Vojnotehnicki glasnik/Military Technical Courier
ISSN: 0042-8469
ISSN: 2217-4753
vojnotehnicki.glasnik@mod.gov.rs
University of Defence
Serbia

Description of the process of tunneling Q signaling in private telecommunication networks

Svrzi#, Sla#an M.; Mili#evi#, Zoran M.; Periši#, Zoran S.
Description of the process of tunneling Q signaling in private telecommunication networks
Vojnotehnicki glasnik/Military Technical Courier, vol. 69, no. 1, 2021
University of Defence, Serbia
Available in: https://www.redalyc.org/articulo.oa?id=661771133003
DOI: https://doi.org/10.5937/vojtehg69-28117

Original scientific papers

Description of the process of tunneling Q signaling in private telecommunication networks

Описание процесса туннилирования Q-сигналов в частных телекомуникационных сетях

Опис поступка тунеловања Q сигнализације у приватним телекомуникационим мрежама

Slađan M. Svrzić
Tesla Systems Ltd, Serbia
milosavljevic_svrzic@hotmail.com
https://orcid.org/0000-0003-4525-9844

Zoran M. Miličević
Serbian Armed Forces, Serbia
zoranmilicko@gmail.com
https://orcid.org/0000-0003-3512-4188

Zoran S. Perišić
Serbian Armed Forces, Serbia
zperisic@gmail.com
https://orcid.org/0000-0003-3803-4786

DOI: https://doi.org/10.5937/vojtehg69-28117
Redalyc: https://www.redalyc.org/articulo.oa?id=661771133003

Received: 24 August 2020
Revised document received: 16 November 2020
Accepted: 18 November 2020

Abstract:

Introduction/purpose: The article should specify the network signaling type Q-SIG, which is standardized especially for implementation in digital telecommunication networks of integrated services (ISDN), emphasizing the possibility of its further application in the Private Telecommunications Network of Integrated Services of the Serbian Armed Forces (PISN of SAF), i.e. in the Private Automatic Telephone Network of the Serbian Armed Forces (PATN of SAF).
Methods: An analysis of the existing standards was performed: ECMA-355 and ECMA-336 and a synthesis of the possibilities of their application in the PATN of SAF.
Results: The procedure for the application of Q-SIG is processed in a situation when the peripheral parts of the PISN of SAF, which operate on the principle of transmission and circuit switching by TDM (Time Division Multiplexing), are connected via a central Core network with the IP (Internet Protocol), which operates on the principle of packet transmission and switching with the SIP (Session Initiation Protocol). A method of the application of the tunneling of encapsulated Q-SIG messages through the IP network, defined by ECMA-355 Standard, has been developed. The necessary functions for mapping the transmission of tunneled signaling messages Q-SIG and mapping voice (and other audio) information to media streams during VoIP (Voice over IP) communication through that network, which are defined by ECMA-336 Standard, are described.
Conclusion: The application of ECMA-355 and ECMA-336 Standards is a new solution in the PATN of SAF with the use of the IP network to connect the IP PINX using the Q-SIG tunneling procedures and mapping functions for their transmission and transmission of audio signals. This then opens up a whole range of new possibilities that, with the growth of the Core network and their application, will rapidly contribute to the creation of a broad Telecommunication information system backbone for the implementation of real-time multimedia communications and the transition to Unified Communications (UC).

Keywords: PATN SAF, Q-signaling, PISN, PINX, Internet protocol, SIP, ECMA standard, Q-SIG tunneling, encapsulation, mapping functions.

Author notes

milosavljevic_svrzic@hotmail.com

Р е з ю м е :

Введение/цель: Цель статьи заключалась в составлении классификации видов сетевой сигнализации Q-SIG, которая специально приспособлена к применению в цифровых телекоммуникационных сетях с интегрированными услугами (ISDN), и в выявлении возможностей ее дальнейшего применения в частных телекоммуникационных сетях с интегрированными услугами Вооруженных сил Республики Сербия (PISN SAF), т.е. в частной автоматической телефонной сети Вооруженных сил Республики Сербия (PATN SAF)
Методы: В статье приведен анализ существующих стандартов: ECMA-355 и ECMA-336 и синтезирования возможностей их применения в PATN SAF.
Результаты: Процедура применения Q-SIG обрабатывалась в ситуации, когда периферийные части PISN SAF, действующие по принципу передачи и коммутации каналов по TDM (Time Division Multiplexing), были соединены через центральное ядро сети с IP (Internet Protocol), работающей по принципу передачи пакетов и коммутации с помощью SIP (Session Initiation Protocol). Разработан метод применения туннелирования инкапсулированных сообщений Q-SIG через IP-сеть, предписанный Стандартом ECMA-355. В статье также описаны необходимые функции для сопоставления передачи туннелируемых сигнальных сообщений Q-SIG и сопоставления голосовой (и другой аудио) информации с медиапотоками во время связи VoIP (Voice over IP) через ту сеть, в соответствии со стандартом ECMA-336.
Выводы: Применение стандартов ECMA-355 и ECMA-336 – это новое решение в PATN SAF при использовании IP-сети для подключения IP PINX и при применении туннелирования Q-SIG и сопоставления функций отображения и передачи, в том числе звуковых сигналов. Это влечет за собой целый ряд новых возможностей, которые по мере роста ядра сети и по мере их применения будут способствовать созданию широкой магистрали телекомуникационно-информационной системы связи для осуществления мультимедийной коммуникации в реальном времени и переходу к унифицированной системе связи (UC).
К л ю ч е в ы е с л о в а : Q-сигнализация, PISN, PINX, интернет-протокол, SIP, стандарт ECMA, туннелирование Q-SIG, инкапсуляция, функции отображения.

Abstract:

Увод/циљ: У чланку је специфицирана мрежна сигнализација типа Q-SIG, која је стандардизована специјално за примену у дигиталним телекомуникационим мрежама интегрисаних сервиса (ISDN), уз потенцирање могућности за њену даљу употребу у Приватној телекомуникационој мрежи интегрисаних услуга Војске Србије (PISN ВС), односно у Приватној аутоматској телефонској мрежи Војске Србије (ПАТлМр ВС).
Методе: Вршена је анализа постојећих стандарда: ECMA-355 и ECMA-336 и синтеза могућности њихове примене у ПАТлМр ВС.
Резултати: Обрађен је поступак за примену Q-SIG у ситуацији када се рубни делови PISN ВС, који функционишу на принципу преноса и комутације кола по TDM (Time Division Multiplexing), повезују путем централне Core мреже са IP (Internet Protocol), а која функционише на принципу преноса и комутације пакета са SIP (Session Initiation Protocol). Разрађен је начин примене поступка тунеловања енкапсулираних Q-SIG порука кроз IP мрежу, који је дефинисан стандардом ECMA-355. Описане су неопходне функције за мапирање преноса тунелованих сигнализационих порука Q-SIG и мапирање говорних (и других аудио) информација на медија-токове током VoIP (Voice over IP) комуникације кроз ту мрежу, а које су дефинисане стандардом ECMA-336.
Закључак: Примена стандарда ECMA-355 и ECMA-336 ново је решење у ПАТлМр ВС уз коришћење IP мреже за повезивање IP PINX, применом поступака тунеловања Q-SIG, и мапирање функција за њихов пренос и пренос аудиосигнала. То отвара читав низ нових могућности које ће нарастањем Core мреже и њеном применом убрзано допринети стварању широке окоснице телекомуникационо-информационог система ВС и послужити за имплементацију мултимедијалних комуникација у реалном времену и прелазак на обједињене комуникације UC (Unified Communications).
Keywords: PATlMr VS, Q-сигнализација, PISN, PINX, интернет протокол, SIP, стандард ECMA, тунеловање Q-SIG, енкапсулација, мапирање функција.

Introduction

The *Serbian Armed Forces* (SAF) in peace have extremely high requirements in terms of the use of modern telecommunications solutions, which primarily refers to the sufficiently fast and quality processing and transmission of accurate and protected information (*spoken* and *non-spoken*). At the same time, it is very important to offer a wide range of modern telecommunication customer services and network services

to the users of the SAF through the transmission of this information, whose technical support it should provide, not only on TDM (*Time Division Multiplexing*) but also on the IP (*Internet Protocol*) platform, modernly organized and functionally oriented *Private Telecommunications-Information System* (PTIS). As such, the PTIS SAF should be a unique telecommunications-information platform, which, in addition to the fixed part, integrates the *Mobile component of the PTIS* (MC of PTIS), primarily intended for communication on the ground and in combat conditions. Due to its complexity, organization, achieved degree of technical integration and geographical distribution, the PTIS SAF coincides with the performance, determinants, and standards of the modern CTN (*Corporate Telecommunication Network*) (University of Belgrade, 2001). This then means that it is not completely closed and self-centered, but that, through different and geographically disparate interconnections, it is connected to the *Public Switched fixed* and *Public Mobile Telecommunications Networks* (PSTN and PMTN), as well as to the existing *Functional, digital trunking mobile radio network TETRA .Terrestrial Trunked Radio*) (Svrzić & Ćosović, 2002).

