



TRANSMISSION OF Q-SIGNALING BY THE TUNNELING PROCEDURE IN THE AUTOMATIC TELEPHONE NETWORK OF INTEGRATED SERVICES OF THE SERBIAN ARMED FORCES

Sladjan M. Svrzić^a, Yulijan K. Boyanov^b

^a Tesla Systems Ltd, Belgrade, Republic of Serbia,
e-mail: milosavljevic_Svrzić@hotmail.com, **corresponding author**,
ORCID iD:  <https://orcid.org/0000-0003-4525-9844>

^b "SoftServe", Sofia, Republic of Bulgaria,
e-mail: abagar111@gmail.com,
ORCID iD:  <https://orcid.org/0000-0001-8765-2439>

DOI: 10.5937/vojtehg70-33204; <https://doi.org/10.5937/vojtehg70-33204>

FIELD: Telecommunications
ARTICLE TYPE: Review paper

Abstract:

Introduction/purpose: To specify the practical application of ECMA-355 and ECMA-336 Standards for Q-SIG tunneling and the implementation of mapping functions via the existing IP (Internet Protocol) network of the Serbian Armed Forces (Intranet SAF), in the Private Automatic Telephone Network SAF (PATN SAF), as the main part of the Private telecommunication-information networks of integrated services SAF (PISN SAF).

Methods: Description of the implemented solution and analysis of the software parameters of the established transmission SIP route, with the display of the results obtained in the fight with jitter and echo in the network.

Results: With such a solution, it was achieved that participants from the peripheral parts of the PISN SAF, which operate on the principle of transmission and circuit switching by TDM (Time Division Multiplexing), can connect with each other via the newly established central IP network SAF (Core network) which operates on the principle of transmission and switching packets with the SIP (Session Initiation Protocol), without losing the functionality of Q-SIG from the framework of the digital telecommunication network of integrated services ISDN (Integrated Services Digital Network).

Conclusion: The article deals with the modern IP PINX (Private Integrated Services Network Exchange) manufactured by Mitel, type MX-ONE Service Node 6.0, which is implemented at the transit level PATN SAF and which successfully implements the process of tunneling Q-SIG through the IP network and the necessary functions for mapping the transmission of tunneled Q-SIG messages and mapping voice (and other audio) information to VoIP (Voice over IP) communication media streams through that network. Also, the basic elements for its software preparation during the introduction of a new SIP route, with a capacity of 30 IP trunks in a transmission beam realized with 100 Mb/s-T Ethernet, are given, and the fight with the present jitter and echo in the network is described. Finally, the paper presents the experience-based values of the parameters for reducing the influence of jitter and suppressing echo.

Key words: PATN SAF, Q-SIG, PISN, IP PINX, MX-ONE, media gateway, media server, tunneling Q-SIG, encapsulation, mapping functions, jitter, echo.

Introduction

The Serbian Armed Forces (SAF) is a specific organization that has its own, modern, functional telecommunications information system (FTIS), for sufficiently fast and quality processing and transmission of accurate and protected information (spoken and non-spoken). In the framework of transmission and switching of this information, the FTIS offers a wide range of modern telecommunication customer services and network services to users in the SAF. For their realization, The FTIS SAF provides stable technical support, not only on TDM (Time Division Multiplexing) but also on a modern IP (Internet Protocol) organized platform.

The FTIS SAF is a functional, integrated telecommunication-information platform, which, in addition to the fixed part, also contains a mobile component of the system (McTIS), primarily intended for communication on the ground and in combat conditions. Therefore - while respecting the complexity of the organization, the achieved degree of technical integration and geographical distribution - the FTIS SAF coincides with the performances, determinants and standards of a large modern CTN (Corporate Telecommunications Network). (Svrzić, 2019; Svrzić et al, 2021)

About 15 years ago, in an important part of the FTIS SAF, i.e. in the Private Automatic Telephone Network SAF (PATN SAF), a network signaling system type Q-SIG (Q-Signalling), oriented to work on CCS (Common Channel Signaling), was put into operation, being specially designed and globally standardized for use in CTN (InterConnect Communication, 1995). Its application, in the PATN SAF, first provided the possibility for ISDN (Integrated Services Digital Network) interoperability between participating Digital Automatic Telephone eXchanges-DATX of different manufacturers. Later, this interoperability was provided between these DATX and the switching centers within the McTIS, as well as the switching center of the Digital Mobile Radio Network TETRA (Terrestrial Trunking Radio) (Svrzić & Jovanovski, 2021a; Svrzić et al, 2021b). Also, interoperability with PINX (Private Integrated Services Network eXchange) was provided from PTNs (Private Telecommunication Networks) of other armies or military alliances, with which the interconnection of the FTIS SAF is planned. In the end, of course, that interoperability is provided with the switching nodes of public mobile telephony operators in Serbia. (Svrzić, 2019; Svrzić et al, 2021)

In this way, high integration has been achieved in the PATN SAF to date, both in terms of complete independence from various ISDN DATX manufacturers and in terms of achieving the planned scope of implementation of basic and additional customer services and network services (specified by the whole family of individual Q-SIG standards), which have become available to PATN SAF users, regardless of which network switching node they are connected to. However, the integrated FTIS SAF today, in addition to the TDM PISN (Private Integrated Services Network), also contains the Intranet SAF. The network layer protocol, in that IP network, is defined according to IETF RFC 760 and IETF RFC 791J Recommendations, while on the application layer the network is based on the SIP (Session Initiation Protocol), which is defined according to IETF Recommendations RFC 3261J and IETF RFC 3311. Such heterogeneous situation (existence of TDM and IP) immediately raised the question of the further application of Q-SIG in the PATN SAF, as a large part of the FTIS SAF, in terms of efficiency, economy and comprehensiveness of customer services and network services, not only on its homogeneous ISDN parts but also on parts with transport IP / SIP networks (proprietary IP networks within the Intranet). Also, it raised the question of the possibility of extending the service life of the existing switching equipment (PINX) during the time when the IP



platform will be the dominant medium for signal transmission between them.

For these reasons, in the last few years, a certain number of node and transit DATXs have been completely replaced or modernized in the PATN SAF, which have (of course) become interoperable with the aforementioned proprietary newly built IP network (Intranet SAF). The Intranet SAF offers a packet mode of switching and transmission of all services (without connection) that are based on Internet Protocol, as the mentioned network layer protocol. The newly introduced, modern digital switching systems of Western origin are the so-called IP PINX, which are specially designed to work in the PISN and, using an integrated gateway, enabled to work with both ISDN and IP / SIP environment. At the same time, which is of crucial importance for their application in the PATN SAF, they enable the continuation of the successful functioning of network signaling of the Q-SIG type. Such IP PINXs today play the role of main entities in the PISN SAF, which basically consist of a switching function and a call management function. Of course, they successfully support the networking and implementation of all additional services and ANFs (Additional Network Features) with the application of Q-SIG, not only in accordance with previous Standards: ECMA-142, ECMA-143, ECMA-165 and relevant individual Q-SIG standards from Annex D Reference: "QSIG. The Handbook for Communications Managers" (InterConnect Communication, 1995), (for the PINS part with TDM organized switching and transport network), but also in accordance with new ECMA-355 and ECMA-336 Standards (for the PINS part with IP organized switching and transport network). (Ecma International, 2002; Ecma International, 2008; Svrzić, 2019; Svrzić et al, 2019a; Svrzić et al, 2021; Svrzić & Jovanovski, 2021a)

Role of ECMA-355 and ECMA-336 Standards in the PATN SAF

Let us recall that ECMA-355 Standard specifies a procedure for tunneling Q-SIG messages over the SIP, which is an application layer protocol for establishing, terminating, and modifying multimedia sessions. The SIP is usually transmitted over the IP, as a network layer protocol, so in this case phone calls are considered a type of multimedia session in which only audio signals are exchanged. Namely, in the real telecommunication network scenario SAF, the application of ECMA-355 Standard solves the case where a Q-SIG call (or only signaling independent of the call), which originates from the "A" user connected to

PINX from some TDM part of the PISN, passes through the central works with the IP network using the SIP, and ends with "B" of the user connected to the PINX from another TDM part of the PISN (or another PINX of the same TDM part of the PISN). It is very important to emphasize that during such a way of connecting, they manage to preserve all the possibilities of Q-SIG during the passage through the IP network. The reason for this is that by applying the Q-SIG tunneling procedure, its original messages are encapsulated within SIP requests and SIP responses, which are exchanged in the context of the prescribed SIP dialogue in the IP network. This then means that, by applying the tunneling procedure for the transmission of signaling messages from the Q-SIG, in the PATN SAF it is possible to call between PINX, i.e. "islands" within the parts of the PISN with circuit switching that use Q-signaling, and in the event that their interconnection (in one part) is realized by a transport IP network (which uses the SIP), without losing Q-SIG functionality. In such situations, PINX provides its participants with a regular Q-SIG call, or a Q-SIG call by type with independent signaling, as well as additional services and all ANFs, as the applied innovated ECMA-355 Standard facilitates the introduction of improved SIP and SDP functionality (Session Description Protocol, defined by IETF Recommendation RFC 3264J). These improvements are of such a nature that they include the possibility of applying encryption of useful signals and mechanisms for more functional exchange of information (offers and responses) within the SDP, which (among other things) include mandatory renegotiation (i.e. negotiation and vice versa) during the exchange of SDP offers/responses on the part of the connection path with the IP network. (Ecma International, 2008; Svrzić, 2019; Svrzić et al, 2021; Svrzić & Jovanovski, 2021a)

In order to more precisely define the role of ECMA-355 Standard, which addresses the issue of modernized use of Q-SIG in the heterogeneous PATN SAF, it should be noted that it covers only the case of this type of connection in which an individual dialogue between two Gateways (edge IP PINX located at both ends of the transport IP network) is used to make one regular Q-SIG call (or one call-independent signaling connection), basically as defined in ECMA-165. This specifically means that ECMA-355 Standard in the PATN SAF applies only to situations where, on a part of the transport IP network, the SIP dialogue is initiated at the beginning of a regular Q-SIG call (or call-independent signaling) and deleted upon their completion (or interruption). An improved scenario, according to which one SIP dialogue would be maintained in the long run and used for tunneling messages of multiple

Q-SIG calls, or multiple connections of independent signaling, with a possibility to accept them at any time (including those calls that are just generated), is not supported in the specifications of the said ECMA standard, so it could not be applied within the PATN SAF. (Ecma International, 2008; Svrzić, 2019; Svrzić et al, 2019a; Svrzić et al, 2021)

The implementation of the mapping functions in the IP switching systems PISN, which are necessary for the use of network intervention scenarios, in the PATN SAF is achieved using ECMA-336 Standard, which is a pragmatic and broad-based consensus for regulating this area of work in the PISN. In fact, this standard specifies functions for using a packet network from an IP framework, as a network layer protocol. In this regard, ECMA-336 Standard specifies how to use the TCP (Transport Control Protocol), as the transport layer protocol defined by IETF Recommendation RFC 761, and the UDP (User Datagram Protocol), Recommendation IETF RFC 768, and to interconnect the two IP PINXs that make up the entities of heterogeneous PTNs (Private Telecommunications Networks), composed of marginal PISNs and central IP networks. The interconnection of the specified IP PINX, connected by the transport IP network, is achieved by transmitting the inter-PINX signaling protocol Q-SIG (as specified in ECMA-143, ECMA-165 and other ECMA standards), directly via TCP, and by transmitting inter-PINX user information (e.g. speech), via the RTP (Real-time Transport Protocol), as defined by IETF RFC Recommendation 1889, whereby the RTP is transmitted within the UDP.

