NICC ND 1620 v1.2.2 (2008-08)

NICC Document

NGN; Voice Line Control Service; Interconnect Architecture

Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London,
SE1 9HA.

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London SE1 9HA.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC.

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC

Introduction

This specification forms part of the Next Generation Network, Multi-Service Interconnect (MSI) Release Structure and ought to be read in conjunction with the associated releases of the standard ‘Multi-Service Interconnect of UK Next Generation Networks’ [1].

1 Scope

This specification defines the interconnect architecture for the Voice Line Control (VLC) service between UK NGNs using IP technology. This service supports the logical extension of analogue line access so that the NGN Call Control in one network has the ability to provide PSTN or other types of voice service via base-band lines in a separate NGN.

This specification defines the service architecture and how it is supported by the MSI Common Transport Specification [2] that supports logical network layer point-to-point connectivity with dedicated bandwidth as the transport between communications providers (CPs). The ongoing work in other standards areas on routed network interconnect is recognised but considered to be insufficiently mature to adopt. However, where possible, options that facilitate the transition to this type of architecture have been followed. This document does not cover the facilities to support a transport function that utilises an IP routed, multi-point, interconnect network.

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ND1610 Next Generation Networks, Release Definition

[2] ND1611 Multi-Service Interconnect Common Transport for UK NGNs

[3] ND1615 Management of the Voice Line Control Service for UK NGNs

[4] ND1621 Generic overload control for use in Interconnect of NGN's

[5] ND1628 NGN Interconnect: Security

[6] ND1633 NA Baseline Document

[7] ND1635 NGN Interconnect: Media Path Technical Specification for PSTN/ISDN Type Service

[8] ND1636 IP Address Allocation

[9] ND1012 Interconnect Stream Control Transmission Protocol (SCTP) and Adaptation Layers

[10] ND1018 TCP Specification

[11] ND1019 Endorsement of TISPAN SIP and SDP

[12] ND1021 Voice Line Control for UK Interconnect using TISPAN IMS-based PSTN/ISDN Emulation: Session Initiation Protocol (SIP) and Session Description Protocol (SDP)

[13] ND1701 Recommended Standard for the UK National Transmission Plan

[14] ETSI TS 181 005 V1.1.1 2006-03 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capabilities Requirements

[15] ETSI ES 282 002 V1.1.1 2006-03 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture

[16] ETSI TS 182 012 V1.1.1 2006-04 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Subsystem; Functional architecture

[17] ETSI TS 183 043 V1.1.1 2006-05 Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); IMS-based PSTN/ISDN Emulation Stage 3 specification

[18] ETSI TS 182.006 V1.1.1 2006-03 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);IP Multimedia Subsystem (IMS);Stage 2 description (3GPP TS 23.228 v7.2.0, modified)

[19] ETSI TS 133 210 V7.0.0 2005-12 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security

[20] RFC 2474 Dec 1998 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

[21] RFC 3261 June 2002 SIP: Session Initiation Protocol

[22] RFC 3310 Sept 2002 Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
[23] RFC 3842 August 2004 A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
[24] IEEE STD 802.1q Virtual Bridged Local Area Networks
[25] TS124.229 V7.7.0 2007-03 Digital cellular telecommunications system (phase 2+); Universal Mobile Telecoms System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.

2.2 Informative references

[i.1] SR 001 262 V2.0.0 2004-07 ETSI drafting rules Section 23:- Verbal Forms For The Expression Of Provisions

3 Definitions and abbreviations

The key words "**shall**", "**shall not**", "**must**", "**must not**", "**should**", "**should not**", "**may**", "**need not**", "**can**" and "**cannot**" in this document are to be interpreted as defined in the ETSI Drafting Rules [i.1].

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

* PSTN and ISDN when used with the term 'service' defines the replication of the service set applied to NGNs rather than the legacy networks in themselves.
* Where used in this document the term VLAN refers to an Ethernet Static VLAN

3.2 Abbreviations

For the purposes of the present document, the abbreviations following apply:

3GPP	3rd Generation Partnership Project
CP	Communications Provider
DNS	Domain Name System
DSCP	Differentiated Service Code Point
ETSI	European Telecommunication Standards Institute
FSK	Frequency Shift Key
IP	Internet Protocol
ISDN	Integrated Services Digital Network*
ITU-T	International Telecommunication Union - Telecoms
kbps	Kilobits per second
MSI	Multi-Service Interconnect
NAT	Network Address Translation
NGN	Next Generation Network
PSTN	Public Switched Telephone Network*
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIP	Session Initiation Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Indicator
VBD	Voice Band Data
VLC	Voice Line Control

4 VLC Service Level Functional Architecture

The Voice Line Control Functional Architecture defines the interconnect interfaces between two UK Next Generation Networks (NGN) with relationship to the NGNs' internal logical network functions.

4.1 Conventions used in the Architecture Figures

The convention used in labelling the functional architecture is as follows:-

- All logical functions and interfaces are labelled with an alpha/numeric identifier.
- All logical functions' identifiers begin with the letter 'f'.
- All interconnect interfaces' identifiers begin with the letter 'i'.
- The second letter of an identifier (function or interface) indicates if it is associated with the Control plane(C) or the Bearer plane (B). 'T' denotes functions or interfaces associated with the MSI Common Transport Specification [2]. E.g. iC5 is control plane interface number 5.
- All functions and interfaces that have their own separate technical definition are labelled with a number unique to the identifier type. E.g. fC1 and iC1 are different defined entities as are iB1 and iB2.
- Multiple instances of separate functions or interfaces that have the same definitions have the same identifier root but are differentiated by appending an alpha letter to the root identifier. e.g. Interfaces with the same root identifier and number and a different suffix letter such as iB1a, iB1b, etc indicate separate instances of the same interface type and definition.
- Green lines between functions indicate logical internal relationships within the NGN which are not defined.
- Red lines indicate interconnect interfaces for the common transport capabilities in the bearer plane.
- Blue lines indicate service level interfaces that sit on top of the associated underlying common transport capabilities.

4.2 Relation to ETSI Standards

This architecture is derived from the PSTN Emulation Services specifications as defined in ETSI standards ES 282 002 [15], TS182 012 [16] and TS 183 043 [17].

