Author(s): Licciardi, Carlo Alberto; Falcarin, Paolo.
Title: Next Generation Networks: the service offering standpoint
Year of publication: 2003
Citation: Licciardi, C.A., Falcarin, P. (2003) 'Next Generation Networks: the service offering standpoint', *IEC Comprehensive Report on IP applications and services*, International Engineering Consortium (IEC), pp. 87-101
Publisher link: http://www.iec.org

Next Generation Networks: The Service Offering Standpoint

Carlo Alberto Licciardi
Carlo.Licciardi@tilab.com
Project Manager
Telecom Italia Lab
Network Intelligence Dept.
Via R. Romoli, 274
I-10148 Torino, Italy

Paolo Falcarin
paolo.falcarin@polito.it
Politecnico di Torino
Control and Computer Engineering Dept.
Corso Duca degli Abruzzi, 24
I-10129 Torino, Italy

Abstract

Next Generation Networks [1] was the buzzword over the last years. Different people imagine different things when they think of NGN. How can this concept be defined? NGN is the application of Internet, IP and IT solutions to Telecom Services, including (but not only) the integration and sometimes the substitution of circuit switching with packet switching either for trunking or for access.

Surprisingly, usually people think of a mere porting of Telecom protocols over an IP network (read H.323 protocol). Why should we reuse existing telecom solutions over an IP transport? The usual answer is to reduce cost of ownership. Is that really true? Is that a reason enough? Indeed, the introduction of NGN opens a huge opportunity for incumbent telecom operators: enabling the renewal in the service offering (meaning cash!)

In this paper, we present results of the Eurescom Project P1109"Next Generation Networks: the service offering Standpoint" [1]. The overall goal is to evaluate solutions for NGNs from a service-offering standpoint and understanding the wider effects of introducing NGNs both in a fixed and 3G mobile network infrastructure, in terms of the inter-operability and functionality of next generation network products. In particular this paper focuses on the implementation of service scenarios (i.e. call center, VPN) on top of NGN platforms. The implementation of the service scenarios is meant to measure the attitude of NGN service platforms to provide new services in a developer friendly way.

1. Introduction

Some basic questions need to be answered when we talk about Next Generation Networks: Why NGNs? Are NGNs programmable? Do NGNs solve the problems of IN? Which NGN solutions? Are NGN interoperable? Are NGNs cost effective? Are NGNs service developed? Is Application Server just a new SCP? Is Voice over IP a value per se?

Finally: are NGN profitable for Network Operators.

Indeed, the introduction of NGN opens a huge opportunity for incumbent telecom operators: enabling the renewal in the service offering (meaning cash!)

In this perspective, NGNs should enable the provisioning of new classes of services:

- any-to-any ubiquitous communication services including unified messaging
- customer-centered/highly personalized services
- mixed voice/data services
- e-call services (web initiated call set-up)
- integrated voice and data VPN
- advanced network call center
- audio video conferencing
- IP multimedia services

A common feature for all these services, is the seamless service access, i.e. users can use their own services, no matter where they are, which terminals they are using, which access network they are attached to. These new classes of services have to be deployable in several network environments: fixed (PSTN, ISDN, xDSL), mobile (GPRS, 3G-UMTS) and Internet.

In this paper, we present the objectives and results of the Eurescom Project P1109 "NGN: the service offering standpoint" [1]. The overall goal is to evaluate solutions for NGNs in terms of functionality, programmability, openness, and of inter-operability among next generation network products. In particular this paper focuses on the implementation of service scenarios (i.e. call center, VPN) on top of NGN platforms.

Section 2 describes the overall reference architecture; sections 3 describes advanced VPN and call center service scenarios which have been implemented on top of the identified architecture; section 4 describes how the overall architecture is applicable to a UMTS environment providing also an example.

2. Architectural framework

This section gives a brief overview on the reference architecture we used in the project, which is depicted in Figure 1.

Application Creation Environment supports the life cycle of a service or an application, which is composed of a series of phases where each phase requires certain activities to be performed, (i.e.: analysis and conception, application creation, acceptance testing, application deployment, application provisioning and operations, application removal).