According to ECMA-336 Standard, two types of inter-PINX connection (IPC) of participating IP PINX are envisaged:

- “on demand”, where a separate TCP connection for Q-SIG is established at the beginning of each call and deleted at the end of that call; and
- “semi-permanent”, where one TCP connection with unlimited duration transmits Q-SIG on behalf of multiple individual calls.

To comply with this standard, each IP PINX in the PATN SAF constructively meets the reference configuration defined in ECMA-133 Standard and the requirements set out in the implementation of the Implementation PICS (Conformance Statement Proforma), the text and form of which are defined in the Annex A of ECMA-336 Standard. Their switching and call management functions communicate logically, via the Q point instance, on both connected IP PINXs. This communication is known as an IPL (Inter-PINX link) and contains a signal channel, known as a D_q channel, and one or more channels for user information, each

known as a U_q channel. One or more IPLs can be established in many ways between the same pair of cooperating IP PINXs. Specifically, in the PATN SAF, some realized IPLs use IP-based IVN (Intervening Network) services. Each IP PINX is physically connected to the IVN at a reference point "C", and the IVN then provides connections, defined as Inter-PINX connections between the reference points "C" of the end PINXs. This then means that the mapping functions, within each of the IP PINX, map the D_q channel and U_q channels at the reference point "Q" to one or more IPCs, which are then held via the reference points "C".

In the PATN SAF, where the IVN is IP-based, ECMA-336 Standard is used to specify mapping functions to establish the following types of IPC:

- For a TCP connection, used to transmit Q-SIG signaling messages and RCI (Resource Control Information).
- To establish a pair of UDP streams, one stream in each direction, to transmit user information (audio and others) over the RTP.

Connecting participating IP PINXs means that the IPL requires one TCP connection, to support the D_q channel, and one pair of UDP streams, to support the U_q channels, and a TCP connection (in addition to carrying the Q-SIG protocol) is also required to transmit information on resource control (RCI), which are essential for establishing UDP flows. (Ecma International, 2002; Svrzić, 2019; Svrzić et al, 2019a; Svrzić et al, 2021)

Description of the IP PINX manufacturer MITEL type *MX-ONE Service Node 6.0* from the PATN SAF

In the current PATN SAF, the main representative of the mentioned IP PINX is Mitel's switching system of the type *MX-ONE Service Node 6.0*, which is by nature a SIP Soft Switch for SaaS applications (Software-as-Service). In the PATN SAF, this type of IP PINX was introduced for its modernization, as it provides users with all integrated IP communications services (modern voice and video services and functions), but also, through the integrated Media Gateway (MGW), very successfully enables servicing inherited protocols, services and functions from the framework of TDM and analog technology (Svrzić, 2019; Mitel Sweden AB, 2018a).

Components and architecture of the MiVoice MX-ONE Service Node communication systems

Each *MiVoice MX-ONE Service Node 6.0* switching system consists of the following three main components:

- Telephony Server *MX-ONE Service Node* (formerly known as *MX-ONE Telephony Server*), which has the task of taking care of signaling. It is actually call management software, based on the Novell SUSE® Linux Enterprise Server (SLES) version 11, with a 64-bit codeword architecture. It can be installed on the private IP network itself (or in the Esxi virtual environment on the cloud), as an instance of VMware Virtual Machine, or it can be installed on a standard physical, Intel-based server (i.e. any other server based on Intel technology).

- Software or hardware Media Server *MX-ONE Media Server*, with DSP (Digital Signal Processor) resources for managing tone detection, multiple conferencing and packet switching between different IP endpoints, i.e. between different protocols and codecs (SIP and H.323 protocols; G.711 and G.729 codecs) in a homogeneous SIP environment, when direct media connection is not possible, i.e. when direct exchange of media streams between terminals is not performed. In installations with the SIP environment only, the Media Server has a load distribution/load balancing function and there is no need for dedicated Media Gateway hardware. For such installations, the Media Server can be located in the same Linux machine as the *MX-ONE Service Node* Call Server, which reduces the user trace, but can also be located on a separate server.

- Media Gateway, which is not a mandatory component, but must exist as a supplement to the IP PINX variant in the PATN SAF. It is one or more hardware units, additionally installed in the IP PINX configuration, to provide everything that the Media Server does, but also to provide users with services on physical participant and transmission interfaces in TDM technology, and according to PINX, public networks and auxiliary devices. The Media Gateway also includes DSP resources for tone management, conferencing, packet switching to IP phones (SIP and H.323) and for media conversion between different protocols. Any combination of the Media Server and the Media Gateway (up to a maximum of 15 Media Gateways) can be connected to the same Server to call the *MX-ONE Service Node*.

An overview of the manufacturer's (proprietary) system main components, terminal devices, applications and parts of the IP PINX *MX-ONE Service Node 6.0* IP monitoring and management system, as well as the systems and applications of other manufacturers that can be included in this system, is shown in Figure 1. It should be immediately pointed out (although part of it is not explicitly seen in the Figure) that the IP PINX itself, in addition to the above basic components, also includes hardware components for capacity building of various non-IP participants (analog and digital), components no IP and no ISDN trunks and power supply components. It also includes various terminal devices, which include all types of Mitel's participating telephones (IP, digital, video, mobile DECT, IP DECT, etc., up to analog), Legacy Terminals of earlier generations-LT and intermediary apparatus-AC (Attendant Clients).

The necessary monitoring and management of this system is realized by connecting an external Directory Server which is not a Mitel product, and which then contains all the necessary dedicated, managerial service software (software packages: Provisioning Manager, Service Node Manager, Traffic Manager, etc.). To support the smooth operation of the IP PINX itself and the monitoring and management system, there are all the necessary software applications. Various 3rd Party devices, systems and other applications (from other manufacturers) can be connected to this IP PINX, such as VoIP Recording, SMS Server, Contact Center, Attendant, IPC, etc. (Mitel Sweden AB, 2018a)

For IP PINX, applied in the PATN SAF, Media Gateway LIMs (Line Interface Modules) type *MX-ONE Classic* with an implemented MGU2 board are implemented and housed in 19 " LIM cabinets type LBP22. In the basic variant (with one MGU2 board) Media Gateway LIM supports up to 4 interfaces of the ISDN/PRA E1 or T1 type, analog and digital extensions, mobile DECT extensions, IP extensions (with H.323 and SIP, including IP DECT and WiFi), IP networking (with H.323 and SIP) as well as Q-SIG networking.

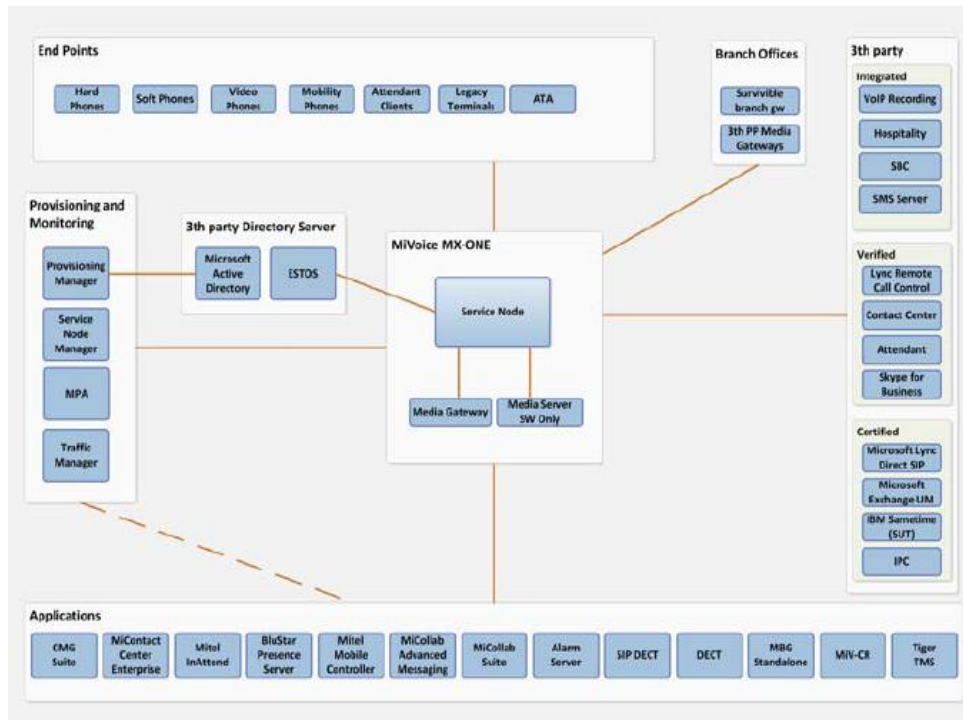


Figure 1 – Overview of the main and additional components, devices and applications of the IP-oriented PINX type MX-ONE Service Node 6.0 (Mitel Sweden AB, 2018a)

Рис. 1 – Обзор основных и дополнительных компонентов, устройств и приложений IP-сервисно-ориентированного узла PINX типа MX-ONE 6.0 (Mitel Sweden AB, 2018a)

Слика 1 – Преглед главних и допунских компоненти, уређаја и апликација IP оријентисане PINX типа „MX-ONE Service Node 6.0” (Mitel Sweden AB, 2018a)

The appearance of a built, modern IP PINX type MX-ONE Service Node 6.0 on one of the telecommunication centers in the PATN SAF, with the architecture of 2 Media Gateway LIMs in one cabinet, type MX-ONE Classic (in the basic variant), is shown in Figure 2 (Svrzić, 2019).



