ATIS-1000066.2016(R2021)

American National Standard for Telecommunications

Emergency Telecommunications Service (ETS) Network Element Requirements for IMS-based Next Generation Network (NGN) Phase 2

Alliance for Telecommunications Industry Solutions

Approved October 10, 2016

American National Standards Institute, Inc.

Abstract

This standard specifies Emergency Telecommunications Service (ETS) requirements for an Internet Protocol (IP) Multimedia Subsystem (IMS) Core Network for support of Next Generation Network (NGN) Government Emergency Telecommunications Service (GETS) Voice and NGN GETS Video. These requirements further refine the procedures defined in the ETS Phase 1 Network Element Requirements for NGN IMS based Deployments standard [ATIS-1000023.2013]. In addition, OA&M requirements are specified.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair and Technical Editor (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communication Sciences)

D. Lukacs, Technical Editor (Applied Communication Sciences)

V. Shaikh, Technical Editor (Applied Communication Sciences)

Table of Contents

Table of Figures

Table of Tables

AMERICAN NATIONAL STANDARD **ATIS-1000066.2016(R2021)**

American National Standard for Telecommunications on –

ETS Network Element Requirements for IMS-based NGN Phase 2

1 Scope

This standard specifies Emergency Telecommunications Service (ETS) requirements for an Internet Protocol (IP) Multimedia Subsystem (IMS) Core Network for support of Next Generation Network (NGN) Government Emergency Telecommunications Service (GETS) Voice and NGN GETS Video.

These requirements further refine the procedures defined in the ETS Phase 1 Network Element Requirements for NGN IMS based Deployments standard [ATIS-1000023.2013]. In addition, OA&M requirements are specified.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

3GPP[1]

[TS 23.002]	3GPP TS 23.002, Network Architecture (Release 11).
[TS 23.203]	3GPP TS 23.203, Policy and Charging Control Architecture (Release 11).
[TS 23.218]	3GPP TS 23.218, IP Multimedia (IM) Session Handling; IM call model; Stage 2 (Release 11).
[TS 23.228]	3GPP TS 23.228, IP Multimedia Subsystem (IMS); Stage 2 (Release 11).
[TS 24.229]	3GPP TS 24.229, Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 11).
[TS 29.212]	3GPP TS 29.212, Policy and charging control over Gx reference point (Release 11).
[TS 29.213]	3GPP TS 29.213, Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping (Release 11).
[TS 29.214]	3GPP TS 29.214, Policy and charging control over Rx reference point (Release 11).
[TS 29.215]	3GPP TS 29.215, Policy and Charging Control (PCC) over S9 reference point; Stage 3 (Release 11).
[TS 29.228]	3GPP TS 29.228, IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents (Release 11).
[TS 29.229]	3GPP TS 29.229, Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 11).
[TS 29.230]	3GPP TS 29.230, Diameter applications; 3GPP specific codes and identifiers (Release 11).
[TS 29.238]	3GPP TS 29.238, Interconnection Border Control Functions (IBCF) - Transition Gateway (TrGW) interface, Ix interface; Stage 3 (Release 11).

[1] These documents are available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[TS 29.328] 3GPP TS 29.328, IP Multimedia Subsystem (IMS) Sh interface; Signalling flows and message contents (Release 11).

[TS 29.329] 3GPP TS 29.329, Sh Interface based on the Diameter protocol; Protocol details (Release 11).

[TS 29.332] 3GPP TS 29.332, Media Gateway Control Function (MGCF) – IM Media Gateway; Mn Interface (Release 11).

[TS 29.333] 3GPP TS 29.333, Multimedia Resource Function Controller (MRFC) – Multimedia Resource Function Processor (MRFP) Mp Interface; Stage 3 (Release 11).

ANSI/ATIS[2]

[ATIS-0100003] ATIS-0100003, User Plane Priority Levels for IP Networks and Services, November 2004.

[ATIS-1000003] ATIS-1000003, Number Portability Databases and Global Title Translations.

[ATIS-1000006] ATIS-1000006, Signalling Systems No. 7 (SS7) - Emergency Telecommunications Service (ETS).

[ATIS-1000018.2007] ATIS-1000018.2007, NGN Architecture.

[ATIS-1000023.2013] ATIS-1000023.2013, ETS Phase 1 Network Element Requirements for a NGN IMS based Deployments.

[ATIS-1000049] ATIS-1000049, End-to-End NGN GETS Call Flows, August 2011.

[ATIS-1000055] ATIS-1000055, Emergency Telecommunications Service Core Network Security Requirements

[ATIS-1000065.2015] ATIS-1000065.2015, ETS EPC Network Element Requirements.

[ATIS-1000067] ATIS-1000067, IP NGN Enhanced Calling Name.

[ATIS-1000111.2005] ATIS-1000111.2005, Signalling System Number 7 (SS7) – Message Transfer Part (MTP) (R2010).

[ATIS-1000112.2005] ATIS-1000112.2005, Signaling System Number 7 (SS7) Signaling Connection Control Part (R2010).

[ATIS-1000113.2005] ATIS-1000113.2005, Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part (Revision of T1.113-2000) (R2010).

[ATIS-0100523.2011] ATIS-0100523.2011, ATIS Telecom Glossary 2011, http://www.atis.org/glossary.

[ATIS-1000679] ATIS-1000679, Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part.

[T1.114] ANSI T1.114-2004, Signaling System Number 7 (SS7) – Transaction Capabilities Application Part (TCAP).

IETF[3]

[RFC 2396] IETF RFC 2396, Uniform Resource Identifiers (URI): Generic Syntax.

[RFC 3261] IETF RFC 3261, SIP: Session Initiation Protocol.

[RFC 3550] IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications.

[RFC 3725] IETF RFC 3725, Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP).

[RFC 3966] IETF RFC 3966, The tel URI for Telephone Numbers.

[2] Available from ATIS at < https://www.atis.org/docstore/default.aspx >.

[3] These documents are available from the Internet Engineering Task Force (IETF) at: < http://www.ietf.org >.

[RFC 4412] IETF RFC 4412, Communications Resource Priority for the Session Initiation Protocol (SIP).

[RFC 4733] IETF RFC 4733, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals.

[RFC 5865] IETF RFC 5865, A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic.

[RFC 6401] IETF RFC 6401, Resource ReSerVation Protocol (RSVP) Extensions for Admission Priority.

[IETF draft-ietf-dime-drmp] IETF draft-ietf-dime-drmp-05, Diameter Routing Message Priority.

ITU[4]

[H.248.1] ITU-T Recommendation H.248.1, Gateway control protocol: Version 2.

[H.248.52] ITU-T Recommendation H.248.52, Gateway control protocol: QoS support packages, June 2008.

[H.248.81] ITU-T Recommendation H.248.81, Gateway control protocol: Gateway Control Protocol: Guidelines on the Use of the International Emergency Preference Scheme (IEPS) Call Indicator and Priority Indicator in ITU-T H.248 Profiles, May 2011.

[M.3060] ITU-T Recommendation M.3060, Principles for the Management of Next Generation Networks, March 2006.

[M.3400] ITU-T Recommendation M.3400, TMN Management Functions, February 2000.

[Q.850] ITU-T Recommendation Q.850, Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part, May 1998.

[Y.2171] ITU-T Recommendation Y.2171, Admission Control Priority Levels in Next Generation Networks, September 2006.

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at: < http://www.atis.org/glossary>.

3.1 Definitions

3.1.1 Advance Priority: The Access Network Signaling priority provided to an NGN GETS subscribed UE (including priority treatment before user invocation of NGN GETS), to improve the probability of an NGN GETS invocation being successfully sent to the Core Network.

3.1.2 NGN GETS Credentials: Credentials assigned to an authorized Service User that can be used to authenticate an NGN GETS invocation from any UE, regardless of whether or not the Service User has an NGN GETS subscription with the Service Provider (although this assumes the UE has a regular subscription for the comparable non-priority service).

3.1.3 NGN GETS subscribed UE: A UE associated with Subscription Credentials.

3.1.4 Public UE: A UE not associated with Subscription Credentials.

3.1.5 Service Provider: With initial capital letters, a Service Provider is a public telecommunications service provider authorized to provide ETS (Legacy GETS, WPS, and/or NGN GETS). When “service provider” (without initial capital letters) is used, it refers to the normal provider of telecommunications services.

3.1.6 Service User: With initial capital letters, a Service User is an individual authorized to use ETS (Legacy GETS, WPS, or NGN GETS) and to whom a user priority level assignment has been granted. When “service user” (without initial capital letters) is used, it refers to the normal user of telecommunication services.

[4] These documents are available from the International Telecommunications Union at: < http://www.itu.int/ITU-T/ >.

3.1.7 Service User's priority level: A number from one to five where one has the highest priority for ETS (Legacy GETS, WPS, or NGN GETS) services and five has the lowest priority for ETS (Legacy GETS, WPS, or NGN GETS) services. The Service User's priority level is assigned to a Service User.

3.1.8 Subscription Credentials: Credentials assigned by a Service Provider to a Service User who has a subscription to NGN GETS with the Service Provider, and allow the Service User to successfully invoke NGN GETS using subscription-based authentication without having to submit NGN GETS Credentials.

3.2 Acronyms & Abbreviations

3G	3rd Generation
3GPP	3rd Generation Partnership Project
3PCC	Third-Party Call Control
A-SBG	Access Session Border Gateway
AAA	AA-Answer
AAR	AA-Request
ACC	Automatic Congestion Control
ACG	Automatic Code Gap
ACM	Address Complete Message
AF	Application Function
ANM	Answer Message
ANS	American National Standard
ANSI	American National Standards Institute
ARP	Allocation and Retention Priority
AS	Application Server
ASA	Abort-Session-Answer
ASCII	American Standard Code for Information Interchange
ASR	Abort-Session-Request
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute Value Pair
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
CAC	Call Admission Control
CCA	CC-Answer
CCR	CC-Request
CDR	Charging Data Record
CNAM	Calling Name
COS	Class Of Service
CPC	Calling Party's Category
CPG	Call Progress
CS	Circuit Switched
CSCF	Call Session Control Function
DiffServ	Differentiated Services
DN	Directory Number
DNS	Domain Name System
DRMP	Diameter Routing Message Priority

DSCP	DiffServ Code Point
DTMF	Dual Tone Multi-Frequency
eCNAM	Enhanced Calling Name
ENUM	E.164 Number Mapping
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETS	Emergency Telecommunications Service
ETSI	European Telecommunications Standards Institute
FC	Feature Code
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FE	Functional Entity
FQDN	Fully Qualified Domain Name
GETS	Government Emergency Telecommunication Service
GETS-AN	GETS-Access Number
GETS-FC	GETS-Feature Code
GETS-NT	GETS-Number Translation
GETS-PDN	GETS-Pseudo Destination Number
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
H-PCRF	Home Policy and Charging Rules Function
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I-CSCF	Interrogating CSCF
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
iFC	initial Filter Criteria
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
IXC	Interexchange Carrier
LIA	Location-Info-Answer
LIDB	Line Information Database
LIR	Location-Info-Request
LSP	Label-Switched Path
LTE	Long Term Evolution
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request

MCC	Machine Congestion Control
MFA	Management Functional Area
MGW	Media Gateway
MGCF	Media Gateway Control Function
MLPP	Multi-Level Precedence and Pre-emption
MPLS	Multi-Protocol Label Switching
MPS	Multimedia Priority Service (3GPP)
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MTP	Message Transfer Part
NANP	North American Numbering Plan
NE	Network Equipment
NGN	Next Generation Network
NNI	Network-to-Network Interface
NPA	Numbering Plan Area
NS/EP	National Security and Emergency Preparedness
OAM&P	Operations, Administration, Maintenance, and Provisioning
OM	Operational Measurement
OS	Operations System
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PHB	Per-Hop Behavior
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PNA	Push-Notification-Answer
PNR	Push-Notification-Request
PPA	Push-Profile-Answer
PPR	Push-Profile-Request
PS	Packet Switched
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
QCI	QoS Class Identifier
QoS	Quality of Service
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
RFC	Request For Comment
RPH	Resource-Priority Header
RTA	Registration-Termination-Answer
RTP	Real-time Transport Protocol
RTR	Registration-Termination-Request
S-CSCF	Serving CSCF
SAA	Server-Assignment-Answer

SAR	Server-Assignment-Request
SBC	Session Border Controller
SCCP	Signaling Connection Control Part
SCIM	Service Capability Interaction Manager
SCTP	Stream Control Transmission Protocol
SDO	Standards Development Organization
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SGW	Signaling Gateway
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscription Locator Function
SPR	Subscription Profile Repository
SS7	Signaling System No. 7
TA	Terminal Adapter
TCAP	Transaction Capability Application Part
TDM	Time-Division Multiplexing
TMN	Telecommunication Management Network
TrGW	Transition Gateway
TS	Technical Specification
UAA	User-Authorization-Answer
UAR	User-Authorization-Request
UDA	User-Data-Answer
UDR	User-Data-Request
UE	User Equipment
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
V-PCRF	Visited Policy and Charging Rules Function
VoIP	Voice over IP
WPS	Wireless Priority Service

4 Reference Architecture

This Clause references the IMS Core Network architecture for specifying the network element requirements in support of ETS. Clause 4.1 describes the IMS Core Network architecture. Clause 4.2 describes the Functional Entities (FEs). Clause 4.2.17 describes the interfaces associated with the IMS Core Network architecture for this Standard.

4.1 IMS Core Network Architecture

Figure 4.1 illustrates the IMS Core Network architecture notated by the bolded FEs and dotted interfaces within the overall reference architecture. This reference architecture is based on the 3GPP IMS and PCC Release 11 Architectures (specified in [TS 23.002], [TS 23.228], and [TS 23.203]) with certain modifications adopted from the ATIS NGN Architecture. These modifications include an additional FE (Signaling Gateway [SGW]) and interface (A1), as illustrated in Figure 4.1, that are not specified in the 3GPP IMS Release 11 architecture. The IP-Access Network defines the Access Network technologies connecting users to the IMS Core Network, supporting public and NGN GETS services. IP-Access Network makes use of different access technologies (e.g., cable, wireless, DSL, routers, etc.). The IP Core Network provides the IP transport for both signaling and media bearer, and transport associated functions (e.g., packet routing, signaling, and management).

The IMS Core Network architecture illustrates the logical separation of Application Service, Signaling/Control, and Transport layers. These independently controlled layers (with control linkages between layers, i.e., vertical interfaces) facilitate a wide spectrum of services (e.g., voice, data, video, messaging, and multimedia) and features offered over the common packet-based IP Core Network. The architecture also provides flexibility in interconnecting to other service providers and third party service/application providers.

The IMS Core Network architecture FEs and interfaces, outlined (bolded) and shaded, are specified in this Standard, in support of NGN GETS. Signaling between FEs is shown as either dotted (in scope) or dashed (out of scope). For example, the dashed line between non-IP User Equipment (UE) to the IP-Access Network is outside the scope of this Standard. The Standard includes support for multiple Application Servers (ASs). Though the Service Broker is not shown as a separate FE in this architecture, it may be required to support multiple Application Servers. A Service Broker can provide service distribution, coordination, and control functions between Application Servers, Media Servers, and application platforms that may use different technologies, in addition to service interactions. Thus, a Service Broker can allow control of applications in conjunction with their media resources to create enhanced services. A Service Broker can reside in an AS.

NOTE: In the 3GPP IMS Release 11 architecture, the Service Broker, referred to as a “Service Capability Interaction Manager” (SCIM), is not specified as a separate entity.

3GPP and other SDOs do not specify network elements, but FEs. The IMS architecture defines a collection of FEs and associated interfaces. Service Providers will use various strategies in their deployment of IMS capabilities. Implementations may combine FEs into a single network element; or a single FE may be instantiated into two or more network elements. Only those aspects of the FEs and interfaces that are relevant for NGN GETS are specified in this Standard.

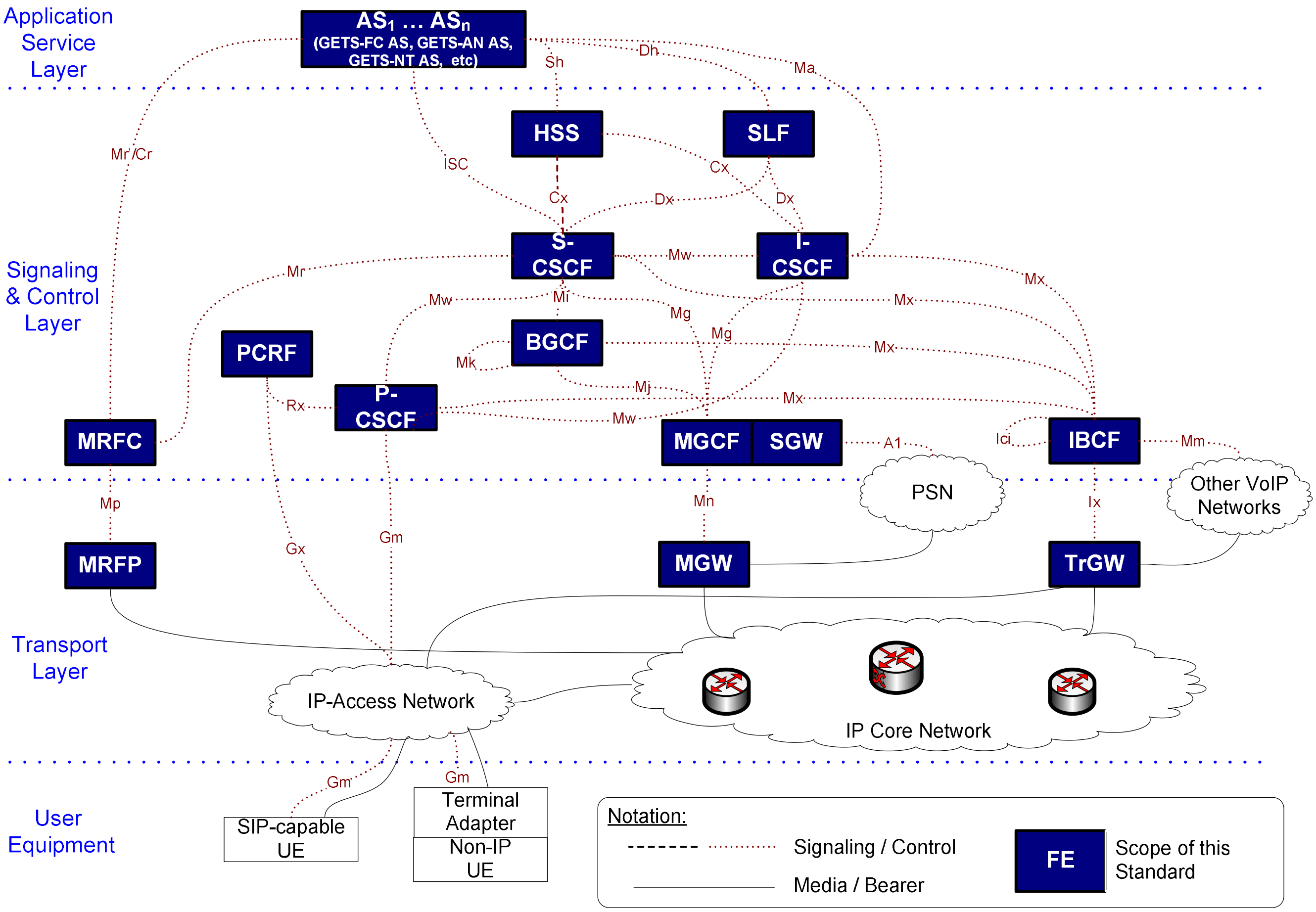

Figure 4.1 – IMS Core Network Architecture within ETS Reference Architecture

NOTE 1: This Standard assumes interconnection to "Other VoIP Networks" is provided via an Interconnection Border Control Function (IBCF).

NOTE 2: The interface between a Media Gateway Control Function (MGCF) and an SGW has not been specified by 3GPP. As specified in the 3GPP IMS Release 11 Architecture, the SGW functionality may be provided within the MGCF.

4.2 Functional Entities

The reference architecture presented in Clause 4.1 contains FEs as described in the subclauses that follow.

FE-specific requirements are provided in Clause 5.3; common requirements are provided in Clause 5.2.

FE-Specific Operations, Administration, Maintenance, and Provisioning (OAM&P) requirements are provided in Clause 6.3; common OAM&P requirements are provided in Clause 6.2.

4.2.1 Application Server (AS)

An AS executes service logic associated with value-added services including NGN GETS applications. The AS can communicate with a number of FEs, including the Home Subscriber Server (HSS), Serving Call Session Control Function (S-CSCF), and Interrogating CSCF (I-CSCF). In addition, an AS can communicate with other ASs in support of value-added services.

For details, refer to [TS 23.002] and [TS 23.228].

Whereas various service control architectures are permitted, this Standard references a (set of) functionally-separate NGN GETS AS(s), labeled as GETS-Feature Code (GETS-FC) AS, GETS-Access Number (GETS-AN) AS, and GETS-Number Translation (GETS-NT) AS. This labeling is not intended to imply that these applications must be deployed on separate AS platforms. Common NGN GETS platform(s) may be used to support multiple (potentially all) of the above NGN GETS call/session types. Alternately, these NGN GETS applications may be deployed on platforms that are shared with other (e.g., general telephony) applications.