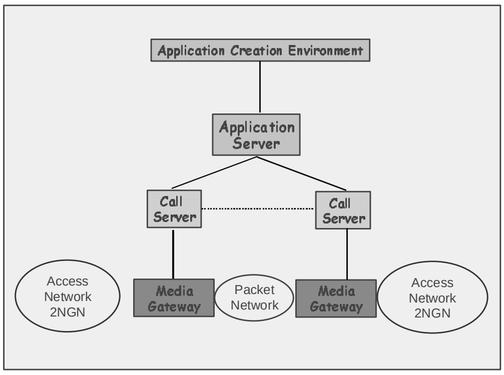

Figure 1. Reference Architecture

In a next generation network context, the concept of **Application Server (AS)** is an evolution of Web-based application servers, which are targeted to service execution and to controlling Call Servers and Special Resources. Application Servers should broaden the role of IN-SCF to cover new network/service scenarios on top of IT platforms. The main functionality that an AS should support are: Service Logic Execution Environment (SLEE), service life-cycle management, support for developing services/policies by means of APIs or scripting language, system and service management, registration mechanisms support.

Call Server mainly provides call control functionality (call routing, call signaling process – SIP [8], H.323, SS7, H.248 – including signaling gateway capability, third party call setup, static/dynamic trigger activation/deactivation, static/dynamic event subscription activation/deactivation, QoS control) according to a given call model. It must provide also an interface (i.e., standard protocol or open API) towards Application Servers to enable service and policy control. Call Agents, Softswitches, Media Gateway Controllers are some of the most common names for Call Servers.

Media Gateway (MG) functions provide conversion between circuit-switched resources (line, trunks) and the packet network (IP, ATM).

Access Network to NGN in Figure 1 represents the different ways to access the services offered by an NGN platform (i.e. PSTN, ISDN, xDSL, PLMN, …) while packet network stands for IP/ATM backbone. Services can be also accessed by UMTS access networks: both Circuit Switched Network and Packet Network.

In our implementation of the architecture the Session Initiation protocol (SIP) has been used as the signaling protocol between terminal and network elements (call server and media gateways) and among network elements. SIP, the Session Initiation Protocol (SIP) [10], is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. SIP mainly addresses the call setup and tear down mechanisms and is independent of the transmission of media streams between caller and callee. SIP is being standardized by IETF and it is emerging within several standardization bodies as the enabling technology to provide the signaling support on Next-Generation Networks. In particular the 3GPP (Third Generation Partnership Project) is producing globally applicable Technical Specifications and Technical Reports for a third generation mobile system. The group is using IP technology end-to-end to deliver multimedia content to mobile handsets. The call control and signaling function will be fulfilled by SIP. 3G is dedicated to using SIP for call control both from terminal to network and between network call nodes. In other words all IP multimedia call signaling will be performed via SIP.

3. Service Scenarios

Let's consider the following example, which cover quite a wide area of service scenarios. Think of a small/medium enterprise with small branches with few employees spread around several locations. It's likely that each branch has Internet connectivity through ADSL access; some users could access the Internet directly from UMTS terminals.

One need customers have, is to place calls within the enterprise (university). Why don't we offer them an IP centrex service (by using VoIP)? Once we provide that, our customers would like to place and receive also off-net calls (to/from PSTN).

Different users (professors, students, secretary, …) would be entitled to place different calls on the basis of their roles in the company or group memberships. For instance, the secretary may receive incoming calls from both the PSTN/PLMN and the IP network; the Director may be enabled to place any kind of calls, or in addition when (s)he goes home, (s)he can transparently receive calls there.

Figure 2 describes an instantiation of the general architecture described in section 2 for the service example described above. The layers here depicted expand the functionality of Figure 1. Servers here reported are described along with detailed case studies descriptions.

In the following sections we address two case studies (scenarios) which we implemented and which challenge NGN service platform. The former describes a VPN service on top of hybrid networks, while the latter describes a distributed call center scenario instantiated in a Campus environment (mainly focusing on personalization features). The service scenarios described in the following sections emphasize the importance of a personalized user profile where users-based/groups-based customizable policies are stored.

Both of them are described in terms of user perspective and service features. An example is also provided in order to show more in detail how the service works.

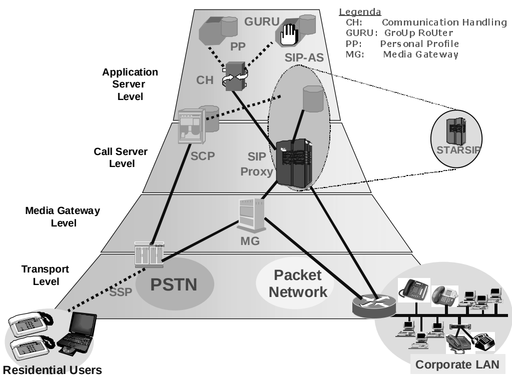

Figure 2. Architecture for services

3.1. Case study 1: hybrid VPN service

This section describes an Advanced VPN POTS and IP for SOHO enriched by features of virtual presence [2], such as closed user groups management, roles management, incoming and outgoing call screening, etc.