After significant modernization and growth of the mobile component of the system, the basic assumption is that the existing fixed part of the PTIS and, within it, the fixed *Private Automatic Telephone Network Serbian Armed Forces* (PATN SAF) must be adequately and efficiently integrated into the rapidly growing *Integrated Telecommunications-Information System SAF* (ITIS SAF), so that, for them, they represent a modern, completely appropriate and stimulating stationary telecommunication-information basis. At the same time, the accepted international obligations of the Republic of Serbia and the commitment to international military integration, require that the fixed PATN SAF be interoperable with adequate systems (networks) of other countries and military organizations (Ministry of Defense of Norwey, 2004). Due to such requirements (for organization, modernity and interoperability), there is a constant obligation to regularly perform comprehensive analyzes of its condition in the PATN SAF and to find principles and methods for necessary selective improvements. Thus, at the beginning of 2005, the existing complex and heterogeneous solution of the *Network signaling system* in the PATN *Serbian* and *Montenegro Armed Forces* (SMAF) (Svrzić, 2019) was comprehensively observed and it was found out that it did not have sufficient power for application in modern conditions. Through the synthesis for the solution of the observed problem, the completely new, towards the ISDN (*Integrated Services Digital Network*) oriented and globally standardized, *System of digital network signaling* type Q-SIG (*Q-Signalization*) was imposed (and later in practice proved to be optimal). The International Telecommunication Union-*Telecommunication Standardization Sector* (ITU-T) has intended and designed such signaling specially for use in CTN, that is, in private ISDNs, the so-called PISNs, which the *PTIS Serbian Armed Forces* certainly is (InterConnect Communications, 1995).

The Q-SIG standard corresponds to the framework of the international standards for open system interconnection and the IPNS ISDN PBX (*Private Branch Exchange*) network specifications, which define how to connect private digital automatic telephone exchanges of integrated services, so-called PINX (*Private Integrated services Network eXchange*), within PISN (*Private Networks of Integrated Services*).

Q-SIG standard in private telecommunications networks

The name Q-SIG came from the fact that it is realized in the "Q" reference point of the ITU-T ISDN reference model, i.e. at the logical level of a digital switching system, which in fact defines the distinction between two connected *Digital automatic telephone exchanges* (DPABX) in an ISDN. Such DPABXs are then called PINXs, because the integration of standardized services is realized through them in the network. In the extended ITU-T ISDN reference model, two new points are identified: *Reference point "Q"* and *Reference point "C"*. The *Reference point "Q"* is the logical point of realization of signaling between two PINX, which means that signaling (i.e. Q-SIG) messages are generated, sent, received and processed on it. The *Reference point "C"* represents the interface through which a physical connection is established with the

participating PINX. For the transmission of Q-SIG messages, as a transport or so-called IVN (*Intervening Network*), dedicated channels (*analog* or *digital*), 2 Mb/s digital multiplex group from TDM or switched connections for VPN (*Virtual Private Networks*) are used. Different interface-dependent protocols may appear at the *Reference point "C"*, which also depends on the type of IVN. These IVNs do not necessarily have to be ISDNs, but are generally assumed to be digital channels, as Q-SIG is primarily intended for use when operating on TDM CCS (*Common Channel Signaling*), using the G.703 interface in the *Reference point "C"* (InterConnect Communications, 1995).

Several individual Q-SIG standards precisely define the signaling system at the *"Q" reference point*, so that it will work successfully in any suitable way of connecting PINX equipment. The Q-SIG protocol stack (*Steck Q-SIG*) is identical to the structure of the DSS1 protocol (*Digital System Signaling 1*), as both follow the *ISO reference model* and can have identical *Layer 1* and *Layer 2* .*Layer 2* - LAPD). However, at the third level, i.e. on *Layer 3*, which is divided into three sublayers here, Q-SIG and DSS1 differ significantly. A simplified messaging sequence, which according to the specifications of ECMA-142/143 Standard takes place on the first sublayer of the *network Layer 3* (Ecma International, 2001a), (Ecma International, 2001b), when establishing Q-SIG BC (*Q-SIG Basic Call*) between the end PINX "X" and "Z", and via the transit PINX "Y", is shown in Figure 1.

The second sublayer of *Layer 3* is the Q-SIG GF (*Q-SIG Generic Fuctional Protocol*), according to the specifications of ECMA-165 Standard (Ecma International, 2001c), which provides a standardized mechanism for exchanging signal information for managing additional services and the ANF (*Additional Network Feature*). The procedures for each of the standard supplementary services are defined in other individual standards presented through *Appendix D* (InterConnect Communication, 1995).

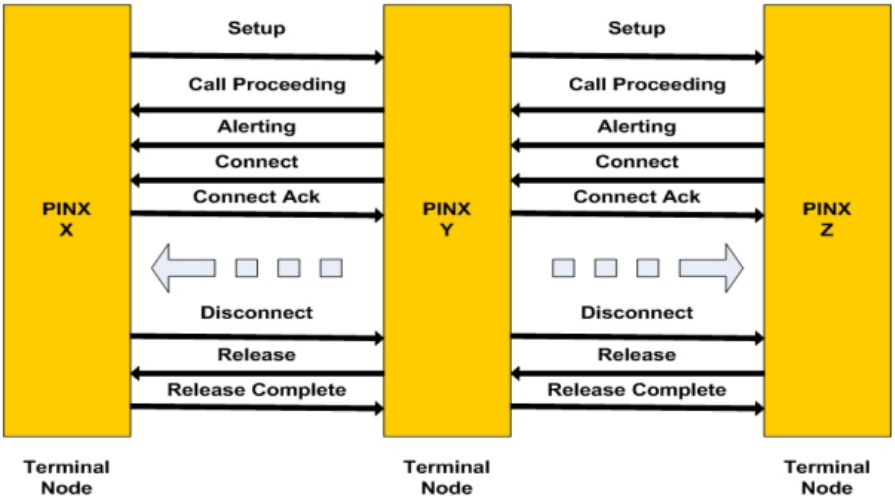

FIGURE 1
Sequence of messaging at QSIG BC which includes the transit node in the network
(InterConnect Communication, 1995)

The third sublayer of *Layer 3* defines specific Q-SIG procedures in the *"Q" reference point* for individual additional services. Within it, CTN users and the world's leading manufacturers of a particular type of PBX have specified some additional services as *proprietary*. In addition to the right of priority use of standardized services, they also demanded the retention of the right to the possibility of innovative extensions to improve their business performance, so ITU-T defined the methodology of standardization of all additional Q-SIG services in Recommendation I.130 (InterConnect Communications, 1995).

Application of Q-SIG in the PATN of the Serbian Armed Forces

At the time of the aforementioned Q-signaling testing, the Army PATN was a complex and heterogeneous functional network of automatic telephony, most of which consisted of dozens of DPABXs and the newly introduced ISDN PABX (*Private Automaticlly Branch Exchange*) of various manufacturers (only a few were partially IP oriented). These ISDN PABXs in the network were connected by a mixed architecture of "*stars*" and "*loops*", with a multi-level structure: *end, node, transit* and *main transit* DPABX. By applying Q-SIG as a CCS-oriented network signaling system, at the beginning, between ISDN DPABXs of different manufacturers in the fixed PATN of the Army, the possibility for their interoperability was first provided. Later, interoperability was provided between these DPABXs and the switching centers within the MC of PTIS, as well as the switching center of the *Digital Mobile Radio Network TETRA* (Svrzić & Ćosović, 2002). In that way, interoperability was ensured in advance with the PINX from the PTN (*Private Telecommunication Networks*) of other armies or military alliances, with which will later be in telecommunication interconnection, and with the switching nodes of public mobile telephony operators. Today, the PATN SAF has achieved complete independence from various ISDN DPABX manufacturers and high integration of the planned scope of implementation of basic and additional user services and network services specified by Q-SIG, which have become available to the users of that network, regardless of which switching node is connected (Svrzić, 2019).

However, when it comes to further continuous application of Q-SIG in the PATN SAF, as a large part of the ITIS SAF which today contains the PISN (*Private Integrated Services Network*) in combination with the Private IP network SAF (*Intranet SAF*) based on the SIP (*Session Initiation Protocol*), the following is undoubtedly the most important priority for the SAF: to ensure that these services are realized in the most economical way, not only on its homogeneous ISDN parts, but also on parts with the IP / SIP transport networks (the IP networks from the framework of the Intranet). In this case, the switching equipment of any of the present manufacturers must not be technologically outdated in the near future, but must be used when the IP platform is the dominant medium for signal transmission between them.

In connection with such obligations, in the last few years a number of node and transit DPABXs have been modernized or completely replaced, which have become interoperable (at the IP/SIP level) with the newly built IP network-*Intranet SAF*, which offers a packet switching mode and transmission of all services (without connection) based on the IP (*Internet Protocol*), as a network layer protocol. This primarily refers to modern hybrid IP/digital switching systems, the so-called IP PINX, which are specially designed to work in the PISN and, using an integrated Gateway, are capable of interacting with both the ISDN and IP/SIP environment, and with the possibility of continuing the successful application of network signaling type Q-SIG. Such IP PINXs today play the role of main entities in the PISN SAF, while successfully supporting networking with the use of Q-SIG, in accordance with ECMA-142 (Ecma International, 2001a), ECMA-143 (Ecma International, 2001b), and ECMA-165 (Ecma International, 2001c), as well as the implementation of all additional services and *Additional network functions*-ANF in accordance with the relevant individual Q-SIG standards (*Annex D* from the literature (InterConnect Communications, 1995) and (Svrzić, 2019).