A GETS-FC AS, GETS-AN AS, or GETS-NT AS will process an NGN GETS call/session for a GETS-FC, GETS-AN, or GETS-NT invocation, respectively. These ASs provide application-specific functions, using the Session Initiation Protocol (SIP)/ Session Description Protocol (SDP) and Diameter protocols on the interfaces.

An NGN GETS AS will access NGN GETS Credentials and/or GETS Translation information, as appropriate. Corresponding information may be stored locally to the NGN GETS AS, or may reside externally. This Standard assumes that such information is maintained locally to the NGN GETS AS.

- NGN GETS Credentials information for the GETS-AN and GETS-NT services includes the Service User’s PIN, priority level, and calling privileges. The GETS-AN AS and GETS-NT AS have access to NGN GETS Credentials information.
- GETS Translation information provides number translation for a GETS-NT-invoked call/session. It also provides GETS-Pseudo Destination Number (GETS-PDN) number translation for a GETS-AN call/session when the DN is a GETS-PDN. A GETS-NT AS has access to GETS Translation information.

4.2.2 Breakout Gateway Control Function (BGCF)

A BGCF identifies a network used for connecting an NGN GETS call/session to the Public Switched Network (PSN). If an S-CSCF determines that a destination address is in the PSN, the S-CSCF forwards the NGN GETS call/session request to a BGCF. Based on further analysis of the destination address and on agreements between Service Providers for PSN termination, the BGCF either selects a local MGCF to perform the termination or forwards the request, via an IBCF, to a BGCF in another Service Provider’s network that selects an MGCF to perform the termination.

For NGN GETS, a BGCF recognizes an NGN GETS call/session and provides priority treatment for NGN GETS call/session signaling and processing.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.3 Call Session Control Function (CSCF)

This Standard focuses on three variants of a CSCF: a Proxy CSCF (P-CSCF), a Serving CSCF (S-CSCF), and an Interrogating CSCF (I-CSCF).

- A P-CSCF is the first point of contact within the Service Provider network for signaling from a UE, via an IP-Access Network. It forwards the call/session requests received from the UE to an S-CSCF and may maintain session states. The P-CSCF maintains call/session state for an NGN GETS call/session.
- An S-CSCF handles functionality related to the NGN GETS call/session control, e.g., call/session processing (call/session setup, modification, and teardown), and routing. An S-CSCF has access to the user subscription data and is involved in processing the NGN GETS call/session request. It may maintain the call/session state, and perform the following functions:
    - Service triggering: Based on an analysis of the NGN GETS call/session control messages (based on initial Filter Criteria [iFC]), it can route the NGN GETS call/session control messages to an appropriate AS.
    - Determination of routing of the NGN GETS call/session control messages: It can determine the routing for the NGN GETS call/session control messages based on information available to it from the appropriate databases (e.g., Domain Name System [DNS]/E.164 Number Mapping [ENUM]).
- Within the Service Provider network, an I-CSCF may locate an S-CSCF associated with the terminating UE. An I-CSCF may be the first contact point within a Service Provider network for incoming NGN GETS

call/session requests from another Service Provider. These requests can be for a home subscriber or for a roaming subscriber. It performs the following functions:

- Obtaining from an HSS the address of an assigned S-CSCF.
- Forwarding an NGN GETS call/session request or response to an S-CSCF determined for that NGN GETS call/session.

During registration, an I-CSCF selects the S-CSCF within a Service Provider network.

For NGN GETS, the P-CSCF recognizes an NGN GETS call/session origination (GETS-AN, GETS-NT, and GETS-FC) and provides priority treatment to enhance the likelihood of NGN GETS call/session processing, including the NGN GETS call/session indication in signaling to other FEs.

For NGN GETS, the S-CSCF recognizes an originating NGN GETS call/session and directs the requests (based on either an iFC or DNS/ENUM response) to an AS for further processing. The S-CSCF applies priority to its processing and signaling. The iFC provides user based criteria that is downloaded from the HSS to the S-CSCF and is used to trigger AS processing based on specific conditions.

For NGN GETS, the I-CSCF recognizes an NGN GETS call/session, provides priority treatment to NGN GETS call/session processing and signaling, and selects an S-CSCF during registration and call/session termination.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.4 Domain Name System (DNS)/Telephone Number Mapping (ENUM)

DNS translates between the domain names and IP addresses. ENUM is one specific case of DNS where the “name” corresponds to an E.164 number. ENUM is used for mapping telephone numbers to Uniform Resource Identifiers (URI).

For NGN GETS, it is desirable to support priority treatment of DNS/ENUM queries. However, such priority treatment is outside the scope of this Standard.

4.2.5 Home Subscriber Server (HSS)

An HSS stores static and dynamic information for a subscriber. An HSS keeps a master list of features and services associated with a subscriber, and also the location and means of access to the subscriber. In addition, an HSS keeps information for UE registration and authentication.

For NGN GETS, an HSS stores the GETS-FC iFC for invoking the GETS-FC (via NGN GETS AS interactions) at the S-CSCF. For a GETS-FC subscription, the Service User’s priority level may be stored either in an HSS or a GETS-FC AS, based on the Service Provider implementation.

NOTE: If a Service User dials GETS-FC + GETS-AN or GETS-FC + GETS-NT, the subscription profile (Service User’s priority level and calling privileges) from the NGN GETS Credentials information takes precedence over the calling privileges in the HSS for the NGN GETS call/session being progressed from the GETS AS.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.6 Interconnection Border Control Function (IBCF)

An IBCF provides application-specific functions at the Session Initiation Protocol/Session Description Protocol (SIP/SDP) protocol layer in order to perform interconnection between two Voice over IP (VoIP) networks. It controls a Transition Gateway (TrGW). An IBCF enables communication between Internet Protocol Version 6 (IPv6) and Internet Protocol Version 4 (IPv4) networks, network topology hiding, controlling transport plane functions, protocol normalization, selecting the appropriate signaling for interconnection (e.g., SIP profile), and generation of charging data records.

For NGN GETS, an IBCF recognizes an NGN GETS call/session request arriving from another IP-based network, determines if the NGN GETS call/session is to be accepted based on interconnection agreements, and provides priority treatment to NGN GETS call/session processing and signaling, as appropriate. For an outgoing NGN GETS call/session, an IBCF forwards the requests to an interconnected network for further processing. The IBCF maintains call/session state for an NGN GETS call/session. This Standard assumes that an I-CSCF does not act as a network entry/exit point but relies on the IBCF. The IBCF and I-CSCF may be co-located for an implementation. For details, refer to [TS 23.002].

4.2.7 IP-Access Network

IP-Access Network is a collection of network access entities and interfaces that provides the underlying IP transport connectivity and signaling between a UE and an IMS Core Network. Examples of IP-Access Networks include cable, Digital Subscriber Line (DSL), and Evolved Packet System (EPS).

For NGN GETS, an IP-Access Network responds to instructions from a Policy and Charging Rules Function (PCRF) to reserve and establish appropriate access resources for handling the NGN GETS call/session and to apply access priority treatment, including marking bearer packets for priority treatment.

4.2.8 IP Core Network

The IP Core Network is the common transport resource used for all services provided by the Service Provider. The IP Core Network can include different types of routers: edge routers, core routers, and border routers (not shown in Figure 4.1). An edge router within an IP-Access Network routes IP packets between a UE and the Service Provider network. A core router transmits IP packets between other routers. A core router also routes IP packets between IMS FEs, and between an edge router and an FE, and between a border router and an FE. Border routers route IP packets between Service Provider networks.

For service differentiation among customers and for multi-service networks that support various traffic types with different QoS requirements, a Service Provider can use various mechanisms for management of traffic and QoS. Such mechanisms apply in the IP Core Network and at network edges (i.e., between IP-Access Network and the IP Core Network, and between two Service Provider networks).

The following are some example traffic management mechanisms that a Service Provider can use to provide priority treatment for NGN GETS Voice traffic (signaling and voice packets):

1. Traffic conditioning: traffic classification, packet filtering and policing
2. Packet marking (DiffServ) and Per-Hop Behavior (PHB): VOICE-ADMIT DiffServ Code Point (DSCP) is being defined for a class of traffic that is subject to strict Call Admission Control (CAC) and includes NGN GETS Voice traffic ([RFC 5865]).
3. Admission control: NGN GETS call/session can be provided priority admission to a Service Provider network ([ATIS-0100003], [Y.2171], and [RFC 6401]).
4. Bandwidth reservation and allocation using various types of Multi-Protocol Label Switching (MPLS) networks (e.g., DiffServ-aware MPLS, reserved Label-Switched Paths (LSPs) for NGN GETS Voice traffic).

A Service Provider can implement a combination of the above mechanisms to give an NGN GETS call/session a high likelihood of being successful, including both establishing and maintaining the NGN GETS call/session with the required QoS.

4.2.9 Media Gateway (MGW)

An MGW terminates bearer channels (i.e., trunks) from a CS network and media streams from a packet network (e.g., Real-time Transport Protocol [RTP] streams in an IP network). An MGW establishes and releases connections between these channels under control of an MGCF in support of calls/sessions between the PSN and an IP network. An MGW may support media conversion, bearer control, and payload processing (e.g., codec, echo canceller). An MGW interacts with an MGCF for resource control.

For NGN GETS, an MGW responds to instructions from an MGCF designating an NGN GETS call/session to be given priority treatment, including marking bearer packets for priority treatment and applying priority treatment features (e.g., trunk queuing in the PSN for an NGN GETS call/session).

For details, refer to [TS 23.002] and [TS 23.228].

4.2.10 Media Gateway Control Function (MGCF)

An MGCF within a Service Provider network provides signaling interconnection for NGN GETS call/session requests to/from a PSN, and controls an MGW in establishing the media connections. It communicates with CSCF, BGCF, and PSN entities. An MGCF performs protocol conversion between Signaling System No. 7 (SS7) ISUP and SIP, and maintains call/session states.

For NGN GETS Voice service, an MGCF performs the signaling translation of SIP NGN GETS priority information to and from the SS7 ISUP GETS priority information. An MGCF recognizes an incoming NGN GETS call/session from the ISUP GETS priority information or dialed digits (i.e., GETS-AN or GETS-NT) and provides priority treatment in call/session processing and signaling. Similarly, an outgoing NGN GETS call/session to the legacy network is provided priority treatment. An MGCF provides the priority indication to a SGW for SS7 priority indication; and to an MGW for IP priority indication.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.11 Multimedia Resource Function Controller (MRFC)

An MRFC controls the media stream resources in the MRFP under direction from an S-CSCF or AS. An MRFC interprets NGN GETS call/session information coming from an AS or S-CSCF and controls the MRFP accordingly.

For NGN GETS Voice service, an MRFC applies priority treatment in NGN GETS call/session processing and signaling for GETS-AN and GETS-NT PIN collection, and for GETS-AN DN collection.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.12 Multimedia Resource Function Processor (MRFP)

An MRFP provides media resources under the direction of the MRFC. It may generate media streams (e.g., multimedia announcements), mix incoming media streams for multiple parties, process media streams (e.g., audio transcoding, media analysis), or manage access rights to shared resources in a conferencing environment.

For NGN GETS Voice service, an MRFP applies priority treatment based on instruction from an MRFC, and associated GETS AS, to provide media resources as necessary for GETS-AN and GETS-NT user interactions (i.e., digit collection, announcements) and for other features or services identified for NGN GETS.

For NGN GETS, the MRFP also performs the digit collection functions.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.13 Policy and Charging Rules Function (PCRF)

A PCRF encompasses IP-Access Network policy control decisions and data/media flow-based charging control functionalities. It provides IP-Access Network control regarding the media/data flow detection, gating (e.g., admission control), QoS, and media/data flow-based charging. The PCRF provides management of IP-Access Network QoS resources necessary to support services to network users. It communicates with the IP-Access Network FEs (e.g., Gateway GPRS Support Node [GGSN], Packet Data Support Node [PDSN]) to provide authorization of resource allocations. It enforces policy decisions with regard to use of the IP-Access Network QoS resources, including consideration of Service Level Agreements (SLAs).

For NGN GETS, a PCRF implements IP-Access Network admission control policies to give an NGN GETS call/session a high likelihood of being successful, including both establishing, maintaining, and terminating the NGN GETS call/session in the IP-Access Network.

This Standard assumes a PCRF either contains or can access a Subscriber Profile Repository (SPR). Within this Standard, the term PCRF also refers to a combined PCRF/SPR.

For details, refer to [TS 23.203].

4.2.14 Signaling Gateway (SGW)

An SGW performs the signaling conversion (both ways) at the transport level between the SS7 based transport of signaling and the IP based transport of signaling (e.g., between SIGTRAN Stream Control Transmission Protocol [SCTP]/IP and SS7 Message Transfer Part [MTP]).

For NGN GETS Voice service, an SGW recognizes GETS-related priority markings and performs the appropriate transport level interworking between the SS7-based transport of signaling and the IP-based transport of signaling to support priority treatment across both network types.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.15 Subscription Locator Function (SLF)

An SLF is:

- Queried by the I-CSCF during the Registration and Session Setup to get the address of the HSS containing the required subscriber-specific data. Furthermore the SLF is also queried by the S-CSCF during the Registration.
- Queried by an AS to get the address of the HSS containing the required subscriber-specific data.

An SLF is not required if a Service Provider network only has a single HSS. An SLF may be required for NGN GETS call/session termination.

For NGN GETS, the SLF recognizes queries identified as NGN GETS-related and applies priority in processing such queries and signaling the results.

For details, refer to [TS 23.002] and [TS 23.228].

4.2.16 Transition Gateway (TrGW)

A TrGW is located within the media path and controlled by an IBCF. It provides functions like network address/port translation and IPv4/IPv6 protocol translation.

For NGN GETS Voice service, a TrGW recognizes NGN GETS priority markings in bearer packets, provides priority treatment in processing, and performs the appropriate protocol interworking to preserve the priority markings.

For details, refer to [TS 23.002].

4.2.17 Number Portability & Supplementary Services

The establishment and completion of an NGN GETS session may involve queries and responses for number portability and supplementary services. This may involve queries and responses to databases such as, but not limited to:

- Number Portability Databases [ATIS-1000003].
- Enhanced Calling Name (eCNAM) Databases [ATIS-1000067].
- Line Information Databases (LIDB).
- Calling Name (CNAM) Databases.
- Supplementary Services Databases.

Regardless of how number portability and supplementary services are supported in the NGN (e.g., use of Application Servers or SS7 over IP to databases) there is a need to ensure that NGN-GETS sessions are not negatively impacted when number portability or supplementary services are involved in an NGN GETS session. Therefore, it is an objective that priority treatment be provided to the number portability or supplementary services queries and responses when associated with an NGN GETS session. It is recognized that number portability and supplementary services databases may not have any explicit protocol information indicating that a particular query message is associated with an NGN GETS call/session. The only information that might be available is the priority information in the IP or transport (e.g., DSCP or Ethernet COS values) protocol in the received message, which could be used for the response messages if possible.

NOTE 1: ENUM is covered in Clause 4.2.4.

NOTE 2: SS7 requirements for number portability and supplementary services queries/responses associated with ETS are specified in [ATIS-1000006].

4.3 Interfaces

This Clause is informative and paraphrases information that is described in more detail in IMS and other relevant specifications. It is provided for information to support the ETS Node Element requirements. This Clause also provides illustrations of possible protocol choices for the requirements specified in this Standard.

This Clause provides the protocols, messages, and parameters for the signaling interfaces between the FEs in the IMS Core Network to support NGN GETS. All interfaces, as described in this Clause, are shown in Figure 4.1.

NOTE: Each interface in this Clause may have a protocol priority specification for FE call/session processing and a corresponding priority mechanism for the transport of the signaling messages between the FEs. Details on the priority marking of the IP packets carrying signaling and bearer are specified in Clauses 5 and 6.

4.3.1 SIP-Based Interfaces

This Clause lists the SIP messages and headers used by the ISC, Mw, Mr, Mr', Mg, Mi, Mm, Gm, Mj, Mk, and Mx interfaces, including a reference to their respective specifications, and a short description of their usages within the interfaces in support of NGN GETS.

4.3.1.1 General Description

SIP may indicate a request for NGN GETS from the UE via the digits in the Request-URI. Within the IMS Core Network, SIP uses the RPH to indicate a request for priority network resources. The ets namespace in the RPH is used to indicate the NGN GETS call/session. The wps namespace in the RPH is used to indicate the Service User's priority level. The RPH with the ets (and possibly wps) namespace is part of the SIP INVITE request and other SIP messages throughout the active phase of the NGN GETS call/session. Based on Authorized Agency policy, all NGN GETS calls/sessions are assigned the ets namespace with the provisioned priority value of "0". The NGN GETS call/session is recognized by the presence of the ets namespace RPH value in the SIP message and accorded priority for resource reservation/assignment and priority treatment.

NOTE: The policy is to use the ets.0 for NGN GETS and the ets.1 through ets.4 are reserved for future use. "y" in the wps.y is set based on the Service User's priority level.

Within the IMS Core Network architecture, SIP is used for call/session control between various IMS FEs. The profiles for these interfaces are in compliance with [TS 24.229]. In addition, SIP is also one of the protocols used between the MRFC and AS. For an NGN GETS call/session, this interface is used for PIN/DN interactions and for playing NGN GETS Voice related network announcements. The profile for this interface is in compliance with [ATIS-1000018.2007] and [ATIS-1000023.2013].

For an NGN GETS call/session, priority processing in the signaling and control plane is triggered by the presence of the RPH with the ets namespace, and possibly the wps namespace, in the SIP signaling messages. In addition for an NGN GETS call/session, the IMS Core Network requires priority transport of the signaling messages and priority transport for the user's bearer information (i.e., RTP packets). It is expected that for NGN GETS, the signaling and user bearer can use the same priority transport mechanisms (e.g., DiffServ Code Point, MPLS

Label Switched Path) in the IMS Core Network without negatively affecting service performance. Priority transport for the NGN GETS signaling provides not only reliable transport of the signaling messages but also, at each FE, facilitates the priority protocol processing (and buffering) of the received signaling messages up the protocol stack to the FE's application processing. This latter capability supports priority processing at each FE associated with an NGN GETS call/session, which is important during congestion or overload conditions.

4.3.1.1.1 SIP Messages

No new SIP messages are needed to support NGN GETS. SIP messages as defined in [TS 24.229], with the exception of OPTIONS and PUBLISH messages, can be used for NGN GETS. The following SIP messages can include an RPH with the ets namespace and the wps namespace for NGN GETS call/session signaling: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, and UPDATE.

The RPH with the ets namespace, and possibly the wps namespace, is also included in 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses associated with NGN GETS call/session signaling, with the exception of the 100 Trying and 403 Forbidden responses.

Within the SIP responses, the first digit of the Status-Code defines the class of response. The last two digits do not have any categorization role. For this reason, any response with a status code between 100 and 199 is referred to as a “1xx response”, any response with a status code between 200 and 299 is referred to as a “2xx response”, and so on. Most commonly used 1xx provisional responses include: 100 Trying, 180 Ringing, 182 Call Queued, and 183 Session Progress.

The coding of the Request-URI uses the sip:URI or tel:URI to carry the DN in the INVITE.

4.3.1.1.2 SIP Headers & Fields

The SIP headers and fields defined in [TS 24.229] can be used for NGN GETS. The following SIP headers and fields (as defined in [RFC 4412]), using the ets namespace, and possibly the wps namespace, are used to support NGN GETS:

- Resource-Priority header – The Resource-Priority request header field marks a SIP request as desiring prioritized access to resources.
- Accept-Resource-Priority header – The Accept-Resource-Priority response header field enumerates the resource values (r-values), i.e., the namespaces and associated priority values, that can be processed.

The syntax of the Resource-Priority header field is as follows:

```
Resource-Priority = "Resource-Priority" HCOLON r-value *(COMMA r-value)

r-value = namespace "." r-priority

namespace = token-nodot

r-priority = token-nodot

token-nodot = 1*( alphanum / "-" / "!" / "%" / "*" / "_" / "+" / "`" / "'" / "~" )
```

The 'r-value' parameter in the Resource-Priority header field indicates the resource priority desired by the request originator. Each resource value (r-value) is formatted as 'namespace' '.' 'priority value'. The priority value is drawn from the namespace identified by the 'namespace' token. Namespaces and priorities are case-insensitive American Standard Code for Information Interchange (ASCII) tokens that do not contain periods. Each namespace has at least one priority value.

The format of the RPH field can be as follows:

```
Resource-Priority: namespace1.value1, namespace2.value2, ...
```

or

```
Resource-Priority: namespace1.value1
Resource-Priority: namespace2.value2
```

or

```
Resource-Priority: namespace1.value1, namespace3.value3
Resource-Priority: namespace2.value2, ...
```

For NGN GETS, the RPH is coded as follows:

ets.x, where x = 0 and wps.y, where y (0 to 4) corresponds to Service User’s priority level. The y values 0 to 4 correspond to the Service User’s priority level 1 to 5.

The syntax of the Accept-Resource-Priority header field is as follows:

```
Accept-Resource-Priority = "Accept-Resource-Priority" HCOLON [r-value
*(COMMA r-value)]
```

For details of the Resource-Priority and Accept-Resource-Priority header fields, refer to [RFC 4412].

NOTE: Handling and processing of other namespaces in the RPH is in accordance with [RFC 4412].