3.1.1. User Perspective

Let's consider different users having different roles within the enterprise. They are summarized within the following table:

User	Role	Site	Enabled Calls
John	Director	London	any (also when outside)
Susan	Secretary	London	within VPN, from PSTN/IP
Mark	Employee	South-ampton	within VPN, from IP
Paul	Guest	London	No calls

The enterprise has two sites: the main site, located in the center of London, and one little branch, located in Southampton.

John is a VPN-user using as terminals his PC, a SIP phone and a UMTS terminal. According to his profile he can:

- place and receive calls from the IP side when he is inside the enterprise (abbreviating dialing is used);

- place and receive calls towards the PSTN when he is within the enterprise. John is allowed to place also off-net calls;

- place calls as a VPN-user, when he is at home or in any other place. If his house-line is VPN-enabled he can also use abbreviated dialing otherwise he has to dial an IN-number to access the VPN and be identified as a VPN-user;

- receive calls, as a VPN-user, when he is at home or in any other place; it's up to the server to find when John is located.

Susan is a VPN-user using her PC and common telephone. She can place and receive calls from both the PSTN and the IP side when she is within the enterprise. No other calls are allowed when she is out of office.

Mark is a VPN-user using as terminals a PC and a SIP-phone. He can place calls within the VPN only. It means that he can reach any VPN-user (even if the last one is outside) but outgoing call screening feature (next section) doesn't enable him to dial public PSTN numbers.

Paul is a company guest. Since he is not a VPN-user, no outgoing calls are allowed.

At last all VPN-users (i.e. John, Susan and Mark) are entitled to customize their own policies for incoming call screening. On the contrary, Paul is only entitled to receive incoming calls upon valid registration, and he cannot change his profile information.

It's worth to remark that employees of the enterprise working in London and employees working in Southampton can communicate between them (through the VPN service features) without taking care of the site where they are physically located.

3.1.2. Service Features

In the following the main features of the enhanced VPN service scenario are described. Policies are based on either users' role or their belonging group.

- ➢ ***Abbreviated Dialing.*** Allows VPN-users to dial a short number to localize another VPN-user.
- ➢ ***Outgoing call screening.*** Call filtering applied to calls placed by VPN-users.
- ➢ ***Incoming call screening.*** Call Filtering applied to calls received by VPN-users.

- ➢ ***On-Net Calls.*** The called user is a member of the VPN: the "dialed number" could be a logical name/number. Different sub scenarios arise from different originating and terminating terminal type (IP or usual phones). Registration scenarios are taken into consideration for all of them.
- ❑ a VPN user A, registered on an IP terminal, calls another VPN user B. The logic verifies that B is registered on an IP terminal: in that case the call is a VoIP call. User A calls user B with a logic number/name that will be translated to the actual IP address of the terminal where user B is registered.
- ❑ a VPN user A, registered on an IP terminal, calls another VPN user B registered on a PSTN phone. The logic translates the logic number/name used by user A to call user B and detects that B is registered on a PSTN phone. The logic performs checks in order to verify if user A is authorized to call user B or a PSTN phone and to verify how B wants to deal with incoming calls from A (e.g., route them to an IP phone). The logic routes the call to the PSTN through a vocal gateway and monitors its termination, e.g., in order to provide accounting support.
- ❑ a VPN user A, registered on a PSTN phone, calls a VPN user B registered on an IP terminal. The phone line is characterized as a VPN line. User A dials a code and the VPN number that identifies user B. The logic, triggered by IN components, routes the call to the IP network, through a vocal gateway, and monitors its termination, in order to provide accounting support. The logic could perform checks on user A's rules for outgoing calls and user B's rules for incoming calls (e.g., conditional routing).
- ➢ ***Off-Net Calls.*** The called user is not a member of the VPN: "the dialed number" is a PSTN number prefixed with a specific code (e.g., "0"). Registration scenarios are not considered in this context.
- ❑ A VPN user A, registered on an IP terminal, calls a user B external to the VPN, by dialing a PSTN number. The logic detects if user A is authorized to perform external PSTN calls (different call classes could be defined: international calls, domestic call, urban calls, etc.). In case of authorized call, the logic routes the call to the PSTN through a vocal gateway and monitors its termination e.g., in order to provide accounting support.