Description of the Q-SIG tunneling principle via the SIP

ECMA-355 Standard (Ecma International, 2008) is in charge of defining the Q-SIG interconnection of services and signaling protocols in modern CTNs, which also contain transport IP boundaries within their PISNs. Specifically, *ECMA-355 Standard* specifies the procedure of *tunneling Q-SIG messages* via the SIP (*Session Initiation Protocol*) defined by Recommendations RFC 3261J and RFC 3311 (Rosenberg et al, 2002), (Rosenberg, 2002). The SIP is an application layer protocol for establishing, terminating and

modifying multimedia sessions and is commonly transmitted over the IP, as defined by Recommendations RFC 760 and RFC 791J (University of Southern California, 1980a), (Deering & Hinden, 1998), where telephone calls are considered a type of multimedia session in which only audio signals are exchanged.

The application of the *Q-SIG message tunneling* procedure allows calling between PINX, i.e. "islands" within PISN parts with circuit-switched circuits using Q-SIG, including the case when they are interconnected by a transport IP network (using the SIP), without losing Q-SIG functionality. This means that even in such situations, they provide their participants with a *basic Q-SIG call*, as well as additional services and all ANF. Namely, this innovated standard facilitates the introduction of improved SIP and SDP functionalities (*Session Description Protocol*) described by Recommendation RFC 3264J (Rosenberg & Schulzrinne, 2002), which include the possibility of using encryption of useful signal and mechanisms for more functional exchange of information (offers and responses) within the functioning of the SDP. Among other things, a more functional exchange of information implies mandatory renegotiation (i.e. negotiation in the opposite direction) during the exchange of bids/responses with the SDP, and, in order to achieve compatibility with the earlier issue of standards, an indicator was introduced to detect changes in signaling procedures. This indicator dynamically detects the need for withdrawal and application of signaling procedures in accordance with the previous edition of the standard (*Annex A, ECMA-355*).

Large CTNs often contain marginal PISNs that use Q-SIG, as well as their own central IP networks (*Core network*) that use the SIP, so in terms of telephony within their framework, two different cases may occur:

1) *Q-SIG call* or *Signaling connection independent of Calls* (SCIoCs) can originate from a user connected to the PISN and end up with a user connected to an IP network or vice versa. In both situations, the Gateway is a network entity that provides Q-SIG and SIP interconnection at the boundary between the PISN and the IP network. The realization of the basic interactive call via the Gateway for such communication, i.e. for the *mode of mutual operation*, is specified in *ECMA-339 Standard* (Ecma International, 2006).

2) *Q-SIG calls* or only SCIoCs, which originate from the "A" user connected to the PISN, pass through the IP network using the SIP, and end with the "B" user connected to another PISN (or another part of the same PISN). *ECMA-355 Standard* deals with just such a case, because in such a connection case all the possibilities of Q-SIG are retained during transport through the IP network. This is achieved by applying the process of *tunneling Q-SIG messages* within SIP requests and SIP responses, which are exchanged in the context of a specified SIP dialogue.

It should be noted that according to *ECMA-339 Standard*, each Gateway can provide a *mode of interaction* between the PISN and the IP network, but only the realization of the *basic Q-SIG call* is enabled (Ecma International, 2006). Thus, this standard specifies the interoperability of the PISN (with Q-SIG) and the IP network (with the SIP), only for the service of the *basic Q-SIG call*, which is then implemented according to the procedures specified in *ECMA-143 Standard* (Ecma International, 2001b). Other features of Q-SIG (support for additional services and ANF), which are specified in other individual ECMA standards for Q-SIG, as well as specifications specific to a particular manufacturer of a particular type of PINX, are not covered by such connections. Some of these additional Q-SIG services are suitable for interconnection with the SIP and are considered by other individual ECMA standards, while others are not suitable for this, as there are no appropriate elements in the SIP (or these services are provided within the SIP in a way that is not compatible with Q-SIG). (Ecma International, 2008), (Svrzić, 2019)

Architecture applicable in practice

From the point of view of the application of *ECMA-355 Standard*, both globally and within the modernized PATN SAF, it is interesting to mention the network scenario indicated in the second case of connection realization, in the *basic Q-SIG call* or only SCIoCs, which is achieved by using the Gateway at each crossing, between the PISN (which uses Q-SIG) and the IP network (which uses the SIP). In this sense, the Gateway

is an IP network entity, which acts as a Q-SIG transit PINX, where the Q-SIG is transmitted via a *circuit-switched connection*, within the PISN (at both ends), and *tunneling via the SIP*, within the IP network (i.e. on the *Core part*) from the PTN. Such an architecture of an interesting part of the heterogeneous PTN is shown in Figure 2.

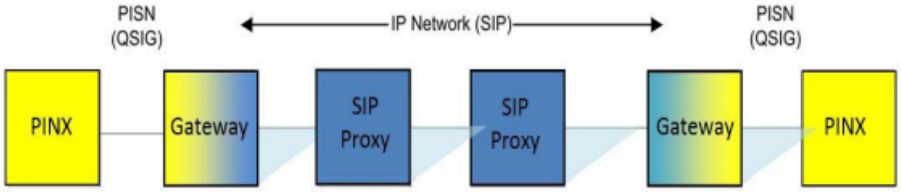

FIGURE 2
Arrangement of entities when making calls from QSIG via the SIP to QSIG
(Ecma International, 2008)

In general, the interoperability between the displayed parts of the network with Q-SIG and the SIP will be limited on the Gateway itself, i.e. only those Q-SIG capabilities that have sufficiently compatible equivalents in the SIP will be transferred, as each of them requires a separate implementation in the Gateway. Therefore, a typical Gateway can provide interoperability of Q-SIG and SIP networks, only for that subset of Q-SIG capabilities for which it possesses the necessary SIP interoperability implementations. This then necessarily implies a possibility of losing some of the possibilities within the realization of Q-SIG calls, both in the direction from Q-SIG to the SIP, and in the opposite direction. Also, for a case similar to the one shown in Figure 2, some of the Q-SIG capabilities may be lost if the two participating Gateways are of different types (from different manufacturers), since only those Q-SIG capabilities that are common to both Gateways enable "*end-to-end*" connectivity.

The practical application of *ECMA-355 Standard* (which is also the case in the PATN SAF), which defines the procedure for *tunneling Q-SIG messages* through an IP network, i.e. their integration (*encapsulation*) within SIP messages, solves such situations and there is no possibility to lose parts of Q-SIG in the mentioned "*end-to-end*" connection. In this case, one of the two Gateways creates a SIP dialog with the other Gateway, and the SIP messages within that dialog are used to *tunnel Q-SIG messages*. Through the use of the SDP, the SIP dialog also establishes a session in which media streams carry user information between two "Q-SIG Gateways", which then function as Q-SIG transit PINX, transmitting both user information and Q-SIG messages, with little or no modification.

In a conventional PISN (meaning TDM/ISDN) that uses Q-SIG, the two PINXs are connected using an IPC (*inter-PINX connection*), which contains CCS signaling (which carries Q-SIG messages) and usually one channel that carries user information (*speech, modem information*, or *data*). However, in the present *Q-SIG tunneling solution*, the IP network provides an IPC between the two Gateways, which can then function as transit PINXs. *The tunnel*, which provides the SIP for Q-SIG messages within an IP, acts as a signaling transmission channel, while the established media streams function as separate receiving and transmitting channels for transmitting user information. The audio stream, or other user information, is transmitted in UDP (*User Datagram Protocol*) packets, as described in RFC 768 Recommendation (Postel, 1980), in which case they contain RTP (*Real Time Transport Protocol*) packets, described by RFC Recommendation 1889 (Schulzrinne et al, 1996). Such transmission is performed in both directions of the connection between the participating Gateways, through an established SIP session, when a pair of media streams is usually established, i.e. one media stream for each direction of communication.

The role of *ECMA-355 Standard* to solve the modernization of Q-SIG use in the PATN SAF is such that it covers only the case of the IPC type in which a single dialogue between two Gateways is used to realize one *Q-SIG call* or one *Signaling connection independent of calls*, as defined in *ECMA-165* (Ecma International, 2001c). This then means that *ECMA-355* in the PATN SAF will only apply to situations

where the SIP dialog is established at the beginning of the establishment of a *Q-SIG call*, or SCIoC, and deleted upon their initiation (or termination). An improved scenario, according to which one SIP dialogue would be maintained in the long run and used to *tunnel* multiple *Q-SIG calls*, or multiple SCIoCs, with the possibility to accept them at any time (including those that are just being generated), is not supported in the specifications of the said standard, so it cannot be applied either within the PATN SAF. (Ecma International, 2008), (Svrzić, 2019)

Realization of the basic Q-SIG call during tunneling via the SIP

When the Ingress Gateway (*Input Gateway*), which manages the establishment of an initiated *Q-SIG call* in the direction of PISN-IP networks, receives from the PISN the initial Q-SIG message "SETUP" (request to establish a *basic Q-SIG call*), it sequentially, according to the IP network, must generate a SIP "INVITE" request using the Request-URI. Within the SIP dialogue procedure, i.e. SIP request/SIP response sessions, the Ingress Gateway will route the request over the IP network to the appropriate Egress Gateway (*Output Gateway*), which will manage the establishment of the *Q-SIG call* at the far end, in the direction from the IP network to the PISN (Figure 2). This then means that the Request-URI within the SIP request must, in some way, be derived from the defined destination of the Q-SIG call (as the indicated number of the called party, in the information of the received Q-SIG message "SETUP"). With its existence, the Request-URI can act in two different ways: 1) to explicitly determine the Egress Gateway for the requested connection, or 2) to simply determine the desired end destination of the connection, without specifying the Egress Gateway.