4.3 Interconnect Architecture Definition

The VLC Functional Architecture defines logical network functions and interconnect interfaces between two Next Generation Networks, NGN A and NGN B. The functional architecture is divided into control and bearer planes and defines the properties of the functions and interfaces. Note that the functional architecture is capable of being realised within a NGN in a number of ways and that no physical implementation is implied.

The VLC service is not a peer-to-peer relationship such as seen with other interconnect types (e.g. ISDN/PSTN) as one network is exposing the control of the access gateway to the other which hosts the call control. In the functional architecture NGN A contains the access network with its associated media gateway and exposure functions and is referred to in this document as the *VLC Provider Network.* NGN B contains the call control application that provides the intelligent control of the end user's line and the service features that end user enjoys. NGN B is called the *VLC User Network.*

The architecture shows the static relationships between network functions and the interconnect interface. Typical outline message flows that show the dynamic behaviour of the architecture are provided in the signalling specification ND1021 [12].

This interconnect architecture does not assume that the VLC User Network is an IMS based network but it does need to support the control interface defined in TS182 012 [16] and TS 183 043 [17] which is specified in terms of an IMS functional architecture.

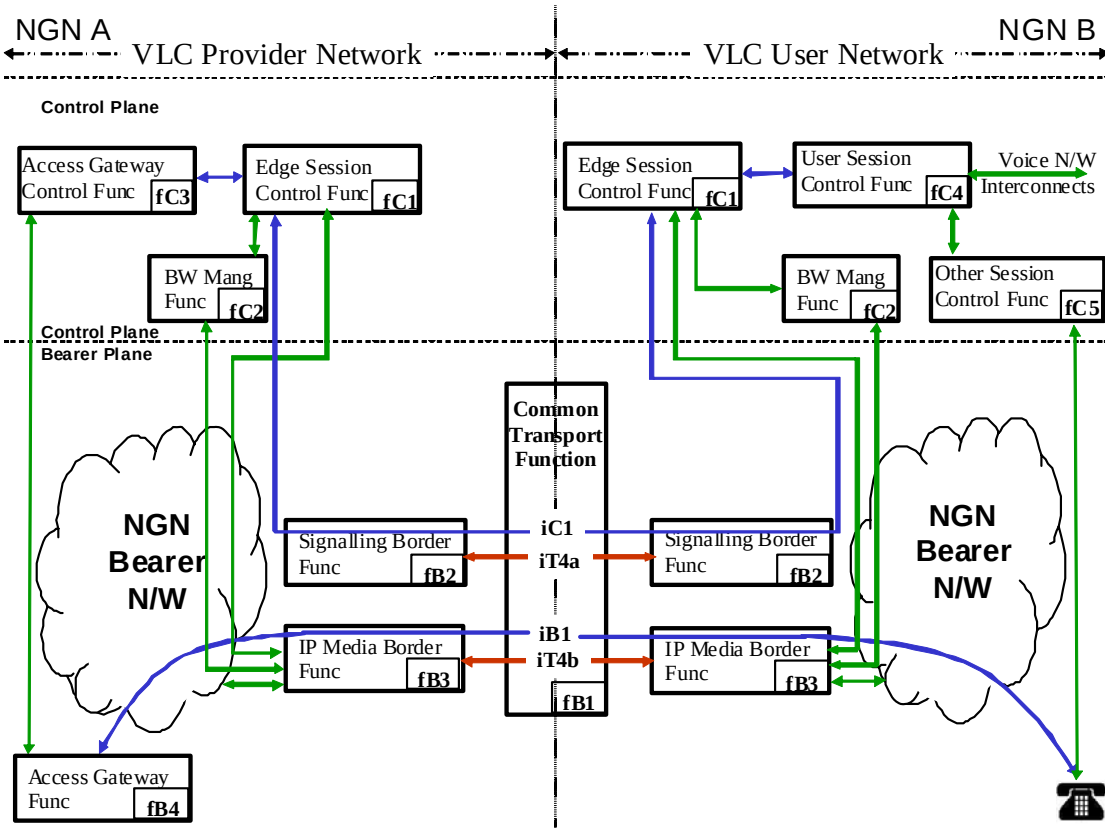

Figure 1: Functional Architecture for VLC Service

[Note: The Blue line shown between fC3, fC1, fC4 and fC1 represents the logical extension of iC1 between the AGCF and the USCF]

4.4 Functional Component Description

4.4.1 Bearer Plane Functions

4.4.1.1 Transport Function (fB1)

This service uses 'trails' that supports the IP capability (iT4) of the common transport function specified in ND1611 [2]. In this document these IP supported transport trails are referred to as VLANs. Separate VLANs **shall** be used for transporting the signalling (iT4a) and media (iT4b) interfaces dedicated to the VLC Service which **may** be carried on the same or separate physical MSIs.

4.4.1.2 Signalling Border Function (fB2)

The Signalling Border Function protects the signalling between Edge Session Control Functions in different networks which are connected via dedicated data channel(s) (iT4a) of fixed bandwidth. Signalling Border Functions support connections that carry the signalling between one or more pairs of Edge Session Controller Functions.

The Signalling Border Function:

a) **shall** provide a firewall between the NGN and the interconnection space.
b) **may** provide translation of the signalling IP addresses.
c) **shall** perform the functions of a Security Gateway as defined in ETSI TS 133 210 [19]
d) **shall** detect the loss and reestablishment of communications with its peer Signalling Border Function and **shall** support monitoring requests from its peer.

e) **should**, if not provided elsewhere, provide the IP address translations for the signalling stream between the different address spaces, if the IP address space within its own network is different to the address space used across the interconnection.

4.4.1.3 Media Border Function (fB3)

The IP Media Border Function provides policing of media streams between networks carried via the iT4b transport interface.

The Media Border Function:

a) **may** open and close individual firewall pinholes for each IP address and port number pair for a RTP media stream on the establishment and termination of a session by the Edge Session Controller (fC1).
b) **may** provide network topology concealment of the CP's NGN.
c) **should** allow the connection of RTP streams, within its own network (with associated IP address space and UDP port numbers) and the RTP streams at the interconnect, with different or overlapping IP address spaces and sets of UDP port numbers.
d) **should** enforce the bandwidth of each media stream as requested in the associated signalling message.
e) **shall** detect the loss and reestablishment of communications with its peer Media Border Function and **shall** support monitoring requests from its peer.
f) **shall** forward RTCP streams associated with each media stream

4.4.2 Control Plane Functions

4.4.2.1 Access Gateway Control Function (fC3)

The Access Gateway Control Function (AGCF) controls the Access Gateway Function (fB4) to apply and detect the analogue line conditions for the VLC user of the service for both originating and terminating sessions.