Advanced features based on the integration of voice and data communication capabilities could also be considered like integration with presence, invitations to application sessions (e.g., joint editing), directory services (e.g., personal address books, click-to-dial) and push services.

3.1.3. Call flow among components

Figure 3 describes the call flow for an On-Net call originated by a PSTN phone. John is a VPN user working at the main site, in London.

This morning John decided to work at home, whose PSTN line is characterized as belonging to the VPN of the enterprise (any call is triggered by SSP and an IN query is sent to SCP). Susan is also a VPN user and she is in her office.

Figure 3 is an instantiation of the architecture represented in Figure 2 for the VPN service scenario. It shows how SIP technology can be used for interworking between IP and the traditional IN architecture. The key element in the architecture is a programmable SIP AS, which behaves also as a SIP Proxy server. SSP and SCP are the usual network elements of IN systems; on top of the SCP box a SIP-UA (User Agent) appears, it enables SCP to interact with the SIP Proxy/AS. SIP-UA has been implemented on a commercial SCP by using the proprietary development environment. The SIP signaling (between SCP and SIP AS) is carried over a TCP-IP connection by using sockets. A SIP-MG "bridges" the PSTN and the Packet Network at transport level and it talk to SIP Proxy/AS to route calls. In this case signaling is carried over UDP.

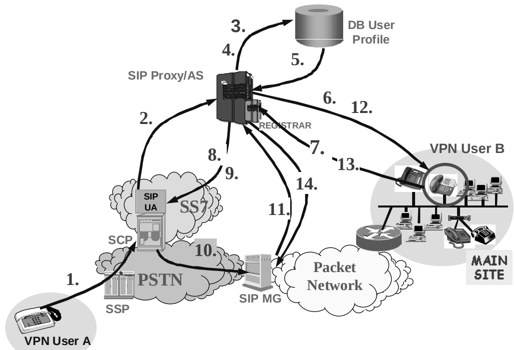

Figure 3. On-net call originated by PSTN terminal

1. John dials Susan's number; SSP contacts the SCP that "knows" how to deal with the call;
2. the SIP-UA (over the SCP) sends a *REFER (from: CLI, to: dialed number)* to the SIP Proxy/AS (to ask the SIP Proxy/AS to send an *INVITE*);
3. the SIP Proxy/AS verify both John's OCS (to check if John is allowed to place this

call) and Susan's TCS (to verify how Susan wishes to deal with the call);

4. the SIP Proxy/AS "translates" the called number;
5. the associated PC's IP-address is returned and the SIP Proxy/AS starts to monitor the call;
6. the SIP Proxy/AS makes an *INVITE [HOLD]* to Susan's PC (this step sets up the session at signaling level but communication is "suspended");
7. Susan accepts the call and her PC sends to the SIP Proxy/AS an *OK* answer; the SIP Proxy/AS replies with an ACK;
8. the SIP Proxy/AS sends *OK* to the SCP (in response to the *REFER* (see step 2.));
9. the SIP Proxy/AS sends *NOTIFY[OK]* to the SCP to inform it about the invitation result;
10. SCP selects a MG and instructs the SSP both to route the call (*CONNECT)* to it and to apply the appropriate charging plan; the SSP routes the call to the selected MG;
11. the SIP-UA upon the MG sends an *INVITE (from: CLI, to: IP address of Susan's PC)* (with the appropriate SDP) to the SIP Proxy/AS (which must work as a back-to-back UA mode); the SIP Proxy/AS identifies the call in hold status and retrieves the relevant information;
12. the SIP Proxy/AS makes a REINVITE to the Susan's PC client, by forwarding it the MG SDP;
13. Susan's PC client modifies the call parameters with the SDP information and sends an *OK* answer to the SIP Proxy/AS;
14. the SIP Proxy/AS sends back both an ACK to the Susan's PC client and the answer with the information related to the PC to the SIP-MG; the SIP-MG sends an ACK to the SIP Proxy/AS;

At this point the MG starts the RTP streaming with the Susan's PC according to the received SDP. John and Susan can talk.

The MSC below (Figure 4) is an example of a possible SIP-based implementation of the scenario for the call activation. Only the SIP-based entities are represented, namely the SCP-UA, the SIP-MG, the SIP-Proxy/AS and the client's PC (i.e. Susan's PC in the above example).