To act in the first case, there must be some capacity in the Ingress Gateway with the ability to search for addresses online, in order to explicitly determine the Egress Gateway. However, to act in the second case, algorithmic mapping of the called page number in the Request-URI may be sufficient, but this then represents a task for the SIP proxy, that it needs to select the appropriate Egress Gateway. In such a situation, the SIP proxy can, for example, route an "INVITE" request to the UAS (*User Agent Server*), which is not the Egress Gateway for Q-SIG, in which case *Q-SIG tunneling* will not be possible. Enabling the realization of *Q-SIG calls* in this way is undesirable, because it creates a situation in which the *mode of mutual operation* via the SIP is more suitable for operation. To prevent such a possibility, an adequate mechanism is defined in the system, initiated only by the presence of "INVITE" requests, which explicitly implies the *Q-SIG tunneling mode*. Namely, the mechanism will be manifested in such a way that the request "INVITE" will be rejected by the *Exit Gateway*, if it does not support this possibility. Otherwise, it would imply a situation where the Ingress Gateway must simultaneously map the Q-SIG message “SETUP” to the SIP request “INVITE”, both in accordance with *ECMA-355 Standard* and in accordance with *ECMA-339 Standard* (Ecma International, 2006), (Ecma International, 2008), (Svrzić, 2019).

Although this situation seems to be only partially feasible, it is architecturally very problematic, because by applying the *Q-SIG tunneling mode* the Input Gateway should behave like a Q-SIG transit PINX, while when applying the *mutual mode operation*, according to (Ecma International, 2006), it should act as a *Q-SIG Outgoing Gateway* PINX. The *Incoming Gateway* will then not know for sure which behavior to accept, until the SIP response "200 OK" arrives, and therefore will not know how to manage information related to certain Q-SIG user capabilities from the Q-SIG message SETUP “(*Additional services*, ANF and *specific capabilities of the manufacturer*). For this reason, *ECMA-355* and *ECMA-339 Standards* require that the *Input Gateway* have the ability to make a precise decision between the application of the *Q-SIG tunneling mode* or the *interoperability mode*, respectively. (Ecma International, 2008)

Call realization using independent signalization during tunneling through the SIP

It should be noted immediately that the determinant of *ECMA-355 Standard*, according to which it also refers to the case of establishing a call by type: only *Signaling connection independent of the call*, should be understood that it also applies to *Q-SIG calls* where only transmission, i.e. transport, signaling information, and without the procedure of establishing voice communication (without media flows).

When the *Input Gateway* from the PISN receives the initial Q-SIG message "FACILITY", as a request for the realization of the communication type SCIoC only, it should generate a SIP "INVITE" request using the Request-URI, which will direct this request to the appropriate *Output Gateway*. So, in this case as well, the Request-URI must be derived in some way from the defined destination from the Q-SIG "FACILITY" message (as the indicated number of the called party). Of course, techniques similar to those described used in making the *basic Q-SIG call* will be used on this occasion as well. Note that even with the implementation of this type of connection (by type of signaling transport without audio connection), it may happen that, based on the requested destination from the Q-SIG "FACILITY" message, the *Input Gateway* finds that the desired destination is not accessible via *Q-SIG tunneling* through an IP network. In this case, the Q-SIG *Input Gateway* can either direct the message further to the PISN or discard it. (Ecma International, 2008), (Svrzić, 2019)

Encapsulation of Q-SIG messages in SIP messages

When performing any of the procedures provided for the *Q-SIG tunneling* process via the SIP, the participating Gateways will behave as a Q-SIG transit PINX, as specified in standard (Ecma International, 2008) and by Recommendation RFC 3264J (Rosenberg & Schulzrinne, 2002), but also somewhat modified, as will be described below.

When *encapsulating a Q-SIG message* within a SIP message, the Gateway first includes that Q-SIG message in the MIME body of the SIP request or the SIP response (according to RFC Recommendation 3204 (Zimmerer et al, 2001), using a media/Q-SIG application, which means that Q-SIG message segmentation does not apply here. If it is necessary to use any other MIME body (e.g. from an SDP offer/response), the Gateway will use a multiple MIME body. In the case of a single MIME body, the Gateway will include the "*Content-Disposition*" header field, which indicates "*signal*" and "*handling = required*", as the SIP request/SIP response header field. In the case of a multiple MIME body, the Gateway will include the "*Content-Disposition*" header field as the header field of only that MIME body, from the SDP bid/response that contains the Q-SIG message. (Ecma International, 2008), (Svrzić, 2019)

Management of Q-SIG "SETUP" messages on the Ingress Gateway

To monitor the workflow of the Ingress Gateway after receiving the Q-SIG message "SETUP", when establishing a Q-SIG call from Q-SIG via SIP to Q-SIG, the flow chart from Figure 3 should be followed.

Sending SIP requests "INVITE"

Upon a receipt of the Q-SIG message "SETUP" from the *calling PINX*, suitable for *tunneling via the SIP* through the IP network to the *Output Gateway*, the *Input Gateway* must generate an initial SIP "INVITE" request, which contains a Request-URI and must be suitable for routing to the Gateway. In doing so, the *Input Gateway* necessarily encapsulates the incoming Q-SIG message "SETUP" within the initial SIP

"INVITE" request. The Request-URI is then derived from the information about the called party number in the Q-SIG message "SETUP", so that the relevant *Output Gateway* can be explicitly identified based on it.

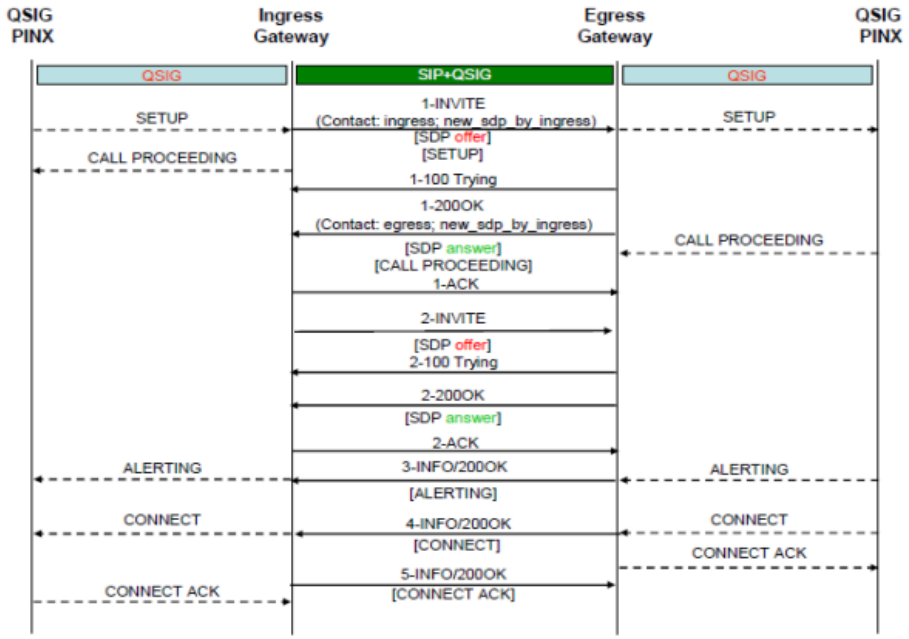

FIGURE 3
Establishing a basic QSIG call from QSIG via the SIP to QSIG
(Ecma International, 2008)

In a SIP "INVITE" request, the "*From*" field is the message header, which identifies the *Incoming Gateway* or the calling party (derived from the Q-SIG "*Calling party*" information element), while the "*Contact*" field is the header of the same SIP "INVITE" messages, which must include information on the capabilities of the UA (*User Agent*), in accordance with Recommendation RFC 3840 (Rosenberg et al, 2004), and the URI parameter type:

"+U.ecma-international.org/ecma355/new_sdp_by_ingress",

which then indicates that there is support for the implementation of the procedures defined under *ECMA-355 Standard*.

Thus, the *encapsulated Q-SIG message* "SETUP" may differ slightly from the received "SETUP" message PINX, all in accordance with an acceptable modification to the Q-SIG Transit PINX (example of changing the element of channel identification). In particular, both the channel number field and the priority/ exclusive field should contain the value "1" (exclusive).

