateway and an incoming call for the dialer should route from the VoIP gateway to the telephony server via the proxy server. The dial plan can be configured in the STG configuration also but it is better to have this in the proxy server itself to integrate more efficiently with any multiple STG application instances. STG configuration files may need modification at this stage.

This configuration is important in order to set up efficient call retry behaviour later for outbound calls. For example customers need to map SIP messages to appropriate dialer call outcome values. In outbound dialing, call retries depend on the outcome generated by dialer and if these outcomes are not mapped properly to SIP messages sent by the network, customers won't be able to set the retries as expected.

You also need to mention the proxy server details in STG configuration settings so that STG can register properly with the proxy server. Selection of appropriate codec for calls on various network routes should also be made at this stage.

Before going into production the following actions should be undertaken:

- **Sanity tests** should be done to check the basic call setup between agent (SIP phone or land line) and external user (SIP phone, land line or mobile) with all possible end-point combinations.
- **Monitor** these test calls at various nodes: STG, proxy server and VoIP gateway. For all these basic tests (which should include calls placed from internal to external network so that any NAT or firewall issues are also uncovered), it is important to check the call session status at all of these nodes so that routing of the calls becomes clear and you can pinpoint any integration problems in the network setup.
- **Verify** the speech quality. Instances of double talk and echo should be minimal or null. Occurrence of noise or gaps in conversation should also be within acceptable limits.
- **Proceed** on to test other features like transfers and conference calls.
- **Ensure testing** of any IVR features (if planning to use them in production) and verify whether the played music is of acceptable quality over G.729. If not, switch to G.711 and compare results. If in both cases the quality is not acceptable then there is some basic integration mistake that has been made since the audio quality over G.711 should the same as that over TDM.

- **If quality is met** using the G.711 codec, better quality wav files should be tried with IVR when reverting back to use G.729. This is one of the reasons why recordings are not stored in a compressed format by Sytel since any additional compression on the recordings created by audio stream received over IP link using G.729 will be probably unacceptable.
- **Additional tests** that verify the AMD, fax machine detection and tone detection should be performed.

After these tests are passed successfully, the following needs to be done next:

- **Load tests** should be initiated to measure the available IP bandwidth and to see if there any bottlenecks in the system: for example IP bandwidth, proxy server, VoIP gateway, or a Sytel component. It is possible for the voice quality to deteriorate after a call is connected in a VoIP environment (unlike traditional telephony) if all of the remaining bandwidth is used for other purposes.
- **Performance levels** (when QOS is met) should be recorded so that they can be used in future to debug issues which may arise in a production environment.
- **Call limits** associated with denial of service threshold (which can be implemented at proxy server or firewall) should also be noted down since when the system will reach this threshold, any additional call will not have enough bandwidth to maintain the QOS and hence will be denied.

If the VoIP system is installed to work with an existing data network, the effects of this data traffic over the VoIP network must also be measured during the pilot test. The best way to do this is to initiate the VoIP system load test during the busiest hours of existing data network and compare the performance figures with the earlier load test done with just the VoIP system. Regular contact with the Sytel support desk during these tests will help in ensuring the best possible system setup with maximum performance.

In complex network setups, additional testing may be required. For e.g.: setting up a conference call between an agent using G.711, an agent using G.729 and a customer using TDM. More time spent on these activities will ensure a better system performance.

6. Security Issues

Customers should be aware of the security threats that can come up in a hosted environment using VoIP. The basic ones are spoofing, eavesdropping and spitting. In the case of a hosted environment, the most vulnerable link to security threats is the consumer VoIP portion of the network – the broadband connection between the SIP phone and the telephony carrier's IP network if the agent is working from home.

If agent is working from home, it is possible to eavesdrop a call between an agent and an external party and then spoof caller id by examining and modifying the headers of IP packets so that the external party believes that

the call is coming from a reliable source. This can be used to extract sensitive information. In a rare scenario, a hacker can spam the voice mailbox of an external VoIP phone user (a process known as spitting) using the same caller id: this can then lead to denial of service for this user, which will mean that callbacks scheduled at the Sytel server will never be successful and the user may complain about spamming done by the telemarketing company. This can be avoided by using alternate protocols like SRTP instead of RTP so that the transmitted voice packets are encrypted.

7. Conclusion

Don't rush – understand the benefits and be sure that you are going to get value out of this solution. Plan the requirements for each site carefully and work closely with Sytel to achieve fast and seamless integration of our VoIP solution with your network.