The mapping between the Service User’s priority level and the SIP RPH (r-priority value in wps namespace) value is shown in Table 4.1.

Table 4.1 – Mapping between Service User’s Priority Level and RPH

Service User’s Priority Level	SIP RPH (r-priority value in wps namespace)
1	0
2	1
3	2
4	3
5	4

4.3.1.2 S-CSCF – AS Interface (ISC)

The S-CSCF – AS interface is identical to the ISC reference point defined in [TS 23.002] and [TS 23.228].

This interface between an S-CSCF and an AS provides services in the IMS Core Network.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.3 CSCF – CSCF Interface (Mw)

The CSCF – CSCF interface is identical to the Mw reference point defined in [TS 23.002] and [TS 23.228].

This interface carries signaling messages between CSCFs, e.g., during registration and NGN GETS call/session control.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.4 S-CSCF – MRFC Interface (Mr)

The S-CSCF – MRFC interface is identical to the Mr reference point defined in [TS 23.002] and [TS 23.228].

This interface allows interaction between an S-CSCF and a MRFC.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.5 MGCF – S/I-CSCF Interface (Mg)

The MGCF – S/I-CSCF interface is identical to the Mg reference point defined in [TS 23.002] and [TS 23.228].

This interface carries session signaling between a PSN and an S/I-CSCF for the purpose of interworking with the PSN.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.6 S-CSCF – BGCF Interface (Mi)

The S-CSCF – BGCF interface is identical to the Mi reference point defined in [TS 23.002] and [TS 23.228].

This interface carries the NGN GETS call/session signaling between an S-CSCF and a BGCF for the purpose of identifying a PSN for interworking.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.7 IBCF – Other IP Networks Interface (Mm)

The IBCF – Other IP Networks interface is identical to the Mm reference point defined in [TS 23.002] and [TS 23.228].

This interface is an IP interface between an IBCF and other IP networks. This interface is used for NGN GETS call/session control with another IP network using SIP.

This interface may carry NGN GETS-specific information in the Request-URI and RPH that may be used to trigger priority treatment.

> NOTE: When the S-CSCF or I-CSCF functionality is incorporated into a Service Provider’s implemented entity that provides interconnection with another IP network, the IBCF functionality also applies to that entity.

4.3.1.8 P-CSCF – UE Interface (Gm)

The P-CSCF – UE interface is identical to the Gm reference point defined in 3GPP [TS 23.002] and [TS 23.228].

This interface via IP-Access Network supports NGN GETS call/session control signaling between a UE and a P-CSCF.

This interface may carry NGN GETS-specific information in the Request-URI that is used to trigger priority treatment in the IMS Core Network, and possibly in the IP-Access Network.

4.3.1.9 BGCF – MGCF Interface (Mj)

The BGCF – MGCF interface is identical to the Mj reference point defined in [TS 23.002] and [TS 23.228].

This interface carries the NGN GETS call/session signaling between a BGCF and a MGCF for the purpose of interworking with the PSN.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.10 BGCF – BGCF Interface (Mk)

The BGCF – BGCF interface is identical to the Mk reference point defined in [TS 23.002] and [TS 23.228].

This interface allows a BGCF to exchange the NGN GETS call/session signaling with another BGCF in the same network.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.11 CSCF/BGCF – IBCF Interface (Mx)

The S-/I-/P-CSCF – IBCF interface and BGCF – IBCF interface is identical to the Mx reference point defined in [TS 23.002] and [TS 23.228].

This interface carries signaling messages between a CSCF and an IBCF, and a BGCF and an IBCF.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.1.12 MRFC – AS Interface for Session Control (Mr')

The MRFC – AS interface for session control uses the Mr' reference point as defined in [TS 23.002] and [TS 23.228].

This interface enables session control for interactions between an AS and a MRFC.

This interface carries NGN GETS-specific information in the Request-URI and RPH that is used to trigger priority treatment.

4.3.2 Diameter-Based Interfaces

This Clause describes the Diameter command-codes (messages) and Attribute-Value-Pairs (AVPs) (parameters) used by the Cx, Dx, Sh, Dh, Rx, and Gx interfaces, including a reference to their respective specifications, in support of NGN GETS.

See [TS 29.230] for an overview of 3GPP Diameter applications.

4.3.2.1 General Description

3GPP has specified 3GPP Diameter applications for the Cx, Dx, Sh, Dh, Rx, and Gx interfaces.

4.3.2.1.1 Diameter Messages

No new Diameter messages are needed to support NGN GETS.

4.3.2.1.2 Diameter AVPs

The Diameter Routing Message Priority (DRMP) AVP, as defined in [IETF draft-ietf-dime-drmp] and added in 3GPP Release 13 specifications, is used to indicate the relative priority of Diameter messages. The DRMP AVP contains a Diameter Routing Message Priority value that may be used by Diameter nodes for routing, resource allocation, and overload abatement decisions. It is allowed to be carried in Diameter responses as well as Diameter requests, to permit the answer message to have a different priority than the priority carried in the request message. The DRMP AVP has been added to the Cx, Dx, Sh, Dh, Rx, and Gx interfaces, in addition to other interfaces that are not in scope of this standard.

NOTE: This Standard does not require DRMP AVP to be included in any Diameter responses, since NGN GETS does not require the FEs with Diameter interfaces to set the priority of a Diameter answer message to a priority different than the priority carried in the request message.

A lower priority value implies a higher relative importance of the message. The DRMP AVP is type ENUMERATED, with values ranging from PRIORITY_0 (0) as the highest priority to PRIORITY_15 (15) as the lowest priority.

The Session-Priority AVP, as specified in [TS 29.229], is used to support NGN GETS. The Session-Priority AVP identifies an NGN GETS call/session and indicates to the FE receiving the Session-Priority AVP that priority treatment for signaling messages for that NGN GETS call/session applies. In addition, the Session-Priority AVP carries the Service User's priority level. The Session-Priority AVP is used on the Cx, Dx, Sh, and Dh interfaces.

The Session-Priority AVP is type ENUMERATED, with the following values: PRIORITY-0 (0), PRIORITY-1 (1), PRIORITY-2 (2), PRIORITY-3 (3), and PRIORITY-4 (4). PRIORITY-0 is the highest priority and PRIORITY-4 is the lowest priority.

This Standard does not require Session-Priority AVP to be included in Diameter response codes, since the FEs with Diameter interfaces are Diameter transaction stateful.

The mapping between the Service User's priority level and the Session-Priority AVP/DRMP AVP value is shown in Table 4.2.

Table 4.2 – Mapping between Service User's Priority Level & Session-Priority AVP/DRMP AVP Value

Service User's Priority Level	Session-Priority AVP Value	DRMP AVP Value
1	0	0
2	1	1
3	2	2
4	3	3
5	4	4

The MPS-Identifier AVP, as specified in [TS 29.214], is used to support NGN GETS. The MPS-Identifier AVP is included in the Diameter AA-Request (AAR) message (sent from the AF [e.g., P-CSCF] to the PCRF) to identify an NGN GETS call/session. The MPS-Identifier AVP is used on the Rx interface.

The MPS-Identifier AVP is of type OctetString, with the value "NGN GETS" defined for the NGN GETS Voice and NGN GETS Video services:

The PCRF differentiates between NGN GETS Voice and NGN GETS Video call/session requests via unique Media-Type AVP values (i.e., 'audio' and 'video') for each of these cases.

NOTE: The Reservation-Priority AVP, as specified in [TS 183.017] and referenced in [TS 29.214], is used to support NGN GETS. The Reservation-Priority AVP at the Diameter AAR level provides the priority level for the session while the Reservation-Priority AVP at the media-component-description level provides the priority level for an IP flow. If the Service User's priority level is not available, a default value is included in the Reservation-Priority AVP. The Reservation-Priority AVP is used on the Rx interface.

This Standard does not require the MPS-Identifier AVP or Reservation-Priority AVP to be included in Diameter response codes, since the FEs with Diameter interfaces are Diameter transaction stateful.

The recommended mapping between the Service User's priority level and the Reservation-Priority AVP value is shown in Table 4.3.

Table 4.3 – Mapping between Service User's Priority Level and Reservation-Priority AVP Value

Service User's Priority Level	Reservation-Priority AVP Value
1	15
2	14
3	13
4	12
5	11

NOTE: Values 0-10 of the Reservation-Priority AVP may not be used for NGN GETS.

The Priority-Level AVP (as part of the Allocation-Retention-Priority [ARP] AVP), as specified in [TS 29.212], is used to support NGN GETS. The Priority-Level AVP provides the priority level for an NGN GETS call/session. The Priority-Level AVP (as part of the ARP AVP) is used on the Gx interface.

The Priority-Level AVP is of type Unsigned 32. The Priority-Level AVP supports 15 priority levels that can be used to request priority treatment. Values between 1 and 15 are in decreasing order of priority with "1" being the highest and "15" the lowest. Priority values 1 to 8 are assigned for services that are authorized to receive prioritized treatment (i.e., NGN GETS). Priority value "0" is spare and treated as a logical error if received.

When the PCRF recognizes that a policy authorization request from an AF is associated with an NGN GETS call/session, it derives the Priority-Level AVP through a Service Provider-specific mapping algorithm and includes it in the Diameter RAR message. The Priority-Level AVP is derived using priority information received over the Rx interface (i.e., user priority level, priority indication, media type, etc.) and indicates the appropriate priority treatment that should be applied by the IP-Access Network. If a bearer needs to be established based on the QoS information received from the PCRF for an NGN GETS call/session, the QoS-Class-Identifier (QCI) AVP, as specified in [TS 29.212], is used to send the QoS information to the IP-Access Network for an NGN GETS call/session. No additional QCI AVP values other than the ones defined in [TS 29.212] are defined for NGN GETS. The QCI AVP is used on the Gx interface.

This Standard does not require the Priority-Level AVP or QCI AVP to be included in Diameter response codes, since the FEs with Diameter interfaces are Diameter transaction stateful.

4.3.2.2 HSS – S/I-CSCF Interface (Cx)

The HSS – S/I-CSCF interface is identical to the Cx reference point specified in [TS 29.228] and [TS 29.229].

This interface supports information transfer between an S/I-CSCF and an HSS.

The main procedures that require information transfer between an S/I-CSCF and an HSS are:

1. Procedures related to S-CSCF assignment.
2. Procedures related to routing information retrieval from an HSS to an S/I-CSCF.
3. Procedures related to authorization (e.g., checking of roaming agreement).
4. Procedures related to authentication: transfer of security parameters of the subscriber between an HSS and an S-CSCF.
5. Procedures related to filter control: transfer of filter parameters of the subscriber from an HSS to an S-CSCF.

This interface carries NGN GETS-specific information that can be used to trigger priority treatment:

- S-CSCF -> HSS: Diameter Server-Assignment-Request (SAR) message, which requests the HSS to store the name of the server that is currently serving the user. The DRMP AVP and/or Session-Priority AVP indicates to the HSS the priority of the message.
- HSS -> S-CSCF: Diameter Server-Assignment-Answer (SAA) message, which includes the initial Filter Criteria (iFC) in the User-Data AVP for NGN GETS.

- I-CSCF -> HSS: Diameter Location-Info-Request (LIR) message for NGN GETS Mobile Termination. The DRMP AVP and/or Session-Priority AVP indicates to the HSS the priority of the message.

4.3.2.2.1 Diameter Messages

The following messages are used for NGN GETS: User-Authorization-Request (UAR), User-Authorization-Answer (UAA), Server-Assignment-Request (SAR), Server-Assignment-Answer (SAA), Location-Info-Request (LIR), Location-Info-Answer (LIA), Multimedia-Auth-Request (MAR), Multimedia-Auth-Answer (MAA), Registration-Termination-Request (RTR), Registration-Termination-Answer (RTA), Push-Profile-Request (PPR), and Push-Profile-Answer (PPA).

4.3.2.2.2 Diameter AVPs

In addition to the DRMP AVP and Session-Priority AVP, the following AVPs are used for NGN GETS:

- Public-Identity AVP contains the public identity of the Service User in the IMS Core Network. The syntax of this AVP corresponds either to a SIP URI (with the format defined in [RFC 3261] and [RFC 2396]) or a TEL URI (with the format defined in [RFC 3966]).
- User-Data AVP contains the user profile, which includes the iFC for GETS-FC. The iFC is carried in the SAA.

For more information, see [TS 29.229], clause 6.3.

4.3.2.3 S/I-CSCF – SLF Interface (Dx)

The S/I-CSCF – SLF interface is identical to the Dx reference point specified in [TS 29.228] and [TS 29.229].

This interface between an S/I-CSCF and an SLF is used to retrieve the address of an HSS which holds the user's subscription.

The Dx interface is always used in conjunction with the Cx interface. The Dx interface is based on Diameter. It is functionality implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the Public Identity from the received requests.

This interface carries NGN GETS-specific information that can be used to trigger priority treatment.

4.3.2.3.1 Diameter Messages

The Dx interface messages that are used for NGN GETS are as specified in Clause 4.3.2.2.1 (for the Cx interface).

4.3.2.3.2 Diameter AVPs

In addition to the DRMP AVP and Session-Priority AVP, the AVPs as defined in [TS 29.228] and [TS 29.229] are used for NGN GETS.

4.3.2.4 HSS – AS Interface (Sh)

The HSS – AS interface is identical to the Sh reference point specified in [TS 29.328] and [TS 29.329].

This interface is used for communication between an AS and an HSS.

This interface carries NGN GETS-specific information that can be used to trigger priority treatment:

- AS -> HSS: Diameter User-Data-Request (UDR) query to HSS for subscription information. The DRMP AVP and/or Session-Priority AVP indicates to the HSS the priority of the message.

- HSS ->AS: Diameter User-Data-Answer (UDA) response to provide the Service User's priority level for an NGN GETS call/session.

4.3.2.4.1 Diameter Messages

The following messages are used for NGN GETS: User-Data-Request (UDR), User-Data-Answer (UDA), Profile-Update-Request (PUR), Profile-Update-Answer (PUA), Subscribe-Notifications-Request (SNR), Subscribe-Notifications-Answer (SNA), Push-Notification-Request (PNR), and Push-Notification-Answer (PNA).

4.3.2.4.2 Diameter AVPs

In addition to the DRMP AVP and Session-Priority AVP, the following AVPs are used for NGN GETS:

- User-Identity AVP contains the IMS Public User Identity, Public Service Identity, or MSISDN of the Service User.
- User-Data AVP contains subscription information.

For more information, see [TS 29.329], clause 6.3.

Subscription data may be sent as (transparent) Repository Data, as specified in [TS 29.328].

4.3.2.5 AS – SLF Interface (Dh)

The AS – SLF interface is identical to the Dh reference point specified in [TS 23.228].

This interface is used to retrieve the address of the HSS that holds the Service User's subscription information.

This interface carries NGN GETS-specific information that can be used to trigger priority treatment.

4.3.2.5.1 Diameter Messages

The Dh interface messages that are used for NGN GETS are as specified in Clause 4.3.2.4.1 (for the Sh interface).

4.3.2.5.2 Diameter AVPs

In addition to the DRMP AVP and Session-Priority AVP, the AVPs as defined in [TS 29.328] are used for NGN GETS.

4.3.2.6 P-CSCF – PCRF Interface (Rx)

The P-CSCF – PCRF interface is identical to the Rx reference point specified in [TS 29.214].

This interface enables transport of application level session information from a P-CSCF to a PCRF. Such information includes, but is not limited to:

- Information to identify the service media/data flow for policy control and/or differentiated charging;
- Media/application bandwidth requirements for QoS control.

This interface carries NGN GETS-specific information that can be used to trigger priority treatment:

- P-CSCF -> PCRF: Diameter AA-Request (AAR) message. The MPS-Identifier AVP indicates to the PCRF the message is related to an NGN GETS call/session. The Reservation-Priority AVP, as described in Clause 4.3.2.1.2, provides the priority level.

4.3.2.6.1 Diameter Messages

The following messages are used for NGN GETS: AA-Request (AAR), AA-Answer (AAA), Re-Auth-Request (RAR), Re-Auth-Answer (RAA), Session-Termination-Request (STR), Session-Termination-Answer (STA), Abort-Session-Request (ASR), and Abort-Session-Answer (ASA).

4.3.2.6.2 Diameter AVPs

In addition to the DRMP AVP, MPS-Identifier AVP, and the Reservation-priority AVP, other AVPs as defined in [TS 29.214], clause 5.3, and clause 5.4, are also applicable to NGN GETS.

4.3.2.7 PCRF – IP-Access Network (Gx)

The PCRF – IP-Access Network interface is identical to the Gx reference point specified in [TS 29.212]. In [TS 29.212], a PCRF interfaces with a Policy and Charging Enforcement Function (PCEF) in an IP-Access Network.

This interface enables a PCRF to have dynamic control over the policy and charging functions within an IP-Access Network.

- This interface carries NGN GETS-specific information that can be used to trigger priority treatment, which includes priority transport in an IP-Access Network: PCRF -> IP-Access Network: Diameter Re-Auth-Request (RAR) message. The Priority-Level AVP (as part of the ARP AVP) provides the priority level for an NGN GETS call/session. If a bearer is to be established based on the QoS information received from the PCRF for an NGN GETS call/session, the QoS-Class-Identifier AVP is used to send the QCI information.

4.3.2.7.1 Diameter Messages

The following messages are used for NGN GETS: CC-Request (CCR), CC-Answer (CCA), Re-Auth-Request (RAR), and Re-Auth-Answer (RAA).

4.3.2.7.2 Diameter AVPs

In addition to the DRMP AVP, ARP AVP (which contains the Priority-Level AVP), and the QCI AVP, the AVPs as defined in [TS 29.212], clause 5.3 are used for NGN GETS.

4.3.2.8 H-PCRF – V-PCRF Interface (S9)

The S9 interface is specified in [TS 29.215]. It is used to support policy control in roaming scenarios involving a home Public Land Mobile Network (PLMN) and a visited PLMN. To support such roaming scenarios, the PCRF functionality is replaced with Home PCRF (H-PCRF) and Visited PCRF (V-PCRF) FEs, and the S9 reference point is added between the H-PCRF (in the home PLMN) and the V-PCRF (in the visited PLMN).

For a more complete understanding of the above processing, the following references may be used:

- [TS 23.203] provides architecture specifications for the S9 reference point.
- [TS 29.213] includes signaling flows for the S9 reference point.
- [TS 29.215] provides protocol specifications for the S9 reference point.

4.3.2.8.1 Diameter Messages

3GPP Release 11 supports two protocols over the S9 interface.

- The S9 protocol may be used over the S9 reference point to exchange PCC rules and QoS rules. In this case, the V-PCRF enforces visited operator policies concerning rules requested by the H-PCRF, and sends corresponding Diameter messages to the PCEF. The corresponding set of Diameter messages (notably the Diameter RAR/RAA and CCA/CCR messages as specified in Clause 5.5 of [TS 29.215]) are briefly described in Clause 4.3.2.7.1.

- The Rx protocol (discussed further in Clause 4.3.2.6) may be used over the S9 reference point to exchange service session information from the V-PCRF to the H-PCRF (when the AF is in the Visited PLMN). Clause 4.3.2.6.1 provides a brief description of these Diameter messages.

The S9 interface messages that are used for NGN GETS are as described in Clause 4.3.2.6.1 for the Rx protocol and Clause 4.3.2.7.1 for the S9 protocol.

4.3.2.8.2 Diameter AVPs

The Diameter AVPs that are used for NGN GETS are as described in Clause 4.3.2.6.2 for the Rx protocol and Clause 4.3.2.7.2 for the S9 protocol.

4.3.3 H.248-Based Interfaces

This Clause lists the H.248 commands and parameters used by the Mn, Mp, and Ix interfaces, including a reference to their respective specifications, and a short description of their usages within the interfaces in support of NGN GETS.

4.3.3.1 General Description

In the IMS Core Network architecture, H.248 is the protocol used between the controller and gateway functions: MGCF – MGW, MRFC – MRFP, and IBCF – TrGW. The profiles for these interfaces are in compliance with [H.248.1]. In the discussion below, the term “controller” refers to an MGCF, MRFC, or IBCF, and the term “gateway” refers to the associated MGW, MRFP, or TrGW.

4.3.3.1.1 H.248 Commands

No new H.248 Commands are needed to support NGN GETS. The Commands defined in [H.248.1] can be used for NGN GETS. Each of the commands enumerated below currently exists in [H.248.1]. The following messages are used with NGN GETS: Add, Modify, Subtract, Move, AuditValue, AuditCapabilities, Notify, and ServiceChange.

4.3.3.1.2 H.248 Parameters

No new H.248 parameters are needed to support NGN GETS. The parameters defined in [H.248.1] can be used for NGN GETS. To enable priority handling in a Service Provider network, the Priority indicator [H.248.1] is used with NGN GETS to enable priority treatment.

For an NGN GETS call/session, the Priority indicator carries the priority levels between the controller and gateway; it currently supports 16 levels of priority. The Priority indicator, which carries the Service User’s priority level, is used for a context in order to provide the gateway with information about a certain precedence handling. Priority 0 is the lowest priority and a priority of 15 is the highest priority. The Priority indicator (Section 6.1.1 of [H.248.1]) is encoded as per Annex A of [H.248.1] (priority) or Annex B of [H.248.1] (priority) context attribute.