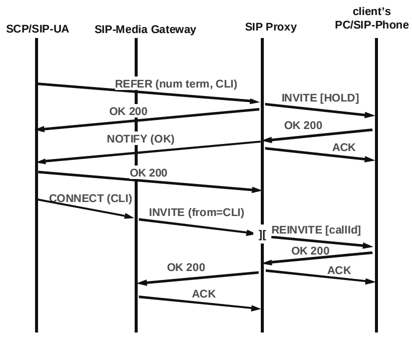

Figure 4. Call Set-up, via SCP, SIP Proxy/AS and SIP-MG

3.2. Case study 2: Campus call center

This scenario models the structure of a university campus, in which people are organized in *virtual groups* according to academic and research involvement. Hence, hierarchies of groups have members among university personnel or enrolled students.

In this scenario, both anonymous and subscribed users can communicate in the campus, through available campus terminals or personal devices, with people within the virtual campus.

3.2.1. User perspective

Entities within a University environment are suitable to be easily modelized as a group hierarchy (i.e. a tree structure). As an example, let's think to a Department, composed of Research Workgroups, whose members may be Professors, Researchers, Group-Leaders and Administrative Employees.

Both Campus and anonymous users can place calls. The call screening feature is just applied to the called user (TCS feature).

The following table is an example of assignment of Campus users to groups and roles.

User/Member	Group	Role
Paul	Network	Professor
Diana	Network	Researcher
Patrick	Robotics	Professor
Jerry/anonymous	No one	No one

Jerry wants to communicate with a Professor belonging to the Network group. To find out the address of the person/department he wants to call, he has just to browse the university Web site:

- if Jerry uses a phone he has to dial a personal number (that identifies a particular role within a group in the Campus);

- if Jerry uses a client application on his PC, he has to call any Professor that belongs to the Network group.

Jerry wants to communicate with Paul:

- if Jerry uses a PC, he has to send an invitation to Paul.

In particular, each group has its own *Administrator* that is a special user. He has to define the group and roles, ha has to set policies for group and for roles, and to assign roles within the group to individual users.

Paul, Patrick and Diana, belonging to the Campus, have to decide and set their own policies for incoming call screening (TCS).

3.2.2. Service features

The University structure can be modelized by a tree composed of groups (as root), subgroups (as intermediate nodes) and roles and members (as leaves).

Service features, from the view of the group administrator, can be summarized like this:

- ***Group Management.*** *T*he ability to:
  - create and remove new groups
  - add and remove roles to/from a group
  - add and remove users to/from a group
  - set policies for incoming calls to a group
- ***Role Management.*** The ability to:
  - create and remove new roles
  - set which members cover a role
  - set policies for incoming calls to a role
- ***User Management.*** The ability to associate a user/member to a role within a group.
- ***Incoming Call Screening.*** The ability to define their policies in order to be reached according to events (i.e. busy) and conditions (time, caller identity, etc). In other words to perform Call Filtering.

3.2.3. Call flow among components

Figure 5 depicts the call flow for the following scenario: Jerry (a normal user) at 4pm decides to communicate with a Professor of the Network group in the Campus. Jerry uses a SIP client application on a PC connected over Internet. Paul, who is a professor in network group, has previously set as his policy to be contacted on his SIP-phone between 8am and 8pm and on his mobile phone conversely.

Several AS are depicted, in addition to the ones in Figure 3.

The GURU server (GroUp RoUter profile manager) hosts group profiles of the service subscribers, including their policies used to resolve communication requests for role and groups. The Personal Profile (PP) is used to store personal member policies to redirect incoming calls toward his actual terminal address (IP or phone).

Communication Handling (CH) is the component that sets up calls between different call servers and resolve personal and group addresses querying in sequence the GURU and PP servers.

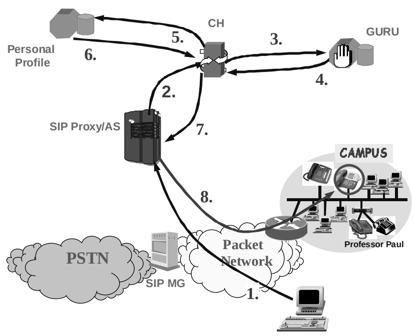

Figure 5. Call for group member originated by PC

When the application servers return an address, the SIP Proxy sends the invitation to the appropriate terminal (or Gateway).