The Access Gateway Control Function:-

a) **shall** provide the appropriate line functionality determined by the end user's line type and features using data provided by the VLC User Network CP. This release **should** include The analogue line types:- Loop calling, Earth calling and PBX; line features shall include Line reversal on answer, hotline and warmline.
b) **shall**, on receipt of a registration from an Access Gateway Function (fB4), provide a SIP registration for each group of users on that Access Gateway to the User Session Control Function (fC4) in the VLC User Network responsible for those users. This registration **shall** contain a SIP Path header as defined in TS124.229 [25] endorsed by ND1019 [11]. This registration **shall** be sent via an interconnect associated with an Edge Session Control function (fC1) chosen from a pre-configured list supplied by each VLC User Network CP. The interconnect priority choices **shall** be against Groups associated with individual Access Gateways and will define the bearer path between the Access Gateway function and the VLC User's interconnections. Subsequent outgoing SIP messages **shall** use the SIP route discovered at registration through the Service Route Header.
c) **shall** control the application of call progress tones and basic announcements at the Access Gateway Function (fB4) as defined in ND1021[12] and signalled by the VLC User Session Control function (fC4) for the VLC users originating calls, except for ring tone which **shall** be provided at the session terminating or inter-working point.
d) **shall** control the application of ring tone to a call terminating on an Access Gateway Function (fB4) as signalled by the VLC User Session Control function (fC4).
e) **shall** control the application of ringing cadences to a VLC user's line receiving a terminating call as signalled by the VLC User Session Control function (fC4).
f) **shall** control the dial tone applied at the Access Gateway Function (fB4). A configured default dial tone **shall** be applied which can be altered from a VLC User Network Function using an implied subscription to either or both of: the "ua-profile" event with dial tone management as defined in TS 183 043 [17] Annex A and/or the "message summary" event package as defined in RFC 3842 [23].
g) **shall** ensure that new calls are only admitted to the VLC provider network where there is sufficient available free bandwidth for that call.
h) **shall** identify if originating calls are to be treated with priority and apply the call treatments described in section 5.

i) **shall** generate application layer continuity test messages for common paths through the control plane in line with section 10.

4.4.2.2 Access Gateway Function (fB4)

The Access gateway Function (fB4)

a) **shall** establish and terminate symmetric RTP media streams for a given access line under the control of the AGCF
b) **shall** support autonomous transition from Audio mode to ITU-T G.711 VBD Mode
c) **shall** detect the analogue line conditions and report them to the AGCF
d) **shall** provide basic programme tones and announcements as requested by the AGCF
e) **shall** send FSK signals to the access line as signalled by the AGCF

4.4.2.3 Edge Session Control Function (fC1)

The Edge Session Control Function provides the co-ordination intelligence for controlling the other functional elements associated with the interconnection.

The Edge Session Control Function:

a) **shall** interact with other session control functions within its own network in order to manage session egress or ingress for the interconnection point it controls. e.g. Access Gateway Control Function (fC3) or VLC User Session Control Function (fC4).
b) **shall** interact with its peer Session Control Functions in the other network, acting as a SIP Back-to-Back User Agent, managing session egress or ingress for the interconnection point(s) it controls.
c) **may** provide the IP address translations for the signalling stream between the two different address spaces, if the IP address space within its own network is different to the address space used across the interconnection.
d) **shall** ensure that the media type and characteristics that are requested in the signalling, (TS124.229 [25] endorsed by Session Description Protocol ND1019 [11]), are compatible with the VLC service as defined in the media stream definition and announcement section. New session requests that do not have compliant SDP parameters **shall** be rejected to ensure compliance with Recommended Standard for the UK National Transmission Plan, NICC [13] and the ETSI NGN Service & Capabilities Requirements [14].
e) **shall**, during session establishment, determine that there is the required bandwidth for the bearer session as requested in the signalling by making requests for bandwidth allocation from the Bandwidth Management Function (fC2).
f) **shall** control the use of the Media Border Function (fB3) where present.
g) **shall** provide the correct IP / port translations, as required, in the signalling streams associated with the media streams if the CP's NGN and the interconnected network have different IP address spaces
h) **may** hide topology information from the peer network contained within session control messages from within its own network in line with TS124.229 [25] endorsed by ND1019 [11]. This applies to all SIP messages that are sent to the peer network which have headers that are capable of containing topology information such as Via, Route, Record Route, Path and Service-Route headers. If an ESCF in the VLC User Network hides topology, it **shall** conform to the convention defined in section 11 in order to provide an abstract representation of the control plane path between it and the User Session Control Function (fC4).
i) **shall** support the transportation of SIP registration dialogues to and from the User Session Control Function (fC4)
j) **shall** support SIP loose routeing using Route / Record Route / Path/ Service Route Headers.
k) **shall** support the transportation of SIP NOTIFY methods from the VLC User Network to the VLC Provider Network.
l) **shall** provide rate restriction capabilities to manage overloads – reference ND1621 [4].
m) **should,** when located in a VLC User Network, provide an independent session rate restriction capability for SIP REGISTER and INVITE methods sent to each User Session Control Function (fC4).
n) **should** produce call detail records which **may** contain any of the following:-
    i. Session time and date.
    ii. SIP Global reference in its P-charging Vector
    iii. Session duration.
    iv. Source and destination IP addresses between the IP Media Border Function (fB3) and the termination point inside the NGN A or B and the IP address between the IP Media Border Functions of the peer networks (fB3-fB3) for fault analysis between CPs.

v. Media quality statistics such as packet loss, jitter and delay

o) **shall,** when located in a VLC Provider Network block SIP redirects. (it is assumed that SIP redirects are handled in the VLC User Network).
p) **may** support dynamic allocation of User Session Control Functions for AGCF as described in the ETSI IP multimedia Subsystem architecture TS 182.006 [18]./ TS124.229 [25] endorsed by ND 1019 [11].

4.4.2.4 Bandwidth Management Function (fC2)

The Bandwidth Management Function within this architecture only relates to the VLANs in the bearer plane that carry the media stream across the interconnect (iT4b). In the general case this function will deal with requests for media sessions of varying bandwidth, but for VLC service, the media sessions are symmetric and of fixed bandwidth (i.e. RTP streams carrying 64kbps payload for PSTN quality voice, and in the future ISDN services, and their associated RTCP streams). Therefore simple session counting could suffice.