Figure 2 – Appearance of a modern, IP-oriented, transit PINX type MX-ONE Service Node 6.0 at a telecommunications center in the Air Force (Svrzić, 2019)

Рис. 2 – Изображение современного, IP ориентированного, транзитного PINX типа MX-ONE Service Node 6.0 в телекоммуникационном центре Военно-воздушных сил (Svrzić, 2019)

Слика 2 – Изглед савремене, IP оријентисане, транзитне PINX типа „MX-ONE Service Node 6.0” на једном телекомуникационом центру у Ратном ваздухопловству и противваздухопловној одбрани (РВ и ПВО) (Svrzić, 2019)

Figure 3 shows the layout of a 7U cabinet of the Media Gateway LIM, type *MX-ONE Classic* (with the MGU2 board), from the composition of the *MX-ONE Service Node 6.0* (Mitel Sweden AB, 2018a).

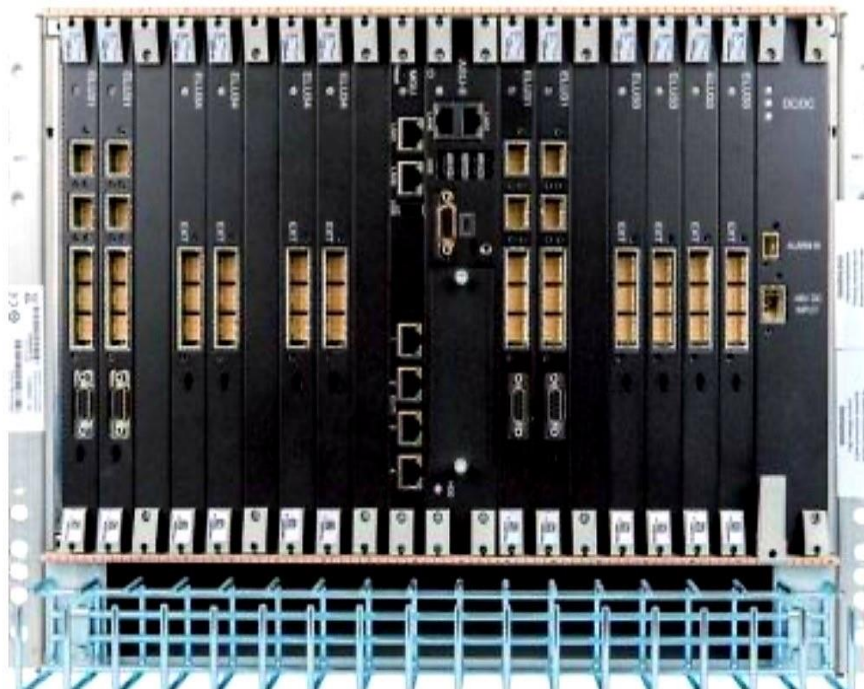


Figure 3 – Appearance of the 7U cabinet of the Media Gateway LIM type *MX-ONE Classic* (with the MGU2 board) from the composition of the *MX-ONE Service Node 6.0* in the PATN SAF (Mitel Sweden AB, 2018a)

Рис. 3 – Изображение шкафа 7U Media Gateway LIM-а типа „MX-ONE Classic (с платой MGU2) из состава сервисного узла MX-ONE 6.0 в PATN Вооруженных Силах Республики Сербия (Mitel Sweden AB, 2018a).

Слика 3 – Изглед 7U кабинета Media Gateway LIM-а типа „MX-ONE Classic“ (са плочом MGU2) из састава „MX-ONE Service Node 6.0“ у ПАТлМр ВС (Mitel Sweden AB, 2018a)

Basic traffic characteristics and components of the IP PINX system
MX-ONE Service Node 6.0

Native support for IPv6 addressing

Regarding the *MX-ONE 6.0* version, in addition to (earlier) IPv4, this switching system also supports new IPv6 addressing. The *MX-ONE Service Node* call server and Gateway components can operate as a native IPv6 network, in accordance with IETF Recommendation RFC 2460 (Deering & Hinden, 1998). It is assumed that the HV platform and OS software can work using IPv4/IPv6 "dual stack" interfaces for the IP network. Alternatives are: IPv4/IPv6 "dual stack" or just IPv4. From a signaling and media perspective, the software components of the *MX-ONE* elements (Call Manager and Media Gateways) can be configured to perform and share standard IPv6 addressing. An IPv4/IPv6 "dual stack" is installed for Inter-server communication, but only IPv6 is used regularly. In fact, the entire system (all servers) must use the same IP version of addressing.

IPv6 and IPv4 addressing are supported for SIP terminals, clients and trunks. According to H.323 terminals, H.323 client and H.323 trunk, only IPv4 addressing system is supported. If one terminal only supports IPv4 and the other terminal only supports IPv6, the call between these two terminals will only be possible with a gateway. The MGU2 and the Media Server support both IPv4 and IPv6 addressing, but, in cases where security (signal encryption) is not used, only the IPv6 addressing variant is used for the MGU2. (Mitel Sweden AB, 2018a)

VoIP protection interfaces, protocols, QoS and telephone applications

The software performs call management functions and has complete control over all ongoing calls as well as resources in the Media Gateway. The following protocols and interfaces are available for the external connection of *MX-ONE Service Node 6.0*, both to systems and applications of the same manufacturer and to systems and applications of other manufacturers ("Third Party"):

- Private networking via SIP trunks as well as via H.323 trunks, where ISDN Q-SIG or proprietary ISDN signaling is transmitted.
- Private networking via E1 (30B + D) and T1 (23B + D) trunks, via ISDN Q-SIG transmission, where T1 is used only in the MGU2.
- Private networking via ISDN trunks E1 and T1, using proprietary signaling.
- Private networking via MFC signaling transmission.
- Private networking via signaling transmission via CAS (Chanel Asotieitid Signalling).

- Private networking via DASS2 signaling transmission.
- Private networking via DPNSS (Digital Private Network System Signaling) and CAS transmission via E1 and T1 trunks.
- Public SIP trunk (with different network operator profiles).
- Public ISDN PRA via E1 and T1 and ISDN BRI (2B + D). (Mitel Sweden AB, 2018a)

When it comes to the quality of service in VoIP, i.e. quality of service - QoS (Quality Of Service), it can be registered upon a call, as follows: delay, jitter, codec used and packet loss rate can be monitored and recorded. The data can be displayed in the Service Node Manage” or via the CIL (Command Line Interface) call log output information.

When it comes to VoIP protection and security, the MX-ONE Service Node supports the use of the SRTP (Security Real-time Transport Protocol), as recommended by IETF RFC 3711 (Baugher et al, 2004). The MX-ONE Service Node also supports TLS (Transport Layer Security), as recommended by IETF RFC 4346/5246 (Dierks & Rescorla, 2006; Dierks & Rescorla, 2008), which provides secure access to IP phones and web services and secure signaling between IP phones and the MX-ONE Service Node. (Mitel Sweden AB, 2018a)

It is quite understandable that the SAF is paying more and more attention to the security aspects of the IP telephony infrastructure, which is also characteristic of the civil sector, where it is taken care of by corporate information directors (CIOs), many IT administrators and users themselves. Voice over IP traffic (signal and media) must be protected from possible numerous attacks. For example: media streams are protected from eavesdropping and intrusion, and signaling from modifications. For this reason, the PATN SAF specifically performs group crypto protection on IP/SIP trunks, which is necessary in order to professionally protect the signaling of VoIP messages and the content of media streams. Regardless of the aforementioned, the MX-ONE Service Node 6.0 system by default supports the following security measures that can be applied in practice:

- Use secured RTP (i.e. SRTP) to protect media streams. MX-ONE supports the use of SRTP to encrypt media streams in IP phones as well as in MGU2,
- Use Transport Layer Security to protect signal messages. In doing so, TLS guarantees the privacy of signaling even when SRTP keys are exchanged between parties, and
- Support a number of flexible security “policies”, i.e. support environments with different security requirements. If extensions are

allowed, then the main principle for security policy is guidance: whether these extensions must be registered in the system or not. After the registration of the realized extension, in terms of security, calls to any other party are allowed. SIP terminals must be authenticated using HTTP digest authentication. If the user is assigned a PIN code, authentication will be performed together with the SIP dialog, and from the SIP framework requires "INVITE". MX-ONE servers "spin" on operating systems that are highly capable of successfully resisting the most common network attacks. In that sense, recognized endangered services are immediately turned off, and the integrity of the files is periodically checked. In addition, clients are advised to implement security "policies" that cover the management of "patches" and antivirus software "updates".

To overcome the separation of VLANs, server "farms" need to be protected by "fire walls" and IDSs (Intrusion Detection Systems), which can block attacks. All control interfaces to MX-ONE servers can be run via secure protocols, such as SSH and HTTPS. Management and access operations of such interfaces are logged to have maximum control in the system. Users and system administrators must always authenticate themselves before obtaining permission to access the system. In addition, the access control mechanism allows different levels of privilege roles to be assigned to both users and system administrators. With *MX-ONE 6.0*, VoIP security keys have been modified to comply with EU legislation 388/2012 (formerly 1232/2011). The VoIP security key is only allowed to work in one system installation. (Mitel Sweden AB, 2018a)

Media Server system component on the ASU-E board

From the aspect of the problem of IP PINX networking type *MX-ONE Service Node 6.0* and the application of the Q-SIG tunneling procedure on the part of the central IP network (Core network) from the PTIS SAF, the system components: Media Server (*MX-ONE Media Server* variants) and the Hardware Media Gateway on the MGU2 board are of certain interest.

The Media Server Unit *MX-ONE Media Server* has a Novells SUSE® Linux Enterprise Server (SLES) version 11 operating system, with a 64-bit architecture. In principle, this variant of the Media Server unit can be implemented in several variants, but the IP PINX *MX-ONE Service Node 6.0* in the PATN SAF uses a variant of the ASU-E Media Server board.