1. It 4 p.m. Jerry invites a professor within the Network group; his SIP client application sends an *INVITE (to: <u>Professor@Network</u>, REQUEST-URI =Professor@Network)* to the SIP proxy server;
2. The invitation is forwarded to the CH component
3. CH asks the GURU server, through the message *communication_evt(<u>Professor@Network</u>, Jerry, <u>Jerry@acme.com</u>)* for the current policies used for the Role “Professor” in the group “Network”;
4. GURU returns a list of members currently covering that role. In case of multiple Professors in the same group, all their policies are checked; the first professor that matches the request will be invited. This is not the case since just Paul fulfils;
5. CH asks to the PP the current location of Paul as a member through *communication_evt(synch, Paul, Jerry , Jerry’s IP address)*
6. PP checks Paul’s personal policies and, if they confirm Paul’s availability, it returns the current terminal address of the requested user (in this case Paul’s SIP Phone);
7. CH asks the SIP proxy server to connect to the desired target address;
8. SIP proxy server sends an *INVITE (to:Professor@Network, REQUEST-URI =Paul@SIP-Phone-IPaddress)*

The following MSC (Figure 6) describes the call set-up in the campus call center scenario. The entities represented are the caller SIP client, the SIP proxy server, the application servers (CH, GURU, PP) and the SIP-phone of the called group member.

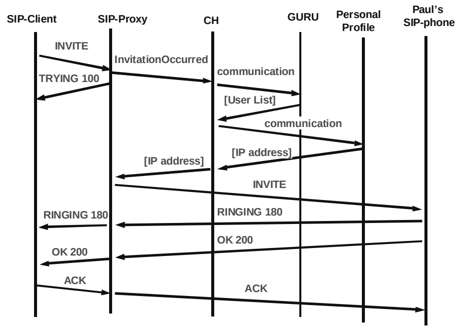

Figure 6. Setup for Group Member, via SIP Proxy/AS

4. NGN Architecture versus UMTS

This section describes how the overall architecture depicted in Figure 2 can be applicable in a UMTS environment. Figure 7 represents the most relevant components, which are envisaged for the provisioning of value added IP multimedia services on UMTS infrastructure.

IP multimedia services are not the evolution of the circuit switched services but represent a new category of services, mobile terminals, services capabilities, and user expectations. Voice communications (IP telephony), Advanced VPN & Call Center are examples of real-time service that could be provided as an IP multimedia application. According to UMTS standards [13], IP Multimedia Core Network Subsystem (IM CN SS) includes a session control function based on SIP coherently with the previously depicted architecture. All scenarios will be supported independently of the access network of the call party (PLMN, Mobile Circuit switched/Packet, PSTN or ADSL).

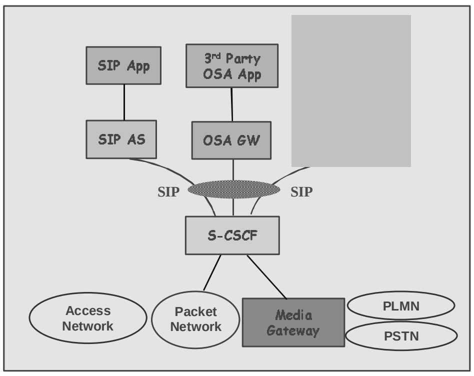

Figure 7. UMTS onto Reference Architecture

IM CN SS comprises all network elements for provision of multimedia services (including signalling and bearer related network elements). The IM CN will enable convergence of, and access to, voice, video, messaging and web based technology for wireless users.

Call State Control Function[1] (CSCF) handles the following functionalities: Incoming call gateway, Call/Session Control Function (CSCF acts as a call server), Serving Profile Database, Address Handling. It can also act as a SIP Proxy server (stateless or stateful). The supported functionality match correctly the ones identified in sec. 2.

The SIP Application Server may host and execute services. It handles SIP Sessions on behalf of the services and it uses SIP+ (SIP+ is based on the SIP protocol information with necessary profiling and enhancements to allow for service control) to communicate with the S-CSCF. Sometimes, it can act as a SIP User Agent.

OSA Gateway offers OSA/Parlay interfaces to 3rd Party OSA application. It supports both Framework and Service Capability Server interfaces. It interacts with CSCF by means of SIP interface.

The purpose of the IP Multimedia Service Switching Function (IM-SSF) is to translate SIP protocol to CAP and to hold the needed functions to do that. This allows the reuse of service logic developed on Camel Service Environment (CSE).