A bandwidth management function:

a) **should** hold a logical model of the bandwidth allocation of the transport trail that is related to the routeing of the session (i.e. iT4b).
b) **should** have a near real time view of the transport operational status with regards to its ability to support the current overall bandwidth on the associated transport VLANs. i.e. the loss and re-establishment of the service offered on a transport VLAN is reflected into the Bandwidth Management Function.
c) **should** keep its bandwidth model in step with any fixed bandwidth policing performed by the transport function on its transport VLANs.
d) **should** process requests from the Edge Session Control Function for bandwidth allocation for a media session against the overall bandwidth on the transport trail across the interconnection.
e) **shall** support the handling of priority calls as defined in section 5

4.4.2.5 User Session Control Function (fC4)

The User Session Control Function (fC4) provides the call control and features offered to the end user. It exchanges signalling with the Edge Session Control Function (fC1) within its network containing information on the session that is being controlled.

a) this signalling path **shall** be determined through the SIP registration mechanism
b) the User Session Control Function **shall** store the SIP URI's received in the Path header established during registration and **shall** include this information in Service Route & Route headers of subsequent SIP messages destined for the AGCF using SIP loose routeing.

The routeing between the Edge Session Control Function (fC1) and the User Session Control Function (fC4) is dependent on the architecture of the VLC User Network which **may** use information in the domain name supplied for registration to identify a specific User Session Control Entity (e.g. CallServerId.CPId.uktel.org.uk) or a dynamic mechanism such as private DNS look-ups with SRV records.

The User Session Control Function (fC4) **may** also be determined using the mechanisms described in the ETSI IP Multimedia Subsystem architecture TS182.006 [18].

4.5 Interface Definitions

4.5.1 Signalling Transport Interfaces

4.5.1.1 Signalling Interconnect Use of the Common Transport Function (iT4a)

The signalling interface **shall** be carried over the IP capability of the common transport function (iT4a) on a single VLAN reserved for VLC signalling only.

Traffic carried on one such VLAN **shall not** affect the capacity of other VLANs. Each VLAN **may** convey messages associated with one or more pairs of AGCF and USCF. The dimensioning of each VLAN **shall** take account of the capacity required for peak load and loads encountered under fault conditions as defined in the planning guidance in VLC Management Document [3].

4.5.1.2 Signalling IP Addressing

An IP subnet **shall** be allocated, in accordance with section 8, for each signalling VLAN between the signalling border functions in each CP's network. Each device, IP interface, or other network element on the connection **shall** be allocated an agreed IP address from within this subnet.

Each CP **shall** inform the other of the IP addresses to be used to communicate with each relevant edge session control function.

4.5.1.3 Signalling VLAN Bandwidth

The bandwidth required for each signalling VLAN **should** be determined by taking account of:

- the number of signalling paths between Access Gateway Control Functions (fC3) and User Session Control Functions (fC4) that are carried on the signalling VLAN
- the peak signalling rate of each of the signalling paths carried on the VLAN
- the failure modes and required resilience of the signalling VLANs

4.5.1.4 Signalling Security

Signalling VLANs **shall** be protected from unauthorised access from inside or outside a CP's network.

Signalling Authentication and Encryption **shall** be provided and be conformant to ND1628 [5].

4.5.1.5 Media Security

Media security **should** be provided by the dynamic pin-hole functions of the Media Border Function (fB3) under the control of the Edge Session Control Function (iC1) which it derives from the internal and interconnect signalling.

Authentication or encryption of the content of a media stream **shall not** be required between the Media Border Functions (fB3) on an interconnect.

4.5.2 Signalling Control Interface (iC1)

4.5.2.1 Application Layer Protocol

The application signalling protocol for iC1 **shall** be as defined in ND1021 [12].

4.5.2.2 Signalling Transport Protocols

The signalling interface (iC1)

- **should** use SCTP as defined in ND1012 [9]
- **may** use TCP as defined in ND1018 [10]

The use of UDP is not defined

The choice of protocol **shall** be governed by the resilience issues described in section 10.3.

4.5.2.3 SIP URI Naming Scheme

This SIP URI naming scheme **shall** conform to ND1633 [6] and the following sub-sections apply additional conditions to that document.

The VLC service **shall** include a <*local application ID*> as defined in ND1633 [6] within its <*domain name*>and it **shall** be the string 'vlc'

4.5.2.3.1 VLC Line ID

The VLC_Line_ID **shall** be used between the VLC User Network and VLC Provider Network as the destination/origin identification in associated SIP messages. It identifies a specific physical line at the Access Gateway Function (fB4). With respect to the associated ETSI documents the VLC_Line_ID **shall** be equivalent to the IMS PublicID.

The VLC_Line_ID:-

c) **shall** set the <*provider identity*> to that of the VLC User Network
d) **may** include a <*network internal part*>
e) **should not** have the <*userinfo*> set to reflect the publicly reachable address, be it telephone number or name, as doing so **may** require the VLC User Network to cease and re-provide a line if the publicly reachable address is changed

Examples of conformant SIP URIs:

sip:Line27.agw94@cs23.vlc.example-cp.uktel.org.uk

sip:887928736@vlc.example-cp.uktel.org.uk

4.5.2.3.2 Registration_Group_ID

The Registration_Group_ID **shall** identify a set of lines that would share a common registration from the AGCF (fC3) to the USCF (fC4), typically all of the lines on a given Access Gateway Function (fB4).

Maximum group size is defined in 9.4.1.

The Registration_Group_ID is the combination of the <*Authorization_Group_ID*> and <*VLC_Line_Group_ID*> *as defined below.*

4.5.2.3.3 Authorization_Group_ID

This field identifies the authorization domain for the VLC service and is only used in the authorization header in the REGISTER request. With respect to the associated ETSI documents the <*authorization_group_id*> **shall** be equivalent to IMS Private ID.