The applied variant of the Media Server board type ASU-E is characterized by improved performance and is based on the COMXpress

standard. The ASU-E server board is included in the configuration of LIMs of the *MX-ONE Classic* type, in variants with service of one or more Media Gateways. It is the latest server board (which has 16 GB of RAM), so in connection with that, there is a novelty in the IP PINX *MX-ONE Service Node 6.0*:

- 64 bit OS (SLES11) and also natural n + 1 redundancy (network redundancy is not necessary; "Split brain" automatic recovery; controlled return and transition; clusters can be added, removed or reconfigured in the system),
- Support for IPv6 addressing, so all components (Media Server and MGW) must be either IPv4 or IPv6 compatible; support for SIP trunks and SIP extensions; Dual stack is provided; IPv4 translations from/to IPv6 must be performed via MGW,
- Media Server enhancements, which include a mix of Media Servers and MGUs, based on a maximum of 15 MGW per server; increased capacity of 2,000 RTP resources; ~ 50,000 users without using MGW for G.729 Codec (1/10 capacity),
- "Ring groups" that include new items in "Hunt groups" (simultaneous ringing permission for up to 16 users - except DECT); RVA, diversions; Ring and Hunt groups, individual log-in / out; new procedures for "log-on / out" of individual groups,
 - Support for CAS extensions on MGU2,
 - Support for CAS trunk signaling, and
 - VMware certified ASU. (Svrzić, 2019; Mitel Sweden AB, 2018b)

Media Gateway system component on the MGU2 board

The Media Gateway board MGU2 is responsible for reconciling the IP and TDM environment in the IP PINX *MX-ONE Service Node 6.0*, with its specific position in the 7U cabinet, LIM type LBP22, which in practice is recognized by a special connector , as shown in Figure 4.

The main functions of the MGU2 board are as follows:

- Mediate in all communications to the *MX-ONE Service Node*,
- Have interfaces for digital ISDN / PRA trunks E1 / T1,
- Provide RTP / SRTP, DTMF detection, DTMF tones and facsimile tones over RTP and removes jitter on RTP, and echo in VoIP communication,
 - Provide T.30 G3 fax transmission using Protocol T.38,
 - Realize the reception and sending of DTMF codes for mobile extensions,
 - Realize the sending of tones in accordance with the standards of particular countries,

- Provide a conference,
- Provide greeting messages, and
- Provide network redundancy.
- Provides external alarms.

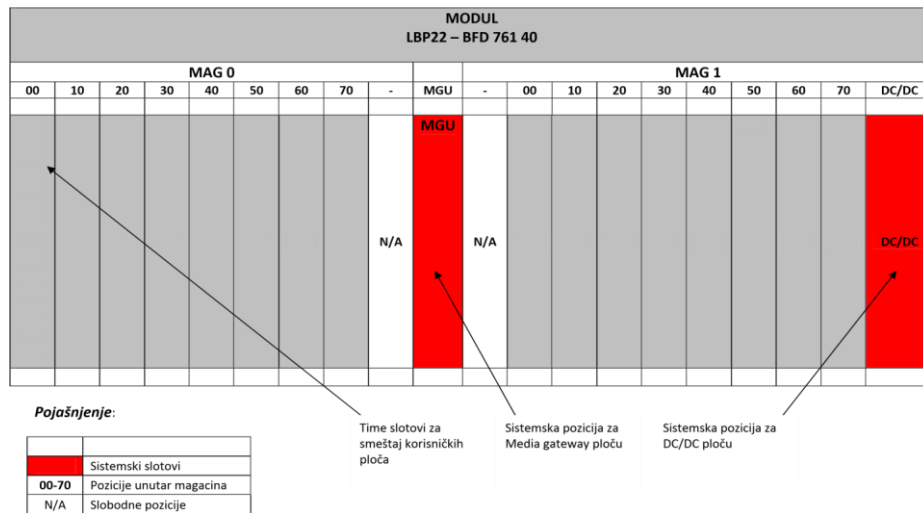


Figure 4 – Appearance of the LIM Media Gateway 7U cabinet type LBP22, with a display of precisely defined positions for the MGU2 board and the DC/DC circuit in it (Mitel Sweden AB, 2017)

Рис. 4 – Изображение шкафа LIM Media Gateway 7U типа LBP22 с отображением точно определенных позиций узлов платы MGU2 и схемы DC/DC преобразователей (Mitel Sweden AB, 2017)

Слика 4 – Изглед LIM Media Gateway 7U кабинета типа LBP22, са приказом тачно дефинисаних позиција за MGU2 плочу и DC/DC склоп у њему (Mitel Sweden AB, 2017)

The layout of the front panel of the Media Gateway MGU2 and an overview of the elements on it are shown in Figure 5.

Also, inside (on the board itself), there is a V24 interface for accessing the board, while on the back of the board there is a Back plane interface that can communicate with 16 position-boards. The displayed LED indication, on the front side of the MGU2 board, indicates the operational states in the operation of the board via visualization, as follows:

- Blinking red - the panel is in “boot mode”,
- Solid red - the board is not active,
- Solid green - the board is registered to MX-ONE as well as its communication ports, and

- Flashing green - active board and STCP packets are sent from MX-ONE to MGU2. (Svrzić, 2019; Mitel Sweden AB, 2017)

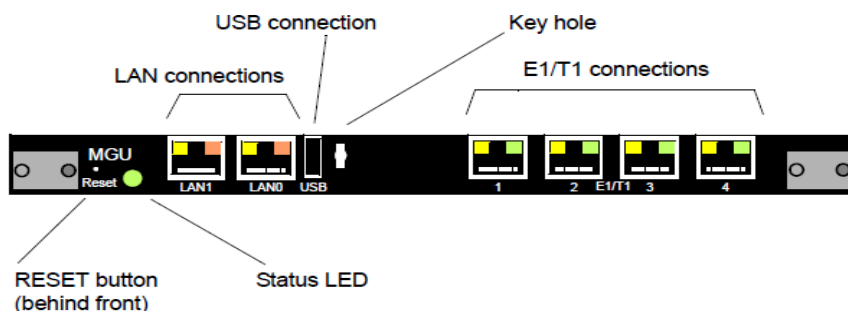


Figure 5 – Appearance of the front panel of the Media Gateway MGU2 (Mitel Sweden AB, 2017)

Рис. 5 – Изображение передней панели Media Gateway MGU2 (Mitel Sweden AB, 2017)

Слика 5 – Изглед фронта плоче Media Gateway-а MGU2 (Mitel Sweden AB, 2017)

MGU2 setting

When initializing the MGU2 board, of course for the role of the Media Gateway in the IP PINX system *MX-ONE Service Node 6.0*, software settings are performed using the following commands:

- "**setpar eth0_ip ip-address/netmask**" - address media_gateway_config,
- "**setpar eth2_ip ip-address/netmask**" - address media_gateway_interface,
- "**setpar def_route ip-address**" - the default Gateway address,
- "**setpar nfs_server ip-address**" - MX-ONE address,
- "**dispar all**" - check parameters,
- "**savepar**" - save parameters, and
- "**restart**" - restart.

Note that in terms of the application of command syntax, in *MX-ONE Service Node 6.0* in CIL, the syntax of MML commands for TDM is retained, as well as the added syntax of new UNIX commands for the IP (these commands have a record in Linux). (Svrzić, 2019; Mitel Sweden AB, 2017)

Reporting the MGW Signaling Interface

The command that defines the applied signaling of the MGU2 Media Gateway and defines the Signaling interface is:

“**media_gateway_config-i-m1A-mgw-type** **MGU-cidr**
192.168.5.56-default gateway 192.168.5.1”, where the most important parameters are:

- *-cidr* - address of the interface with the network mask in the format X.X.X.X / X,
- *-default-gateway* - gateway address,
- *-ip-configuration-mode* (static, dhcp, slaac),
- *-l* - number of sheets,
- *-link-mode* - interface speed,
- *-media-gateway* - number of lim and gateway; format: LG, L = 1-124, G = A-O, and
- *-mgw-type* - type mgw (lsu, mgu). (Svrzić, 2019; Mitel Sweden AB, 2017)

Reporting the MGW RTP interface

The command that defines the RTP data for media streams in the MGU2 Media Gateway and defines the Signaling Interface is:

“**media_gateway_interface-i-media-gateway** **1A-cidr**
192.168.5.55-default gateway 192.168.5.1”, and the parameters are exactly the same, as well as when registering the Signaling Interface, with the following two parameters:

- *-port-start* and
- *-port-stop*, which defines the range of ports for the media. (Svrzić, 2019; Mitel Sweden AB, 2017)

MGW information

The command that prints MGW data is: “**media_gateway_info**”, and the important parameters are:

- *-attrib* - Feature name,
- *-boo* - Bool value,
- *-mgw-name* - Resource instance,
- *-print* - Read general Media gateway information,
- *-set* - Set data in the resource name,
- *-string* - String value, and
- - Other parameters used to set MGU2. (Svrzić, 2019; Mitel Sweden AB, 2017)

SIP trunking and other features of a modern private automatic telephone network

The IP PINX *MX-ONE Service Node 6.0* is certified for a large number of SIP network providers and complies with the SIP Connect 1.1

standard. The MX-ONE SIP trunking interface is also the basis for integration with "third party" systems, such as Microsoft Lync 2013/Skype-for-Business, IBM Sametime SUT and other platforms to enable "federation" between different communication platforms (Mitel Sweden AB, 2018a).

The PINX type *MX-ONE Service Node 6.0* can be connected to a private network with other such MX-ONE systems or Mitel's TSW/MD110 systems, as well as with switching systems from other manufacturers. In order to use network services between all participants in such a private network, it must be homogeneous, in terms of the system of applied standardized signaling. This means that trunks to connect telephone exchanges must use the same standardized signaling system, since in the network scenario of switching from one signaling system to another, network services are not supported on the Gateway. Private networks in which trunk connections use ISDN, SIP and H.323 signaling systems are considered homogeneous networks (in terms of signaling). Figure 6 shows the basic scenario of the PINX connection in a modern PISN of a functional user, which can be analogously copied for use in the PATN SAF, provided that the shown IP network Intranet WAN is understood as an existing IP network SAF (Intranet).