Expect some teething problems but if you follow the steps laid down in this paper you can look forward not just to a successful installation but a way of working that may well transform how you do business.

white paper

white paper

Appendix 1. Definitions

AMD – answering machine detection

Bandwidth - rate at which bits are transferred through the system

Call admission control – rejection of calls associated with real time media traffic to avoid congestion

Codec – software capable of encoding/decoding digital data

CTI – computer telephony integration

Denial of service – traffic threshold at which additional resources to setup a new session are denied

Dial Plan – A translation which is configured to modify or route the SIP/SDP message fields

Double talk – A scenario where a person starts speaking at the same time when the voice is just received from the other end of the call

DSP – digital signal processor

DTMF – dual tone multi-frequency

E1 – TDM link having 32 circuits (2 for signaling and 30 for voice)

Eavesdropping – Listening to an ongoing private conversation by capturing RTP packets from various end points associated with the call

G.114 – an ITU recommendation for transmission quality for telephone connections

IVR – interactive voice response

ITSP – internet telephony service provider used for making telephone calls using VoIP

LAN – local area network

NAT – Network address translation, used for translating an IP address in one network to a different IP address in another network. SIP/SDP fields are modified to avoid issues related to this

NIC – Network interface controller, a hardware that is used by computers to communicate over network

PRI – primary rate interface standard for an E1/T1

QOS – quality of service

RTP – real time protocol

RFC2833 – specification describing RTP packet characteristics for DTMF, tones and signals

SPIT – Spam over Internet Telephony

Spoofing – Identifying yourself as someone else by presenting a false Caller ID in a VoIP call

SIP – session initiation protocol

Softdial Contact Center – Our complete software suite

Softdial Telephony Gateway (STG) – Sytel's telephony software

SRTP – Secure RTP

T1 – TDM link having 24 circuits (1 for signaling and 23 for voice)

TCP – Transmission Control Protocol, used for reliable transmission of IP packets between two end points and used for transmitting SIP messages.

TDM – Time division multiplex

Telco – organization providing the basic telephony services

Transcoding – conversion from one codec to another

Transmission time – equipment processing time + propagation delay

UDP – User Datagram Protocol, used to carry RTP packets and sometimes SIP signals also

VoIP – Voice over Internet Telephony

VoIP gateway – interface that translates traditional TDM signaling to SIP messages and vice-versa

VLAN – virtual LAN

Appendix 2. Predictive Outbound VoIP call (see call flow diagram below)

Below we give an example of all the events involved in making a predictive outbound call using VoIP technology. An inbound scenario has a similar callflow (for further details contact Sytel).

1. Assuming that agent is registered with the proxy server, he tries to login using a desktop scripting application.

2. CallGem authenticates the login attempts and creates a session ID. Internal message exchange happens between CallGem and STG.

3. STG invokes the SIP messaging for this call session. Agent's sip phone starts ringing and he picks up the phone.

4. CallGem/STG completes the resources allocation for this agent end point and confirms this by sending 'Login OK' event back to the scripting application.

5. Media is established for the agent endpoint. Agent can now hear the heartbeat tone/music indicating that he is now successfully logged into a campaign.