The <*authorization_group_id*>**:-**

a) **shall** use the format specified in ND1633 [6] where <*provider*> is the VLC **User** Network.
b) **may** have a <*userinfo*> field and if so it **shall** be specified by the VLC User Network
c) **may** have a <*network internal part*> field to indicate different internal authorization domains
d) **should** have a minimal set of <*Registration Domain*> values per CP

Examples of conformant Authorization_Group URI:

sip:pstn@authenticate1.vlc.example-cp.uktel.org.uk

sip:centrex@vlc.example-cp.uktel.org.uk

4.5.2.3.4 VLC Line Group ID

The VLC_Line_Group_ID identifies a group of lines that share a common registration. All lines in such a group **shall** be on the same AGF (fB4), AGCF (fC3) and **shall** use the same USCF (fC4).

While a VLC user **may** typically have a single VLC_Line_Group_ID per AGF (fB4) more granular groupings **shall** be supported.

Maximum group size is defined in 9.4.1.

The VLC_Line_Group_ID **shall** only be used in the "To" and "From" header fields of a REGISTER request and the permissible responses to this request (e.g. 200 OK or 401 Unauthorized).

The Request URI of a REGISTER request **shall** be set to the

<*domain name*> of the VLC_Line_Group_ID. With respect to the associated ETSI documents the VLC_Line_Group_ID **shall** be equivalent to the Temporary Public ID.

The VLC_Line_Group_ID:-

a) **shall** use the same domain name as the VLC_Line_ID

b) **shall** have the <*userinfo*> part determined by the VLC Provider Network

c) **shall** have the <*userinfo*> structured in the form:- <*labels***.***VLC_Provider_Network_ID*> where <*labels*> **shall** be one or more free format strings separated by dots and '*VLC_Provider_Network_ID'* **shall** be the same as the registered <*provider*> of the VLC Provider Network.

Example of a conformant VLC Line group ID, SIP URI:

sip:agw2298.example-provider-cp@vlc.example-user-cp.uktel.org.uk

4.5.2.3.5 Format for Conveying Dialled Digits

Where dialled digits and other terminal events are to be conveyed from the VLC Provider network to the VLC user network in a SIP URI within the "To:" field of a SIP INVITE, the format to be used **shall** be

<*event string*>@<*domain name*>

where

a) <*domain name*> **shall** be the same as the **VLC_Line_ID**
b) <*event string*> **shall** be used for carrying dialled digit strings, keywords or both, in the format digits;keyword, that represent other terminal events.

For dialled digits from the customer, <*event string*> **shall** contain only the digits 0 to 9, * or #.

For specific terminal events (e.g. recall) the valid keywords **shall** be those defined in ND1021 [12].

Example of conformant Event SIP URIs:

sip:02033448724@vlc.example-user-cp.uktel.org.uk

sip:flashhook@ vlc.example-user-cp.uktel.org.uk

sip:02033448724;flashhook@ vlc.example-user-cp.uktel.org.uk

4.5.2.4 SIP URI to IP Address Binding

The binding of SIP URI for Edge Session Control Functions (fC1) to IP address **shall** be passed as management information at the time of service establishment or as a result of any subsequent modifications.

4.5.2.5 Circular Routeing Limitation in SIP

The AGCF (fC3) **shall** set the SIP Max-Forwards count to 70.

Edge Session Control Functions (fC1) and any other SIP proxy **shall** decrement this value when messages pass through them.

Any SIP server that decrements the Max-Forwards to zero **shall** reject the call with the code '483 Too Many Hops'.

4.5.2.6 Unsupported Media Types

If the media type and characteristics that are requested in the signalling, (TS124.229 [25] endorsed by Session Description Protocol ND1019 [11]), are not compatible with the VLC analogue line service as defined in the media stream definition and announcement section. The SIP request **shall** be rejected with the SIP message, '415 Unsupported media type' .

4.5.2.7 Session Processing Overload Control

SIP has no mechanism for managing processing overloads resulting from high levels of offered session set-up traffic and other transaction types. Therefore, overloads **shall** be controlled using static rate limitations at the Edge Session Control Functions (fC1) which **shall** be conformant to ND 1621 [4]**.**

Note:- This mechanism will be replaced with a dynamic control mechanism when defined in the standards bodies and available from suppliers.

4.5.3 Media Stream Transport Interfaces

Shall be conformant to the format defined in ND1635 [7]

4.5.4 Media Stream Definition and Announcement (iB1)

The media stream **shall** be announced across the signalling interface (iC1) using the Session Description Protocol (SDP) defined in TS124.229 [25] endorsed by ND1019 [11], in which the "a=ptime:" attribute **shall** be present in order to specify that a 10 ms encoding packet size **shall** be used.

The coding types supported by the NGN for VLC service **shall** be G.711 A-law.

For generic Media Stream definitions including Voice Band Data , Voice Activity Detection, Error Performance and Packet Loss, Delay and Packet Variation, echo Control, Media Stream Synchronisation and Monitoring of IP Streams shall comply with ND1635 [7].

5 Priority Calls

5.1 Priority Call Detection

The AGCF **shall** determine if an originating call is to be handled with priority by reference to the identity of the calling line or by detecting that the called number is one of a limited and defined set. For calls that are to be handled with priority an indication to that effect **shall** be include in the signalling.

Terminating priority calls **shall** be indicated in the signalling from the USCF (fC4) e.g. as a result of dialled digit number analysis or by the signalling received from other networks.

5.2 Media Path Bandwidth and Admission Control

A media path that carries both ordinary and priority traffic between two NGNs **shall** be configured so that the total bandwidth available on that media path **shall** be equal to the bandwidth configured for ordinary calls plus that reserved exclusively for priority calls.

On ordinary or priority call set up and release, the bandwidth in use on the media path **shall** be increased and decreased respectively by that used for the call.

5.2.1 Ordinary Call Treatment

For ordinary calls, where the bandwidth currently being used on the media path plus the bandwidth required for a new call is less than or equal to the bandwidth configured for ordinary calls, the call **shall** be allowed. However, if this condition is not met (i.e. there is insufficient spare bandwidth available for a new ordinary call), then this call attempt **shall** be rejected with a congestion cause.

5.2.2 Priority Calls Treatment

For priority calls, where the bandwidth currently being used on the media path plus that required for the new priority call is less than or equal to the total (i.e. ordinary plus priority) bandwidth on the media path, the call **shall** be allowed. However, if there is insufficient spare bandwidth on the media path the call attempt **shall** be rejected with a congestion cause.

5.3 Priority Calls and Overload Management

A priority call **shall not** be subject to any inbound or outbound call rate restrictors at the interconnect interface if, and only if, the agreed static rate limitation level can not be met by discarding ordinary call attempts.

