Intelligent Network Services in the Time of Network Migration

Igor Miladinovic
Forschungszentrum Telekommunikation Wien (ftw.)
Donau-City Strasse 1
A-1220 Vienna, Austria
e-mail: miladinovic@ftw.at,
phone / fax: +43-1-502830-54 / -99

Klaus Umschaden
Institute of Communication Networks
Vienna University of Technology
Favoritenstrasse 9/388,
A-1040 Vienna
Austria

Abstract

Over the last several years, the telephony has been moving from the circuit switched (CS) networks, such as Public Switched Telecommunication Network (PSTN), towards the packet switched (PS) networks, or more exactly Internet Protocol (IP) networks. This migration process should be as transparent as possible for subscribers. Therefore, the existing telephony services in CS networks are also needed in PS networks. These services are realized by the Intelligent Network (IN) today. In this paper we present a novel architecture that enables using of IN services from both, CS and PS networks, transparently for subscribers. The architecture supposes the Session Initiation Protocol (SIP) as the signaling protocol in the PS network. It introduces a new entity responsible for the translation of SIP addresses. For better understanding of our architecture, we discuss how the Voice Virtual Private Network (VPN) service, which is a widely used IN service, can be realized with it.

1 Introduction

Intelligent network (IN) [1][2] is widely used to implement services for the traditional telephony in circuit switched (CS) networks nowadays. Given that it separates service logic from the basic switching functionality, IN enables the creation, deployment, and management of services in an efficient way. Some examples of IN services are *freephone*, *call forwarding*, *calling name delivery*, *televoting*, and *virtual private networks* (VPN). These services are widely used today and they will also be needed in the future.

In the last several years, the telephony has moved from CS networks, like Public Switched Telecommunication Network (PSTN), to packet switched (PS) networks, in particular Internet Protocol (IP) networks. This trend will continue in the future until the telephony in CS networks completely disappears. However, this will last several years and during this period the CS and PS networks will coexist. The telephony in PS networks, called IP telephony or Voice over IP (VoIP), and the telephony in CS networks, called traditional telephony, must be able to interwork, since some users will reside in PS networks and some in CS networks. This interworking is provided by gateways that translate signaling and media data between these two telecommunication worlds.

Most of the services from traditional telephony are also needed for IP telephony [3]. Instead of implementing these services for IP telephony again, it is more efficient to enable the use of IN services from PS networks. Given that these services have already been implemented and widely tested, reusing them for the IP telephony saves time and costs. It should also be possible to apply IN services on calls that involve both, PS and CS networks.

In this work we assume the Session Initiation Protocol (SIP) [4][5] as the signaling protocol in the PS network. We have chosen SIP not only because of its flexibility and extensibility, but also because SIP will be used by the Third Generation Partnership Project (3GPP) for signaling in the Universal Mobile Telecommunication System (UMTS) (release 5 and above) [6]. UMTS is expected to become the most important representative of the third generation networks.

The need to use IN services from SIP networks has been recognized before. Rotchel et al. proposed an IN extension to SIP [7] in order to enable the use of IN services by SIP entities. In [8], Bouabid et at. discussed the mapping between the SIP state machine and the IN state model. The last proposal of the Internet Engineering Task Force (IETF), described in [9], specifies a so-called SIP IN (SIN) enabled SIP entity that is capable of applying IN services on SIP calls, or more general SIP sessions. The mapping of the SIP state machine to the IN state model is also defined there. However, it is not specified how to apply services on calls between PS and CS networks.

In this paper we propose an architecture that enables the use of IN services during the network migration, when some users reside in the PS network and some in the CS network. The architecture includes a SIN enabled SIP entity that provides the PS network with IN services, and a new entity that makes translation between SIP addresses. We call this entity the SIP Address Translator (SAT) and explain its functionality in Section 3. As an example, we show how the VPN IN service can be applied using our architecture. The message flows necessary for the core service feature of VPN, the *Private Numbering Plan* (PNP), are discussed in detail.

The remainder of this paper is organized as follows. The next section gives background information, including a brief description of the IN concept and SIP. Section 3 introduces our architecture and describes its entities. In Section 4, we discuss the VPN example and show the message flow in different call scenarios. The most important findings of this paper are emphasized in Section 5.