It worthwhile highlighting how SIP will be used in the 3G mobile environment: All IP multimedia call signalling will be performed via SIP. Users will be identified by SIP URLs and/or E.164 numbers, the numbering system of the telephone system. The bearer system (GPRS or mobile IP) will manage micro-mobility (the movement of the mobile user from one base station to another). Macro-mobility, the movement of the mobile user from one domain to another, will be handled by SIP. SIP will route signalling so that services are available from the originating or terminating network. Call State Control Function (CSCF) is the equivalent of a SIP server. There will be three different kinds of CSCF:

Proxy CSCF - this is the first point of contact in a visited network and will find the user's home network and provide some translation, security and authorization functions

Serving CSCF - controls sessions, acts as registrar and triggers and executes services. The serving CSCF will access the user's profile. It can be located in the home or visited network

---

[1] According to 3GPP specifications, CSCF may play different roles, namely Proxy-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) and Serving-CSCF (S-CSCF). Only when it plays the role of S-CSCF, it interacts with the Application Server level.

Interrogating CSCF - the first point of contact in the home network. It assigns the serving CSCF, contacts the HSS and forwards SIP requests.

4.1. An example

Let's consider the case study in section 3.1in a UMTS environment. Suppose that John wants to call his son Michael (at home) to ask him to have dinner together this evening. John is at a meeting and he has just his UMTS phone only with him.

The steps for the call set-up are:

1. John sends an invitation to Michael. A SIP *INVITE* is sent to the S-CSCF. The originating endpoint determines the complete set of codecs that it is capable of supporting for this session. It builds an SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow.
2. The S-CSCF performs an analysis of the destination address and determines, with support of the SIP AS, that the session is destined to the PSTN; the service logic performs checks in order to verify if John is authorized to call a PSTN number and to verify how Michael wants to deal with incoming calls from John (e.g., route them to an IP phone). The SDP contains a restricted set of codecs allowed by the network operator.
3. The SIP AS, together with the SIP Application, translates the destination address into the phone number of Michael and sends it to the S-CSCF;
4. The invitation is forwarded to the Media Gateway, which answer with the SIP message *100 Trying*(forwarded to the originating endpoint);
5. Then, the Media Gateway sends the SIP message *183 Session Progress*, which contains the media stream capabilities of the destination to be returned along the signalling path. Resources necessary for this session are authorised by S-CFCF .
6. After receiving the SIP message *183 Session Progress*, the originating endpoint sends to the S-CFCF a SIP message *PRACK* that contains the negotiated resources; this message is forwarded to the Media Gateway;
7. The Media Gateway confirms through a SIP message *OK 200*; the S-CSCF, after completing the resource reservation procedures forwards this message to the UMTS terminal.
8. The originating endpoint sends the SIP message *COMIT* to the S-CSCF that forwards it to the Media Gateway. This message "notifies" the success of the resource reservation process.
9. The Media Gateway sends a setup message to the called party; the ISDN phone of the called party answers with a progress message;
10. The Media Gateway sends backs a *ringing* message (*OK 180*) to the S-CSCF; S-CSCF forwards it to the UMTS terminal;
11. Michael off-hooks!
12. An ISDN message *CONNECT* is sent to the Media Gateway, which sends a SIP message *OK 200* to the S-CSCF. It is forwarded to the UMTS terminal.
13. John's terminal sends to the Media Gateway (via the S-CSCF) a SIP message *ACK* to confirm the receipt of *OK 200* result; the RTP flows;
14. John: "Hello Michael! How are you? I would like to have dinner with you this evening …".

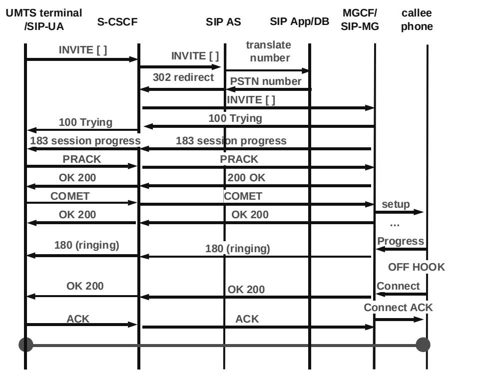

Figure 8. UMTS-terminal to PSTN-phone: call setup

Note that the presented scenario has been simplified from the UMTS architecture perspective, where, for example, if the destination is a PSTN number, the S-CSCF forwards the request to a local Breakout Gateway Control Function (BGCF), which selects a suitable MGCF in the network. Interactions represented in this section and in particular in don't depict these details.

5. Conclusions

The paper highlights benefits for network operators in adoption of NGN with respect to existing solutions. It has shown how Next Generation Service platforms can provide advanced services and which benefits come from using SIP protocol and programmable SIP AS in terms of easy-to-use, flexibility and programmability.