For an NGN GETS call/session, the H.248.1 Priority indicator must be present. If the Service User’s priority level is not available, a default value is included in the Priority indicator.

NOTE: Per [H.248.81], the Priority indicator is optional and included over the H.248 interface only if the Service User’s priority level is received in the call control signaling (i.e., SIP/ISUP) at the controller (e.g., MGCF). This Standard specifies mandatory use of the Priority indicator for NGN GETS whenever an NGN GETS call/session is indicated with or without the presence of a priority level in call control signaling.

If a Service Provider uses DiffServ for prioritizing user plane traffic related to an NGN GETS call/session and if NGN GETS requires a specific NGN GETS DSCP marking, the controller can configure the gateway to apply a specific NGN GETS DSCP marking to the user data transport packets to indicate that the packets are of a higher priority than those for normal calls. The DSCP package is defined according to the DSCP property in [H.248.52].

NOTE: The Priority indicator can be used to derive Layer 2 QoS marking and trigger priority identification and priority treatment.

The mapping between the Service User's priority level value carried in the ISUP Precedence parameter and Service User's priority level value carried in the H.248.1 Priority indicator is shown in Table 4.4. Table 4.4 also shows the corresponding Service User's priority level.

Table 4.4 – Mapping between ISUP and H.248

ISUP Precedence Value	H.248.1 Priority Indicator Value	Service User's Priority Level
0	15	1
1	14	2
2	13	3
3	12	4
4	11	5

NOTE: Values 0-10 of the H.248.1 Priority indicator are not used.

The mapping between the Service User's priority level value in the wps namespace carried in the SIP RPH and Service User's priority level value carried in the H.248.1 Priority indicator is shown in Table 4.5. Table 4.5 also shows the corresponding Service User's priority level.

Table 4.5 – Mapping between SIP and H.248

SIP RPH wps Value	H.248.1 Priority Indicator Value	Service User's Priority Level
0	15	1
1	14	2
2	13	3
3	12	4
4	11	5

NOTE: Values 0-10 of the H.248.1 Priority indicator are not used.

The Priority indicator may be associated with ADD, MOVE, or MODIFY commands.

4.3.3.2 MGCF – MGW Interface (Mn)

The MGCF – MGW interface is identical to the Mn reference point defined in [TS 29.332].

This interface allows communication between a MGCF and a MGW for call/session requests to/from a PSN.

The H.248 protocol contains the Priority indicator [H.248.1] and Differentiated Services package [H.248.52] to trigger appropriate priority treatment at a MGW for an NGN GETS call/session. Priority values 11-15 of the Priority indicator are reserved for NGN GETS in [TS 29.332].

4.3.3.3 MRFC – MRFP Interface (Mp)

The MRFC – MRFP interface is identical to the Mp reference point defined in [TS 29.333].

This interface allows a MRFC to control media stream resources provided by a MRFP.

The H.248 protocol contains the Priority indicator [H.248.1] and Differentiated Services package [H.248.52] to trigger appropriate priority treatment at a MRFP for an NGN GETS call/session. Priority values 11-15 of the Priority indicator are reserved for NGN GETS in [TS 29.333].

4.3.3.4 IBCF – TrGW Interface (Ix)

IBCF – TrGW Interface (Ix) is identical to the Ix reference point defined in [TS 23.002] and [TS 23.228].

This interface is used by the IBCF to control the TrGW, e.g., to request network address translation information.

The H.248 protocol contains the Priority indicator [H.248.1] and Differentiated Services package [H.248.52] to trigger appropriate priority treatment at a TrGW for an NGN GETS call/session. Priority values 11-15 of the Priority indicator are reserved for NGN GETS in [TS 29.238].

4.3.4 HTTP/HTTPS-Based Interfaces

This Clause provides a general description of the HTTP/HTTPS protocol, and a short description of its usage within the Cr interface in support of NGN GETS.

4.3.4.1 General Description

In the IMS Core Network architecture, IETF HTTP and HTTPS protocols are used between the MRFC and AS.

For an NGN GETS Voice or NGN GETS Video call/session, the Mr’/Cr interface is used for PIN/DN interaction and playing NGN GETS voice-related network announcements. The profile for this interface is in compliance with HTTP.

4.3.4.2 MRFC – AS Interface for Media Control (Cr)

The MRFC – AS interface for media control is based on the Cr reference point defined in [TS 23.002] and [TS 23.218]. The AS provides remote prompts and scripts to the MRFC using the AS-MRFC Cr interface.

This interface enables the MRFC to interact with the AS for PIN, DN, and announcement information.

4.3.5 SS7-Based Interfaces

This Clause lists the SS7 messages and parameters used by the A1 interface, including a reference to the respective specification, and when needed, a short description of the usage within the interface in support of NGN GETS Voice service.

4.3.5.1 General Description

The standard ANSI SS7 (MTP [ATIS-1000111.2005], ISUP [ATIS-1000113.2005], SCCP [ATIS-1000112.2005], and TCAP [T1.114]) protocol is used.

4.3.5.2 MGCF/SGW – PSN (A1)

The MGCF/SGW – PSN (A1) interface is used for signaling between the MGCF/SGW and a PSN. This interface carries NGN GETS-specific information in the ISUP Calling Party’s Category and Precedence parameter that can be used to trigger priority treatment. The protocol used for this interface is SS7 (MTP, ISUP, and TCAP). The MTP priority of the SCCP and TCAP messages associated with a GETS call is set to 2.

4.3.5.2.1 ISUP Messages

For an NGN GETS call/session routed to a PSN, the ISUP Initial Address Message (IAM) sent by the MGCF/SGW is the same as the corresponding ISUP IAM message for a non-NS/EP call [ATIS-1000679] except with the following GETS-specific coding:

1. The Calling Party's Category parameter is coded with a value 11100010 (NS/EP Call).
2. The Precedence parameter is included only if the Service User's priority level is available. If included, the Precedence parameter is coded as shown in Table 4.6. In particular, the Precedence Level field is populated with a value of 0 through 4, corresponding to the Service User's priority level.
3. The MTP priority of the IAM is set to 1.

For an NGN GETS call/session routed to a PSN, the coding of the Calling Party's Category and Precedence parameters in the IAM are based on the coding of the received SIP INVITE request as shown in Table 5 5.

4.3.5.2.2 ISUP Parameters

For an NGN GETS call/session routed to a PSN, the Precedence parameter in the ISUP IAM message sent by the MGCF/SGW is populated as shown in Table 4.6. If the IAM received by the MGCF/SGW for a GETS or WPS call from a PSN includes the Precedence parameter, the Precedence parameter coding shown in Table 4.6 is expected.

Table 4.6 – Precedence Parameter Encoding

Field	Description	Value
Look Ahead for Busy	Indicates whether look ahead for busy is allowed or whether the path has been reserved	10 (Look Ahead for Busy not allowed)
Precedence Level	GETS calling user's priority level	0 through 4, based on GETS calling Service User's priority level: Service User's priority 1 = Precedence Level 0 Service User's priority 2 = Precedence Level 1 Service User's priority 3 = Precedence Level 2 Service User's priority 4 = Precedence Level 3 Service User's priority 5 = Precedence Level 4
Network Identity	Identifies the network or country which administers the service	0100 (indicating the U.S.A.)
MLPP Service Domain	GETS Service Domain	NCS Wireless Priority Service-1 (4194891) [0100 0000 0000 0010 0100 1011] NCS Wireless Priority Service-2 (4194892) [0100 0000 0000 0010 0100 1100] NCS Wireless Priority Service-3 (4194893) [0100 0000 0000 0010 0100 1101] NCS Wireless Priority Service-4 (4194894) [0100 0000 0000 0010 0100 1110]

		NCS Wireless Priority Service-5 (4194895) [0100 0000 0000 0010 0100 1111]

5 Functional Entity Requirements

5.1 Introduction

This Clause provides FE requirements for an IMS Core Network in support of NGN GETS. Both common requirements, which pertain to more than one FE, and FE-specific requirements are specified.

This material is organized as follows:

- Clause 5.1 – Introduction.
- Clause 5.2 – Common Requirements.
- Clause 5.3 – FE Specific Requirements.

5.1.1 Terminology

The following terminology is used in this Clause:

1. The term “provisioned ets.x” refers to the resource value (r-value) for the ets namespace in the RPH that is set by Authorized Agency policy and is provisioned as specified in Clause 6.
2. An “NGN GETS SIP-capable FE” is an FE that has NGN GETS SIP-related capabilities, including the ability to process the RPH with the ets and wps namespaces. An NGN GETS SIP-capable FE maintains the following information for the duration of a SIP dialog:
    - That a SIP dialog is associated with an NGN GETS call/session, and
    - The Service User’s priority level, if known.

    The wps.y r-value can be modified during a SIP dialog associated with an NGN GETS call/session (e.g., for an NGN GETS call/session invoked via GETS-FC + GETS-AN).
3. The term “Priority Treatment” is described in Clause 5.2.4.

5.1.2 Assumptions

The following assumptions apply:

- The IBCF is assumed to be the FE within the IMS Core Network bordering the NNI to an adjacent IP network. The IBCF can be combined with other FEs (e.g., I-CSCF) for implementations when interconnecting to another network at an NNI. When the IBCF functionality is incorporated into an entity that supports other FE capabilities, that entity must comply with all IBCF requirements in this Standard.

5.2 Common Requirements

This Clause specifies requirements that are applicable to multiple FEs within the IMS Core Network. FE-specific requirements are specified in Clause 5.3.

5.2.1 Common NGN GETS Requirements Applicable to NGN GETS SIP-capable FEs

The following FEs within the IMS Core Network are NGN GETS SIP-capable FEs:

- P-CSCF,

- S-CSCF,
- I-CSCF,
- NGN GETS AS (i.e., GETS-FC AS, GETS-AN AS, or GETS-NT AS),
- MRFC,
- IBCF,
- BGCF, and
- MGCF/SGW.

The common SIP requirements in this subclause address the general processing related to SIP RPH with the namespaces associated with NGN GETS. While these requirements apply to multiple NGN GETS SIP-capable FEs within the IMS Core Network, their applicability to specific FEs is identified in the corresponding FE-specific clauses. In addition, the FE-specific clauses identify the modifications or exceptions to the common requirements.

If an NGN GETS SIP-capable FE understands namespaces other than ets and wps, these requirements do not affect treatment based on those other namespaces.

5.2.1.1 Detection of an NGN GETS Call/Session

[63] An NGN GETS SIP-capable FE shall identify an NGN GETS call/session based on the presence of a Resource-Priority Header field (RPH) with either:

- **A valid ets.x r-value and no wps namespace in a SIP INVITE request, or**
- **A valid ets.x r-value and a valid wps.y r-value in a SIP INVITE request.**

When referring to RPH in the context of NGN GETS, the ets and wps namespaces specified in [RFC 4412] are relevant. For an NGN GETS call/session, the ets.x and possibly the wps.y are included in an RPH. The processing of other namespaces specified in [RFC 4412] is beyond the scope of this Standard, and those namespaces are processed according to [RFC 4412]. Identification of an NGN GETS call/session based on the SIP Request-URI is described in appropriate FE-specific subclauses.

[64] An NGN GETS SIP-capable FE shall accept the ets and wps namespaces as valid with only the following resource values:

- **For the ets namespace: ets.0, ets.1, ets.2, ets.3, or ets.4,**
- **For the wps namespace: wps.0, wps.1, wps.2, wps.3, or wps.4.**

The resource values listed in requirement [64] enable the NGN GETS SIP-capable FE to recognize and validate the resource values that it supports for NGN GETS call/session processing. The resource values listed in requirement [64] are also used to populate the Accept-Resource-Priority (ARP) header field, when used.

5.2.1.2 General Processing of SIP RPH & Related Header Fields

[65] For an NGN GETS call/session, when multiple namespaces are sent, an NGN GETS SIP-capable FE generating the RPH shall use one of the following formats in accordance with [RFC 4412]:

Resource-Priority: namespace1.value1, namespace2.value2, …

or

Resource-Priority: namespace1.value1
Resource-Priority: namespace2.value2

…

or

Resource-Priority: namespace1.value1, namespace3.value3

Resource-Priority: namespace2.value2, …

The following are examples of the RPH format for an NGN GETS call/session when only an ets namespace is sent or when only ets and wps namespaces are sent:

Resource-Priority: ets.0

or

Resource-Priority: ets.0
Resource-Priority: wps.3

or

Resource-Priority: ets.0, wps.3

The format in the last example is the preferred format when both the ets and wps namespaces are sent.

[389] For an NGN GETS call/session, it is desirable that an NGN GETS SIP-capable FE generating the RPH shall use the following format:

Resource-Priority: namespace1.value1, namespace2.value2, …

For an NGN GETS call/session, the Accept-Resource-Priority header field can be populated as follows:

Accept-Resource-Priority: ets.0, ets.1, ets.2, ets.3, ets.4, wps.0, wps.1, wps.2, wps.3, wps.4.

For an NGN GETS call/session, an NGN GETS SIP-capable FE includes the ‘resource-priority’ option tag in the Supported header field.

[501] For an NGN GETS call/session, an NGN GETS SIP-capable FE shall send the Supported header field with the 'resource-priority' option tag in the initial SIP INVITE request.

An errored ets or wps namespace in a SIP request is handled as specified in requirements [72] through [77].

5.2.1.3 Population of RPH in SIP Messages Sent

[67] For an NGN GETS call/session, an NGN GETS SIP-capable FE shall include the RPH when the FE sends the following SIP requests: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, and UPDATE. The RPH shall include ets.x, or ets.x and wps.y, where x is 0 to 4 and y is 0 to 4.

[68] For an NGN GETS call/session, an NGN GETS SIP-capable FE shall include the RPH when the FE sends the following SIP responses: 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses, with the exception of SIP 100 (“trying”) and SIP 403 (“forbidden”) responses. The RPH shall include ets.x, or ets.x and wps.y, where x is 0 to 4 and y is 0 to 4. For a SIP 400 (Bad Request) response with a 417 code in the Reason header field, the RPH shall include the provisioned ets.x and no wps namespace.

The population of ets.x and wps.y resource values, including FE-specific cases when the provisioned ets.x is used, are specified in the FE-specific subclauses.

NOTE: The RPH, containing appropriate ets.x and wps.y resource values, is intended to be included in SIP signaling when an NGN GETS call/session is forwarded. Service Providers need to support this capability (i.e., include the appropriate RPH) for any deployments of call forwarding that they support. For example, when an AS receives a SIP INVITE request, it may invoke call-forwarding by populating the forward-to DN in a SIP INVITE request, in order to route the SIP INVITE request to an alternate DN. For such an approach, the AS should include the RPH in the SIP INVITE request that is sent, populated as specified in requirement [67]. Other call-forwarding arrangements (e.g., using a SIP REFER request or a SIP 3xx response) may alternately be deployed by the Service Provider. The requirements for alternate arrangements not supported by requirements [67] and [68] are addressed on a case by case basis between the Authorized Agency and a Service Provider.

5.2.1.4 Validation of RPH Settings in SIP Messages Received

[72] through [76] pertain to the validation of RPH settings in any SIP request for an NGN GETS call/session.

[72] When an NGN GETS SIP-capable FE receives a SIP request with an RPH with multiple instances of the ets namespace (e.g., Resource-Priority: ets.0, ets.2), the FE shall reject the request with a SIP 400 (Bad Request) response with a 417 code in the Reason header field. The response shall include the RPH with the provisioned ets.x and without a wps namespace. The FE shall generate an error log entry containing the complete SIP request received, and the date and time of the error.

[73] When an NGN GETS SIP-capable FE receives a SIP request with an RPH with multiple instances of the wps namespace (e.g., Resource-Priority: ets.0, wps.2, wps.4), the FE shall reject the request with a SIP 400 (Bad Request) response with a 417 code in the Reason header field. The response shall include the RPH with the provisioned ets.x and without a wps namespace. The FE shall generate an error log entry containing the complete SIP request received, and the date and time of the error.

[74] When an NGN GETS SIP-capable FE receives a SIP request with an RPH with an invalid ets.x (e.g., Resource-Priority: ets.7), the FE shall reject the request with a SIP 400 (Bad Request) response with a 417 code in the Reason header field. The response shall include the RPH with the provisioned ets.x and without a wps namespace. The FE shall generate an error log entry containing the complete SIP request received, and the date and time of the error.

[75] When an NGN GETS SIP-capable FE receives a SIP request with an RPH with an invalid wps.y (e.g., Resource-Priority: ets.0, wps.9), the FE shall reject the request with a SIP 400 (Bad Request) response with a 417 code in the Reason header field. The response shall include the RPH with the provisioned ets.x and without a wps namespace. The FE shall generate an error log entry containing the complete SIP request received, and the date and time of the error.

[76] When an NGN GETS SIP-capable FE receives a SIP request with an RPH with wps.y and no ets.x (e.g., Resource-Priority: wps.4), the FE shall reject the request with a SIP 400 (Bad Request) response with a 417 code in the Reason header field. The response shall include the RPH with the provisioned ets.x and without a wps namespace. The FE shall generate an error log entry containing the complete SIP request received, and the date and time of the error.

When more than one of [72] to [76] applies for an NGN GETS call/session message, the response, error processing, and error logging may be based on the first error detected.

[77] When an NGN GETS SIP-capable FE receives a SIP ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, or UPDATE request or a SIP response with an RPH including an ets namespace for a call/session that was not initially recognized as an NGN GETS call/session, the FE shall:

1. **Use neither the ets nor wps namespaces in SIP requests and SIP responses associated with this call/session, and**
2. **Process the SIP requests and SIP responses associated with this call/session as for a normal call/session.**

The FE shall generate an error log entry containing the complete SIP request or response received that included an RPH with an ets namespace, and the date and time of the error.

5.2.2 Common NGN GETS Requirements Applicable to Diameter-capable FEs

The following FEs are Diameter capable:

- P-CSCF,
- I-CSCF,
- S-CSCF,
- PCRF,
- HSS,
- NGN GETS AS (e.g., GETS-FC AS, GETS-AN AS, or GETS-NT AS), and
- SLF.

With the introduction of the DRMP AVP in 3GPP Release 13, all Diameter-capable FEs support the following common Diameter requirement associated with NGN GETS processing related to the DRMP AVP.

[722] **When a Diameter-capable FE that supports the DRMP AVP sends a Diameter request message for an NGN GETS call/session, it shall include the DRMP AVP (populated as described in** Error! Reference source not found.**). The DRMP AVP shall be populated with a default value if the originating Service User's priority level is unknown.**

The DRMP AVP, as described in Clause 4.3.2.2.2, is of type ENUMERATED and contains information to indicate that priority processing is needed. The DRMP AVP values are mapped to the corresponding Service User's priority level as described in **Error! Reference source not found.**.

The default value (in the range 0 – 4) to be included in the DRMP AVP for an NGN GETS call/session should be based on Authorized Agency policy, and provisioned in the FE. The configuration requirement to set the default value is specified in [723].

If the DRMP AVP is included in a Diameter message for an NGN GETS call/session, then the message receives priority processing.

NOTE: This Standard does not require the DRMP AVP to be included in any Diameter responses, since NGN GETS does not require the FEs with Diameter interfaces to set the priority of a Diameter answer message to a priority different than the priority carried in the request message.

All Diameter-capable FEs, with the exception of the P-CSCF and PCRF, support the following common Diameter requirement associated with NGN GETS processing related to the Session-Priority AVP.

The Session-Priority AVP is specified in [TS 29.229], clause 6.3.56. It is of type ENUMERATED and contains information to indicate that priority processing is needed. If the Session-Priority AVP is included in a Diameter message for an NGN GETS call/session, then the message receives priority processing at the FE.

[503] **A Diameter-capable FE that provides a Cx, Dx, Sh, or Dh interface shall support the Session-Priority AVP for NGN GETS call/session processing. The Session-Priority AVP is type ENUMERATED, with the following values:**

- **PRIORITY-0 (0),**
- **PRIORITY-1 (1),**
- **PRIORITY-2 (2),**

- **PRIORITY-3 (3),**
- **PRIORITY-4 (4).**

PRIORITY-0 is the highest priority and PRIORITY-4 is the lowest priority.

NOTE: Support for the Session-Priority AVP could be omitted, assuming universal support for the corresponding DRMP AVP. However, the above requirement is retained for backwards compatibility reasons. If the DRMP AVP is supported in the future by all Diameter-capable FEs that provide a Cx, Dx, Sh, or Dh interface, then this requirement could potentially be deprecated.

The default value (in the range 0 – 4) to be included in the Diameter Session-Priority AVP should be based on Authorized Agency policy, and provisioned in the FE. The Diameter Session-Priority AVP priority values are mapped to the corresponding Service User's priority level as described in **Error! Reference source not found.**.

Diameter-capable FE processing requirements associated with the Session-Priority AVP are specified in FE-specific clauses. This Standard does not require Session-Priority AVP to be included in Diameter responses, since the FEs with Diameter interfaces are Diameter transaction stateful.

5.2.3 Common NGN GETS Requirements Applicable to H.248-capable FEs

The following FEs are H.248-capable FEs:

- IBCF,
- MGCF/SGW,
- MGW,
- MRFC,
- MRFP, and
- TrGW.

The common H.248 requirements in this subclause address the general processing related to the Priority indicator and [H.248.52] (for implementations using DiffServ) associated with NGN GETS. While these requirements apply to multiple H.248-capable FEs within the IMS Core Network, the specific FEs to which they apply are identified in the FE-specific clauses.