Also, in the case of establishing a *basic Q-SIG call*, the SIP "INVITE" request must contain an SDP offer, which proposes a pair of media streams, i.e. one stream in each direction (". = *sendrecv*"), so that the *Input Gateway* can later map them in the user information channel, which is specified in the channel identification information element in the received Q-SIG message. Media streams will be suitable for use in accordance with the carrier capability information element from the received Q-SIG message "SETUP". It should be noted that in the case of establishing a SCIoCs-only call, the "INVITE" request must contain a different SDP offer, which contains the zero "m" line ("*m = 0*") (Rosenberg & Schulzrinne, 2002).

After sending the SIP "INVITE" request, the *Incoming Gateway* will not encapsulate any further message received from the Q-SIG media, until it receives the SIP response "1-200 OK" from the IP media (i.e. from the Output Gateway) with the *encapsulated Q-SIG message* "SETUP ACKNOVLEDGE" or "CALL PROCEEDING". The SIP response "1-200 OK" also contains an adequate SDP response to the initiated negotiation procedure. (Ecma International, 2008), (Svrzić, 2019)

Receipt of a response to the SIP request "INVITE"

The usual way of the UA managing the SIP response, upon the request "INVITE", means that the *Input Gateway*, upon receipt of the final SIP response type "*4-xx*", "*5-xx*" or "*6-xx*", with the *encapsulated return Q-SIG message*, must take an alternative action: 1) to route *Q-SIG calls*/ SCIoC calls, or 2) to delete them. The routing method is not described by *ECMA-355 Standard*, while the deletion activity is performed using the corresponding causal value in the "*Cause*" information element, from the encapsulated Q-SIG message for disconnection ("DISCONNECT", "RELEASE" or "RELEASE COMPLETE").

Therefore, when the SIP response contains the *encapsulated Q-SIG message* "RELEASE COMPLETE", the *Input Gateway* should use the causal value, from the "*Cause*" information element in that message, to define the causal value for the implementation of Q-SIG or SCIoC call deletion activities. The *Input gateway* then defines a causal value that reflects the fact that the next PINX is unavailable (e.g., causal value "3" = "*No route to destination*"). In case the selected UAS does not support the *encapsulated Q-SIG*, the final SIP response can be expected in the form of a SIP message: "*415*" = "*Unsupported media type*".

By receiving the SIP response "1-200 OK" with the *encapsulated Q-SIG message* "CALL PROCEEDING" and containing the SDP response, the *Input Gateway* receives an order to perform normal SIP processing, including the generation and transmission of pure SIP requests "1-ACK", and to continue acting on each *encapsulated Q-SIG message*. In this regard, the *Input Gateway* first checks for the presence of a URI parameter in the "*Contact*" field of the SIP response header "1-200 OK":

"*+U.ecma-international.org/ecma355/new_sdp_ by_ingress*".

If the URI parameter is present, then the *Input Gateway* must immediately generate a SIP request "re-INVITE", in which the same SDP bid data from the initial SIP "INVITE" request is used again. After that, the *Input Gateway* must continue to operate in accordance with the definition in the standard (Ecma International, 2008), and continue to accept incoming SIP responses "INFO", from the established *tunnel* of Q-SIG information on the IP network, regardless of the fact it is still waiting for a response to its SIP request "re-INVITE". However, if the URI parameter is not present, the *Input Gateway* will not immediately generate a "re-INVITE" SIP request. Namely, when the received SDP response on the line "*m*" indicates "*port = 0*", the *Input Gateway* will wait with the sending of the SIP request "re-INVITE" (with the new SDP offer included) to the *Output Gateway*, and will then act in accordance with (Rosenberg et al, 2002). This means that the *Input Gateway* will continue to accept incoming SIP responses of the "INFO" type, including those with an *encapsulated Q-SIG message*.

At this stage, the *Input Gateway* will only try to realize the connection of the Q-SIG channel of user information with the media flows specified in the SDP response. Namely, in the case when the line "*m*" means "*port = 0*", the *Input Gateway* will not be able to establish a two-way media flow through the IP network, for the directions of receiving and transmitting user information, so the required two-way connection will be achieved only after successful completion the SIP transaction requires "re-INVITE" or "UPDATE". Also, if by the time of receiving the Q-SIG message "CONNECT" the *Input Gateway* has not received a non-zero port "*m*" line for establishing media streams, it will not act on the received *encapsulated Q-SIG message* "CONNECT" from the SIP response "4-INFO/200 OK "and will act as if the Q-SIG timer "*T301*"has expired. (Ecma International, 2008), (Svrzić, 2019)

Manage Q-SIG "SETUP" messages on the Egress Gateway

To monitor the workflow of the Engress Gateway after receiving the Q-SIG message "SETUP", when establishing a Q-SIG call from Q-SIG via SIP to Q-SIG, the flow chart from Figure 3 should be followed again.

Receipt of the SIP request "INVITE"

Upon receipt of the initial SIP request "INVITE", which contains an *encapsulated Q-SIG message* "SETUP" and an SDP offer, the *Output Gateway* orders to check the presence of the URI parameters:

"*+U.ecma-international.org/ecma355/new_sdp_by_ingress*",

in the "*Contact*" field of its header, and sends an SIP response "1-200 OK". If the URI parameter is present, then the SIP response "1-200 OK", together with the SDP response, will contain the URI parameter in the "*Contact*" field of the header:

"*+U.ecma-international.org/ecma355/new_sdp_by_ingress*.

If this parameter is not present, the *Output Gateway* must omit the URI parameter from the SIP response "1-200 OK". The contained SDP response (in the SIP response "1-200 OK") with its parameters should enable the establishment of symmetrical media flows, unless the received SDP bid contained zero on the "*m*" line, "*m = 0*" (and then benchmark for establishing a connection by the type of SCIoC call, when there is no establishment of media streams). However, if the *Output Gateway* cannot determine the appropriate SDP parameters at the time of sending the SDP response, it will send an SDP response in which the line is "*m = 0*". In this case, the IP address in the "*c =*" line is irrelevant. It can only be important if it indicates the SIP signaling part of the *Output Gateway*.

When the received Q-SIG message "SETUP" is acceptable for further routing to the PISN (according to the called PINX), the *Output Gateway* must select CCS for signaling to the PISN side and forward the Q-SIG message "SETUP" to it. The forwarded Q-SIG "SETUP" message may differ from the received "SETUP" message according to an acceptable modification to the Q-SIG Transit PINX. In particular, the channel identification information element must reflect the TDM channel selected for the transmission of user information. To establish a *Q-SIG call*, the *Output Gateway* must also connect the established IP page streams to the selected user information channel in the PISN TDM transmission system. The *Output Gateway* in the SIP response "1-200 OK", to the initial SIP request "INVITE", may include an *encapsulated Q-SIG message*: "SETUP ACKNOVLEDGE" or "CALL PROCEEDING". Otherwise, the *Output Gateway* will transmit the first later, corresponding Q-SIG message only in one of the next SIP messages of the type "x-INFO/200 OK" (*x = 3,4,5*).

Further procedures on the *Output Gateway* depend on whether a URI parameter was present in the "*Contact*" header field from the initial "INVITE" SIP request. If it was present, then the *Output Gateway* will wait to receive the "re-INVITE" SIP request from the *Input Gateway*, regardless of whether valid SDP parameters can be determined earlier. In the event that valid SDP parameters are still not present, the *Output Gateway* will acknowledge a receipt of the SIP "re-INVITE" request by sending a "provisional" SIP response: "2-100 Traying". However, when valid SDP parameters are available in this situation, or will become available at a later stage of establishing a *Q-SIG call*, the *Output Gateway* will, upon receiving the SIP request "re-INVITE", use these SDP parameters for a later SDP response within the SIP answers "2-200 OK". In this case, the *Output Gateway* may (upon the SIP request "re-INVITE") include an *encapsulated Q-SIG message* in the SIP response frame "2-200 OK", combined with the SDP response.

If the specified URI parameter was not present, then the *Output Gateway* in the SIP negotiation process will not receive a SIP "re-INVITE" request. Only when the SDP parameters become available at a later stage of establishing a *Q-SIG call*, the *Output Gateway* will have to renegotiate media flows by sending a SIP request "re-INVITE" or a SIP request "UPDATE" with an SDP offer that reflects these parameters. Of course, it should be immediately noted that this approach, which represents a return to the procedures of early editions of the standard, can cause problems with the specific behavior of certain SDP extensions such as key management and SDP negotiation options.