6 Lawful Interception

Provision of Lawful intercept features is a matter for the User Network, and places no specific additional requirements on this interconnect.

7 Packet / Frame Marking

In order to introduce new and as yet undefined services to the MSI without changing this service, IP packet marking (DSCP) [20] or Ethernet frame marking [24] are not used. Media and signalling rely on being carried in independent VLANs, each with its own shaped and policed bandwidth, as a service provided by the Common Transport Function [2]. Therefore, these packet marking fields **should** be ignored**.**

8 IP Addressing

Details of IP Addressing issues including Version of Internet Protocol, IP address ranges and Network Address Translation (NAT) can be found in ND1636[8].

9 Registration Procedures

9.1 Pre-Registration Data Exchange

Before Registration Procedures can begin, the information for the Registration_Group ID and its associated interconnect points **shall** be exchanged via a management process. In addition information on the proffered interconnect points for each VLC_Group.

9.2 Registration Overview

Before any session establishment can take place, an AGCF (fC3) **shall** register a group of users (lines) with the User Session Control Function (fC4). A group of users **shall** all be on the same access gateway destined for the same USCF (fC4).

Registration **shall** occur when

a) an Access Gateway (fB4) registers with an AGCF (fC3)

b) an existing registration expires

c) the signalling or media path between the AGCF (fC3) and the User Session Control Function (fC4) for an existing registration is detected as failed, in order to establish a new interconnect path.

d) The set of VLC_Line ID changes within a group

9.3 Point of Interconnect

The AGCF (fC3) **shall** hold a registration priority list for each Access Gateway (fB4). This is an ordered list of the VLC Network Provider's Edge Session Control Functions (fC1) that are associated with the VLC User Network's specified Points of Interconnect to be used for VLC service to lines on that Access Gateway Function. Every registration attempt **shall** be made in priority order.

9.4 Registration Types

There are two registration mechanisms identified in the 'Registration Procedures' described in TISPAN PES Stage 3 Specification TS 183 043 [17]; group and individual line registration.

9.4.1 Group Registration and Maximum Group Sizes

To minimise the registration processing effort and the time taken to register users and also to avoid overloads due to registration storms, registration using a private user identity which is assigned to a group of subscribers **shall** be supported. The assigned VLC Line group **shall** be used as the temporary public user identity as described in TS 183 043 [17].

If the P-Associated-URI is used then the maximum group size that both a Provider and a User Network **shall** support is 30.

9.4.2 Individual Line Registration

Individual line registration **may** be supported in which case a pair of private and public VLC_Line_Id's is associated with each analogue port connected to the Access Gateway.

9.5 Registration Authentication

Each initial registration request in a registration sequence **shall** be authenticated by a registration rejection challenge using the digest method specified in RFC 3261 [21] as opposed to the more complex procedures specified in RFC3310 [22] which is intended to address vulnerabilities associated with a radio access network. The authentication process **shall** use the "MD5-sess" encryption algorithm.

9.6 Valid Registration Periods

Normal AGCF Registrations **shall** request a registration expiry period of 600,000 seconds (see de-registration for exception). Registration responses **shall** set the registration expiry period to not less than 1800 seconds. AGCFs **may** reject any requests to reduce below this period.

9.7 User Service Status

Authorised registration acknowledgements from the User Session Control Function **shall** include a list of all the 'in-service' line identifiers recognised for that group. This list **shall** be returned as a list of URIs in the P-Associated-URI header in accordance with the procedures in TS 124 229 [25] endorsed by ND1019[11] noting that the VLC Line Group (temporary user identity) **shall not** be returned and therefore shall be considered as barred from session initiation. Users **shall** receive service following an authorised registration acknowledgement.

Note: Subsciption Management as an alternative to usage of the contents of the P-Associated-URI is not precluded in future releases and may be used by bilateral agreement.

9.8 De-Registration

In support of maintenance processes, if an AGCF registers a group with a requested expiration interval of "0", the User Session Control Function (fC3) **shall** release all route bindings and consider the group and all its associated users/lines as un-registered. All SIP entities shall release the route bindings on receipt of the 200 OK acknowledgement. Calls will no longer be able to be made to or from the lines associated with the group.

10 Resilience

10.1 Definitions of Terms in this Section

A Signalling Path is defined as the signalling connection between the Access Gateway Controller Function and User Session Control Function.

A Signalling Route is defined as the signalling connection between Signalling Border Functions

A Media Route is defined as the managed bandwidth between paired, peer Media Border Functions.

10.2 Interconnect Connectivity Failure Detection

A border function **shall** detect the loss of connectivity on an interconnect VLAN using the BFD continuity check service provided by the Multi Service Interconnect described in ND1611 [2]. ICMP 'Pings' **may** be used. This path continuity **shall** be checked every 1 sec. The absence of any responses to six consecutive continuity check requests **shall** be classed as a path failure and trigger the associated resilience actions. Following a path failure, responses to each of three consecutive continuity check requests **shall** be classed as a path restoration and available for use.

When connectivity between Media Border Functions (fB3) or Signalling Border Functions has failed then the corresponding Edge Session Control Function (fC1) **shall** be notified. Whilst connectivity failure exists the Edge Session Control Function **shall** reject any SIP requests including SIP options messages with 503 "Service Unavailable".

Signalling path failure **may** be detected via the underlying transport protocol e.g. SCTP.

10.3 Interconnect Signalling & Media Route Resilience

Media and Signalling Paths **may** have their own resilience provided at the common transport function layer (fB1).

Where signalling peers, i.e. ESCFs (fC1), are connected by only one logical path which provides performance that is acceptable to CPs concerned, either a single-homed SCTP[9] path or TCP [10] **may** be used. Otherwise multi-homed SCTP [9] **shall** be used.