[81] For an NGN GETS call/session, an H.248-capable FE shall include the Priority indicator in the H.248 Add_Request and Modify_Request commands to indicate the Service User's priority level. See Table 4.4 and Table 4.5 for appropriate mapping.

[82] An H.248-capable FE shall encode the Priority indicator (Section 6.1.1 of [H.248.1]) as per Annex A of [H.248.1] (priority) or Annex B of [H.248.1] (priority) context attribute.

If a Service Provider uses DiffServ for prioritizing user plane traffic related to an NGN GETS call/session and if NGN GETS requires a specific NGN GETS DSCP marking, an H.248-capable FE (controller) can instruct a gateway to apply a specific NGN GETS DSCP marking. Configuration requirements related to the setting of DSCP are specified in Clauses 6.2.4, 6.3.4.1, and 6.3.11.

[671] If both the H.248-capable controller and gateway FEs support [H.248.52] and NGN GETS call/session requires a specific NGN GETS DSCP marking, an H.248-capable FE shall include the DiffServ Code Point in all the H.248 commands to allow a gateway to apply a specific NGN GETS DSCP marking to the signaling and bearer packets.

This Standard does not require the Priority indicator to be included in H.248 responses, since the FEs with H.248 interfaces are H.248 transaction stateful.

5.2.4 Common FE Priority Treatment Requirements

Priority treatment for an NGN GETS call/session applies to (a) call/session processing, (b) processing and transport of SIP, Diameter, H.248, and HTTP signaling messages related to the call/session, and (c) processing and transport of media (RTP) packets related to the call/session. Priority treatment for NGN GETS call/session processing includes (1) exemption of NGN GETS calls/sessions and related signaling messages from Machine Congestion Control (MCC) and (2) priority Call Admission Control (CAC) for NGN GETS calls/sessions. In addition, priority treatment for NGN GETS includes enhanced call/session routing capabilities beyond those provided for normal calls/sessions. Specific priority treatment mechanisms are described throughout this Standard.

This clause specifies FE requirements for NGN GETS call/session priority treatment for processing and transport of SIP (Clauses 5.2.4.1, 5.2.4.6), Diameter (Clauses 5.2.4.2, 5.2.4.6), HTTP (Clauses 5.2.4.3, 5.2.4.6), and H.248 (Clauses 5.2.4.4, 5.2.4.6) signaling messages, and for processing and transport of media (RTP) packets (Clauses 5.2.4.5, 5.2.4.6). MCC is described in Clause 5.2.4.7. Requirements for priority CAC for NGN GETS calls/sessions are not specified in this Standard and are for future study.

Each FE within the IMS Core Network is configured with an IP header DSCP value to be used for the IP packets it generates to carry SIP, Diameter, HTTP, and H.248 signaling messages related to an NGN GETS call/session. MRFP, MGW, and TrGW are configured with an IP header DSCP value to be used for the IP packets they generate to carry RTP payload related to an NGN GETS call/session. At the NNI, a fixed DSCP value (VOICE-ADMIT) is used for signaling and bearer IP packets.

5.2.4.1 SIP-Related Priority Treatment

The following SIP processing requirements apply to all the SIP-capable FEs enumerated in Clause 5.2.1:

[83] **An NGN GETS SIP-capable FE shall provide priority treatment (e.g., exemption from MCC as described in Clause 5.2.4.7) for the following SIP requests related to an NGN GETS call/session: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.**

[84] **An NGN GETS SIP-capable FE shall provide priority treatment (e.g., exemption from MCC as described in Clause 5.2.4.7) for the following SIP responses related to an NGN GETS call/session: 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx, except for SIP 100 (Trying) and SIP 403 (Forbidden).**

[85] **When an NGN GETS SIP-capable FE is waiting for resources external to the FE (e.g., transport resources) to process a SIP INVITE request for an NGN GETS call/session and has queued the request, the FE shall send a SIP 182 (Queued) response.**

When the required resources to process a queued NGN GETS call/session request become available, normal NGN GETS call/session processing resumes at the NGN GETS SIP-capable FE.

[86] **When an NGN GETS call/session request is queued and the queue timer expires, the NGN GETS SIP-capable FE shall send a SIP 408 (Request Timeout) response. The response shall include the Reason header field with the provisioned [Q.850] cause value.**

[87] **When an NGN GETS SIP-capable FE receives a SIP CANCEL request for an NGN GETS call/session request that it has queued, it shall remove the request from the queue and process the SIP CANCEL request as for a normal call/session, but with priority.**

[88] **When an NGN GETS SIP-capable FE attempts to queue an NGN GETS call/session request, but fails because the queue is full, it shall send a SIP 503 (Service Unavailable) response. This response shall include a Reason header field with the [Q.850] cause value of 34 (no circuit**

available).

[89] **An NGN GETS SIP-capable FE shall set the IP header DSCP value to the provisioned DSCP value for the IP packets it generates to carry SIP messages that are related to an NGN GETS call/session and that are provided priority treatment per [83] and [84].**

All SIP messages except SIP 100 (trying) and SIP 403 (forbidden) that are related to an NGN GETS call/session SIP dialog, including NGN GETS call/session establishment, have priority treatment. The DSCP marking is also used for SIP messages that are sent towards the UE and are related to an NGN GETS call/session.

An NGN GETS SIP-capable FE exempts an NGN GETS call/session and related SIP messages from MCC as described in Clause 5.2.4.7.

5.2.4.2 Diameter-related Priority Treatment

The following Diameter processing requirement applies to all the Diameter capable FEs enumerated in Clause 5.2.2:

[90] **A Diameter-capable FE shall set the IP header DSCP value to the provisioned DSCP value for the IP packets it generates to carry Diameter messages that are related to an NGN GETS call/session.**

A Diameter-capable FE exempts an NGN GETS call/session and related Diameter messages from MCC as described in Clause 5.2.4.7.

5.2.4.3 HTTP(S)-related Priority Treatment

The following FEs are HTTP(S)-capable FEs:

- NGN GETS AS (e.g., GETS-FC AS, GETS-AN AS, or GETS-NT AS), and
- MRFC.

The following HTTP(S) processing requirement applies to these FEs:

[91] **An HTTP(S)-capable FE shall set the IP header DSCP value to the provisioned DSCP value for the IP packets it generates to carry HTTP(S) messages that are related to an NGN GETS call/session.**

An HTTP(S)-capable FE exempts an NGN GETS call/session and related HTTP(S) messages from MCC as described in Clause 5.2.4.7.

5.2.4.4 H.248-related Priority Treatment

The following H.248 processing requirement applies to all the H.248-capable FEs enumerated in Clause 5.2.3:

[92] **An H.248-capable FE shall set the IP header DSCP value to the provisioned DSCP value for the IP packets it generates to carry H.248 messages that are related to an NGN GETS call/session.**

An H.248-capable FE exempts an NGN GETS call/session and related H.248 messages from MCC as described in Clause 5.2.4.7.

5.2.4.5 RTP-related Priority Treatment

The following FEs are RTP-capable FEs:

- MRFP,
- MGW, and
- TrGW.

The following RTP [RFC 3550] processing requirement applies to these FEs:

[93] An RTP-capable FE shall set the IP header DSCP value to the provisioned DSCP value for the IP packets it generates to carry RTP media packets that are related to an NGN GETS call/session.

The DSCP marking is also used for media packets that are sent towards the UE and are related to an NGN GETS call/session.

An RTP-capable FE exempts an NGN GETS call/session and related RTP messages from MCC as described in Clause 5.2.4.7.

5.2.4.6 Packet Level Priority Treatment

[390] and [391] apply to the processing of IP packets for an NGN GETS call/session.

[390] For an NGN GETS call/session, it is desirable that an FE shall provide priority treatment at the IP layer (L3) to the SIP, Diameter, HTTP, and H.248 messages as applicable to the FE, based on the provisioned NGN GETS marking (e.g., DSCP value, IP address) for an NGN GETS call/session.

[391] For an NGN GETS call/session, it is desirable that an FE shall provide priority treatment to the RTP (media) packets at the IP layer (L3) based on the provisioned IP header DSCP value for an NGN GETS call/session.

[390] and [391] apply to the processing of the innermost IP header when an IP tunnel (e.g., an IPSec tunnel or an MPLS LSP) is present. [390] and [391] may be implemented by an IP packet queuing treatment that is separate from the treatment of non-NGN GETS call/session related signaling and RTP packets. It may also be provided by separate policing of NGN GETS related traffic, or distinct capacity allocation/reservation.

NOTE: Refer to Clause 11.1.3 of [ATIS-1000055] for requirements on population of priority in the outer IP header when encryption is used.

If an FE within the IMS Core Network supports an Ethernet interface with Class Of Service (COS) capabilities, [326] applies for an NGN GETS call/session. In this case, the FE is configured with an Ethernet Frame Header COS parameter value (the “NS/EP” COS value) to be used for an NGN GETS call/session.

[326] If an FE supports the Ethernet COS capabilities on an Ethernet interface between the FE and an IP router/Ethernet switch, the FE shall set the Ethernet Frame Header COS parameter on the Ethernet interface to the provisioned “NS/EP” COS value for an NGN GETS call/session.

[326] ensures that the Ethernet Frame Header COS parameter is set to the “NS/EP” COS value for the Ethernet frames containing signaling and RTP payload related to an NGN GETS call/session. [326] allows priority treatment to be provided to these frames through the Ethernet. It is expected that the “NS/EP” COS value provides the highest priority treatment appropriate for user signaling and bearer on the interfaces. The FE provides ingress priority treatment and egress priority treatment (e.g., priority outgoing queuing and scheduling) for Ethernet frames with the “NS/EP” COS value. Configuration for the above is specified in [361].

NOTE: The use of additional lower level mechanisms for identifying and transporting NGN GETS related messages, such as use of logical port numbers on FEs, are for further study.

[724] When an NGN GETS call/session involves querying a database for number portability or supplementary services, priority treatment shall be provided to any outgoing query message if the NE supports and uses a protocol stack that supports priority mechanisms (e.g., the use of DSCP or Ethernet COS values).

[725] When a NE (e.g., database) receives a query message (e.g., number portability or supplementary services) with priority marking (e.g., indicated in the DSCP or Ethernet COS values), it is desirable that the response(s) be similarly marked with priority if the NE supports and uses a protocol stack that supports priority mechanisms.

5.2.4.7 Machine Congestion Controls

Most Functional Elements have some form of Machine Congestion Controls (MCC) in order to maximize the productive processing under signaling overload. This typically involves shedding a significant portion of the incoming signaling load. Usually, there is some level of discrimination in which incoming messages/packets are shed, not just blindly shedding a certain percentage.

While machine congestion itself occurs at the machine (Network Element) level rather than at the Functional Element level, the congestion control (e.g., blocking or shedding packets or messages) is often protocol-specific. The same Network Element may use one mechanism for filtering SIP messages, and a different mechanism for filtering Diameter messages. Or it may use different methods on different interfaces or ports, corresponding to different functions. Therefore, we describe the MCC requirements in terms of Functional Elements, even though they will be deployed by Network Element.

Typically, messages/packets that are known to be associated with existing calls/sessions dialogs are accepted, while messages/packets known to be associated with newly invoked calls/sessions are subject to shedding.

A basic principle of machine congestion control is that the shedding process should not increase the workload on the already overloaded Element. Therefore a message or packet can only be exempt from shedding based on information already known. For instance, if a SIP message has not yet been parsed, it cannot be exempt from shedding based on the presence of RPH. But it can be exempt from shedding based on a specific DSCP on the signaling packet, or any other criteria that is known at this point in the processing.

Machine Congestion Controls are typically proprietary, and specific to a particular vendor. While they are not usually covered by standards, there is industry activity (e.g., in IETF, 3GPP) evaluating mechanisms for various signaling (e.g., SIP, Diameter) overload control. Machine congestion controls often have multiple layers of controls. For instance, at the lowest level of congestion control, it may only shed routine administrative updates. At the highest level of congestion control, it may shed everything except the network control traffic necessary to keep the network and the FE from crashing. Ultimately, the FE may shed all packets/messages to keep itself alive.

It is the intent of this Standard that, where possible, all NGN GETS Voice packets/messages shall be exempt from MCC. The phrase “where possible” encompasses both “where the packet/message can be identified as NGN GETS” and “where exempting the NGN GETS packet/message will not cause the element (or the network) to crash”. It is not necessary to provide differentiated MCC overload treatment based on the Service User’s priority level.

In general, NGN GETS signaling packets can be identified by specific information in the packet header (e.g., a specific DSCP and unique COS on Ethernet), and NGN GETS signaling messages can be identified by protocol specific markings, such as the RPH including the ets namespace for SIP messages; the Session-Priority or MPS-Identifier AVP for Diameter messages; the Priority indicator in H.248; and for SS7 the Calling Party’s Category (CPC) in the IAM coded as “NS/EP Call” in ISUP and MTP message priority level 1.

NOTE: Specific requirements concerning MCC are for further study.

5.3 FE Specific Requirements

5.3.1 P-CSCF

This Clause specifies requirements associated with the P-CSCF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic P-CSCF functionality as defined in 3GPP Release 11 specifications.

5.3.1.1 General SIP Processing

The P-CSCF supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1, with exceptions and additions as described in this Clause. Table 5.1 summarizes the applicability of the common SIP requirements, as specified in Clause 5.2.1, to a P-CSCF.

[94] The P-CSCF shall support common SIP requirements as summarized in Table 5.1.

Table 5.1 – Summary of Common Requirements Applicable to P-CSCF

Sec 5.2.1 Req't	Requirement Applicability		Topic
	P-CSCF	Clause Ref.	
[63]	Replaced by [95] & [96]	Clause 5.3.1.2	Detection of an NGN GETS call/session.
[64]	Yes	Clause 5.2.1	Valid RPH namespaces.
[65]	Yes	Clause 5.2.1	RPH-format requirement.
[389]	Yes	Clause 5.2.1	RPH-format objective.
[501]	Yes	Clause 5.2.1	Inclusion of Supported header field with the 'resource-priority' option tag in outgoing SIP INVITE request.
[67]	Replaced by [99], [504], [103], [505], [506] & [106]	Clause 5.3.1.3.1 & Clause 5.3.1.3.2	The population of RPH in particular SIP requests.
[68]	Replaced by [504], [105], & [106]	Clause 5.3.1.3.1 & Clause 5.3.1.3.2	The population of RPH in particular SIP responses.
[72]	Yes	Clause 5.2.1 & Clause 5.3.1.3.1	Detection of multiple ets namespaces.
[73]	Yes	Clause 5.2.1 & Clause 5.3.1.3.1	Detection of multiple wps namespaces.
[74]	Yes	Clause 5.2.1 & Clause 5.3.1.3.1	Detection of invalid ets.x.
[75]	Yes	Clause 5.2.1 & Clause 5.3.1.3.1	Detection of invalid wps.y.
[76]	Yes	Clause 5.2.1 & Clause 5.3.1.3.1	Detection of invalid ets/wps namespace combination.
[77]	Yes	Clause 5.2.1	Processing of subsequent SIP messages with RPH (for non-NGN GETS call/session).

5.3.1.2 Detection of an NGN GETS Call/Session

The P-CSCF supports more advanced capabilities for detecting an NGN GETS call/session, beyond the corresponding common SIP requirement [63]. Common SIP requirement [63] is replaced with the P-CSCF requirements presented in this clause.

Three mechanisms are defined to allow a P-CSCF to determine if NGN GETS priority treatment is to be applied for a received SIP message:

1. Recognition of an NGN GETS priority marking within a received SIP message (within the RPH). This capability is specified in sub-item 1 of requirement [95].
2. Recognition of a GETS-FC, GETS-AN, or GETS-NT within the Request-URI of a received SIP INVITE request. This capability is specified in sub-item 2 of requirement [95], including the ability to provision GETS strings that are matched as described in requirement [96].
3. Recognition that a SIP message is received within the context of an existing SIP dialog that is associated with an NGN GETS call/session, based on call/session state information maintained by the P-CSCF. This capability is specified in requirement [106].

Mechanisms 1 and 2 are used for initial detection of an NGN GETS call/session by the P-CSCF, whereas mechanism 3 allows the P-CSCF to apply NGN GETS priority treatment when processing subsequent SIP messages associated with an existing NGN GETS call/session.

[95] A P-CSCF shall recognize that a received SIP INVITE request is associated with an NGN GETS call/session by:

1. **The presence of an RPH with a valid ets.x and no wps, or with a valid ets.x and a valid wps.y, from a S-CSCF or an IBCF within its IMS Core Network, or**
2. **Within the Request-URI, the presence of a provisioned GETS string (as specified in [96]).**

The specific set of GETS strings (corresponding to GETS-FC, GETS-AN, or GETS-NT) are provisionable, as specified in [282] and [283].

The following requirement supports matching against a Request-URI based on either (the user portion of) a SIP:URI with user=phone or (the ‘telephone-subscriber’ portion of) a TEL:URI.

[96] A P-CSCF shall be able to perform string matches between the Request-URI and the provisioned GETS strings, to determine if a provisioned string matches the received user string in the Request-URI. The term ‘received user string’ refers to the user portion of a SIP:URI with user=phone or the ‘telephone-subscriber’ portion of a TEL:URI (ignoring any visual separators).

For matching against a provisioned GETS-FC string (of length [n]), a successful match is detected when:

- **The received user string is in the local–number format (i.e., without a leading ‘+’),**
- **The received user string contains at least [n] characters, and**
- **The provisioned GETS-FC string matches the leading [n] characters of the received user string.**

For matching against a provisioned GETS-AN or GETS-NT string (of length [m]), a successful match is detected when:

- **The received user string contains at least ten digits, and**

- **The provisioned GETS-AN or GETS-NT string matches the first [m] of the last ten digits of the received user string.**

When any of the above matches is successful, the P-CSCF shall treat that call/session as an NGN GETS call/session.

In requirement [96], [m] represents the number of digits used in a match for a provisioned GETS-AN or GETS-NT string and [n] represents the number of characters used in a match for a provisioned GETS-FC string.

Since any match (between the received user string and any of the provisioned GETS-FC, GETS-AN, or GETS-NT strings) designates an NGN GETS call/session, no further matching of the received user string is necessary once an initial match is detected. The corresponding NGN GETS call/session treatment is specified in subsequent P-CSCF requirements.

Since GETS-FC strings (as applicable to numbers dialed with a *FC [Feature Code] prefix) are matched based on the leading characters, the P-CSCF must receive the GETS-FC as the leading prefix (consistent with current WPS dialing).

Once an NGN GETS call/session request is detected by a P-CSCF, the P-CSCF provides NGN GETS priority treatment to that call/session (as specified in clauses 5.2.4 and 5.3.1, and their associated subclauses) until the NGN GETS call/session is released or authorization is denied. NGN GETS priority treatment is applied even before NGN GETS authorization has been performed, to allow the NGN GETS call/session to progress successfully to an NGN GETS AS that can perform NGN GETS authorization. Thus, the P-CSCF treats the SIP INVITE request as being associated with an NGN GETS call/session, and relies on the NGN GETS AS to deny the call/session request if the calling party is subsequently determined to be unauthorized for NGN GETS.

5.3.1.3 P-CSCF RPH-Related Processing Requirements

This clause specifies requirements associated with P-CSCF processing of RPH within SIP messages. These requirements focus on the ets and wps namespaces. The treatment of other RPH namespaces (other than ets and wps namespaces) is subject to policies adopted for other services, and is outside the scope of this Standard.

5.3.1.3.1 P-CSCF Processing of SIP Messages Received

When a P-CSCF receives a SIP INVITE request from the direction of a UE that includes a GETS-FC, GETS-AN, or GETS-NT within the Request-URI (independent of whether an RPH is included), the request may be rejected by the throttling mechanism described in requirements [108] and [109], or may be accepted and processed normally, in which case [99] is applicable.

[99] When a P-CSCF receives a SIP INVITE request from the direction of a UE that includes a GETS-FC, GETS-AN, or GETS-NT within the Request-URI, and the P-CSCF sends a corresponding SIP INVITE request to an FE within its IMS Core Network, it shall include an RPH with the provisioned ets.x.

[504] When a P-CSCF receives a SIP INVITE request from the direction of a UE that contains an RPH with an ets namespace (and may contain other namespaces including a wps namespace) but that does not include a GETS-FC, GETS-AN, or GETS-NT within the Request-URI:

> **When the received RPH includes only an ets namespace or only ets and wps namespaces, the P-CSCF shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with two Reason header fields: (1) a Reason header field with SIP cause value of 417 (RPH header), and (2) a Reason header field with [Q.850] cause value of 21 (call rejected). The response shall not contain an RPH. Otherwise, when the received RPH includes other namespaces, the P-CSCF shall remove any ets and wps namespaces and process the request as if the ets and wps namespaces were not present (i.e., a non-NGN GETS request with other namespaces).**

The P-CSCF shall provide an alert and create a log entry that contains the identification of the entity that sent the SIP INVITE request and the date and time of the event.

Clause 5.2.1.4 describes the validation of RPH settings for SIP requests received. When the P-CSCF receives a SIP request containing an RPH, the P-CSCF performs validation of the RPH ets and wps namespace settings as indicated in requirements [72] through [76]. Note that the P-CSCF may reject a SIP message with a "valid" ets.x for other reasons (e.g., based on [504]).