Note that the *Output Gateway* can reject the SIP request "INVITE" in accordance with (Rosenberg et al, 2002). For example, if the SIP UAS does not support the *encapsulated Q-SIG*, and therefore is not able

to play the role of an *Output Gateway*, the SIP response with the code "*415*" = "*Unsupported Media Type*" will be applied. If the SIP UAS is unable to accept the SDP offer, the SIP code "*488*" = "*Not Acceptable*" will apply. However, the *Exit Gateway*, which is not able to confirm the SDP offer from the initial SIP request "INVITE", will still accept the SDP offer before sending the SIP response "2-200 OK", but will use the parameters of the SDP offer received to negotiate media flows. as part of the SIP request "re-INVITE". Of course, the *Output Gateway*, which is compatible with the early release of this standard, would send a SIP request "re-INVITE" or a SIP request "UPDATE" to re-negotiate the Media stream. (Ecma International, 2008), (Svrzić, 2019)

Rejection of a Q-SIG message from the "INVITE" request

If the *Output Gateway* receives an "INVITE" request with an *encapsulated Q-SIG message* that is not acceptable (eg: "SETUP" message that is not suitable for further routing; inappropriate Q-SIG message; "SETUP" message for a *Q-SIG call* for which appropriate media streams cannot be established), the *Output Gateway* further sends a Q-SIG response message according to standards (Ecma International, 2001b) or (Ecma International, 2001c) (e.g.: "RELEASE COMPLETE" message containing the corresponding value in the Q-SIG information element "*Cause*"). The corresponding *encapsulated Q-SIG message* will be sent either in a SIP message of the "INFO" type or in the SIP message "BYE", in the case of the Q-SIG message "RELEASE COMPLETE". If there is an unresolved SIP request "re-INVITE" at the time of refusing to accept the *Q-SIG call*, the *Output Gateway* will terminate the pending transaction by sending the SIP response: "*487*" = "*Request completed*". (Ecma International, 2008), (Svrzić, 2019)

Subsequent Q-SIG messages

After transmitting the SIP response "200 OK", to the initial SIP request "INVITE" (*Output Gateway*), or transmitting the SIP message information "ACK", after receiving the SIP response "200 OK" (*Input Gateway*), both Gateways must be able to send and receive from the opposite gateway the following *encapsulated Q-SIG messages* in the body of the SIP request and the SIP response "INFO" ("ALERTING", "CONNECT", "CONNECT ACK") (Donovan, 2000), (Ecma International, 2008). Exceptions to these situations are the SIP request "BYE", which can *encapsulate the Q-SIG message*: "RELEASE COMPLETE" and the SIP request "re-INVITE" or the SIP request "UPDATE" (Rosenberg, 2002), which can *encapsulate the Q-SIG message* on waiting during the process of establishing a new *Q-SIG call* or during the renegotiation process while the active *Q-SIG call* is in progress. (Ecma International, 2008), (Svrzić, 2019)

End of the SIP dialog

When disconnecting a Q-SIG call or SCIoC call, the participating gateways exchange the SIP request "1-INFO" with the encapsulated Q-SIG message "DISCONNECT" and the SIP response "2-INFO" with the encapsulated Q-SIG message " RELEASE "(these Q-SIG messages are transmitted to the end PINX through the PINS at both ends), as shown in the flow chart in Figure 4.

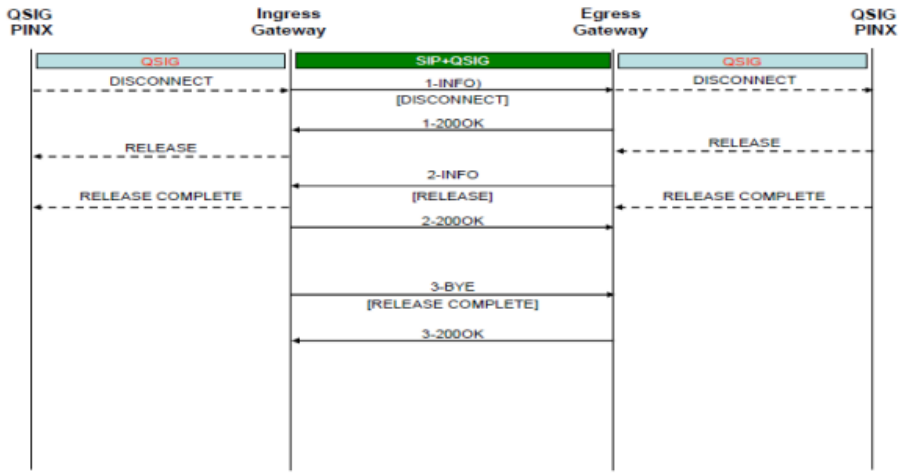

FIGURE 4
Termination of a QSIG call from QSIG via the SIP to QSIG
(Ecma International, 2008)

When the *Incoming Gateway* determines that a *Q-SIG call* or connection by the SCIoC call type is terminated, it will terminate the established SIP session by transmitting the SIP request "BYE". If in that case, according to the procedure, the *Input Gateway* sends the final message "RELEASE COMPLETE", it can *encapsulate*that *Q-SIG message* within the SIP request "BYE". After the final Q-SIG message is sent or received, the Gateway typically forwards the SIP request "BYE" without *encapsulating* that Q-SIG message. If a "re-INVITE" SIP request is pending during the end of the SIP dialog, the *Output Gateway* will terminate the transaction with the SIP response: "*487*" = "*Request Terminated*". (Ecma International, 2008), (Svrzić, 2019)

Manage Q-SIG messages to establish independent signaling calls on the Input Gateway

When establishing a call with an SCIoC, the Q-SIG message "FACILITY" (including addressing elements) is used, as specified in the standard (Ecma International, 2001c). The SIP request "INVITE" is used to *tunnel the Q-SIG message* "FACILITY", but the full negotiation session described earlier when establishing the *basic Q-SIG call* is not established. Namely, immediately after receiving the Q-SIG message "FACILITY", in this case the SIP request "INVITE" is rejected, and the flow diagram has a slightly different, simplified scenario. "INVITE" actually avoids the load, which is created when establishing the SIP dialogue for media streams, as the call establishment process is released from it. (Ecma International, 2008), (Svrzić, 2019)

Description of the mapping functions for tunneling Q-SIG through an IP network

To define the mapping functions required for the use of network intervention scenarios, within the IP switching systems from the PISN, use *ECMA-336 Standard* (Ecma International, 2002). This standard specifies the mapping functions for the use of a packet network within the Internet Protocol (University of Southern California, 1980a), (Deering & Hinden, 1998), as a network layer protocol, and the UDP (*User Datagram Exchange Protocol*) (Postel, 1980) and the TCP (*Transmission Management Protocol*) (University of Southern California, 1980b), as a transport layer protocol, to interconnect the two IP PINXs that make up the PTN entities composed of the edge PISN and central IP networks—*Core networks* (a scenario similar to that shown in Figure 2).

Interconnection is achieved by transmitting the inter-PINX signaling protocol, directly via the TCP, and inter-PINX user information (e.g. *speech*), via the RTP (*Real-Time Transmission Protocol*) (Schulzrinne et al, 1996), whereby the RTP is transmitted within the UDP. Of course, the Q-SIG functions as an inter-PINX signaling protocol, as stated in ECMA-143 (Ecma International, 2001b), ECMA-165 (Ecma International, 2001c) and other ECMA standards. Thus, the standard is applied to IP PINXs that can be interconnected to form a PISN, using Q-SIG as the inter-PINX signaling protocol. (Ecma International, 2002), (Svrzić, 2019)

To comply with *ECMA-336 Standard*, each IP PINX must constructively and functionally meet the reference configuration, defined in *ECMA-133* (Ecma International, 1998) and the requirements set out in the PICS (*Implementation Conformance Statement Proforma*). The text and format of the PICS are presented in the *Annex A* of *ECMA-336*. Within *ECMA-336 Standard*, the previously adopted terms: service/service and signaling, defined according to ITU-T Recommendation I.112, Glossary of terms for ISDN (ITU, 1988), as well as some other terms, are used as follows:

- *Caller IP PINX*, entity which sends the initial Q-SIG message "SETUP" via the IPL (*Inter PINX link*), to establish a *basic Q-SIG call* or SIoC *connection*.

- *Called IP PINX*, entity which receives the Q-SIG message "SETUP" via the IPL, to establish a *basic Q-SIG* call or SIoC *connection*.

- *A channel* is a medium for two-way transmission of user or signal information between two points in a PTN. The D. channel is used to transmit call management information (signaling) between the *"Q" reference points*, two directly connected IP PINXs. The U_Q *channel* is used to transfer user information between the *"Q" reference points*, the two end-participant PINXs of the established Q-SIG call ("*peer to peer*"). (Ecma International, 2002), (Svrzić, 2019)

Reference configuration and specific scenarios

The PISN, the IP PINX reference configuration and the connecting IVN, are defined in ECMA-133 Standard (Ecma International, 1998). The switching and call management functions on the participating IP PINXs communicate logically via the "Q" reference point instance. This communication between two connected IP PINXs is known as an IPL (Inter-PINX link) and contains a signal D. channel and one or more U. channels for user information. Through an IVN, one or more IPLs can be established in many ways between the same pair of connected IP PINXs. The IP PINX connects to the IVN at the Reference point “C”, which provides the connections defined as IPC between the cooperating IP PINXs. The mapping functions, which exist within each of the IP PINX, serve to map the D. channel and U. channels in the Reference point “Q” to one (or more) of the IPCs thus established. The concept of this standard is illustrated in Figure 5.

ECMA 336 Standard specifies mapping functions when the IVN is IP-based and when the established IPC is implemented: 1) TCP connection, which is used to transmit signal information and resource control information-RCI (Resource Control Information), and which are exchanged between the connected IP PINXs for the purpose of establishing UDP streams, and 2) establishing a pair of UDP streams, one stream in each direction, for the transmission of user information via the RTP. In doing so, one IPL requires one TCP connection, to support the D. channel, and one pair of UDP streams, to support the U. channels. In addition to transmitting Q-SIG protocol messages, a TCP connection is also required to transmit resource control information-RCI, which is essential for establishing a pair of UDP streams.