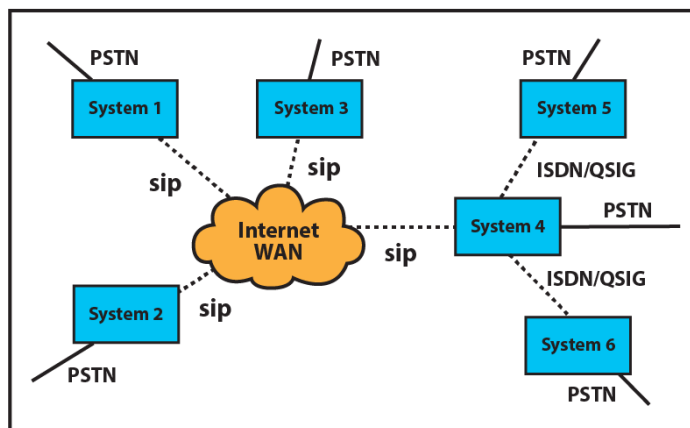


Figure 6 – Principle of the organization of homogeneous PATN with the switching systems Mitel MX-ONE, Mitel TSW/MD110 and those of other manufacturers (Mitel Sweden AB, 2018a)

Рис. 6 – Принцип организације однородног ПАТН са комутационним системима Mitel MX-ONE, Mitel TSW/MD110 и системима других произвођача (Mitel Sweden AB, 2018a)

Слика 6 – Принцип организације хомогене ПАТН са комутационним системима Mitel „MX-ONE”, Mitel „TSW / MD110” и других произвођача (Mitel Sweden AB, 2018a)

The figure shows that switching systems 1 to 4, in fact IP PINX of the same manufacturer, are interconnected via the IP network with SIP (and additional proprietary signaling), while switching systems 5 and 6 are ISDN PINX (possibly another manufacturer), connected to the network via transit IP PINX 4 using ISDN Q-SIG (Q-signaling), via transmission systems using TDM. In such an ATN organization, all switching systems shown, i.e. IP PINX and ISDN PINX, can have their own incoming and outgoing external trunks for connection to the PSTN (Public Automatic Switched Telephone Network).

The IP PINX *MX-ONE Service Node 6.0* supports a number of shared user services and ANFs (Additional Network Functions). Typical customer services and network features are: "Call Diversion", "Call Back", "Call Intrusion", "Call Waiting", and "Bypass Diversion" (overcoming redirects). In order for the mentioned customer services and ANFs to be fully used throughout the entire private automatic telephone network, it is necessary that there exist a "powerful" signaling system in that network, which can transmit all the necessary signaling information. (Svrzić, 2019) (Mitel Sweden AB, 2018a). There are two groups of common network characteristics, i.e. system functions and customer services (which include basic and additional services). System functions are those used to switch and route calls in the network, in a controlled and fast way to the called destinations. The user can only request or influence user services, while he cannot exert any influence on system functions.

In addition to the above, the following interesting features are supported within this type of PINX: "Customer Group", "Hospitality", "VoIP Recording", "Recorded Voice Announcement", "Blasklisting Of Calling Public Subscribers", "Streaming On Idle Extension", some of which could be applicable in the PATN SAF. (Svrzić, 2019; Mitel Sweden AB, 2018a)

Description of the realized software preparation procedures for practical application of Q-SIG tunneling solution on the part of the PATN SAF

The tunneling of Q-signaling through IP proxy using the SIP is practically realized on one part of the PATN SAF, where the interconnection between two participating transit IP PINX type Mitel *MX-ONE Service Node 6.0*, is realized by a transmission beam of 30 IP trunks, and via a connection path organized with a capacity of 10/100 Mb/s Ethernet. The participating end PINXs from the corresponding ISDN

parts of the PISN SAF are connected to both transit IP PINX, via the transmission beams of 30 TDM trunks each (with E1/ISDN PRI) and with the application of Network Signaling type Q-SIG. In connection with such a new situation in the PATN SAF, the necessary software interventions (for local resources on the IP PINX itself, and for network resources) were performed on both respective transit IP PINX, necessary to adapt user and network traffic data to the new situation, which was created by introducing a new route and establishing an IP/SIP transmission beam on it. (Svrzić, 2019; Svrzić et al, 2019a)

Numbering plan

The first, and very important, step in defining user data was to supplement the existing Numbering Plan (additional configuration). Therefore, it was very important to determine the parameters for the destination of the newly established route and direct the relevant external destinations from the Numbering Plan to it. The commands that define the numbering plan and read the entered data are: "**number_initiate**" and "**number_end_number_print**".

Common categories

The next step was to define the amendments to the Common Categories, which determine the privileges in the process of making a basic call and user and network services over the newly established route. In this regard, we note that the only some categories of locals have the right of access to external destinations; that the length of dialing digits varies from category to category, etc. In doing so, we distinguish two types of Common Categories: for IP extensions and for analog/digital extensions, which are defined through the CIL interface with different commands. Common categories of IP extensions are defined with the command "**Extension_profile**", while Common categories of analog and digital extensions are defined through the MML commands, with the command "**EXCCS**".

Description of the SIP route definition

To administer specific data about the new route with SIP trunks, the command: "**sip_route**" was used. This specific data is used as a supplement, in addition to the data for defining traditional ISDN routes. Namely, when defining a new SIP trunk, the command "**sip_route**" is used first, and then the so-called "RO" commands: "**ROCAI**", "**RODAI**" and "**ROEQI**". In this case, if necessary, changes in the data to be created with the piece: "**sip_route**", can be made without removing the

"RO" data. Therefore, in the given case, the initialization of the new SIP route took place in 5 steps.

Functioning related to the "sip_route" command

As explained, when the "**sip_route**" command is used, then the new data is used in addition to the traditional "RO" route data. So, the command "**sip_route**" must be used first, then "**ROCAI**", "**RODAI**" and "**ROEQI**". Of course, SIP route data must be present before using the "**ROEQI**" command. Note that the SIP routes can also be configured to only register subscribers in the remote system, without traffic configuration. In the command "**sip_route**", to bind external to internal numbers, together with the command to convert "**number_conversion_initiate**", the commands are used: "**RODDI**: ADC =", "**LCDDI**: BTON =", with parameters "*uristringN*" and "*fromuriN*" (with value N =: 0-7). (Svrzić, 2019; Mitel Sweden AB, 2017)

Appearance of the requested printout to check the set parameters of the initiated SIP route

In order to check the correctness and comprehensiveness of the set parameters of the new SIP route, specific commands are used to print the "RO" and "**sip_route**" parameters. In the practice of the PATN SAF, it could be clearly seen that the default set of parameters, specific to the "**sip_route**" command, is much richer than it was needed for a concrete solution of establishing a new SIP route. Namely, many parameters are irrelevant for a specific case, so they are without set values. (Svrzić, 2019; Svrzić et al, 2019a)

Description of the realized connection of the end ISDN PINX, through tunneling Q-SIG via IP/SIP in the PATN SAF

The scenario for connecting participants from the final ISDN PINX (located on TKC1 and TKC4), realized by applying the Q-SIG tunneling procedure via IP/SIP on the part of the connecting road between transit IP PINX (located on TKC2 and TKC3), in the Private Automatic Telephone Network SAF, is shown in Figure 7 (Svrzić, 2019) (Svrzić et al, 2019a). This situation, which arose on the Core part of the PATN SAF, completely coincides with the situation shown on the standardized PISN model from Figure 4 from the literature: (Ecma International, 2008) and Figure 1 from the literature: (Svrzić et al, 2019a).

In this way, the Q-SIG call initiated by the digital participant "A", connected to the participant board ELU-28 end ISDN PINX, numbering "380-xxx" with TKC1, first uses Q-signaling and voice transmission to the 2 Mbit/s E1 transmission beam according to the transit IP PINX with TKC2, to which the specified ISDN PINX is connected, via the E1 connection on the transmission board TLU-76 and via the transmission system ODS 2.5 Gb/s.

The Q-SIG call initiated by this transmission system comes to the transit IP PINX, as it is brought from its E1 port to the 2 Mb/s E1 interface port of its Media Gateway on the MGU2 board (plays the role of the Inbound Gateway). On the transit IP PINX, the call is processed in cooperation with the Media Server on the ASU-E board, in terms of encapsulating incoming Q-SIG messages (for signaling) and establishing media streams (for speech) within the SIP dialogue (TCP for Q-signaling and UDP for media streams). By applying the Q-SIG and media tunneling process by voice transmission within the SIP, the call over 100 Mb/s IP Switch and 100 Mb/s Ethernet port ODS 2.5 Gb/s crosses over the proprietary IP network with the SIP to the second transit IP PINX with TKC3. With a 100 Mb/s Ethernet port ODS 2.5 Gb/s and via the IP Switch, the call comes to the MGU2 board and the transit IP PINX, i.e. to its Media Gateway (plays the role of the Exit Gateway).

The cooperation between the Media Gateway and the Media Server translates encapsulated Q-SIG messages and UDP media streams from the SIP dialog box into the original Q-SIG processions and the original speech signal in the ISDN format. With a 2Mb / s E1 interface on the MGU2, which is connected to the E1 port of the 2.5 Gb / s ODS transmission system, the Q-SIG call comes to the final ISDN PINX with TKC4. Namely, from the E1 connection of ODS 2.5 Gb / s, the call comes to the transmission board TLU-76, and through local switching ends at the participant "B" connected to the board of digital participants ELU-28, this ultimate ISDN PINX with the numbering "350 -xxx " which uses Q-SIG on the transmission beam to connect to the transit IP PINX with TKC3. (Svrzić, 2019; Svrzić et al, 2019a)