5.3.1.3.2 P-CSCF Population of RPH in SIP Messages

Common SIP requirements [67] and [68] are replaced with the following requirements for the P-CSCF. The P-CSCF includes RPH with the provisioned ets.x, and if available the wps.y in the SIP messages it sends to an FE within its IMS Core Network or, based on local policy, to an enterprise network as these are trusted networks. However, the P-CSCF excludes ets and wps namespaces from any RPH in the SIP messages it sends to a UE since a UE is not a trusted entity.

[103] **For an NGN GETS call/session, a P-CSCF shall include RPH with the provisioned ets.x, and if available the wps.y based on [106] in the following SIP requests it sends to an FE within its IMS Core Network or, based on local policy, to an enterprise network: ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.**

[505] **For an NGN GETS call/session, based on local policy, a P-CSCF shall include RPH with the provisioned ets.x, and if available the wps.y based on [106] in SIP INVITE request it sends to an enterprise network.**

[506] **For an NGN GETS call/session, a P-CSCF shall exclude ets and wps namespaces from any RPH that is sent in SIP requests and responses to a UE.**

[105] **For an NGN GETS call/session, a P-CSCF shall include the RPH in 1xx, 2xx, 3xx, 4xx, 5xx and 6xx responses it sends to an FE within its IMS Core Network or, based on local policy, to an enterprise network, with the exception of 100 ("Trying") and 403 ("Forbidden"). The RPH shall include the provisioned ets.x, and if available the wps.y based on [106] except as follows. For a SIP 400 (Bad request) response with a 417 code in the Reason header field, the RPH shall include the provisioned ets.x without the wps namespace. The RPH shall be included in responses that are sent to an FE within its IMS Core Network or, based on local policy, to an enterprise network, even if the received response does not include an RPH.**

For [103], [505], and [105], the P-CSCF replaces any valid ets.x value that may have been in the received message with the provisioned ets.x value when it sends SIP messages to either an FE within the IMS Core Network or, based on local policy, to an enterprise network.

[106] **For an NGN GETS call/session, a P-CSCF shall retain the wps.y resource value most recently received within the SIP dialog from an IMS Core Network FE. Any wps.y value received from a UE shall not be retained.**

5.3.1.4 Throttling of NGN GETS Call/Session Requests

A throttling mechanism is used to throttle excessive NGN GETS call/session requests from a set of IP addresses assigned to an enterprise.

[108] **The first NGN GETS SIP-capable FE facing an enterprise network (e.g., P-CSCF or an SBC implementation) shall support a throttling mechanism that controls the number of NGN GETS call/session requests received from configured IP addresses (assigned to the enterprise). The throttling mechanism shall be invoked for a configured IP address when at least one of the following two cases for a configured IP address occurs: 1) the configured maximum number of NGN GETS call/session requests processed during a configured time interval is exceeded or 2) the configured maximum number of concurrent NGN GETS calls/sessions during a**

configured time interval is exceeded.

The above throttling limits the number of NGN GETS call/session requests from a particular IP address (as indicated via the topmost Via header of the SIP INVITE request) that are processed during a particular interval. For example, if a maximum rate of 100 NGN GETS call/session requests is configured for a 5 minute interval, the first 100 NGN GETS call/session requests received during any 5 minute interval will be processed, and any subsequent NGN GETS call/session requests received during the remainder of that 5 minute interval will be rejected (until the counter is reset at the end of that interval, at which time additional NGN GETS call/session requests are processed).

The above "maximum number of concurrent NGN GETS calls/sessions" represent the number of currently-active SIP dialogs associated with NGN GETS calls/sessions from a particular IP address, for which SIP 200 responses have been received for the SIP INVITE requests.

Configuration requirements to support the [108] throttling mechanisms are specified in [286] and [287].

Beyond the above treatment for *configured* IP addresses, similar capabilities are applied for the throttling of NGN GETS call/session requests received from other entities for which the IP addresses are dynamically allocated by the IMS Core Network.

[392] It is desirable that the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall support a throttling mechanism that controls the number of NGN GETS call/session requests originating from UNIs other than those that have the configured IP addresses for which [108] applies. The throttling mechanism shall be invoked for any individual IP address when at least one of the following two cases for any individual IP address occurs: 1) the configured maximum number of NGN GETS call/session requests received during a configured time interval is exceeded, or 2) the configured maximum number of concurrent NGN GETS calls/sessions during a configured time interval is exceeded.

The configuration requirement to support the [392] throttling mechanism (applicable for non-configured IP addresses) is specified in [396].

[109] Based on configuration, the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall allow a Service Provider to either allow or block NGN GETS call/session requests from each configured IP address. When an NGN GETS call/session is blocked, the FE shall send a SIP 403 (Forbidden) response with a Reason header field with [Q.850] cause value of 21 (call rejected). The response shall not contain any ets or wps namespaces in an RPH.

[109] takes precedence over [108]. [108] applies only if the [109] configuration allows an NGN GETS call/session from the IP address. The configuration requirement to support [109] is specified in [288].

[110] When the rate of NGN GETS call/session requests (as specified in [108] and [392]) exceeds the configured threshold, the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall provide an alert and create a log entry that contains:

- **Date and time of the event,**
- **Identification of the entity that sent the SIP INVITE request.**

[111] When the number of concurrent NGN GETS calls/sessions (as specified in [108] and [392]) exceeds the configured threshold, the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall provide an alert and create a log entry that contains:

- **Date and time of the event,**
- **Identification of the entity that sent the SIP INVITE request.**

As an alternative to the rate-based throttling mechanism, a Service Provider may consider the following mechanism to throttle NGN GETS calls/sessions. The first NGN GETS SIP-capable FE at the border may be configured to support a preset gap interval and two values for the gap interval limits (minimum and maximum). If the number of NGN GETS calls/sessions exceeds the configured maximum number of NGN GETS call/session requests processed during a particular interval, call gapping is invoked with the configured preset gap interval. Each time an NGN GETS call/session attempt is successfully validated, the gap interval is reduced by a preset number until the minimum gap interval for that site has been reached. Each time an invalid NGN GETS call/session attempt is detected, the gap interval is increased by a preset number. This continues until the maximum gap interval for that site is reached. With this alternative, on a dynamic basis, the number of NGN GETS calls/sessions at the site could vary up to a dynamically set value based on the ratio of the valid attempts to the number of invalid attempts.

NOTE: Additional details, including configuration details, and the application to the throttling mechanism based on the maximum number of concurrent NGN GETS calls/sessions, may be considered in a future version of this Standard.

5.3.1.5 Diameter Processing

To support policy control, the P-CSCF uses Diameter to query the PCRF for an NGN GETS call/session.

[507] When the P-CSCF sends a Diameter AA-Request (AAR) message to the PCRF for an NGN GETS call/session, the P-CSCF shall include the MPS-Identifier and Reservation-Priority AVPs [TS 29.214]. The P-CSCF shall populate the MPS-Identifier AVP with a value of 'NGN GETS'. If the originating Service User's priority level is available, the P-CSCF shall populate the Reservation-Priority AVP with a value that corresponds to the originating Service User's priority level, consistent with Table 4.3. The Reservation-Priority AVP shall be populated with a default value if the originating Service User's priority level is unknown.

Configuration requirement to set the default value is specified in [578].

[TS 29.213] Section B.2.1 allows an originating P-CSCF to send a Diameter AAR message to a PCRF upon receipt of a SIP INVITE request (containing an SDP offer) from an originating UE, or to defer the sending of the initial Diameter AAR message until negotiated SDP parameters are received from the terminating side. For NGN GETS, the Diameter AAR message includes Session Information which uses the MPS-Identifier AVP (to indicate that this is an NGN GETS call/session) and a Reservation-Priority AVP (set to a default value when the priority level of the originating Service User is unknown) at the session level. The DRMP AVP is also included, as specified in requirement [722] of Clause 5.2.2.

The Diameter AAR message, that is sent based on the SDP offer from the SIP INVITE request, includes the Service-Info-Status AVP set to the "PRELIMINARY SERVICE INFORMATION" value. In a non-GPRS network, this enables the PCRF to ensure that the Default Bearer and IMS Signaling Bearer are set for the appropriate priority treatment for NGN GETS originations for particular wireless access technologies.

[508] When the P-CSCF receives a SIP INVITE request from an originating UE, that corresponds to an NGN GETS call/session request, the P-CSCF shall send a Diameter AAR message to the PCRF.

For the scenario covered by [508], the Diameter AAR message is populated in accordance with requirement [507] (i.e., the P-CSCF includes the MPS-Identifier AVP and populates a default value in the Reservation-Priority AVP, when the originating Service User's priority level is unknown).

In order to provide a timely indication to the IP-Access Network of the priority nature of an incoming NGN GETS call/session, a terminating P-CSCF initiates PCC interactions upon receipt of a SIP INVITE request. This facilitates the IP-Access Network's ability to apply priority paging (and to provide priority treatment during subsequent interactions with the terminating UE) for particular wireless access technologies.

[509] When the P-CSCF receives a SIP INVITE request, destined for a terminating UE, that corresponds to an NGN GETS call/session request, the P-CSCF shall send a Diameter AAR

message to the PCRF.

For the scenario covered by [509], the NGN GETS call/session request is identified via the presence of a corresponding SIP RPH value, and the Diameter AAR message is populated in accordance with requirement [507] (i.e., the P-CSCF includes the MPS-Identifier AVP and populates the Reservation-Priority AVP with a value that corresponds to the originating Service User's priority level, consistent with Table 4.3).

5.3.1.6 Priority Treatment Requirements

The P-CSCF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1) and Diameter-capable FEs (Clause 5.2.4.2) are applicable to the P-CSCF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.2 I-CSCF

This clause specifies requirements associated with I-CSCF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic I-CSCF functionality as defined in 3GPP Release 11 specifications.

When the I-CSCF functionality is incorporated into an entity that supports other FE capabilities, the composite set of requirements apply to that entity. For example, when an entity provides interconnection with another VoIP network, the IBCF requirements in Clause 5.3.4 also apply to that entity.

5.3.2.1 SIP Processing

The I-CSCF supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1 with the following addition.

[113] **When an I-CSCF receives a SIP message with an RPH associated with an NGN GETS call/session, the I-CSCF shall include the same RPH in any corresponding SIP requests or responses that it sends, with the exception of the cases identified in [68].**

5.3.2.2 Diameter Processing

The I-CSCF uses Diameter messages to support HSS interactions. The I-CSCF supports the common set of Diameter processing capabilities for NGN GETS, as discussed in Clause 5.2.2 with the following addition.

[510] **For an NGN GETS call/session, when the I-CSCF attempts to locate the S-CSCF associated with the called party, the I-CSCF shall send a Diameter Location-Info-Request (LIR) message with the Session-Priority AVP (populated as described in [503]). The Session-Priority AVP shall be populated with a default value if the originating Service User's priority level is unknown.**

Configuration requirement to set the default value is specified in [576].

5.3.2.3 Priority Treatment Requirements

The I-CSCF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1) and Diameter-capable FEs (Clause 5.2.4.2) are applicable to the I-CSCF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.3 S-CSCF

This clause specifies requirements associated with S-CSCF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic S-CSCF functionality as defined in 3GPP Release 11 specifications.

When the S-CSCF functionality is incorporated into an entity that also supports other FE capabilities, the composite set of requirements apply to that entity. For example, when an entity provides interconnection with another VoIP network, the IBCF requirements in Clause 5.3.4 also apply to that entity.

5.3.3.1 SIP Processing

The S-CSCF supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1 with the following addition.

[115] When an S-CSCF receives a SIP message with an RPH associated with an NGN GETS call/session, the S-CSCF shall include the same RPH in any corresponding SIP requests or responses that it sends, with the exception of the cases identified in [68].

Existing S-CSCF mechanisms (as specified by 3GPP) are used to recognize that the appropriate triggering conditions are satisfied for a particular NGN GETS call/session. For GETS-FC invocations, iFC are provisioned in the HSS and downloaded to the S-CSCF during registration to enable subsequent GETS-FC AS involvement. For GETS-AN and GETS-NT invocations, DNS/ENUM interactions may be used to enable the corresponding GETS-AN AS or GETS-NT AS involvement.

5.3.3.2 Diameter Processing

The S-CSCF uses Diameter messages to support HSS interactions.

The S-CSCF supports the common set of Diameter processing capabilities for NGN GETS, as discussed in Clause 5.2.2 with the following addition.

[511] When the S-CSCF attempts to establish an NGN GETS call/session to an unregistered user, the S-CSCF shall send a Diameter Server-Assignment-Request (SAR) message with the Session-Priority AVP. If the originating Service User's priority level is available, the S-CSCF shall populate the Session-Priority AVP with a value that corresponds to the originating Service User's priority level, consistent with Error! Reference source not found.**. The Session-Priority AVP shall be populated with a default value if the originating Service User's priority level is unknown.**

Configuration requirement to set the default value is specified in [576]**.**

Clause 5.12 of [TS 23.228] illustrates attempted call/session delivery to an unregistered user, resulting in further actions as appropriate for this call/session attempt (e.g., routing to voicemail).

5.3.3.3 Priority Treatment Requirements

The S-CSCF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1) and Diameter-capable FEs (Clause 5.2.4.2) are applicable to the S-CSCF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.4 IBCF

This clause specifies requirements associated with IBCF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic IBCF functionality as defined in 3GPP Release 11 specifications.

5.3.4.1 General SIP Processing

The IBCF supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1, with exceptions and additions as described in this clause.

For the purpose of this clause, an external entity is an adjacent entity that communicates with an IBCF through an NNI of the IMS Core Network. An IBCF needs to determine whether it should honor RPH information that is received from an external entity, and whether it should send RPH information to a particular external entity. Corresponding management requirements specified in Clause 6.3.4.1 are used to select the appropriate RPH treatment for a particular external entity. The choice of a particular RPH treatment is influenced by business decisions.

Table 5.2 summarizes the applicability of the common SIP requirements, as specified in Clause 5.2.1, to an IBCF.

[117] The IBCF shall support common SIP requirements as summarized in Table 5.2.

Table 5.2 – Summary of Common Requirements Applicable to IBCF

Cl. 5.2.1 Req't	Requirement Applicability		Topic
	IBCF	Reference	
[63]	Replaced by [118] and [119]	Clause 5.3.4.2	Detection of an NGN GETS call/session.
[64]	Yes	Clause 5.2.1	Valid RPH namespaces.
[65]	Yes	Clause 5.2.1	RPH-format requirement.
[389]	Yes	Clause 5.2.1	RPH-format objective.
[501]	Yes	Clause 5.2.1	Inclusion of Supported header field with the 'resource-priority' option tag in outgoing SIP INVITE request.
[67]	Replaced by [121], [122], [123], [125] (sub-item 1a), & [126]	Clause 5.3.4.3.2	The population of RPH in particular SIP requests.
[68]	Replaced by [124], [125] (sub-item 1b), & [126]	Clause 5.3.4.3.2	The population of RPH in particular SIP responses.
[72]	Yes	Clause 5.2.1	Detection of multiple ets namespaces.
[73]	Yes	Clause 5.2.1	Detection of multiple wps namespaces.
[74]	Yes	Clause 5.2.1	Detection of invalid ets.x.
[75]	Yes	Clause 5.2.1	Detection of invalid wps.y.
[76]	Yes	Clause 5.2.1	Detection of invalid ets/wps namespace combination.
[77]	Yes	Clause 5.2.1	Processing of subsequent SIP messages with RPH (for non-NGN GETS call/session).

5.3.4.2 Detection of an NGN GETS Call/Session

The IBCF supports more advanced capabilities for detecting an NGN GETS call/session, beyond the corresponding common SIP requirement [63]. Common SIP requirement [63] is replaced with the IBCF requirements presented in this clause.

[118] An IBCF shall recognize that a received SIP INVITE request is associated with an NGN GETS call/session by:

1. **The presence of an RPH with a valid ets.x and no wps, or with a valid ets.x and a valid wps.y, from another FE within its IMS Core Network,**
2. **The presence of an RPH with a valid ets.x and no wps, or with a valid ets.x and a valid wps.y, from an external entity (whose IP address or Fully Qualified Domain Name (FQDN) is provisioned at the IBCF to support option 1 of [122]), or**
3. **Within the Request-URI, the presence of a provisioned GETS string (as specified in [119]).**

[119] An IBCF shall be able to perform string matches between the Request-URI and the provisioned GETS strings, as specified in [96].

The specific set of GETS strings (corresponding to GETS-FC, GETS-AN, or GETS-NT) are provisionable, as specified in [293] and [294].

5.3.4.3 IBCF RPH-Related Processing Requirements

This Clause specifies requirements associated with IBCF processing of RPH within SIP messages. These requirements focus on the ets and wps namespaces. The treatment of other RPH namespaces (other than ets and wps namespaces) is subject to policies as adopted for other services, and is outside the scope of this Standard.

5.3.4.3.1 IBCF Processing of SIP Messages Received

[121] When an IBCF receives a SIP INVITE request from an external entity that includes a GETS-FC, GETS-AN, or GETS-NT within the Request-URI, the IBCF shall send to the appropriate internal FE a corresponding SIP INVITE request that includes an RPH with the provisioned ets.x, and if received the wps.y, if the IP address or FQDN of the external entity is provisioned at the IBCF to support option 1 of [122].

A wps.y r-value is received by an IBCF for the scenario when an NGN GETS call/session is invoked via a GETS-FC + GETS-AN/NT and the GETS-FC authorization occurs prior to receipt of the SIP INVITE request by the IBCF.

Recognition of the GETS-FC by the IBCF is needed for inserting an RPH if the SIP INVITE request is received from a visited IP network that does not support population of an RPH with ets and wps namespaces.

[122] Based on the IBCF's configuration per external entity IP address or FQDN, an IBCF shall follow one of the following procedures when processing a SIP INVITE request received from an external entity that contains an RPH with an ets namespace (and may contain other namespaces including a wps namespace) but that does not include a GETS-FC, GETS-AN, or GETS-NT within the Request-URI:

1. **The IBCF shall send to the appropriate internal FE a corresponding SIP INVITE request that includes an RPH with the provisioned ets.x, and if received the wps.y .**
2. **The IBCF shall send to the appropriate internal FE a corresponding SIP INVITE request that does not include any ets or wps namespaces in an RPH.**
3. **When the RPH includes only an ets namespace or only ets and wps namespaces, the IBCF shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with two**

Reason header fields: (1) a Reason header field with SIP cause value of '417' (RPH header), and (2) a Reason header field with [Q.850] cause value of 21 (call rejected). The response shall not contain an RPH. Otherwise, when the RPH includes other namespaces, the IBCF shall remove any ets and wps namespaces and process the request as if the ets and wps namespaces were not present (i.e., a non-NGN GETS request with other namespaces).

When option 2 applies, if the RPH in the received SIP INVITE request does not contain namespaces other than ets and wps, then an RPH is not sent. For options 1 and 2, if namespaces other than wps or ets are contained in the received RPH, an RPH is sent with those other namespaces. The specific option is chosen based on the IP address or FQDN contained within the topmost Via header of the received SIP INVITE request. The associated provisioning requirement for the above options is specified in [295].

A SIP INVITE request as received in requirement [121] or [122] may instead be rejected by the IBCF, if a throttling mechanism is applicable to that call/session, as specified in requirements [128] and [129].

5.3.4.3.2 IBCF Population of RPH in SIP Messages

Common SIP requirements [67] and [68] are replaced with the following requirements for the IBCF.

[123] **For an NGN GETS call/session, an IBCF shall include the RPH with the provisioned ets.x, and if available the wps.y based on [126] in the following SIP requests it sends to an FE within its IMS Core Network: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.**

[124] **For an NGN GETS call/session, an IBCF shall include the RPH in 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses it sends to an FE within its IMS Core Network, with the exception of SIP 100 ("Trying") and SIP 403 ("Forbidden") responses. The RPH shall include the provisioned ets.x, and if available the wps.y based on [126], except as follows. For a SIP 400 (Bad request) response with a 417 code in the Reason header field, the RPH shall include the provisioned ets.x without the wps namespace. The RPH shall be included in responses that are sent to an FE within its IMS Core Network, even if the received request or response does not include an RPH.**

[125] **Based on configuration per IP address or FQDN of an external entity, for an NGN GETS call/session, an IBCF shall follow procedures in item 1 or 2 when sending a SIP message to an external entity:**

1. **The IBCF shall include an RPH with the provisioned ets.x, and if available the wps.y based on [126]) in the following SIP messages:**
   a. **SIP requests: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.**
   b. **1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses, with the exception of SIP 100 ("Trying") and SIP 403 ("Forbidden") responses. The RPH shall include the provisioned ets.x, and if available the wps.y, except as follows. For a SIP 400 (Bad request) response with a 417 code in the Reason header field, the RPH shall include the provisioned ets.x without the wps namespace. The RPH shall be included in responses that are sent to an external FE, even if the received request or response does not include an RPH.**
2. **The IBCF shall not include any ets or wps namespaces in an RPH.**

The specific option is chosen based on the IP address or FQDN of the external entity. The associated provisioning requirement for the above options is specified in [296].