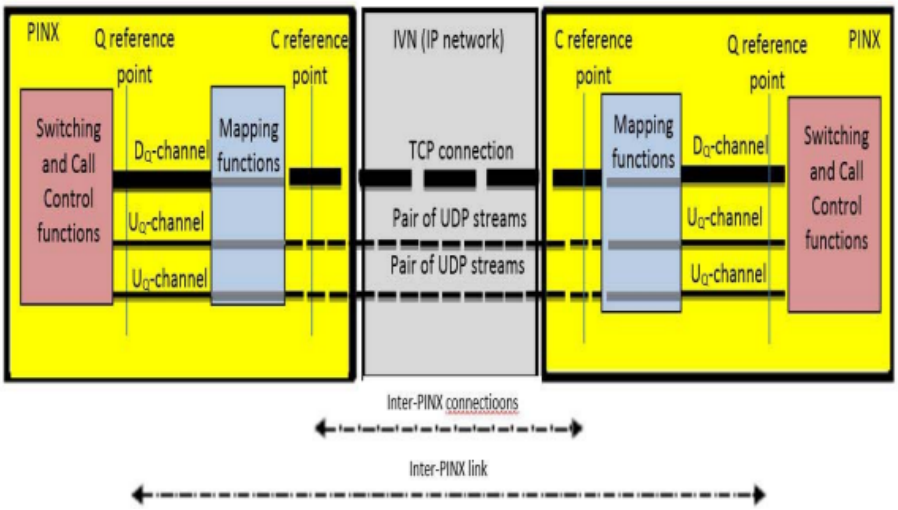

FIGURE 5
IPC concept for Semipermanent TCP connection
(Ecma International, 2002)

ECMA 336 Standard supports two types of IPCs between the PINX "peers", i.e. interconnections between the participating IP PINX: 1) "on demand", where one TCP connection (for Q-SIG transmission) and a pair of UDP streams (for user information transmission) are established at the beginning of each call and deleted at the end of that call, and 2) "semi-permanent", where one TCP connection, with unlimited duration, transmits Q-SIG for many calls. In this case, a TCP connection can support zero, one or more calls at the same time, while a pair of UDP streams (for user information) is established at the beginning of each call and deleted at the end of that call. (Ecma International, 2002), (Svrzić, 2019)

Possibilities at the reference point "Q"

One signal channel (D_Q) is provided for each instance of the *Reference point "Q"*, for the transmission of the *Layer 3* protocol signal between the IP PINX, and zero, one or more user channels (U_Q) for the media streams. On this occasion, the following basic capabilities are provided for the U_Q channel: circuit transmission mode; information transfer rate of 64 kbit/s; ability to transmit speech information or 3.1 kHz audio; and *Layer 1* user layer protocol: codec G.711 A (or "μ"), while other carrier capabilities are outside the scope of this standard. The following basic capabilities are provided for the *D_Q channel*: packet transmission mode; implementation-dependent information transfer rate; and ability to transmit unlimited digital information. In the special case of the interconnection "on demand", and when it is used only for SCIoC calls, *U_Q channels* for media streams are not established, but only a signaling DQ channel is established. (Ecma International, 2002), (Svrzić, 2019)

Possibilities at the reference point "C"

The PINX mapping functions must meet the following requirement for a TCP connection: the IP PINX must be able to support the IP packet network interface, which is suitable for communication according to the TCP (*Transmission Control Protocol*), and according to IETF Recommendation RFC 761 (University of Southern California, 1980b). The protocol stack, used in this standard, is shown in the graph in Figure 6.

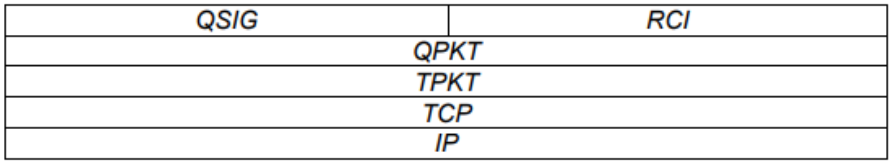

FIGURE 6
Mapping protocol / IP protocol stack - Q-SIG
(Ecma International, 2002)

The TPKT is the format of the ISO Protocol package at the *top of TCP* (ITOT) defined by Recommendation IETF RFC 2126 (Pouffary & Young, 1997). It is used to delimit individual UDP messages within a TCP stream, which provides a continuous stream of octets (bytes) without explicit boundaries. The TPKT packet consists of a version number field (8 bits long), followed by one reserved field (8 bits), then a field for determining the length of the entire TPKT (16 bits), and finally the "*actual data*". The version number field contains the value *"3"*, while the reserved field contains the value *"0"*. The length determination field should contain information about the length of the entire TPKT package, which includes: the version number field, the reserved and the length field, as well as the large final 16-bit codeword ("*actual data*").

The QPKT is a packet format consisting of a "*len*" length field (of 16 bits), followed by an entire Q-SIG message, followed by the RCI. The RCI parameter provides the information needed to establish the path (s) of the media stream. The first octet of the Q-SIG message will be immediately after the "*len*" length field, while its last octet will be the octet immediately preceding the RCI. The "*len*" field is important because it indicates the length of the Q-SIG message and thus indicates the beginning of the RCI. In cases where no stream media is established, the RCI field may be omitted.

At the *Reference point "C"*, the D_Q *channel* is mapped to a known TCP port ("*4029*") or to a dynamically assigned port, and the RCI parameter must comply with the *Annex B, ECMA-336*.

The PINX mapping functions must meet the following requirements for UDP streams: U_Q *cannels* are mapped to receive UDP and transmit UDP streams, each of which carries RTP packets. The receiving UDP stream must be received at the local IP address and the port, as indicated in the broadcast RCI, and the transmitting UDP stream is transmitted to the remote IP address and the port, as indicated in the received RCI. The IP PINX can use the RTCP to monitor the quality of the RTP transmission over the UDP streams, as defined in IETF Recommendation RFC 1889 (Schulzrinne et al, 1996). (Ecma International, 2002), (Svrzić, 2019)

Functions for DQ and UQ channel mapping

When an IPC is established at the *Reference point "C"*, the functions for mapping D_Q and U_Q *channels* are implemented. For the D_Q *channel* transmission, the complete Q-SIG message and the RCI will be embedded in the QPKT packet within the TPKT packet, which means that the segmentation and reassembly procedures of Q-SIG messages, provided by ECMA-143, will not be used. The RCI parameter implicitly refers to the same call as the Q-SIG message, so it will be included in the first forwarded and the first remaining Q-SIG message of each call and will no longer be included in subsequent messages. The RCI parameter will not be included in the messages transmitted during *Q-SIG calls* of the SCIoC type.

Each U_Q *channel* must be mapped to a pair of one-way UDP streams, with the appropriate transport capabilities defined by the RCI. The mapping function is responsible for proper packaging, unpacking, transcoding, etc. media data. (Ecma International, 2002), (Svrzić, 2019)

IPC control functions

Procedure for establishing and deleting DQ channels

To establish an IPC for a D_Q *channel*, the calling IP PINX, which initiates the TCP connection, must know the IP address of the second-*called IP PINX*. For the "*on demand*" scenario, the calling IP PINX will establish a TCP connection for the D_Q *channel* following the procedure specified by IETF Recommendation RFC 761 (University of Southern California, 1980b), and whenever necessary establish or delete a *basic Q-SIG call* or SCIoC type call.

For a "*semi-permanent*" scenario, when a *basic Q-SIG call* or a SSIoC needs to be established, if there is already a previously established D_Q *channel* (or TCP connection) between the end IP PINXs, the *calling IP PINX* will use that D_Q *channel*. If there is no already established D_Q *channel* between the end IP PINXs, the *calling IP PINX* will establish a TCP connection for the D_Q *channel* following the procedure specified by RFC 761 (University of Southern California, 1980b). The issue of implementation was previously mentioned, and it refers to the moment when the TCP connection should be deleted, since it is important that it is not deleted while it is still used for *Q-SIG call* or SCIoC *connection.* (Ecma International, 2002), (Svrzić, 2019)

Procedure for establishing and deleting UQ channels

The establishment of a U_Q c*hannel* will occur each time a *Q-SIG call* is established, when both the *calling* and *called IP PINX* will send an RCI in accordance with the *Annex B, ECMA-336*. The *calling IP PINX* will transmit the RCI in the same QPKT packet as the Q-SIG message: "SETUP". The *called IP PINX* will check if the received RCI information is acceptable and if so, it will forward the RCI in the same QPKT return packet as the Q-SIG message: "SETUP ACKNOVLEDGE" or "CALL PROCEEDING", whichever is first transmitted. Also, if the first response to the message "SETUP" is not "SETUP ACKNOVLEDGE", nor "CALL PROCEEDING" (but, for example, "RELEASE COMPLETE"), the RCI information will not be returned to the *calling IP PINX*. After transmitting the RCI information, the *calling IP PINX* will be ready to receive the RTP packet at the IP address and the port specified in its transmitting RCI information.