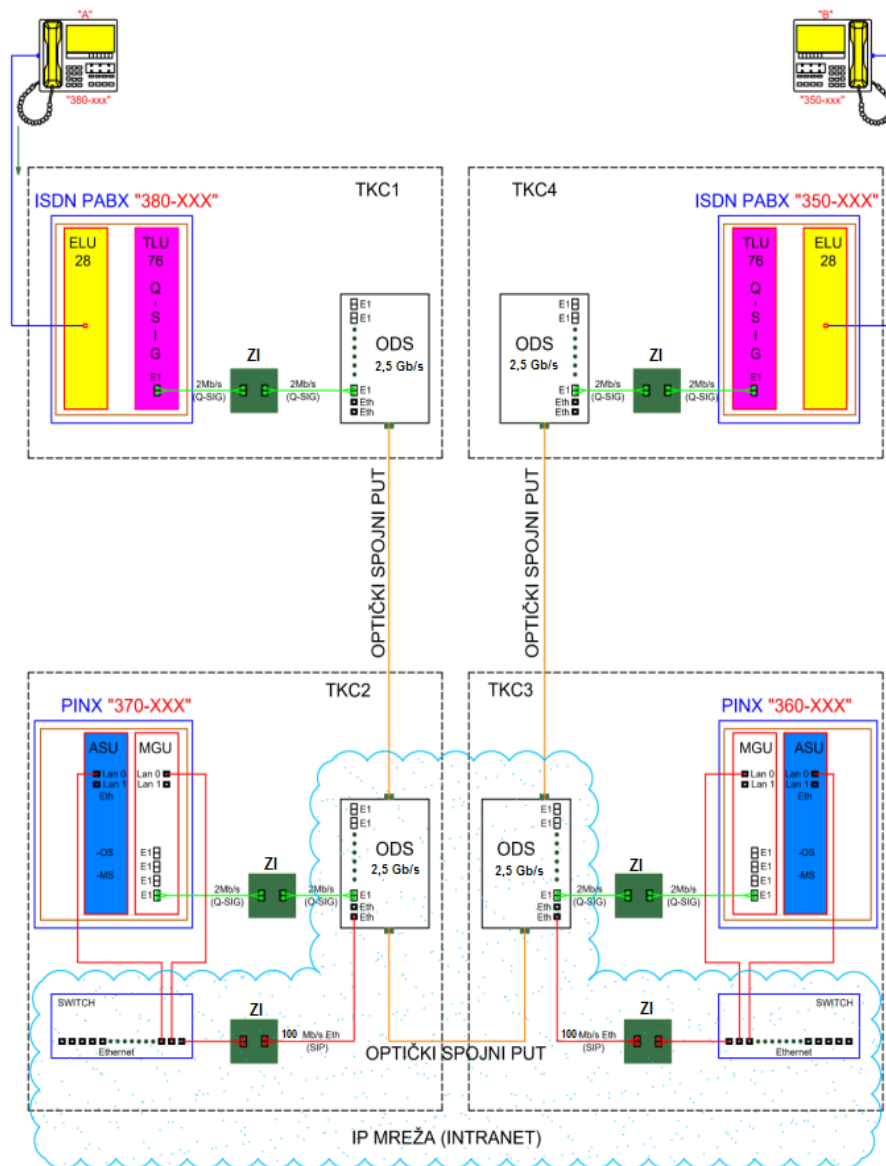


Figure 7 – Scenario of tunneling Q-SIG over the proprietary IP network with the SIP in the PATN SAF (Svrzić, 2019; Svrzić et al, 2019a)

Рис. 7 – Сценарий туннелирования Q-SIG по проприетарной IP-сети с SIP в PATN Вооруженных Сил Республики Сербия (Svrzić, 2019; Svrzić et al, 2019a)

Слика 7 – Сценарио тунеловања Q-SIG преко власничке IP мреже са SIP у ПАТлМр ВС (Svrzić, 2019; Svrzić et al, 2019a)

The realized solution has achieved that, in the PATN SAF, in terms of transmission of basic and additional user services and all network services (as well as special Mitel "proprietary" services), there are no restrictions in terms of either compatibility of Inbound and Outbound Gateways or Q-SIG capabilities and equivalents of the SIP IP network, and there is no loss of parts of Q-SIG in the presented scenario of network "end-to-end" connection. Namely, for Q-SIG tunneling within the SIP, the necessary inter-PINX TCP connection between two Media Gateways from the transit IP PINX with TKC2 and TKC3 is provided via the proprietary IP network. Then the tunnel, provided by the SIP for the transmission of signaling Q-SIG messages via the TCP, acts as a Dq signaling channel. At the same time, within the SIP established, UDP media streams function as Uq-channels for the transmission of user information (voice, modem information, fax per t.38, data and system messages). (Svrzić, 2019; Svrzić et al, 2019a; Svrzić et al, 2021 – Figure 8).

On the newly established 30-channel SIP transmission beam, the external group protection of information (ZI) was realized regarding tunnel-transmitted signaling criteria from the Q-SIG framework, as well as all user information transmitted through media streams. For this purpose, two types of devices for group crypto protection (GCP) of transmitted information were used:

1) For IP/SIP packet transmission, at the level of 10/100 Mb/s Base-Tx Ethernet which are mounted on both sides of the transmission SIP beam, i.e. of TKC2 and TKC3, and

2) For 2 Mb/s E1 transmission of voice circuits which are mounted on both sides of the transmission ISDN beams, i.e. on TKC1-TKC2 and TKC3-TKC4.

In this way, the necessary continuity of professional information protection was achieved along the entire connection path from the ISDN PINX "380-xxx" with TKC1, through the transit IP PINX "370-xxx" and "360-xxx" with TKC2 and TKC3, to ISDN PINX "350-xxx" with TKC4.

The presented transmission network transmission systems (IVN) are IRITEL's Optical Digital Transmission Systems type ODS 2.5 Gb/s, for operation via optical media with applied SDH technology and digital transmission hierarchy. On the participant side, they are configured according to the principle of flexible multiplexers, based on the specific needs of users for capacities of 2 Mb/s E1 and 10/100 Mb/s Base-Tx Ethernet connecting paths, of each of TKC where they are mounted (for connecting telephone exchanges and others functions). As it can be seen

from Figure 7, the capacity of 100 Mbit/s Base-Tx Ethernet ports was used to interconnect the transit IP PINX, with ODS 2.5 Gb/s, while the capacities of E1 ports 2 Mb/s were used to connect the ISDN PINX. (Svrzić, 2019; Svrzić et al, 2019a)

Implementation of the parameters for jitter impact reduction and echo cancellation

During the testing of the implemented solution in the PATN SAF, it was noticed that there were no major problems with the set "RO" and "*sip_route*" parameters, i.e. that

they are professionally set up and that they generally form a realistic backbone for the successful implementation of communications through the network as a whole. The second situation arose with the appearance of jitter on the processions of the RTP packets and echo on the VoIP communication channels, which appeared in the network from the very beginning, so activities had to be taken to reduce the impact of jitter and suppress echoes in order to maintain the quality of audio speech transmission (Svrzić, 2019; Svrzić et al, 2019a; Svrzić et al, 2019b).

There are three basic components on the MGU2 (Media Gateway Unit) boards of the implemented Media Gateways of both transit IP PINX type *MX-ONE Service Node 6.0*:

- TDM Switch, with a switching matrix type T-S-T (Time-Space-Time) 2048 x 64 kb/s,
- Ethernet (Layer 2) LAN, with two 10/100/1000 Base-Tx connections, and
- Media Stream Processor (MSP) for VoIP phone applications and DSP oriented functions, related to the MGU2 (such as VoIP, T.38 and DTMF receivers).

This allows Ethernet signaling packets, such as Non-RTP (say from the TCP), to be routed to the DP (Device Processor) via Switch Layer 2, while Ethernet packets to VoIP, such as the RTP, are routed to the same DP in the Media Steam Processor. (Svrzić, 2019; Mitel Sweden AB, 2017).

On the newly established SIP route between the transit IP PINX (on TKC2 and TKC3), with the TCP protocols for signaling and UDP/RTP for media streams, the network operation was tested in terms of checking the quality of realized VoIP channels, primarily in terms of real presence of jitter on the RTP packets, as well as echoes in speech transmission. The essence was to check, for the first time applied (found), the compromise values of the relevant parameters for reducing the impact of jitter and suppressing the existing echo. Due to the fact that in a given

situation, "circuit-switched" calls can sometimes pass through certain VoIP channels (e.g. between two analog phones via two different Gateways), which then leads to a new delay of about 100 ms, this also had to be taken into account during the testing. (Svrzić, 2019; Svrzić et al, 2019b)

Reducing the impact of jitter

The fact is that the RTP packets, transmitted over the IP network, can realistically have random variations of delay, can arrive out of order, and can be ejected from the procession (in case of excessive delay), which significantly reduces the quality of audio signals. To mitigate this negative impact, a JB (Jitter Buffer) circuit, installed on the MGU2 board, is used. In essence, improving the quality of the audio signal via the JB circuit can only be achieved by applying increased RTP packet delays, which then (when transmitting speech, and especially in combination with the echo at the far end) makes the echo more noticeable and disturbing. "Ad-hock" attempts to minimize this delay in noticeable echo situations can directly affect the degradation of speech quality (e.g. a situation with dropped packets can have a negative impact on the echo transmitter).

In terms of the necessary adaptation of the participating IP PINX to the established jitter in the PATN SAF, the administration of their MGU2 boards was realized with the use of the configuration parameters specially intended for adjusting the JB circuit to real network conditions. The JB circuit can be configured to operate in "adaptive" or "non-adaptive mode", whereby its configuration is realized on one MGU2 board and affects all VoIP calls in it, including inter-GW media over the IP. (Mitel Sweden AB, 2017). It turned out that the parametric configuration of the JB on the MGU2 of each of the participating IP PINX had to be a compromise between the required audio signal quality and the real increase in delay. By default for "typical networks", the JB in the MGU2 is set to work in the adaptive mode with pre-set, default parameter values in order to preserve the quality of the audio signal in relation to minimizing delays.

However, for those networks that are very sensitive to signal delay, where the desired audio quality must be achieved by adjustment, and/or in the case of a very good network, reconfiguration must be considered, i.e. changing the default values of individual JB circuit parameters, which was also the case in the PATN SAF. Achieved in testing and acceptable in practice, the values of parameters for reducing the impact of jitter on RTP packets in the subject part of the PATN SAF, i.e. in the Core network, through which the prescribed quality of speech through VoIP was achieved, are shown in the table in Figure 8 (Svrzić, 2019; Svrzić et al, 2019b).