2 Background Information

This section provides information about technologies necessary for understanding the reminder of this paper. First, it gives an overview to the IN and afterwards it briefly describes SIP, the signaling protocol in IP networks.

2.1 Intelligent Network

Intelligent network (IN) concept has been developed in order to support a growing number of services in the PSTN. It was very difficult to introduce a new service in PSTN without IN, because it required the modification of software in switches that are spread over the network. The idea of IN is to separate service logic from the basic call processing. To deploy a new service, only the service logic needs to be modified. Figure 1 shows a simplified IN architecture. Bold lines indicate transport links, normal lines signaling, and dashed lines operation.

The service logic is placed in the service control point (SCP). The service switching points (SSPs) are switches responsible for the basic call processing. They also contact the SCP for calls on which some IN services should be applied. These calls are recognized on the basis of the dialing number. The Service Management Point (SMP) is involved in activities for service creation, deployment, provisioning, control, monitoring and billing. It operates with the SCP. The Service Data Point (SDP) is a database that contains information related to the service. The Service Resource Point (SRP) provides resources such as customized and concatenated voice announcements, voice recognition, and Dual-Tone Multi-Frequencies (DTMF) digit collection. This entity was originally called the Intelligent Peripheral (IP), but this name is abolished because of confusion with the Internet Protocol (IP). Communication between these entities is ensured through the Signaling System 7 (SS7) network [10].

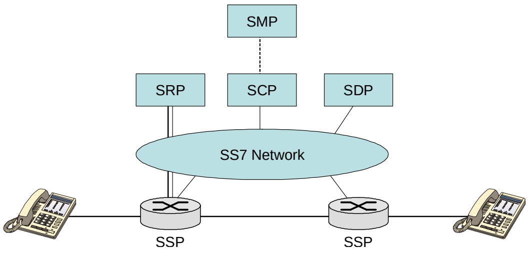

Fig. 1: IN architecture

IN services are composed of service features. Each service has one or more core service features and zero or more optional service features. There are several phases in the development of the IN services, each of which is defined in a Capability Set. The first one, the CS-1, supports so-called *single ended* services and service features. A single ended service feature applies to just one party in a call. It is independent on services of any other party that may be involved it this call. Some examples of CS-1 services are *freephone*, *credit card calling*, *mass calling*, *televoting*, and *VPN*. The CS-1 is followed by CS-2, CS-3, and CS-4, which specifies more sophisticated service and service features.

2.2 Session Initiation Protocol

The Session Initiation Protocol (SIP) [4][5] is an application layer signaling protocol that allows establishment, modification and termination of any kind of multimedia sessions in IP networks. Originally, it was developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Nowadays, a SIP working group continues the development of this protocol.

Basically, there are two types of SIP entities, SIP User Agents (UAs) and network servers. UAs are user terminals and they represent endpoints for a SIP communication. According to their functionalities, SIP network servers can be divided into proxy servers, redirect servers, and registrar servers. The primary functionality of proxy servers is routing of SIP messages. Depending on holding states during a session, proxy servers can be stateless, transaction stateful, or call stateful. Stateless proxy servers do not hold any state, transaction stateful proxies hold states during a transaction such as session initialization, modification or termination, and call stateful proxies hold the state during the whole time a session lasts. Redirect servers are also used for the routing of SIP messages, but unlike proxy servers, they simply redirect incoming messages instead of forwarding them.

An important feature of SIP is supporting user mobility. This means that a user can consume the same service using any terminal at any place. The mechanism that enables user mobility in SIP is the registration mechanism. Each SIP user possesses a globally unique SIP Unified Resource Identifier (URI), which is called *Address-of-Records* (AoR). On the other side, each SIP device obtains its own SIP URI. When using a SIP device, such as UA, a user can be contacted over the SIP URI of this device. This SIP URI is called *contact address*. In order to be reachable over the AoR, a user has to register at a SIP registrar server. The REGISTER request contains both, the AoR and the contact address of the user. The register server stores these binding between user's AoR and one or more contact addresses. This information is used by a redirect or a proxy server to redirect respectively forward the messages to the corresponding user's device. It is even possible to register several times using different priorities for different contact addresses. In this case proxy servers are allowed to fork messages to each of the devices where the user is to be contacted.