10.4 Signalling Path Continuity Checks

The AGCF shall send a SIP OPTIONS method every 10 secs on each unique Signalling Path to the User Session Control Function(s) in order to maintain an integrity check of the signalling path. Signalling Path integrity is considered maintained if a 200 OK response is returned. If error response codes are received from the VLC user network, they shall be forwarded to AGCF unchanged. The registered Service Route **shall** be deemed to have failed in any of the following events:

a) the AGCF cannot establish connection with the ESCF in the VLC provider network

or

b) the AGCF does not receive a response to an OPTIONS method after a standard SIP retry strategy as defined in RFC 3261 [21]

or

c) the AGCF receives a SIP error response 408 (Request Timeout), 500 (Server Internal Error), 502 (Bad Gateway) or 606 (Not Acceptable) message to an OPTIONS request

or

d) the AGCF receives a SIP error response 503 (Service Unavailable) message with no Retry-After header to an OPTIONS request,

On detecting such a failure, the AGCF **shall** immediately attempt to re-register with the User Session Control Function using its registration prioritisation scheme (see 9.3 Point of Interconnect) including the interconnect associated with the signalling path that has failed. Receipt of other error responses **shall** not trigger immediate re-registration, however an alarm event **shall** be sent to the VLC user network via the management interface.

For the purpose of identifying unique Signalling Paths, between the AGCF (fC3) and the USCF (fC4) (to avoid redundant continuity checking), the Signalling Paths for two or more individual registrations shall be deemed identical if either:-

a) the associated Service Routes contain SIP URIs which are identical in content and order, and no topology hiding encryption field is present

or

b) the associated Service Routes contain unencrypted SIP URIs which are identical in content and order, along with a topology hiding encryption field with identical PathReferences (see 10.6).

10.5 Media Route Failure

If the Edge Session Control Function (fC1) determines that the Media Route under its control which is terminated by the Media Border Function (fB3) cannot be used then, when it receives any SIP request, it **shall** respond with a SIP Response 503 (Service Unavailable) with no “retry after” field. Additionally, if an ESCF becomes isolated from its internal network it should respond to any SIP request by sending back a 503 (Service Unavailable) with no “retry after” field. On receipt of a 503 in response to an OPTIONS request the AGCF (fC3) **shall** immediately re-register.

Reasons why the Media Route cannot be used include, but are not limited to:-

- The Edge Session Control function (fC1) is unable to communicate with the Media Border function (fB3).
- The Bandwidth Management function (fC2) is unable to communicate with the Media Border function (fB3).
- The Edge Session Control function (fC1) is unable to communicate with the Bandwidth Management function (fC2).
- The Media Border function (fB3) is isolated from its own internal network (i.e. facing into its own NGN) and therefore end-to-end media flows (iB1) cannot be established.
- The Media Route on interface iT4b (i.e. connection between Media Border functions) has failed.

10.6 Topology Hiding and Path References

If a VLC User Network ESCF(fC1) encrypts the SIP Service-Route header in the 200 OK response to a REGISTER request, the encryption token inserted **shall** conform to TS124.229 [25] endorsed by ND1019[11] and **shall** follow the profiling syntax shown below:-

<sip:Token (<encrypted string of SIP URIs>)>; tokenized-by =

OptionalUserInfo@OptionalLabels•***PathReference***•*ESCFid*•vlc•*VLCUserNetworkId*•uktel•org•uk

Where ***PathReference***

a) **shall** be the 7th level domain field.
b) **shall** have a one-to-one association with all identical control plane paths between itself and the USCF (fC4)
c) **shall** be an Alpha – Numeric string of no more that 8 characters
d) **shall not** explicitly contain the information that is being hidden

The following is a an example of a Service Route header as seen at the AGCF (fC3) after it has been processed by a topology hiding ESCF (fC1) in the VLC User Network that conforms to the above requirement:

Service-Route: <sip: agc.vlc.provider-network.uktel.co.uk;lr>,

<sip:sbc.vlc.provider-network.uktel.co.uk;lr>,

<sip:sbc.vlc.user-network.uktel.co.uk;lr>,

<sip:Token (hsgewwfejhacvcdsberw8342r7cbc88123949ck)>;

tokenized-by = 7FJ3LKM31@98283452.sbc3.vlc.cp.uktel.co.uk

Annex A (Informative)

The following example shows the naming and addressing schemes defined in this document as used in an initial SIP registration message sent from an AGCF to a Call Server. This Annex does not show all the fields that would be expected in a typical SIP REGISTRATION. For the sake of showing the information flows, this example assumes that the Edge Session Control Functions sbc12 and sbc_a are not providing any topology hiding.

The example follows uses the component and CP naming as shown in Figure 2.

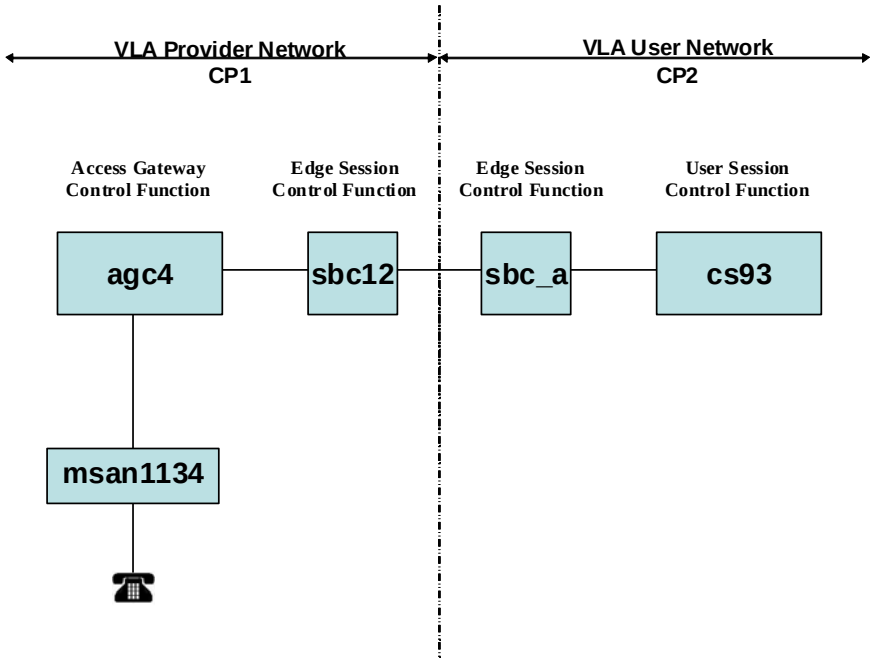

Figure 2: Example Configuration to Show Registration Headers

1st Registration Request

From AGCF to SBC12

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= " " ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= " "

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk;branch=z9hG4bKhjhs8ass871

Route: sbc12.cp1.uktel.org.uk; lr

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt @cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 70

Supported: path

Path: <sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

From sbc12 to sbc_a

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= " " ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= " "