For [123], [124], and [125], the IBCF replaces any valid ets.x value that may have been in the received message with the provisioned ets.x value. The IBCF retains a wps.y value as specified in [237]. This wps.y value is used when sending any subsequent SIP messages associated with that NGN GETS call/session.

[126] An IBCF shall retain a wps.y resource value for inclusion in subsequent messages within a SIP dialog associated with an NGN GETS call/session. The most recently received wps.y value, corresponding to one of the following conditions, shall be retained:

1. **When a wps.y value is received from an FE within its IMS Core Network, the received wps.y value shall be retained.**
2. **When a SIP message (containing a wps.y) is received from an external entity whose IP address or FQDN is provisioned at the IBCF per item 1 of [122].**

If none of the above conditions are applicable during an NGN GETS call/session, no wps.y is included in the subsequent SIP messages. The inclusion of the retained wps.y in SIP messages (sent to an FE within its IMS Core Network or to an external entity) is specified in [123] through [125].

5.3.4.4 Throttling of NGN GETS Call/Session Requests

A throttling mechanism is used to throttle excessive NGN GETS call/session requests from a set of configured IP addresses or FQDNs associated with the NNI.

[128] An IBCF shall support a throttling mechanism that controls the number of NGN GETS call/session requests originating from an external entity. The throttling shall be invoked when at least one of the following two cases is exceeded for each configured IP address or FQDN of an external entity: 1) the configured maximum rate of NGN GETS call/session requests processed during a particular interval or 2) the configured maximum number of concurrent NGN GETS calls/sessions.

[129] Based on configuration, an IBCF shall allow a Service Provider to either allow or block NGN GETS call/session requests from a set of configured IP addresses or FQDNs. This processing is as described in [109], but is applied to external entities for the IBCF.

Configuration requirements to support the above throttling mechanisms are specified in [297], [298], and [299].

[130] When the maximum rate of NGN GETS call/session requests (as specified in [128]) is exceeded, the IBCF shall provide an alert and create a log entry that contains:

- **Date and time of the event, and**
- **Identification of the entity that sent the SIP INVITE request.**

[131] When the maximum number of concurrent NGN GETS calls/sessions (as specified in [128]) is exceeded, the IBCF shall provide an alert and create a log entry that contains:

- **Date and time of the event, and**
- **Identification of the entity that sent the SIP INVITE request.**

As an alternative to the rate-based throttling mechanism, a Service Provider may consider a mechanism as discussed in Clause 5.3.1.4 to throttle NGN GETS calls/sessions.

5.3.4.5 H.248 Requirements

The IBCF supports the common set of H.248 processing capabilities for NGN GETS, as specified in Clause 5.2.3 with the following additions.

[512] When an IBCF determines that an H.248 context needs to be created on receipt of a SIP INVITE request, or a subsequent SIP message, with RPH including ets.x and wps.y, it shall include the Priority indicator with the appropriate priority value in the H.248 Add_Request and Modify_Request commands sent to a TrGW. The mapping of the Service User's priority level value (y) in the wps namespace to the Service User's priority level value carried in the Priority indicator shall be as shown in Table 4.5.

[513] When an IBCF determines that an H.248 context needs to be created on receipt of a SIP INVITE request, or a subsequent SIP message, with RPH including ets.x but without wps.y, it shall

include the Priority indicator with a default priority value in the H.248 Add_Request and Modify_Request commands sent to a TrGW.

[514] When an IBCF determines that an H.248 context needs to be created for a received SIP INVITE request without an RPH and the IBCF determines that the call/session is an NGN GETS call/session (based on the Request-URI), the IBCF shall include the Priority indicator with a default priority value in the H.248 Add_Request command sent to a TrGW.

For requirements [513] and [514], the default value (in the range 11 – 15) to be included in the H.248 Priority indicator should be based on Authorized Agency policy, and provisioned in the IBCF.

Configuration requirement to set the default value is specified in [276].

5.3.4.6 Priority Treatment Requirements

The IBCF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1, with [89] replaced by [135] and [136]) and H.248-capable FEs (Clause 5.2.4.4) are applicable to the IBCF, beyond the general priority treatment requirements (Clause 5.2.4.6).

[135] When sending SIP messages with RPH including ets.x to an external entity related to an NGN GETS call/session, an IBCF shall set the IP header DSCP value to DSCP value 101100 (44) (VOICE-ADMIT) for the IP packets that carry those SIP messages.

[136] When sending SIP messages to an FE within its IMS Core Network related to an NGN GETS call/session, an IBCF shall set the IP header DSCP value to the provisioned DSCP value for the IP packets that carry those SIP messages.

The provisioning requirement to support [136] is specified in [277].

5.3.5 Application Server

This clause provides requirements associated with NGN GETS AS processing for NGN GETS. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic AS functionality as defined in 3GPP Release 11 specifications.

Common NGN GETS AS requirements, as applicable to an NGN GETS AS that supports GETS-FC, GETS-AN, and/or GETS-NT functionality, are discussed in Clause 5.3.5.1. These requirements are applicable to a standalone NGN GETS AS providing the corresponding NGN GETS capabilities. Clauses 5.3.5.2 through 5.3.5.4 provide requirements specific to a standalone NGN GETS AS that supports GETS-FC, GETS-AN, or GETS-NT functionality, respectively.

Various implementation options are possible for the NGN GETS AS interactions with the MRFC. The NGN GETS AS could download a script to the MRFC for execution, or the script can be located at the MRFC. An additional implementation option is to have the NGN GETS AS provide “atomic” instructions to the MRFC for execution. In all cases, the NGN GETS AS controls the user interactions via the MRFC/MRFP.

5.3.5.1 General NGN GETS AS Requirements

5.3.5.1.1 SIP Processing

The NGN GETS AS supports the common set of SIP processing capabilities for NGN GETS, as specified in Clause 5.2.1.

5.3.5.1.2 Diameter Processing

The GETS-FC AS may optionally use Diameter messages to support HSS interactions for an NGN GETS call/session. If this interface is used, the GETS-FC AS supports the common set of Diameter processing capabilities for NGN GETS, as discussed in Clause 5.2.2.

If the Service User subscription information is maintained in the HSS, the NGN GETS AS sends a Diameter UDR message to an SLF or HSS to access that subscription information.

[672] If an NGN GETS AS sends to an SLF a Diameter User-Data-Request (UDR) message, the NGN GETS AS shall include the Session-Priority AVP in the Diameter UDR message.

[673] If the Service User subscription information is maintained in an HSS, the NGN GETS AS shall send a Diameter User-Data-Request (UDR) message with the Session-Priority AVP to the HSS. The NGN GETS AS shall use the subscription information returned in the User-Data AVP of the corresponding Diameter User-Data-Answer (UDA) message to authorize and determine the priority level of the Service User.

The GETS-AN AS and GETS-NT AS support the common set of Diameter processing capabilities for NGN GETS, as discussed in Clause 5.2.2.

5.3.5.1.3 Priority Treatment Requirements

The NGN GETS AS applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1) are applicable to the NGN GETS AS, beyond the general priority treatment requirements (Clause 5.2.4.6). Corresponding requirements related to Diameter-capable FEs (Clause 5.2.4.2) may be applicable to a GETS-FC AS, if the optional use of a Diameter interface is chosen to support HSS interactions.

To the extent that common resources are used to support both NGN GETS and other (non-NGN GETS) services, an NGN GETS call/session should be given preferential access to shared resources (over a non-NGN GETS call/session).

[334] If an NGN GETS AS supports services in addition to NGN GETS, the AS shall support mechanisms to allow an NGN GETS call/session to be given preferential access to shared resources (over a non-NGN GETS call/session).

5.3.5.1.4 Common Requirements Related to MRFC Interactions

Table 5.3 summarizes the applicability of common MRFC/MRFP-related requirements to each type of NGN GETS AS.

[518] The GETS-FC AS, GETS-AN AS, and GETS-NT AS shall support common MRFC/MRFP-related requirements as summarized in Table 5.3.

Table 5.3 – Summary of Common MRFC/MRFP-related Requirements Applicable to GETS-FC AS, GETS-AN AS, and GETS-NT AS

Common Requirement	GETS-FC AS	GETS-AN AS	GETS-NT AS	Topic
[675]	-	✓ [143]	✓ [525]	NGN GETS AS – MRFC/MRFP selection
[519], [520]	-	✓	✓	NGN GETS AS – MRFC/MRFP interactions (PIN)

An NGN GETS AS applies priority treatment for selection of an MRFC. This priority treatment is implementation-dependent, but may include a selection from a set of MRFCs that is larger than that available to a normal call/session, and queuing and automatic reattempts if no MRFCs are available.

[675] If priority treatment includes reattempting an MRFC a configured number of times in event of an unsuccessful attempt, then the following procedures apply:

When an NGN GETS AS attempts to access an MRFC by sending a SIP INVITE request, the NGN GETS AS timer for the reattempt (see [302]) shall be started. If a SIP response indicating MRFC unavailability is received, then the NGN GETS AS timer for the reattempt shall be reset and started again. If the NGN GETS AS timer for the reattempt times out (e.g., the MRFC does not respond in a timely manner with a SIP 200 OK response), the NGN GETS AS shall reattempt accessing the MRFC by sending another SIP INVITE request (unless the configured maximum number of attempts have already been made).

The NGN GETS AS interacts with an MRFC/MRFP to collect a PIN from the calling party. The NGN GETS AS allows up to three attempts for the calling party to enter a valid PIN.

[519] The NGN GETS AS shall provide up to three prompts to the calling party to enter a valid PIN.

1. **When the calling party fails to respond to a prompt for PIN collection within a configurable time, then the NGN GETS AS shall instruct the MRFC to again prompt the calling party to enter the PIN.**
2. **When the calling party enters an invalid PIN, then the NGN GETS AS shall instruct the MRFC to again prompt the calling party to enter the PIN.**

[519] does not dictate the location of the timer.

[520] When the calling party fails to enter a valid PIN on the third attempt, the NGN GETS AS shall apply priority treatment to instruct the MRFC to provide the treatment resulting in the same user experience as in the case of a service option not available (e.g., an information tone followed by an announcement: "Your service request is denied.").

5.3.5.2 GETS-FC AS

The GETS-FC AS supports the NGN GETS-specific service logic, as described in this Clause, as required to control the processing of a GETS-FC-invoked call/session.

[137] When a GETS-FC AS receives a SIP INVITE request with the Request-URI that contains only a GETS-FC without a following DN, the GETS-FC AS shall initiate procedures with priority treatment to reject the call/session (e.g., treat as an invalid feature code) with SIP 403 (Forbidden) response with a Reason header field [Q.850] cause value of 21 (call rejected).

[139] When a GETS-FC AS receives a SIP INVITE request including a GETS-FC and does not contain the RPH with the ets namespace, the GETS-FC AS shall initiate procedures with priority treatment to continue the call/session and create a log of the error condition that contains:

- **Date and time of the event, and**
- **Copy of the SIP INVITE request.**

The GETS-FC AS then invokes NGN GETS-specific processing to determine if the calling party is authorized to originate an NGN GETS call/session. Various options can be used by the GETS-FC AS to obtain Service User subscription information to perform authorization.

[140] A GETS-FC AS shall attempt to authorize and determine the priority level of the calling party for a GETS-FC-invoked service based on one of the following options:

1. **If GETS-FC Service User subscription information is maintained in the GETS-FC AS, then the GETS-FC AS uses locally-stored information to authorize the NGN GETS call/session and determine the priority level of the Service User.**
2. **If GETS-FC Service User subscription information is maintained in an HSS, then the GETS-FC AS retrieves the Service User subscription information from the HSS. The GETS-FC AS uses the retrieved information to authorize the NGN GETS call/session and determine the priority level of the Service User.**

For Option 2, the GETS-FC AS sends a Diameter UDR message to an SLF or HSS to access Service User subscription information maintained in the HSS. Corresponding procedures are specified in [672] and [673] of Clause 5.3.5.1.2. The Diameter UDR message may be sent at registration or as needed for an NGN GETS call/session. The subscription information associated with GETS-FC service is specified in [366] of Clause 6.3.9. The NGN GETS subscription information includes information that is unique to particular NGN GETS (Voice and Video) service types.

If the calling party is subscribed for GETS-FC service or if the GETS-FC AS is unable to determine the authorization status of the calling party (e.g., fail-open scenario), then the calling party is granted service; otherwise, the calling party is denied service.

[141] Based on the GETS-FC Service User subscription information of the calling party,

1. **When the NGN GETS call/session is authorized, the GETS-FC AS shall send to the S-CSCF a SIP INVITE request, without the GETS-FC in the Request-URI and including the remainder of the Request-URI. The SIP INVITE request shall include the RPH with the provisioned ets.x, and the wps.y based on the Service User's priority level.**
2. **When the NGN GETS call/session is not authorized, the GETS-FC AS shall reject the call/session with a SIP 403 (Forbidden) response with a Reason header field [Q.850] cause value of 21 (call rejected).**

When the GETS-FC AS is unable to determine the authorization status of the call/session because of network impairments (e.g., server outage), the GETS-FC AS shall send to the S-CSCF a SIP INVITE request, without the GETS-FC in the Request-URI and including the remainder of the Request-URI. The SIP INVITE request shall include the RPH with the provisioned ets.x and without a wps namespace.

For option 1 above, the r-priority value of the wps.y namespace is based on Service User's priority level. See Clause 4.3.3.1.2 for mapping between Service User's priority level and r-priority.

5.3.5.3 GETS-AN AS

The GETS-AN AS functionality supports the NGN GETS-specific service logic required to control the processing of a GETS-AN-invoked NGN GETS call/session. Since the same GETS-AN value applies to different NGN GETS (Voice and Video) service types, the GETS-AN AS differentiates these service invocations based on the contents of the SDP information as contained in the SIP INVITE request.

[142] When the user string in the Request-URI in the received SIP INVITE request contains at least ten digits, the GETS-AN AS shall determine whether the received user string matches one of the provisioned GETS-AN strings, starting the match with the first of the last ten digits of the received user string.

[521] When the user string in the Request-URI in the received SIP INVITE request is received by the GETS-AN AS, the GETS-AN AS shall differentiate amongst different types of NGN GETS service invocations based on the SDP contents as contained in the SIP INVITE request.

The term ‘user string’ refers to the user portion of a SIP:URI with user=phone or the ‘telephone-subscriber’ portion of a TEL:URI (ignoring any visual separators).

[143] When there is a match between the received user string in the Request-URI and a provisioned GETS-AN string per [142], the GETS-AN AS shall recognize the SIP INVITE request as a GETS-AN request, shall give priority treatment in all subsequent processing of the call/session, and shall mark all subsequent signaling for the call/session with appropriate NGN GETS markings. The GETS-AN AS shall initiate procedures to select an MRFC. Priority treatment shall be provided for this selection process.

The priority treatment in [143] is implementation-dependent, but may include a selection from a set of MRFCs that is larger than that available to a normal call/session, and queuing and automatic reattempts if no MRFCs are available. Corresponding procedures are specified in [675] of Clause 5.3.5.1.4.

[144] When the received user string in the Request-URI matches none of the provisioned GETS-AN strings per [142], or the user string in the Request-URI contains less than ten digits, the GETS-AN AS shall reject the call/session request with a SIP 488 (Not Acceptable Here) response and create a log of the error condition that contains:

- **Date and time of the event, and**
- **Copy of the SIP INVITE request.**

The GETS-AN AS controls the user interaction via the selected MRFC for collection of PIN and DN. After being prompted, the calling party enters a PIN or a PIN followed immediately by a DN. For a GETS-AN call/session request, the MRFC sends the user-entered PIN or the PIN together with a DN to the GETS-AN AS. The GETS-AN AS treats the first 12 digits received from the MRFC as the PIN, and any additional digits as the DN.

For the establishment of the NGN GETS Video call/session, the GETS-AN AS needs to manipulate the media streams (i.e., to initially establish an audio stream to an MRFC for collection of a PIN and DN, and to subsequently establish video and audio streams to the destination UE). The GETS-AN AS establishes an audio stream from the originating UE to the MRFC/MRFP while making the video media stream (as requested by the originating Service User) inactive during the initial UE to MRFC interactions.

[522] Upon receipt of the SIP INVITE request supporting both audio and video media streams for the NGN GETS Video service, the GETS-AN AS shall setup the audio stream from the originating UE to the MRFC and shall set the video media stream to inactive during the UE to MRFC interactions.

The GETS-AN AS stores GETS-AN service-related information including Service User’s credentials (i.e., a Service User’s PIN, priority level, and calling privileges). Clause 6.3.10 specifies the information stored and additional provisioning requirements associated with NGN GETS Credentials.

[145] The GETS-AN AS shall validate the PIN received from the MRFC using NGN GETS Credentials information. For a valid PIN, the GETS-AN AS retrieves the Service User’s priority level and calling privileges.

[146] When the GETS-AN AS cannot validate the PIN received from the MRFC because of network impairments (e.g., server outage), the GETS-AN AS shall treat the PIN as valid.

The above requirement defines the “fail-open” scenario. The NGN GETS Credentials may be maintained locally with the GETS-AN AS.

The GETS-AN AS interacts with an MRFC/MRFP to collect a PIN from the calling party. The GETS-AN AS provides up to three prompts to the calling party to enter a valid PIN. Corresponding procedures are specified in [519] and [520] of Clause 5.3.5.1.4.

[149] When the GETS-AN AS determines that a user-entered PIN is valid, or treats the user-entered PIN as valid (i.e., fail-open scenario), and the user had not entered a DN together with the PIN, the GETS-AN AS shall instruct the MRFC to prompt the calling party to enter the DN.

For a fail-open scenario, the network continues the NGN GETS call/session as if the Service User has been authorized, with full calling privileges as specified in [151]. The MRFC sends the user-entered DN to the GETS-AN AS.

[150] After the GETS-AN AS (a) determines that a user-entered PIN is valid, (b) obtains the Service User's priority level and calling privileges, and (c) obtains the user-entered DN (the GETS-AN AS may have received the DN from the MRFC together with the PIN or separately), the GETS-AN AS shall apply priority treatment to process the DN as follows. If the DN is a valid:

1. **NANP number, including 8YY number (but excluding the numbers treated in 2, 3, and 4) and the Service User is authorized to make an NANP call/session;**
2. **E.164 international number and the Service User is authorized to make an international call/session;**
3. **GETS-NT and the Service User is authorized to invoke a GETS-NT call/session; or**
4. **GETS-PDN and the Service User is authorized to invoke a GETS-PDN call/session,**

then the GETS-AN AS shall apply priority treatment for further call/session processing based on the DN.

[150] specifies that a Service User's NGN GETS service profile overrides the user's normal service profile. For example, item 2) of [150] potentially overrides a Service Provider's restrictions on a subscriber UE (i.e., it may be possible to make NGN GETS international calls/sessions from a UE barred from originating normal international calls/sessions).

[151] When the GETS-AN AS (a) determines that a user-entered PIN is to be treated as valid (i.e., fail-open scenario), and (b) obtains the user-entered DN (the GETS-AN AS may have received the DN from the MRFC together with the PIN or separately), the GETS-AN AS shall apply priority treatment to process the call/session based on the DN as if the user is authorized for the NGN GETS call/session, with full calling privileges.

[153] After a GETS-NT or GETS-PDN is translated, or after a user-entered DN that is not a GETS-NT or GETS-PDN is validated, the GETS-AN AS shall instruct the MRFC to provide the Service User an indication that NGN GETS is being used (e.g., an announcement "You are using GETS (with Service Provider Identifier of NGN GETS authorizing carrier)"). If the announcement cannot be provided, the GETS-AN AS shall continue to process the NGN GETS call/session without a confirmation announcement. The GETS-AN AS shall establish the call/session between the calling and called parties when the MRFC interactions are completed.

[154] When MRFC interactions as specified in [153] are completed, the GETS-AN AS shall apply priority treatment to progress the NGN GETS call/session. The GETS-AN AS shall send a SIP INVITE request with the Request-URI corresponding to the destination DN and an RPH including the provisioned ets.x and wps.y, where "y" corresponds to the Service User's priority level. The GETS-AN AS shall include this wps.y resource value in all subsequent SIP messages sent. In the case of a fail-open scenario, the RPH shall only include the provisioned ets.x.

Illustrative flows to progress the NGN GETS call/session are described in Clause 6.1.3 of [ATIS-1000049] (for an NGN GETS Voice call/session). Third-Party Call Control (3PCC) procedures may alternately be used, as applicable, to establish the call/session between the calling and the called parties, as discussed in [RFC 3725]. This Standard does not impose requirements on the specific set of procedures used to establish the call/session between the calling and the called parties. Note that the provisioned ets.x value in an NGN GETS AS may be different from the ets.x value provisioned in other FEs.

Given the need to revert the audio media stream to both audio and video streams towards the originating UE for the NGN GETS Video call/session, the GETS-AN AS activates the video media stream via a SIP message towards the originating UE that indicates acceptance of a particular set of (audio and video) media streams by the destination UE.

[523] Upon completion of the SDP negotiations towards the called party for the NGN GETS Video service, the GETS-AN AS shall set the video media stream to active towards the originating UE.