A successful session invitation consists of a three-way handshake that begins with an INVITE request. The body of the initial INVITE request carries the offered session parameters encapsulated in the Session Description Protocol [11]. On call acceptance, the terminal of the callee completes the session parameter negotiation sending the session parameters in the body of a 200 OK response. The caller terminal acknowledges the session initiation with an ACK request, the only SIP request that is not followed by a response. Beside the REGISTER, INVITE and ACK request, there exists the BYE request to teardown existing sessions, the CANCEL request to cancel a request and the OPTIONS request to query the capabilities of a server.

3 Architecture

In order to enable SIP networks to use IN services, we propose the architecture shown in Figure 2. The idea is based on using a SIN enabled SIP entity [9] for applying IN services in the IP network. We will call it the SIN entity in the reminder of this paper. A SIN entity is usually a call stateful SIP proxy server that is provided with the IN functionality, which is normally placed in a SSP. Therefore, a SIN entity is able to route SIP messages and to communicate with a SCP over the SS7 network.

Although the SIN entity can assess the IN services from a PS network, there is still a problem with the mapping between SIP URIs and E.164 numbers. As mentioned in the last section, SIP URIs are used to uniquely identify a SIP resource. Furthermore, each SIP user has a unique SIP URI, called Address of Record (AoR), which is independent on the device that this user is currently using. E.164 numbers, on the other side, are used to uniquely identify a PSTN resource, such as traditional phones or fax machines.

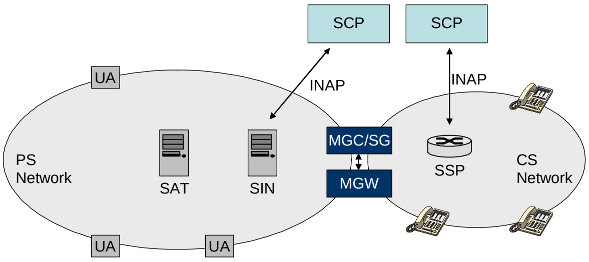

Fig. 2: Proposed architecture

To solve this problem, we have introduced a new entity called SIP Address Translator (SAT), as shown in Figure 2. A SAT entity is a SIP proxy server that performs mapping between commonly used SIP URIs, such as *sip:name@domain*, and E.164 conform SIP URIs, such as *sip:phonenumber@domain*. For example, for a user that has sip:miladinovic@ftw.at as the AoR and phone number 431505283054, there would be the following entry in the mapping table of the SAT entity:

sip:miladinovic@ftw.at	*sip:431505283054@sin.ftw.at*

All SIP requests addressed to a user's AoR are forwarded to the SAT entity first, and it is the responsibility of the SAT entity to forward these requests to the SIN entity. However, the separation between the SAT and SIN entities is only logical, and they can be implemented on a single physical entity.

The introduction of the SAT entity has several advantages:

- The mapping between commonly used SIP URIs and E.164 conform SIP URIs is done transparently for users. This means that a call can be created using the user's AoR regardless if this user is currently using a SIP UA or a PSTN phone.
- Each user can be provided with a SIP URI, even those users that have no UA. Calls for these users will always be routed to the corresponding PSTN phone device.
- Some IN features, such as Private Numbering Plan (PNP), can be realized easily, as we will see in Section 4.

The Media Gateway (MGW) provides conversion of media data between CS and PS networks. The Media Gateway Controller/Signaling Gateway (MGC/SG) is responsible for translation of signaling data between PS and CS networks. Furthermore, MGC/SG performs the control of MGW using a gateway control protocol, such as the Gateway Control Protocol/H.248.1 [12].

There are two important notes to Figure 2. First, for the sake of clarity, SCPs are shown above the PS network and the CS network. In fact, they are placed in the SS7 network that is used for signaling in the CS domain. Second, MGC and SG are shown as one entity (MGC/SG). However, they are two different logical entities and can be placed together in a physical entity, but they need not to be. For this work this is not essential, and hence, we will consider them as a single entity.