Besides the paper demonstrate how to reuse and take advantage of existing legacy systems (IN) and services (VPN). It has proved the benefits of implementing a SIP UA in the SCP to allow inteworking of IN with external IP server (see SIP proxy and AS). SIP can be considered a suitable protocol for development of services over hybrid networks.

The paper has also shown how the reference architecture and the use of SIP protocol are suitable for the deployment of advanced multimedia communication services in a UMTS environment.

In conclusion, NGN service platform ease the provisioning of advanced services, which span over heterogeneous network (packet, circuit, fixed and mobile). Our analysis demonstrated that NGN must be seen by incumbent network operators as revenue generators (new services) more than as cost saving equipment. Interoperability among product from different vendors is still an issue mainly for two reasons: proliferation of optional features in standards (SIP, JAIN, …) and vendor specific implementations of them.

Acknowledgements

The information presented in this paper is based on the work done in the EURESCOM project P1109 "Next Generation Networks: the service offering standpoint" [1]. The authors would like to thank all EURESCOM P1109 participants.

Acronyms

ADSL	Asymmetric Digital Subscriber Line
AS	Application Server
ATM	Asynchronous Transfer Mode
CAMEL	Customised Application Mobile Enhanced Logic
CAP	CAMEL Application Part
CH	Communication Handling
CLI	Calling Line Identifier
CSE	Camel Service Environment
CSFC	Call State Control Function
GPRS	General Packet Radio Service
GURU	GroUp RoUter Profile Manager
IM-SSF	IP Multimedia Service Switching Function
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Service Digital Network
MG	Media Gateway
MGCF	Media Gateway Control Function
MSC	Message Sequence Chart
NGN	Next Generation Network
OCS	Originating Call Screening
OSA	Open Service Architecture
PP	Personal Profile
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real Time Protocol
S-CSCF	Serving- CSFC
SCP	Switching Control Point
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SSP	Service Switching Point
SCP	Service Control Point
TCS	Terminating Call Screening
UA	User Agent
UMTS	Universal Mobile TLC System
VoIP	Voice Over IP
VPN	Virtual Private Network
xDSL	x Digital Subscriber Line

References

[1] Eurescom Project P1109 *Next Generation Networks: The services offering standpoint.* On-line at http://www.eurescom.de/secure/projects/P1100-series/P1109/P1109.htm

[2] P. Lago, C.A. Licciardi, G. Canal, A. Andreetto, *An architecture for IN-Internet hybrid services*. In Computer Networks Journal, Special Issue on Intelligent Networks and Internet Convergence, T. Magedanz, H. Rudin, I. Akyildiz (Eds.), Elsevier, Vol. 35(5), April 2001, pp. 537-549

[3] M. Barry et al., *What an IN system should be*, EURESCOM P909 Deliverable1, http://www.eurescom.de/Public/Publications/Projectresults/P909-series/909d1.htm, October 1999.

[4] H. Schulzrinne, J. Rosenberg, *The IETF Internet Telephony Architecture and Protocols*, IEEE Network, May/June 1999.

[5] A. Andreetto, G. Canal, P. Lago, C. A. Licciardi, *Ubiquitous communication over IN and Internet*, In Proccedings of the 6th ITU International Conference on Intelligence in Networks (ICIN '2000), Bordeaux, France, pages 35-40, January 2000.

[6] V. Blavette et al., *Architecture and service scenarios for Internet-IN convergence*, EURESCOM P909 Deliverable 2, http://www.eurescom.de/public/projectresults/P900-series/909d2.htm , March 2000.

[7] Cuda A., Canal G., *From a proxy to "the" Next Gen Network Element*, Proceedings SIP2001 conference.

[8] Rosemberg J., *Architecting SIP Networks for ITSPs*, Proceedings SIP2001 conference.

[9] Canal G., Cuda A., Lago P., *IN-like Services Enabled by Open SIP System*, Proceedings SIP2000 conference

[10] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg *SIP: Session Initiation Protocol*, RFC 2543, March 1999.

[11] Laetitia Boetselaars et al., CD-ROM: *Enabling technologies for IN - Internet integration*, EURESCOM P909 Deliverable 4, January 2001.

[12] 3GPP TS 23.002 v.5.3.0: *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;*

Network Architecture (Release 5),June 2001.

[13] 3GPP TS 23.228 v.5.0.0: *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP multimedia subsystem; Stage 2 (Release 5)*, June 2001.

[14] 3GPP TS 24.228 V1.0.0: *3rd Generation Partnership Project; Technical Group Core Network;Signalling flows for the IP multimedia callcontrol based on SIP and SDP (Release 5)*, June 2001.