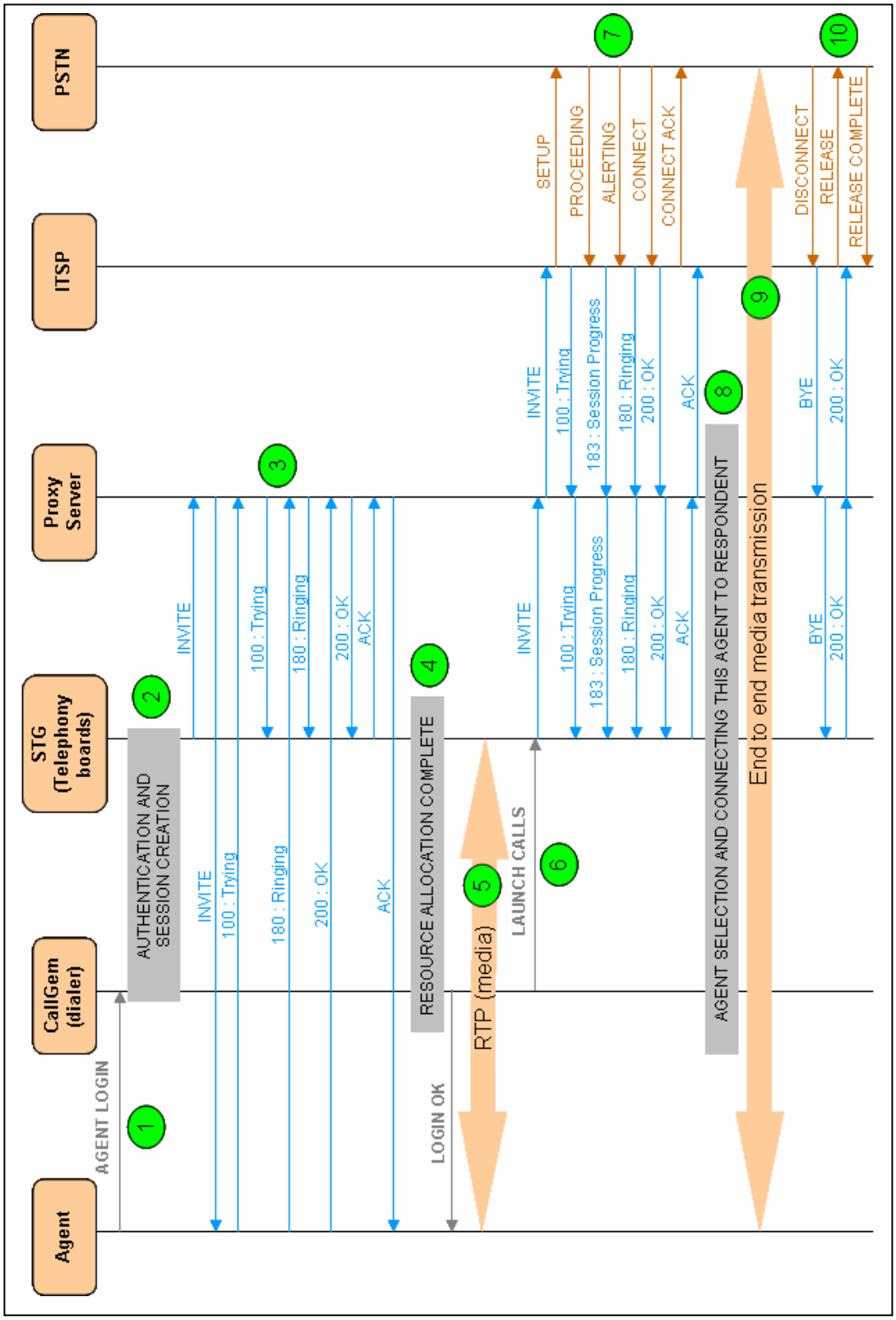
6. After agent decides to go available, CallGem directs the telephony gateway to launch call to the telephone network.

7. This leads to various message flows (starting from INVITE message send from STG) between the STG, Proxy server, ITSP and the PSTN. Finally the call is established when a CONNECT event is received from the PSTN. In the call flow, '183: Session Progress' message may indicate 'early media' (like pre-ringback tone). Instead of this SIP message, ITSP can alternatively send RTP packets to represent this media.

8. As soon as the call with the respondent is connected, an agent is selected to take this call and both endpoints (agent and respondent) are put in same context.

9. Two-way media transmission is established so that both sides can now talk and hear each other.

10. After the conversation is finished, the respondent hangs up the receiver (which corresponds to DISCONNECT message). Due to this, the media path is cleared and the call is cleared at the STG/ITSP level. Agent goes into wrap at this point and the internal session is cleared only when agent completes the transaction.


Agent
CallGem (dialer)
STG (Telephony boards)
Proxy Server
ITSP
PSTN
1
AGENT LOGIN
2
AUTHENTICATION AND SESSION CREATION
INVITE
100 : Trying
3
180 : Ringing
200 : OK
ACK
4
RESOURCE ALLOCATION COMPLETE
LOGIN OK
5
RTP (media)
6
LAUNCH CALLS
INVITE
100 : Trying
183 : Session Progress
180 : Ringing
200 : OK
ACK
7
SETUP
PROCEEDING
ALERTING
CONNECT
CONNECT ACK
8
AGENT SELECTION AND CONNECTING THIS AGENT TO RESPONDENT
9
End to end media transmission
10
DISCONNECT
RELEASE
RELEASE COMPLETE
BYE
200 : OK

white paper

www.sytelco.com
info@sytelco.com
+44 (0)1296 381 200

Sytel Limited 1 Cromwell Court New Street Aylesbury Buckinghamshire HP20 2PB UK