4 Virtual Private Network Service Example

This section describes how the *private numbering plan* (PNP) service feature can be realized with the proposed architecture. We have chosen this feature because it is the only core feature of the VPN service, which is a widely used IN service today. It is specified in the IN CS-1 [13]. However, other IN service features, for example *one number* or *reverse charging*, necessary for the *freephone* service, can also be realized with this architecture.

The PNP service feature allows a subscriber to maintain a numbering plan within this subscriber's private network. This numbering plan is separated from the public numbering plan. In this way, an end user can dial a short private number rather than the complete public number in order to contact another user within the same VPN. In the scenario we want to discuss here, we suppose that there are both, traditionally PSTN phones and SIP UA in the same VPN. Users from the PSTN should be able to make calls to other users within the same VPN by dialing a private number, regardless whether the called user resides in the PSTN or in the IP network. Similarly, users from the IP network should be able to place a call, or more generally a multimedia session, to any other user using the AoR of this user. In this work we will use the term *caller* for the calling user and *callee* for the called user.

We can differentiate between for types of calls in a VPN:

- **On-net calls** are calls between two users within the same VPN. With other words, both users are subscribed to the same PNP. The caller dials the short private number of the callee.
- **Off-net calls** are calls when the callee is not within the VPN of the caller. In this case, the caller dials the public number of the callee.
- **Forced on-net calls** are, similar to the on-net calls, calls between two users within the same VPN. However, in this type of call the caller dials the public number of the callee, although they are both members of the same PNP.
- **Virtual on-net calls** allow that the callee physically resides outside the VPN of the caller, but the caller is able to dial a short private number to make a call with the callee.

These call types are relevant only for users that reside in the PSTN, because they sometime have to use the public number and sometimes the private number of the callee. Users in the IP network always use the AoR of the callee in order to make a call, independently which type of call will be made.

Now we will consider scenarios in which we deploy the PNP service feature on a network with both, SIP UAs and traditionally phone terminals, using the architecture introduced in Section 3.

4.1 Registration

The first step is the registration of users that reside in the IP network. As mentioned in Subsection 2.2, a user has to register in order to be reachable over this user's AoR in the SIP network. Figure 3 shows the message flow during the registration.

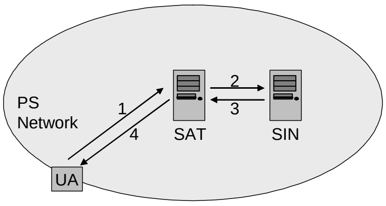

Fig. 3: Registration of a SIP UA

In order to register, a UA sends the REGISTER request to the SAT entity (1). This request contains the AoR of the user and the contact address which depends on the device that this user is currently using. The SAT entity substitutes the user's AoR in the request with the E.164 number conform SIP URI of that user, according to its mapping table. Thereafter, it forwards this request to the SIN entity (2). The SIN entity acts as a SIP registrar server in this scenario and stores this binding between the user's E.164 number conform SIP URI and the user's contact address in a database. After that, the SIN entity replies with a 200 (OK) response (3) to the SAT entity that forwards this response to the user's UA (4).

The registration ensures that all users residing in the IP network are registered at the SIN entity. Those users that are not registered are supposed to reside in the CS network. They will be contacted on the appropriate traditional phone device.

4.2 Originating Call from the PS network

Here we want to show how a call can be placed when the caller resides in the PS network. As stated before, in this case there is no difference for the caller between different call types. In order to place a call, the caller always uses the AoR of the callee. Figure 4 illustrates the message flow in this scenario. Because of clarity, we only show the flow of the initial request. The corresponding response takes the same route but in reverse direction.

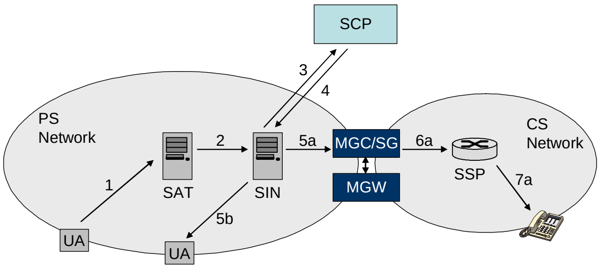

Fig. 4: Originating call from a SIP UA

The caller's UA sends the INVITE request to the SAT entity (1). This request is addressed to the AoR of the callee. The SAT entity substitutes the callee's AoR with the callee's E.164 number conform SIP URI, according to its mapping table (see Section 3). Afterwards, it forwards the request to the SIN entity (2) acting as a proxy server.