	PARAMETAR	VREDNOST	DEFINICIJA I OBJAŠNJENJE
RTP PARAMETRI	<i>ConfortNoiseGeneration</i>	–	Parametar is not used = 0.
	<i>JB_adaptionPeriod</i>	1000 – 65535 ms	Controls the speed at which the jitter buffer can adapt downwards when current network conditions allow. Default is 10 s, which can be set lower for good networks. Postavili smo vrednost 10.000 ms.
	<i>JB_delayInit</i>	0 – 200 ms	Initial delay jitter buffer. Default is 0 ms. Postavili smo vrednost 0 ms.
	<i>JB_delayMax</i>	0 – 200 ms	Controls maximum size of jitter buffer. Default is 200 ms. If „Hardmode“ is selected this is the maximum size jitter buffer can Grow. If „Softmode“ then deletion occurs at „JB_deletionThreshold“. Postavili smo vrednost 200 ms.
	<i>JB_delayMin</i>	0 – 200 ms	Controls minimum size of jitter buffer. Default is 0 ms. Postavili smo vrednost 0 ms.
	<i>JB_deletionMode</i>	0 – 1 (boolean)	0 = Softmode (audio quality focus, default). 1 = Hardmode (delay focus). Postavili smo vrednost 0.
	<i>JB_deletion Threshold</i>	delay Max 500 ms	Packets exceeding deletion Threshold are deleted. Default is 500 ms. Postavili smo vrednost od 500 ms.
	<i>PacketLossThreshold</i>	–	Parametar is not used = 0.
	<i>VADTune</i>	.0 - 4	Control VAD threshold to improve bandwidth (low value) or Improve voice quality (high value). Too low value might give Nudesirable impact on voice quality. It is recommended to set at least 1 (default). Postavili smo vrednost 1.
	<i>VLANTagValue</i>	0 – 4095	VLAN ID for RTP packets (0 disables VLAN tagging). Postavili smo vrednost 0.
Note: Setting <i>delayMin</i> = <i>delayMax</i> = <i>delayInit</i> makes jitter buffer non-adaptive.			

Figure 8 – Set parameters and their values to reduce the impact of jitter on RTP packets (Svrzić, 2019; Svrzić et al, 2019b)

Рис. 8 – Установленные параметры и их значения для снижения влияния джиттера на пакеты RTP (Svrzić, 2019; Svrzić et al, 2019b)

Слика 8 – Постаељени параметари и њихове вредности за смањење утицаја дитера на RTP пакетима (Svrzić, 2019; Svrzić et al, 2019b)

During the testing, some experiences related to the "fight" against jitter were gained. Namely, the JB circuit is primarily intended for the adaptation of the MGU2 to the negative effects caused by the IP network itself, but it should always be borne in mind that VoIP endpoints (IP phones, gateways, IP proxies, etc.) are also parts of the network that can cause such influences.

Soft SIP clients without a dedicated HW timeslot number (e.g. Digital Signal Processor) in VoIP media will have significantly more jitter in outgoing RTP packets than it is the case with HW (Mitel Sweden AB, 2017). This can then cause an increase in the time buffer in the JB, thus further increasing the total delay present. Therefore, in these and similar network scenarios, the delay over the MGU2 may be longer than expected, which should certainly be taken into account in further practice. (Svrzić, 2019; Svrzić et al, 2019b)

Echo suppression

The EC (Echo Canceled) is an integrated circuit on the MGU2 board designed to suppress the echo for calls over the IP-IP network with packet switching (VoIP). On the part of the circuit-switched network, echo is created when a part of the packet network transmitting signal is mapped to the return signal, i.e. the packet network receiving signal.

Echo is usually caused by reflections at the transitions from 2-wire to 4-wire transmission media (on the part of the circuit-switched network), but there is also acoustic echo in telephones. This then means that, in a real network, the EC setting must also be performed as a compromise. Namely, in VoIP calls, the occurrence of echo, in combination with delays caused by the IP network, is more disturbing than the echo in the TDM network with circuit switching, in which it may happen that there is no signal delay at all. In fact, on the packet-switched network side, the user perceives echo as the sum of echoes: from the source + from the suppression operation + from the packet network delays (includes: delays in Media Gateways during encoding/decoding and in the JB); delay in the transport part of the network during switching and in routers; delay at endpoints when encoding/decoding and in the JB). (Mitel Sweden AB, 2017; Svrzić, 2019; Svrzić et al, 2019b)

The MGU2 board, implemented in the IP PINX PATN SAF, supports two types of EC for VoIP Gateway calls: Standard EC and Dual Filter EC (DFEC). Care should be taken when choosing the type of echo suppressors and their settings, because in addition to affecting all VoIP calls established via this MGU2 board (including inter-GW media over the IP), they also have a large impact on the load of the MSP (Media Steam Processor). Of course, changing the EC type will immediately trigger a restart of the MCA (Media Control Application) as well as the MSP. The EC circuit also includes a NLP (Non-Linear Processor), i.e. a sub-function that is able to "handle" the nonlinear part of the residual echo, and which the linear EC filter from the circuit cannot cancel. By default, the NLP is "disabled" during setup and is recommended to be "enabled"

only when necessary. When the NLP is "enabled" and switched on, it generates CN (Comfort Noise) to the IP network. However, if for any reason it is not desirable, CN Generating can also be discontinued to produce silence (Mitel Sweden AB, 2017).

With the selected "Standard EC", the length of the "Echo tail" can be adjusted from 8 to 128 ms, in steps of 8 ms, while the filter window is fixed at 24 ms. The advantage of "Sparse EC" is MIPS savings that correspond to higher channel density. "Standard EC" can be improved by "enabling EPCD (Echo Path Change Detection)", which then improves the adaptation of the filter window position. Setting up the EPCD will cause the MCA (Media Control Application) to be restarted (Mitel Sweden AB, 2017).

With the selected "DFEC (Dual-Filter EC)" the length of the "Echo tail" can also be set from 8 to 128 ms, in steps of 8 ms, with the advantages of its application: avoidance of increased echo levels caused by filter divergence during bidirectional conversations and robust and fast detection of echo path changes. The main disadvantage is that DFEC reduces the density of DSP channels. (Mitel Sweden AB, 2017).

During the testing, all the mentioned conditions were taken into account, so through several iterations, a configuration of parameters acceptable for practice was reached and their values are shown in the table in Figure 9 (Svrzić, 2019; Svrzić et al, 2019b).

The experience gained shows that the following practical procedures are recommended for suppressing disturbing echo network VoIP traffic in the PATN SAF:

1. The EC must be switched on thus enabling the Echo suppression function. The path of the media on which the transition from the IP to the TDM takes place (in the Media Gateway where calls are routed to/from the public ISDN trunk) is interesting. The "ClearChannel" parameter (i.e. ClearMode) must not be enabled, as this type of codec is not used for RTP. The RTP mode requires that the EC is always on.

2. The NLP (Non Linear EC Processor) function must be enabled, as it eliminates nonlinear residual echo which cannot be solved by a linear plate filter.

3. The "Dual-Filter EC" algorithm must be included, as it significantly improves echo suppression, but with caution, as DFE may have some negative impact on the capacity of the MGU2.

4. If, after (re) configuration, echo reappears, you should check whether the new parameter configuration is fixed. For example: whether the parameters for "reload" are marked in the PINX itself, and whether a "back-up" of data has been made.

Name	Value range	Description	EC type
EC_EcType	0..1	Select Echo Canceller type 0=Standard Echo Canceller (STD) 1=Dual-Filter Echo Canceller (DFE)	STD
EC_DFECFilterSize	8..128ms (in step of 8 ms)	Filter length for DFEC=64ms	DFE
EC_DFECMinErl		DFEC Minimum ERL setting (do not change) =20675	DFE
EC_DFECAttenuation		DFEC Rx output digital gain (do not change) =0	DFE
EC_ECCrossCorrelationCalculation		Not used	-
EC_EchoPathChange	„false“/„true“	„false“=Disable EPCD „true“=Enable EPCD	STD
EC_ErlChangeDetection		Not used	-
EC_FastConvergenceControl	„false“/„true“	Accelerates filter convergence for long filters=„false“	STD
EC_ECWindowsSize	24 ms	EC windows size for standard EC=24ms	STD
EC_NLPControl	„false“/„true“	„false“=Disable EPCD „true“=Enable EPCD	STD
EC_ELPTune	0..2	Not used	STD
EC_ECTailLenght	8..128ms (in step of 8 ms)	Filter length for STD EC=64ms	STD
EC_EchoCancellerEnable		Not used	-
EC_CNGEnable	„false“/„true“	CNGEnable =„true“	STD
SilenceToPCMInterface	„false“/„true“	Not used (parameter is controlled indirectly by CNG settings) =„true“	-

Note: The column tells for which EC type the parameter is valid.
Note: Changing EC parameters for default values might lower VoIP channel and other DSP resource densities.

Figure 9 – Adjusted parameters for echo cancellation on VoIP channels (TDO MO) (Svrzić, 2019; Svrzić et al, 2019b)

Рис. 9 – Скорректированные параметры для эхоподавления на каналах VoIP (TDO MO) (Svrzić, 2019; Svrzić et al, 2019b)

Слика 9 – Подешени параметри за потискивање еха на VoIP каналима (TDO MO) (Svrzić, 2019; Svrzić et al, 2019b)

5. When, in practice, the echo duration is longer than the default value of 64 ms, the set EC cannot cancel it, so the default EC setting must be changed and adjusted to the actual echo duration. The duration of echo is the time that elapses from the moment when the speaker (medium) from the IP side sends a signal to the TDM side of the network to the moment when a part of that signal is returned (from the TDM network) to the speaker on the IP side (of course, attenuated). Changes to this parameter are made in steps of 8 ms, up to a maximum value of 128 ms.

6. If the duration is 64 ms $<$ Echo $<$ 128 ms, then the appropriate length of the filter window can be set in the EC. Since the usual echo length is less than 10 ms, the length of the filter window should be set to 24 ms. However, in exceptional situations, the duration of echo can be much longer, so this should be taken into account. Inadequately set duration of the filter window can have a certain negative impact on the capacity of the MGU2. (Svrzić, 2019; Svrzić et al, 2019b)

Conclusion

In the PATN SAF, the applied tunneling procedure for the transmission of encapsulated messages from Q-SIG, defined by the global ECMA-355 Standard, enabled calling between PINX, i.e. "islands" within PISN parts with circuit-switched circuits that use Q-signaling, although they are interconnected, in one part, by the transport IP network (which uses the SIP). At the same time, without any loss of Q-SIG functionality, the connection of participants with the specified end PINX is realized, by transiting through the IP PINX type Mitel *MX-ONE Service Node 6.0*, which are interconnected by Core network. This then concretely means that through the heterogeneous

Telecommunication-information Network of the Serbian Armed Forces, according to the type of connection "from end to end", all basic and additional participation services and network functions of the ISDN are successfully transmitted.

The realized solution, through the Intranet SAF, logically connected the mentioned transit IP PINX, i.e. helped establishing their mutual communication known as an Inter-PINX link, which contains a signal channel, known as a D_q-channel, and one or more channels for user information, known as U_q channels. Through the IPL, Mitel's IP PINX *MX-ONE Service Node 6.0* successfully realizes one required TCP connection to support the D_q-channel and one pair of UDP media streams to support the U_q-channels, thanks to the use of mapping functions that take place in accordance with the global ECMA-336

Standard. Within the TCP connection, these IP PINXs transmit the encapsulated Q-SIG messages and Resource Control Information, which are necessary for the establishment of UDP streams, together on the Dq channel.