The *called IP PINX* will include in its transmitting RCI the same type of codec and payload period, as specified in the RCI information previously received from the *calling IP PINX*. After sending the RCI, and as soon as the media stream becomes available, the *called IP PINX* will start transmitting RTP packets to the IP address and the port which are specified in the received RCI, and according to the codec type and payload period, as specified in the received RCI. The *called IP PINX* will also be prepared to receive RTP packets at the IP address and the port specified in its transmitting RCI.

After receiving the RCI parameter in the first response message, and after receiving the Q-SIG message "CONNECT", the *calling IP PINX* will start transmitting RTP packets to the IP address and the port which are specified in the received RCI, and according to the type codec and payload period, also specified in the received RCI. If, when establishing a U_Q *channel*, any IP PINX (*calling* or *called*) receives unacceptable content in the RCI, that IP PINX will behave as specified in ECMA-143, in case the content of the channel identification information element is unacceptable.

Before sending a *Q-SIG call* clear message ("DISCONNECT", "RELEASE" or "RELEASE COMPLETE"), the IP PINX will stop transmitting RTP packets and ignore the contents of any further received RTP packets. After transmitting or receiving the Q-SIG message "RELEASE COMPLETE", the IP PINX should release the resources associated with the U_Q *channel.* (Ecma International, 2002), (Svrzić, 2019).

Conclusion

The important standards *ECMA-355*, for *tunneling encapsulated messages from Q-SIG*, and *ECMA-336*, for *defining mapping functions in PISN switching systems*, were used to organize automatic telephone traffic in the SAF, connecting two modern transit IP PINXs via the SIP transmission beam, through its own IP network (*Intranet*) in the part of the Automatic Telephone Network SAF, which is a novelty in the organization and functioning of its PTN (Svrzić et al, 2019a), (Svrzić et al, 2019b). The use of the CCS network signaling system type Q-SIG, previously applied and proven in practice, via its tunneling and transmission without degradation through the mentioned IP network with the SIP (*encapsulation of Q-SIG messages in SIP dialogue messages*), contributed to the PATN SAF without degrading the previously built PISN status, including parts where its TDM/ISDN parts connect to the *IP Proxy*. In this regard, it can be said that high integration has been achieved today in the PATN SAF, both in terms of complete independence from various ISDN PBAX manufacturers, and in terms of achieving the planned scope of implementation of basic and complementary customer services and network services specified by relevant ECMA standards for Q -SIG. Basic and complementary customer services and network services have now become available to PATN SAF users, regardless of which network switching node they are connected to.

In addition to the above, the new solution using the IP network to connect IP PINXs using the Q-SIG tunneling procedures, in the PATN SAF (Svrzić et al, 2019a), (Svrzić et al, 2019b), opens up a whole range of new possibilities that will undoubtedly contribute rapidly to the growth of the *Core network* and their application, creating a broad backbone of the system for the implementation of real-time multimedia communications and the transition to unified communications UC (*Unifed Communications*).

References

Deering, S. & Hinden, R. 1998. RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc2460 [Accessed: 1 November 2020].

Donovan, S. 2000. RFC 2976 - The SIP INFO Method. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc2976 [Accessed: 1 November 2020].

-Ecma International. 1998. *Standard ECMA-133: Private Integrated Services Network (PISN) - Reference Configuration for PISN Exchanges (PINX)* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-133.htm [Accessed: 1 November 2020].

-Ecma International. 2001a. *Standard ECMA-142: Private Integrated Services Network (PISN) - Circuit Mode 64kbit/s Bearer Services - Service Description, Functional Capabilities and Information Flows (BCSD)* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-142.htm [Accessed: 1 November 2020].

-Ecma International. 2001b. *Standard ECMA-143: Private Integrated Services Network (PISN) - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol (QSIG-BC)* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-143.htm [Accessed: 1 November 2020].

-Ecma International. 2001c. *Standard ECMA-165: Private Integrated Services Network (PISN) - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol (QSIG-GF)* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-165.htm [Accessed: 1 November 2020].

-Ecma International. 2002. *Standard ECMA-336: Private Integrated Services Network (PISN) - Mapping Functions for the Tunnelling of QSIG through IP Networks (Mapping/IP-QSIG)* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-336.htm [Accessed: 1 November 2020].

-Ecma International. 2006. *Standard ECMA-339: Corporate Telecommunication Networks - Signalling Interworking between QSIG and SIP - Basic Services* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-339.htm [Accessed: 1 November 2020].

-Ecma International. 2008. *Standard ECMA-355: Corporate Telecommunication Networks - Tunnelling of QSIG over SIP* [online]. Available at: https://www.ecma-international.org/publications/standards/Ecma-355.htm [Accessed: 1 November 2020].

-InterConnect Communication Ltd. 1995. *QSIG. The Handbook for Communications Managers*. Gwent, U.K: InterConnect Communications Ltd. ISBN: 1870935098.

-ITU - International Telecommunication Union. 1988. *I.112 : Vocabulary of terms for ISDNs. ITU - International Telecommunication Union: ITU-T: Telecommunication standardization sector of ITU* [online]. Available at: https://www.itu.int/rec/T-REC-I.112-198811-S [Accessed: 1 November 2020].

-Ministry of Defense of Norwey. 2004. *General presentation for MoD of Serbia & Montenegro as part of the program Partnership for peace "Combined Endeavour"*. Oslo: Ministry of Defense of Norwey.

Postel, J. 1980. RFC 768 - User Datagram Protocol. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc768 [Accessed: 1 November 2020].

Pouffary, J. & Young, A. 1997. RFC 2126 - ISO Transport Service on top of TCP (ITOT). In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc2126 [Accessed: 1 November 2020].

Rosenberg, J. 2002. RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc3311 [Accessed: 1 November 2020].

Rosenberg, H. & Schulzrinne, H. 2002. RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP). In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc3264 [Accessed: 1 November 2020].

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. & Schooler, E. 2002. RFC 3261 - SIP: Session Initiation Protocol. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc3261 [Accessed: 1 November 2020].

Rosenberg, J. Schulzrinne, H. & Kyzivat, P. 2004. RFC 3840 - Indicating User Agent Capabilities in the Session Initiation Protocol (SIP). In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc3840 [Accessed: 1 November 2020].

Schulzrinne, H., Casner, S., Frederick, R. & Jacobson, V. 1996. RFC 1889 - RTP: A Transport Protocol for Real-Time Applications. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc1889 [Accessed: 1 November 2020].

Svrzić, S. 2019. *Analiza mogućnosti i primene Q signalizacije u heterogenoj telefonskoj mreži funkcionalnog korisnika*. MSc thesis. Belgrade: University of Belgrade - School of Electrical Engineering (in Serbian).

Svrzić, S., Čiča, Z., Miličević, Z. & Perišić, Z. 2019a. Q-SIG over SIP tunneling in PISN with integrated services of functional user (in Serbian). In: *Proceedings of 6th IcETRAN - International Conference on Electrical, Electronic and Computing Engineering*, Silver Lake, Serbia, pp.1009-1014, June 3-6 [online]. Available at: https://etran.rs/2019/Proceedings_IcETRAN_ETRAN_2019.pdf [Accessed: 1 November 2020].

Svrzić, S.M., Čiča, Z.M., Miličević, Z.M. & Perišić, Z.S. 2019b. Echo Cancellation and Jitter Reduction in Q-SIG Tunneling over SIP in the Private Integrated Services Network (in Serbian). In: *Proceedings of TELSIKS - 14th International Conference on Advanced Technologies, Systems and Services in Telecommunications*, Niš, Serbia, pp.286-289, October 23-25.

Svrzić, S. & Ćosović, D. 2002. Digitalni tranking sistemi mobilnih radio veza po TETRA standardu (special report - separat). *Novi glasnik*, 2-3, pp.3-36 (in Serbian).

-University of Belgrade - School of Electrical Engineering. 2001. *Studija optimizacije integrisanog sistema veza Vojske Srbije i Crne Gore, Knjiga I*. Belgrade: University of Belgrade - School of Electrical Engineering (in Serbian).

-University of Southern California - Information Sciences Institute. 1980a. RFC 760 - DoD Standard Internet Protocol. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc760 [Accessed: 1 November 2020].

-University of Southern California - Information Sciences Institute. 1980b. RFC 761 - DoD Standard Transmission Control Protocol. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc761 [Accessed: 1 November 2020].

Zimmerer, E., Peterson, J., Vemuri, A. Ong, L., Audet, F., Watson, M. & Zonoun, M. 2001. RFC 3204 - MIME media types for ISUP and QSIG Objects. In: *IETF - Internet Engineering Task Force* [online]. Available at: https://tools.ietf.org/html/rfc3204 [Accessed: 1 November 2020].

Additional information

FIELD: Telecommunications

ARTICLE TYPE: Original scientific paper

Alternative link

https://scindeks.ceon.rs/article.aspx?artid=0042-846921010315 (html)
https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2021/0042-846921010315.pdf (pdf)
https://www.elibrary.ru/item.asp?id=44584148 (pdf)
http://www.vtg.mod.gov.rs/archive/2021/military-technical-courier-1-2021.pdf (pdf)