The SIN entity queries its registration database using the callee's E.164 number conform SIP URI. If this query is successfully, this means that the callee currently resides in the IP network (see Subsection 4.1). This information is important for step 5. Now, the SIN entity contacts the SCP (3) and gives the SCP the possibility to apply some IN services on this call. The SCP replies with the callee's public phone number (4). If the callee resides in the IP network, this public phone number is ignored and the INVITE requests is forwarded to the callee's contact address obtained from the database (5b). Otherwise, the callee is contacted using the public phone number. The SIN entity forwards the INVITE request to the MGC/SG (5a) that creates a PSTN call using the public number of the callee (6a and 7a).

In this scenario, for the message flow it is not important whether the callee resides in the same VPN as the caller or not. Therefore, there is no difference for signaling between different call types mentioned in Section 4. However, these call types can be charged differently, but it is out of scope of this paper.

4.3 Originating call from the CS network

In this scenario the caller resides in the CS network of the VPN. The callee can reside either in the same VPN or anywhere else. Given that the call originates from the CS network, which means from a traditional phone device, the caller is not able to use callee's AoR, although the callee may reside in the PS network. Therefore, the caller can dial either the short private number or the public number of the callee. In the first case, it is either an on-net or a virtual on-net call, depending whether the callee is a member of the same VPN or not. In the second case, the caller dials the public number of the callee's phone and creates a call with this phone. It is not necessary to apply any IN service on this call. Therefore, we will consider only the first case here.

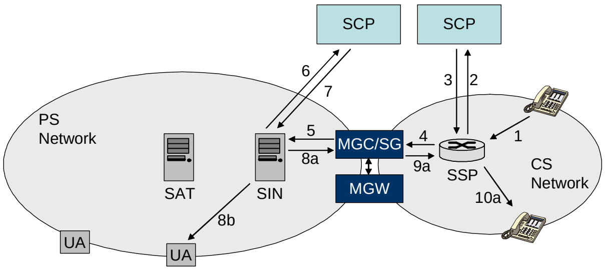

Fig. 5: Originating call from a PSTN phone

Figure 5 shows the message flow in this scenario. The caller dials the short private number of the callee and contacts the corresponding SSP (1). It interacts with the SCP (2, 3) in order to obtain information necessary for routing of the call. The SCP is configured to route this call to the SIN entity over the MGC/SG. Therefore, the SSP contacts the MGC/SG (4) that creates the SIP INVITE request and sends it to the SIN entity (5). This request is addressed to the E.164 number conform SIP URI of the callee. Note that this SIP URI contains the callee's private number and not the public number.

From this point on, the call setup is very similar to the last scenario after step 2. The SIN entity first makes a lookup in its registration database in order to determinate whether the callee is located in the IP network or not. Thereafter, it interacts with the SCP to obtain the callee's public number and to give the SCP the possibility to apply some other IN services for this call. Depending on the network where the callee resides, the SIN entity forwards the INVITE request either using the callee's contact address in the IP network (8b), or using the SIP URI that contains the callee's public number to the MGC/SG (8a). In the second case, the callee is contacted over the CS network on the corresponding traditional phone device (9a and 10a).

Considering this scenario we can notice that each call is routed over the SIN entity, even if the call originates and terminates in the CS network. This is necessary because the SIN entity is the central point which communicates with the SCP. The second SCP, which is contacted by the SSP, only forwards calls from this VPN to the corresponding MGC/SG. All other IN services for this VPN are deployed on the SCP contacted by the SIN entity. This has two main advantages:

- All IN services are deployed only once and can be used from both, PS and CS networks.

- Moving the service contact point into the IP network represents an important step towards all-IP networks. In this phase of migration, it is significant that also some SIP services can be applied on a call that originates, terminates, or both in the CS network. SIP services can be deployed on the SIN entity by means of several ways, including SIP servlets, Call Processing Language (CPL) and SIP Common Gateway Interface (CGI) [14].