The applied solution for tunneling Q-signaling via the transit IP PINX, through the organization of the SIP transmission beam through its own IP network (Intranet SAF) on the Core part of the Automatic Telephone Network SAF, represents a novelty in the organization and operation of the PTN SAF. In this way, the service life of the Q-SIG type network signaling system, proven in practice, has been extended in the PATN SAF. By tunneling Q-SIG and transmitting without degradation through the mentioned IP network with the SIP (encapsulation of Q-SIG messages into SIP dialogue messages), it was achieved that the PATN SAF does not violate the previously built PISN status, also in parts where its TDM/ISDN parts connect to IP Proxy. In addition, monitoring the operation in the network helped in gaining necessary experience related to quality software preparation and to defining traffic parameters of the SIP route as well as to the application of the necessary procedures to reduce the impact of jitter and suppress echoes, with a view to raising the quality of VoIP communications in the network. Equally important is the practical knowledge acquired during the physical realization of completing, connecting, adapting and adjusting the necessary participating hardware equipment (for switching, IP transmission, IP Switching, group cryptosecurity on IP and TDM trunks) and using its elements and details, which will, together with the knowledge acquired in the preparation of software and the selection of the traffic parameters of the SIP route, as well as in "fights" with jitter and echo, be applied to some of future TKC SAF, following the growth rate of the Core network.

In addition to the above, in the PATN SAF, the new solution with the use of the IP network to connect the IP PINX using the Q-SIG tunneling procedures opens a whole range of other modern possibilities that will, with the undoubted growth of the Core network, contribute to the creation of a wide territorial platform and the implementation of multi-timed communications in real time, thus leading to the transition to UC (Unified Communications).

References

Baugher, M., McGrew, D., Naslund, M., Carrara, E. & Norrman, K. 2004. RFC-3711: The Secure Real-time Transport Protocol (SRTP). In: *IETF - Internet Engineering Task Force* [online]. Available at: <https://tools.ietf.org/html/rfc3711> [Accessed: 16 February 2021].

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: 16 February 2021].

Dierks, T. & Rescorla, E. 2006. RFC-4346: The Transport Layered Security (TLS), Version 1.1. In: *IETF - Internet Engineering Task Force* [online]. Available at: <https://tools.ietf.org/html/rfc4346> [Accessed: 16 February 2021].

Dierks, T. & Rescorla, E. 2008. RFC-5246: The Transport Layered Security (TLS), Version 1.2. In: *IETF - Internet Engineering Task Force* [online]. Available at: <https://tools.ietf.org/html/rfc5246> [Accessed: 16 February 2021].

-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: 16 February 2021].

-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: 16 February 2021].

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

-Mitel Sweden AB. 2017. *MiVoice MX-ONE Media Gateway Unit MGU2 Description. 21/1551-ANF 901 36 Uen D*. Stockholm, Johanneshov, Sweden: Mitel Sweden AB.

-Mitel Sweden AB. 2018a. *MiVoice MX-ONE System Description. 21/1551-ASP 113 01 Uen AA*. Stockholm, Johanneshov, Sweden: Mitel Sweden AB.

-Mitel Sweden AB. 2018b. *MiVoice MX-ONE Media Server Description. 70/1551-ANF 901 14 Uen F*. Stockholm, Johanneshov, Sweden: Mitel Sweden AB.

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: 16 February 2021].

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 TELSIS - 14th International Conference on Advanced Technologies, Systems and Services in Telecommunications*, Niš, Serbia, pp.286-289, October 23-25.

Svrzić, S. & Jovanovski, P. 2021a. Description of the TETRA1 technology and standard for modern digital trunking systems of functional mobile radio communications. *Vojnotehnički glasnik/Military Technical Courier*, 69(3), pp.687-726. Available at: <https://doi.org/10.5937/vojtehg69-30858>.

Svrzić, S.M., Miličević, Z.M. & Perišić, Z.S. 2021b. Description of the process of tunneling Q signaling in private telecommunications networks. *Vojnotehnički glasnik/Military Technical Courier*, 69(1), pp.31-63. Available at: <https://doi.org/10.5937/vojtehg69-28117>.

ПЕРЕДАЧА Q-СИГНАЛИЗАЦИИ МЕТОДОМ ТУННЕЛИРОВАНИЯ В АВТОМАТИЧЕСКОЙ ТЕЛЕФОННОЙ СЕТИ ИНТЕГРИРОВАННЫХ СЛУЖБ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ СЕРБИЯ

Сладжан М. Сврзич^а, Юлиан К. Боянов^б

^а ООО "Тесла системи", г. Белград, Республика Сербия, **корреспондент**

^б «SoftServe», г. София, Республика Болгария

РУБРИКА ГРНТИ: 49.00.00 СВЯЗЬ:

49.33.00 Сети и узлы связи;

49.33.29 Сети связи

ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: Цель данной статьи заключается в упорядочении практического применения Стандартов ECMA-355 и ECMA-336 туннелирования Q-SIG и реализации функций мапирования через существующую сеть IP (Интернет-протокол) Вооруженных сил Республики Сербия (Интранет SAF) в Частной автоматической телефонной сети SAF (PATN SAF), которая является основной частью Частной телекоммуникационно-информационной сети интегрированных услуг BC (PISN SAF).

Методы: Описание внедренного решения и анализ программных параметров установленного маршрута передачи SIP, с представлением результатов, полученных в процессе предотвращения джиттера и эхоподавления в сети.

Результаты: С помощью данного решения участникам из периферийных частей PISN SAF, которые работают по принципу передачи и коммутации каналов с помощью TDM (Мультиплексирование с временным разделением), обеспечена связь друг с другом через новосозданную центральную IP-сеть SAF (Опорная сеть), которая работает по принципу передачи и коммутации пакетов с SIP (Протокол установления сеанса), без потери функциональности Q-SIG в рамках цифровой телекоммуникационной сети интегрированных услуг ISDN (Интегрированные услуги цифровой сети).

Выводы: В статье рассматриваются особенности современной сети IP PINX (Частная сеть с интеграцией услуг) производства Mitel, тип MX-ONE Service Node 6.0, которая внедрена на транзитном уровне PATN SAF и успешно осуществляет процесс туннелирования Q-SIG через IP-сеть и необходимые функции для мапирования передачи туннелированных сообщений Q-SIG и мапирования голосовой (и другой аудио) информации в медиапоток VoIP (Передача голоса по IP) по данной сети. Также приведены основные элементы для ее программной подготовки во время внедрения нового маршрута SIP с пропускной способностью 30 IP-магистралей в луче передачи, реализованном со скоростью Интернета 100 Мб/с-Т, и описаны методы эхоподавления и устранения джиттера. В заключении статьи представлены экспериментально полученные значения параметров для уменьшения влияния джиттера и эхоподавления.

Ключевые слова: PATN SAF, Q-SIG, PISN, IP PINX, MX-ONE, медиасервер, туннелирование Q-SIG, инкапсуляция, функции мапирования, джиттер, эхо.

ПРЕНОС Q-СИГНАЛИЗАЦИЈЕ ПОСТУПКОМ ТУНЕЛОВАЊА У АУТОМАТСКОЈ ТЕЛЕФОНСКОЈ МРЕЖИ ИНТЕГРИСАНИХ СЕРВИСА ВОЈСКЕ СРБИЈЕ

Слађан М. Сврзић^а, Јулијан К. Бојанов^б

^а Тесла системи д.о.о., Београд, Република Србија, **аутор за преписку**

^б „SoftServe”, Софија, Република Бугарска

ОБЛАСТ: телекомуникације

ВРСТА ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: Циљ овог рада је да се специфицира практична примена Стандарда ЕСМА-355 и ЕСМА-336 за тунеловање Q-SIG и реализацију функција мапирања, преко постојеће IP (Internet Protocol) мреже Војске Србије (Интранет ВС), у приватној аутоматској телефонској мрежи ВС (ПАТлМр ВС), која чини главни део приватне телекомуникационо-информационе мреже интегрисаних услуга ВС (ПИСН ВС).

Методe: Описано је имплементирано решење и анализирани софтверски параметри успостављене преносничке SIP руте, са приказом резултата добијених у борби са џитером (Jitter) и ехом (Echo) у мрежи.

Резултати: Приказаним решењем постигнуто је да учесници са рубних делова ПИСН ВС, који функционишу на принципу преноса

и комутације кола по TDM (Time Division Multiplexing), могу међусобно остварити везу и преко новоуспостављене централне IP мреже BC (Core мрежа), која функционише на принципу преноса и комутације пакета са SIP (Session Initiation Protocol), а без губитка функционалности Q-SIG из оквира дигиталне телекомуникационе мреже интегрисаних сервиса ISDN (Integrated Services Digital Network).

Закључак: *Анализирана је савремена IP PINX (Private Integrated Services Network Exchange) произвођача Mitel, типа „MX-ONE Service Node 6.0”, која је имплементирана на транзитном нивоу ПАТлМр BC. Она успешно реализује како поступак тунеловања Q-SIG кроз IP мрежу, тако и неопходне функције за мапирање преноса тунелованих порука Q-SIG и мапирање говорних (и других аудио) информација на медија токове VoIP (Voice over IP) комуникације кроз ту мрежу. Такође, наводе се основни елементи за њену софтверску припрему при увођењу нове SIP руте, капацитета 30 IP транкова у преносничком снопу реализованом 100 Mb/s-T Ethernet-ом, те описује борба са присутним Jitter-ом и Echo-ом у мрежи. На крају се презентују и искуствено постигнуте вредности параметара за смањење утицаја џитера и потискивање еха.*

Кључне речи: *ПАТлМр BC, Q-SIG, PISN, IP PINX, MX-ONE, медија гејтвеј, медија сервер, тунеловање Q-SIG, енкапсулација, мапирање функција, џитер, ехо.*

Paper received on / Дата получения работы / Датум пријема чланка: 19.07.2021.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 03.01.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 04.01.2022.

© 2022 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2022 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и распространяется в соответствии с лицензией «Creative Commons» (<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2022 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у складу са Creative Commons licencom (<http://creativecommons.org/licenses/by/3.0/rs/>).