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn1

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass871

Route: sbc_a.cp2.uktel.org.uk; lr

From: <sip:msan1134.bt @cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt @cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 69

Supported: path

Path: <sip: sbc12.cp1.uktel.org.uk ;lr>,<sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

From sbc_a to cs93

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= " " ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= " "

Via: SIP/2.0/TCP sbc_a.cp2.uktel.org.uk; branch=z9hG4bKgh7653hpo31

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn1

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass871

Route: cs93.cp2.uktel.org.uk; lr

From: <sip:msan1134.bt @cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt @cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 68

Supported: path

Path: < sip:sbc_a.cp2.uktel.org.uk;lr>, <sip: sbc12.cp1.uktel.org.uk ;lr>, <sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

1st Registration Response

From cs93 to sbc_a

SIP/2.0 401 Unauthorized

WWW-Authenticate: Digest realm= “cs93.cp2.uktel.org.uk” ,

nonce= Fva37UTWpGNB34JP ,

algorithm= MD5-sess

Via: SIP/2.0/TCP sbc_a.cp2.uktel.org.uk; branch=z9hG4bKgh7653hpo31

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn1

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass871

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 70

Content-Length: 0

From sbc_a to sbc12

SIP/2.0 401 Unauthorized

WWW-Authenticate: Digest realm= “cs93.cp2.uktel.org.uk” ,

nonce= Fva37UTWpGNB34JP ,

algorithm= MD5-sess

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn1

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass871

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 69

Content-Length: 0

From sb12 to agc4

SIP/2.0 401 Unauthorized

WWW-Authenticate: Digest realm= “cs93.cp2.uktel.org.uk” ,

nonce= Fva37UTWpGNB34JP ,

algorithm= MD5-sess

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass871

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 68

Content-Length: 0

2nd Registration Request

From AGCF to SBC12

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= "Fva37UTWpGNB34JP" ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= "H77dJkw8157G8U02"

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk;branch=z9hG4bKhjhs8ass872

Route: sbc12.cp1.uktel.org.uk; lr

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63105 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 70

Supported: path

Path: <sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

From sbc12 to sbc_a

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= "Fva37UTWpGNB34JP" ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= "H77dJkw8157G8U02"

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn2

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass872

Route: sbc_a.cp2.uktel.org.uk; lr

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63105 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 69Supported: path

Path: <sip: sbc12.cp1.uktel.org.uk ;lr>, <sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

From sbc_a to cs93

REGISTER sip:cs93.cp2.uktel.org.uk SIP/2.0

Authorization: digest username="usr_grp11_private_id@cs93.cp2.uktel.org.uk",

realm= "cs93.cp2.uktel.org.uk" ,

nonce= "Fva37UTWpGNB34JP" ,

uri= "sip:cs93.cp2.uktel.org.uk" ,

response= "H77dJkw8157G8U02"

Via: SIP/2.0/TCP sbc_a.cp2.uktel.org.uk; branch=z9hG4bKgh7653hpo32

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn2

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass872

Route: cs93.cp2.uktel.org.uk; lr

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63105 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 600000

Max-Forwards: 68

Supported: path

Path: < sip:sbc_a.cp2.uktel.org.uk;lr>, <sip: sbc12.cp1.uktel.org.uk ;lr>, <sip:agc4.cp1.uktel.org.uk;lr>

Content-Length: 0

2nd Registration Response

From cs93 to sbc_a

SIP/2.0 200 OK

Via: SIP/2.0/TCP sbc_a.cp2.uktel.org.uk; branch=z9hG4bKgh7653hpo32

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn2

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass872

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 1800

Max-Forwards: 70

Supported: path

Service-Route: <sip:agc4.cp1.uktel.org.uk;lr>, <sip: sbc12.cp1.uktel.org.uk ;lr>, <sip:sbc_a.cp2.uktel.org.uk;lr>,<sip:cs93.cp2.uktel.org.uk;lr>

P-Associated-URI: <sip:line_a.identity@ cs93.cp2.uktel.org>,

<sip:line_g.identity@ cs93.cp2.uktel.org>,

<sip:line_h.identity@ cs93.cp2.uktel.org>,

<sip:line_b.identity@ cs93.cp2.uktel.org>

Content-Length: 0

From sbc_a to sbc12

SIP/2.0 200 OK

Via: SIP/2.0/SCTP sbc12.cp1.uktel.org.uk; branch=z9hG4bKkks28736mn2

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass872

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 1800

Max-Forwards: 69

Supported: path

Service-Route: <sip:agc4.cp1.uktel.org.uk;lr>, <sip: sbc12.cp1.uktel.org.uk ;lr>, <sip:sbc_a.cp2.uktel.org.uk;lr>,<sip:cs93.cp2.uktel.org.uk;lr>

P-Associated-URI: <sip:line_a.identity@ cs93.cp2.uktel.org>,

<sip:line_g.identity@ cs93.cp2.uktel.org>,

<sip:line_h.identity@ cs93.cp2.uktel.org>,

<sip:line_b.identity@ cs93.cp2.uktel.org>

Content-Length: 0

From sb12 to agc4

SIP/2.0 200 OK

Via: SIP/2.0/SCTP agc4.cp1.uktel.org.uk; branch=z9hG4bKhjhs8ass872

From: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>;tag=1928301774

To: <sip:msan1134.bt@cs93.cp2.uktel.org.uk SIP>

Call-ID: a84b4c76e66710

CSeq: 63104 REGISTER

Contact: <sip:agc4.cp1.uktel.org.uk>; expires 1800

Max-Forwards: 68

Supported: path

Service-Route: <sip:agc4.cp1.uktel.org.uk;lr>, <sip: sbc12.cp1.uktel.org.uk ;lr>,
<sip:sbc_a.cp2.uktel.org.uk;lr>,<sip:cs93.cp2.uktel.org.uk;lr>

P-Associated-URI: <sip:line_a.identity@ cs93.cp2.uktel.org>,

<sip:line_g.identity@ cs93.cp2.uktel.org>,

<sip:line_h.identity@ cs93.cp2.uktel.org>,

<sip:line_b.identity@ cs93.cp2.uktel.org>

Content-Length: 0

History

Document history		
1.1.1	June 2008	Initial issue
1.2.1	July 2008	Updated to include amendment to section 4.5.2.3.5
1.2.2	August 2008	Editorial update to remove duplicate [25] reference.