However, only the signaling part of the gateway and not the media gateway (MGW) is involved in this scenario when a call originates and terminates in the CS network. Media data are exchanged between the terminals as usual.

4.4 Terminating call

IN services can be applied on the originating side, terminating side, or both. Until now, we have discussed the originating side only. For applying IN services in a VPN realized with the described architecture, there is no need to differentiate between cases when the call terminates in the PS or the CS network. This is because all calls are routed over the SIN entity that applies IN services. Calls that originate in the PS network are routed over the SAT entity and calls that originate in the CS network over the MGC/SG. The SIN entity contacts the SCP with the data of the callee, so that the SCP can apply any IN service for the callee on this call. This does not depend on where the callee currently resides.

When the call originates from the CS network, IN services for the callee can be applied only if the caller dials the callee's private number. Only in this case the call is routed to the MGC/SG. Using the public number, the callee can be contacted directly without applying any IN service.

5 Conclusions

One of the trends in the telecommunications is moving the telephony from the CS network towards the PS network. Given that this migration process will last several years, during this period it will be necessary that CS and PS telephony interworks. In particular, IN services that have already been implemented for the traditional CS telephony are also needed for IP telephony.

In this paper we have proposed an architecture which enables using IN services not only for the PS network telephony, but also for the telephony between CS and PS network. We have introduced a new entity, the SIP Address Translator (SAT), that is responsible for the translation between regular SIP URIs and E.164 number conform SIP URIs. In this way, each user can be contacted using a SIP URI, regardless if this user has a SIP UA or not. Those users that are not registered in the PS network are contacted in the CS network.

The proposed architecture also enables that IP telephony services can be applied for the traditional telephony. This architecture can be applied even when the CS network totally disappears and therefore, it is also suitable for enabling IN services in all-IP networks.

6 Literature

[1] Magedanz, T., Popescu-Zeletin, R.: Intelligent Networks. International Thomson Computer Press, 1996

[2] Sharp, C.D., Clegg, K.: Advanced intelligent networks: now a reality. IEEE Electronics & Communication Engineering Journal, Vol. 6, No. 3, June 1994, pp. 153 – 162

[3] Lennox, J., Schulzrinne, H., La Porta, T.F.: Implementing Intelligent Network Services with the Session Initiation Protocol. Tech-Report Number CUCS-002-99, 1999

[4] Rosenberg, J., et al.: SIP: Session Initiation Protocol. IETF RFC 3261, 2002

[5] Schulzrinne, H., Rosenberg, J.: The Session Initiation Protocol: Internet-Centric Signaling. IEEE Communications Magazine, Vol. 38, No. 10, 2000, pp. 134 – 141

[6] 3GPP TSG SSA: IP Multimedia Subsystem (IMS) - Stage 2. Tech-Report Number TS 23.228, 2003

[7] Rotchel, A. and Evloguieva, E.: IN (Intelligent Network) protocol extension to SIP (Session Initiation Protocol) Study and Prototype. 8th International symposium on services and local access, 2000

[8] El Ouahidi, B., Bouhdadi, M., Bourget, D.: Extending the Internet with the intelligent network capabilities. 1st European Conference on Universal Multiservice Networks, 2000, pp. 80 – 86

[9] Gurbani,V.K., Haerens, F., Rastogi, V.: Interworking SIP and Intelligent Network (IN) Applications. IETF Internet Draft, 2002, work in progress

[10] Modarressi, A.R., Skoog, R.A.: An overview of Signaling System No.7. Proceedings of the IEEE, Vol. 80, No. 4, April 1992, pp 590 -606

[11] Handley, M., Jacobson, V.: SDP: Session Description Protocol. IETF RFC 2327, 1998

[12] Groves, C., Pantaleo, M., Anderson, T., Taylor, T.: Gateway Control Protocol Version 1. IETF RFC 3525, 2003

[13] ITU-T: Introduction to Intelligent Network Capability Set 1. ITU-T Recommendation number: Q.1211, 1993

[14] Glasmann, J., Kellerer, W., Muller, H.: Service development and deployment in H.323 and SIP. Sixth IEEE Symposium on Computers and Communications, 2001, pp. 378 - 385