[155] After the GETS-AN AS (a) determines that a user-entered PIN is valid, (b) obtains the Service User's priority level and calling privileges, and (c) obtains the user-entered DN, the GETS-AN AS shall apply priority treatment to process a DN satisfying any of the following criteria:

1. **An invalid DN, as determined by the GETS-AN AS;**
2. **A GETS-AN;**
3. **An NANP number and the Service User is not authorized to make NANP calls/sessions;**
4. **An E.164 international number and the Service User is not authorized for international calls/sessions;**
5. **A GETS-NT and the Service User is not authorized for GETS-NT calls/sessions; or**
6. **A GETS-PDN and the Service user is not authorized for GETS-PDN calls/sessions,**

then the GETS-AN AS shall apply priority treatment to instruct the MRFC to provide the treatment resulting in the same user experience as in the case of a public call/session to an invalid DN or for service option not available (e.g., an information tone followed by an announcement: "Your call cannot be completed as dialed. Please check the number and try again.").

[156] After the GETS-AN AS (a) determines that a user-entered PIN is valid, and (b) obtains the Service User's priority level and calling privileges, but the user fails to respond to the prompt to enter the DN (with at least the first digit of the DN) within a configured time, the GETS-AN AS shall apply priority treatment to instruct the MRFC to provide the treatment resulting in the same user experience as in the case of a public call/session to an invalid DN or for service option not available (e.g., an information tone followed by an announcement: "Your call cannot be completed as dialed. Please check the number and try again.").

5.3.5.4 GETS-NT AS

The GETS-NT AS functionality supports the NGN GETS-specific service logic as required to control the processing of a GETS-NT-invoked NGN GETS call/session. Since the same GETS-NT value applies to different NGN GETS (Voice and Video) service types, the GETS-NT AS differentiates these service invocations based on the contents of the SDP information as contained in the SIP INVITE request.

[157] When the user string in the Request-URI in the received SIP INVITE request contains at least ten digits, the GETS-NT AS shall determine whether the first three digits of the last ten digits of the received user string are a provisioned GETS-NT 3-digit string (per [588]). If there is not a match, see [159].

[524] When the user string in the Request-URI in the received SIP INVITE request is received by the GETS-NT AS, the GETS-NT AS shall differentiate amongst different types of NGN GETS service invocations based on the SDP contents as contained in the SIP INVITE request.

The term 'user string' refers to the user portion of a SIP:URI with user=phone or the 'telephone-subscriber' portion of a TEL:URI (ignoring any visual separators).

[525] When the first three digits of the last ten digits of the received user string in the Request-URI are a provisioned GETS-NT 3-digit string per [157], and when the last ten digits do not match any of the secondary (negative) matching strings as specified in [588], the GETS-NT AS shall recognize the SIP INVITE request as a GETS-NT-invoked call/session request, shall give priority treatment in all subsequent processing of the call/session, and shall mark all subsequent signaling for the call/session with appropriate NGN GETS markings. If the

call/session was not received from a GETS-AN AS, the GETS-NT AS shall initiate procedures to select an MRFC. Priority treatment shall be provided for this selection process.

The priority treatment in [525] is implementation-dependent, but may include a selection from a set of MRFCs that is larger than that available to a normal call/session, queuing and automatic reattempts if no MRFCs are available. The GETS-NT AS sends a SIP INVITE request toward the selected MRFC. Corresponding procedures are specified in [675] of Clause 5.3.5.1.4.

[159] When the first three digits of the last ten digits of the received user string in the Request-URI are not a provisioned GETS-NT 3-digit string per [157], or the user string in the Request-URI contains less than ten digits, the GETS-NT AS shall reject the call/session request with a SIP 488 (Not Acceptable Here) response and create a log of the error condition that contains:

- **Date and time of the event, and**
- **Copy of the SIP INVITE request.**

For a GETS-NT call/session request, the MRFC send**s** the user-entered PIN to the GETS-NT AS.

For the establishment of the NGN GETS Video call/session, the GETS-NT AS needs to manipulate the media streams (i.e., to initially establish an audio stream to an MRFC for collection of a PIN, and to subsequently establish video and audio streams to the destination UE). The GETS-NT AS establishes an audio stream from the originating UE to the MRFC/MRFP while making the video media stream (as requested by the originating Service User) inactive during the UE to MRFC interactions.

[526] Upon receipt of the SIP INVITE request supporting both audio and video media streams for the NGN GETS Video service, the GETS-NT AS shall setup the audio stream from the originating UE to the MRFC and shall set the video media stream to inactive during the UE to MRFC interactions.

The GETS-NT AS maintains GETS Translation information which provides number translation for a GETS-NT-invoked call/session and number translation for a GETS-AN-invoked call/session when a GETS-NT or GETS-PDN is entered by a Service User. Clause 6.3.10 specifies the information stored and additional provisioning requirements for GETS Translation information.

The GETS-NT AS stores GETS-NT service-related information including Service User's credentials (i.e., a Service User's PIN, priority level, and calling privileges). Clause 6.3.10 specifies the information stored and additional provisioning requirements associated with NGN GETS Credentials.

[160] The GETS-NT AS shall validate the PIN received from the MRFC using NGN GETS Credentials information. For a valid PIN, the GETS-NT AS retrieves the Service User's priority level and calling privileges.

[161] When the GETS-NT AS cannot validate the PIN received from the MRFC because of network impairments (e.g., server outage), the GETS-NT AS shall treat the PIN as valid.

The above requirement defines the "fail-open" scenario. The NGN GETS Credentials may be maintained locally with the GETS-NT AS.

The GETS-NT AS interacts with an MRFC/MRFP to collect a PIN from the calling party. The GETS-NT AS provides up to three prompts to the calling party to enter a valid PIN. Corresponding procedures are specified in [519] and [520] of Clause 5.3.5.1.4.

Given the need to revert the audio media stream to both audio and video streams towards the originating UE for the NGN GETS Video call/session, the GETS-NT AS activates the video media stream via a SIP message towards the originating UE that indicates acceptance of a particular set of (audio and video) media streams by the destination UE.

[527] Upon completion of the SDP negotiations towards the called party for the NGN GETS Video service, the GETS-NT AS shall set the video media stream to active towards the originating

UE.

[164] After the GETS-NT AS (a) determines that a user-entered PIN is valid, (b) obtains the Service User's priority level and calling privileges, and (c) determines that the user is authorized for a GETS-NT or GETS-PDN-invoked call/session, as appropriate, the GETS-NT AS shall translate the GETS-NT or GETS-PDN to a destination DN.

[165] The GETS-NT AS shall be able to operate in a PIN bypass mode when this mode is activated per the Authorized Agency directive. When the PIN bypass mode is activated, the GETS-NT AS shall not prompt the user for a PIN, shall treat the Service User as authorized, and shall proceed with GETS-NT processing of the call/session.

[166] When the GETS-NT AS determines that a user-entered PIN is to be treated as valid (i.e., fail-open scenario) or the PIN-bypass mode is activated, the GETS-NT AS shall apply priority treatment to process the NGN GETS call/session as if the user is authorized for the GETS-NT-invoked call/session.

[167] After GETS-NT or GETS-PDN translation, the GETS-NT AS shall apply priority treatment to instruct the MRFC to provide the Service User an indication that NGN GETS are being used (e.g., an announcement: "You are using GETS (with Service Provider Identifier of NGN GETS authorizing carrier)"). This announcement shall also be provided in the PIN Bypass mode. If the announcement cannot be provided, the GETS-NT AS shall continue to process the NGN GETS call/session (without a confirmation announcement) as described in [168].

[168] When MRFC interactions are completed, the GETS-NT AS shall apply priority treatment to establish the NGN GETS call/session between the calling and called parties. The GETS-NT AS shall send a SIP INVITE request with the Request-URI including the destination DN and an RPH including provisioned ets.x and wps.y, where "y" corresponds to the Service User's priority level. The GETS-NT AS shall include this wps.y resource value in all subsequent SIP messages sent. In the case of fail-open or PIN-bypass scenarios, the RPH shall only include the provisioned ets.x.

[169] When the GETS-NT AS determines that a user-entered PIN is valid but determines that the call/session cannot proceed (e.g., the Service User does not have GETS-NT calling privileges or the GETS-NT cannot be translated), the GETS-NT AS shall apply priority treatment to instruct the MRFC to provide the treatment resulting in the same user experience as in the case of a public call/session to an invalid DN or for service option not available (e.g., an information tone followed by an announcement: "Your call cannot be completed as dialed. Please check the number and try again.").

5.3.6 MRFC

This Clause specifies requirements associated with MRFC processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic MRFC functionality as defined in 3GPP Release 11 specifications.

Various implementation options are possible for the NGN GETS AS (i.e., GETS-AN AS or GETS-NT AS) interactions with the MRFC. The NGN GETS AS could download a script to the MRFC for execution, or the script could be located at the MRFC. An additional implementation option is to have the NGN GETS AS provide "atomic" instructions to the MRFC for execution. In all cases, the NGN GETS AS controls the user interactions.

The MRFC may use VoiceXML and HTTP for the purpose of retrieving scripts/instructions from an NGN GETS AS, for sending PIN and DN collected from the calling party to an NGN GETS AS, and for getting instructions from an NGN GETS AS for further interaction with the calling party.

5.3.6.1 SIP Processing

The MRFC supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1 with the following addition.

[170] Upon receipt of an RPH in a SIP message associated with an NGN GETS call/session, an

MRFC shall include the same RPH value in any corresponding SIP requests or responses that it sends, with the exception of error cases identified in [68].

5.3.6.2 H.248 Processing

The MRFC supports the common set of H.248 processing capabilities for NGN GETS, as specified in Clause 5.2.3 with the exception of supporting the Priority indicator in the H.248 Modify_Request command in [81].

5.3.6.3 Priority Treatment Requirements

The MRFC applies the priority treatment requirements in processing the signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clauses 5.2.4.1 (SIP-Related Priority Treatment), 5.2.4.3 (HTTP-Related Priority Treatment), 5.2.4.4 (H.248-Related Priority Treatment), and 5.2.4.6 (General Priority Treatment).

5.3.6.4 Other MRFC Requirements

The MRFC meets the following requirements when it executes GETS-AN or GETS-NT-invoked call/session processing:

[172] **On receipt of a SIP INVITE request containing an RPH with a valid ets.x, the MRFC shall initiate procedures with priority treatment to allocate processing and media resources for use in a two-way media path between the UE of the calling party and a selected MRFP. The priority treatment can include a MRFC mechanism for choosing one of multiple MRFPs or queueing for MRFP resources.**

If the MRFC is successful, the MRFC sends a SIP 200 OK response including the RPH with ets.x toward the NGN GETS AS. If the MRFC cannot proceed successfully, normal SIP procedures are applied, allowing the NGN GETS AS to reattempt using an alternate resource.

[173] **The MRFC shall respond to instructions from the NGN GETS AS to enable MRFP interactions with the calling party for collection of digits (e.g., PIN and/or DN) and for playing NGN GETS announcements.**

When an announcement is completed (and when the corresponding SIP dialog is to be terminated) for an NGN GETS call/session, the MRFC notifies the NGN GETS AS.

The MRFC includes appropriate priority indications (e.g., RPH with ets.x for SIP messages) when it interacts with the NGN GETS AS for an NGN GETS call/session, consistent with the general requirements referenced in Clauses 5.3.6.1 and 5.3.6.3.

[554] **When the MRFC determines that an H.248 context needs to be created on receipt of a SIP INVITE request with RPH including ets.x and wps.y, it shall include the Priority indicator with the appropriate priority value in the H.248 Add_Request command sent to an MRFP. The mapping of the Service User's priority level value (y) in the wps namespace to the Service User's priority level value carried in the Priority indicator shall be as shown in Table 4.5.**

[555] **When the MRFC determines that an H.248 context needs to be created on receipt of a SIP INVITE request with RPH including ets.x but without wps.y, it shall include the Priority indicator with a default priority value in the H.248 Add_Request command sent to an MRFP.**

The default value (in the range 11 – 15) to be included in the H.248 Priority indicator should be based on Authorized Agency policy, and provisioned in the MRFC.

Configuration requirement to set the default value is specified in [276].

5.3.7 MRFP

This clause specifies requirements associated with MRFP processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic MRFP functionality as defined in 3GPP Release 11 specifications.

[556] **An MRFP shall apply the procedures of [H.248.1] for the processing of the Priority indicator in the H.248 Add_Request command. Based on the presence of the Priority indicator populated with a value as indicated in Table 4.5 in the H.248 Add_Request command, an MRFP shall mark the contexts accordingly, and apply the priority treatment specified in Clauses 5.2.4.4 (H.248-Related Priority Treatment), 5.2.4.5 (RTP-Related Priority Treatment), and 5.2.4.6 (General Priority Treatment) for an NGN GETS call/session.**

[177] **For NGN GETS call/session user interactions, the MRFP shall support Table 3, Section 3.2 and Sections 2.2, 2.3, and 3.2 of [RFC 4733] for all codecs that the MRFP supports. For G.711 codecs, in addition to supporting [RFC 4733], the MRFP shall be capable of receiving Dual Tone Multi-Frequency (DTMF) in the Clearmode payload type.**

5.3.8 PCRF

This Clause specifies requirements associated with PCRF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic PCRF functionality as defined in 3GPP Release 11 specifications.

5.3.8.1 Diameter Processing

To support policy control, an AF (P-CSCF) uses Diameter messages (as described in Clause 4.3.2) to interact with the PCRF (via the Rx interface) for an NGN GETS call/session.

5.3.8.2 Priority Treatment Requirements

The PCRF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to Diameter-capable FEs (Clause 5.2.4.2) are applicable to the PCRF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.8.3 Other PCRF Requirements

When the PCRF receives a Diameter message associated with an NGN GETS call/session, the MPS-Identifier AVP indicates that this is a priority session.

[557] **When a PCRF receives a Diameter AA-Request (AAR) message with the MPS-Identifier AVP, the PCRF shall initiate Access Network-specific policy control procedures with priority.**

The MPS-Identifier AVP is described in Clause 4.3.2.1.2. MPS-Identifier AVP value ‘NGN GETS’ is used with the NGN GETS Voice and Video services.

NOTE: Subject to future study, unique values of the MPS-Identifier AVP may be used to allow the PCRF to distinguish between variants of NGN GETS.

In addition to the MPS-Identifier AVP, the Diameter AAR message contains a Reservation-Priority AVP value that is based on the Service User’s priority level, and a Media-Type AVP (within the Media-Component-Description

AVP) to indicate the type of media (e.g., audio, video, etc.) used for the NGN GETS call/session. The DRMP AVP is also included, as specified in requirement [722] of Clause 5.2.2.

[558] When a PCRF receives a Diameter AA-Request (AAR) message that includes the MPS-Identifier AVP, the PCRF shall consider that the request is associated with NGN GETS and shall derive appropriate values for the required bearer(s) based on the values of the MPS-Identifier AVP, the Reservation-Priority AVP, and the Media Type AVP.

When [557] applies, the corresponding PCRF procedures (e.g., population of specific AVPs over the Gx interface) are specific to the particular Access Network.

- For the NGN GETS Voice and Video services, the PCRF may send to the IP-Access Network a Diameter RAR message, populated with appropriate QCI and ARP AVPs. These AVPs are used to trigger the appropriate priority processing for the NGN GETS call/session.

Corresponding PCRF requirements specific to an LTE Access Network are described in [ATIS-1000065.2015].

5.3.9 HSS

This clause specifies requirements associated with HSS processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic HSS functionality as defined in 3GPP Release 11 specifications.

5.3.9.1 Diameter Processing

The HSS is a Diameter-capable FE.

The HSS supports the common set of Diameter processing capabilities for NGN GETS, as discussed in Clause 5.2.2.

[559] When an HSS receives from an NGN GETS AS a Diameter UDR message with the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the HSS shall initiate procedures with priority processing to retrieve subscription information.

The HSS sends to the NGN GETS AS a Diameter User-Data-Answer (UDA) message that includes the subscription information for the Service User in the User-Data AVP.

For NGN GETS call/session terminations, the HSS is queried by the I-CSCF to locate the S-CSCF associated with the called party (via a Diameter Location-Info-Request (LIR) message).

[560] When an HSS receives from an I-CSCF a Diameter LIR message with the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the HSS shall initiate procedures with priority processing to determine the S-CSCF assigned to the called party.

When [560] applies, the HSS sends to the I-CSCF a Diameter Location-Info-Answer (LIA) message that includes the S-CSCF assigned to the called party.

For NGN GETS call/session terminations, the HSS is queried by the S-CSCF to establish an NGN GETS call/session to an unregistered terminating user (via a Diameter Server-Assignment-Request [SAR] message).

[561] When an HSS receives a Diameter SAR message with the the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the HSS shall initiate procedures with priority processing to respond to the query.

When [561] applies, the HSS sends a Diameter Server-Assignment-Answer (SAA) message.

5.3.9.2 Other HSS Requirements

The HSS stores the Service User's profile for GETS-FC-invoked service. The Service User's profile includes the iFC, as required at the S-CSCF to trigger the corresponding NGN GETS AS processing. The population and usage of iFC for an NGN GETS call/session represents normal IMS behavior for an HSS, and thus does not require any NGN GETS-specific capabilities. Associated provisioning requirements are included in Clause 6.3.9.

The HSS may optionally store NGN GETS subscription information (e.g., Service User's priority level) for Service Users. Associated provisioning requirements are included in Clause 6.3.9. The NGN GETS AS can retrieve the NGN GETS service subscription information for a GETS-FC-invoked call/session via a Diameter User-Data-Request (UDR) message.

5.3.9.3 Priority Treatment Requirements

The HSS applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to Diameter-capable FEs (Clause 5.2.4.2) are applicable to the HSS, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.10 TrGW

This Clause specifies requirements associated with TrGW processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic TrGW functionality as defined in 3GPP Release 11 specifications.

[567] A TrGW shall apply the procedures of [H.248.1] for the processing of the Priority indicator in the H.248 Add_Request and Modify_Request commands. Based on the presence of the Priority indicator populated with a value as indicated in Table 4.5 in the H.248 Add_Request and Modify_Request commands, a TrGW shall mark the contexts accordingly, and apply the following priority treatments for an NGN GETS call/session:

- **H.248-Related Priority Treatment as specified in Clause 5.2.4.4,**
- **RTP-Related Priority Treatment either: a) as specified in Clause 5.2.4.5 for the IP packets that it sends within its IMS Core Network or b) set the IP header DSCP value to the fixed DSCP value (VOICE-ADMIT) for the IP packets that it sends to an entity outside its IMS Core Network,**
- **General Priority Treatment as specified in Clause 5.2.4.6.**

5.3.11 BGCF

This Clause provides requirements associated with BGCF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic BGCF functionality as defined in 3GPP Release 11 specifications.

When the BGCF functionality is incorporated into an entity that supports other FE capabilities, the composite set of requirements apply to that entity. For example, when an entity provides interconnection with another VoIP network, the IBCF requirements in Clause 5.3.4 also apply to that entity.

5.3.11.1 SIP Processing

The BGCF supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1 with the following addition.

[189] Upon receipt of an RPH in a SIP message associated with an NGN GETS call/session, a BGCF shall include the same RPH value in any corresponding SIP requests or responses that it sends, with the exception of error cases identified in [68].

5.3.11.2 Priority Treatment Requirements

The BGCF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to NGN GETS SIP-capable FEs (Clause 5.2.4.1) are applicable to the BGCF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.12 MGCF/SGW

This Clause specifies requirements associated with MGCF/SGW processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic MGCF/SGW functionality as defined in 3GPP Release 11 specifications.

The MGCF/SGW implements standard ANSI SS7 (MTP, ISUP, TCAP, SCCP) protocols and implements SIP-ISUP interworking as specified in [ATIS-1000679].

5.3.12.1 SIP Processing

The MGCF/SGW supports the common set of SIP processing capabilities for NGN GETS, as discussed in Clause 5.2.1 with the exception of common SIP RPH requirement [63].

5.3.12.2 H.248 Processing

The MGCF/SGW supports the common set of H.248 processing capabilities for NGN GETS, as specified in Clause 5.2.3 with the exception of supporting the Priority indicator in the H.248 Modify_Request command in [81].

5.3.12.3 Priority Treatment Requirements

The MGCF/SGW applies the priority treatment requirements in processing the signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clauses 5.2.4.1 (SIP-Related Priority Treatment), 5.2.4.4 (H.248-Related Priority Treatment), and 5.2.4.6 (General Priority Treatment) for an NGN GETS call/session routed to a PSN, and for an NGN GETS call received from a PSN and routed to a Service Provider network.

If Network Traffic Management code controls are implemented at the MGCF/SGW, the MGCF/SGW provides treatments for identified NGN GETS call/session requests with regard to the Network Management Controls as specified in [344] to [355].

[344] **If Automatic Code Gap (ACG) controls are implemented at the MGCF/SGW and a GETS call encounters an ACG control with an infinite gap interval (i.e., a value of Gap Interval = stopAllCalls), the call shall be subject to the ACG control.**

[345] **If ACG controls are implemented at the MGCF/SGW and a GETS call encounters an ACG control with a finite gap interval, the call shall not be blocked.**

[346] **If manual cancel-to controls are implemented at the MGCF/SGW, GETS calls shall be exempt from such controls. This implies that the call will be routed on the trunk group even if the manual cancel-to control is set at 100%.**

[347] **If manual skip controls are implemented at the MGCF/SGW, GETS calls shall be subject to manual skip control action set at 100% but otherwise shall be exempt.**

[348] **If ACC is implemented at the MGCF/SGW, GETS calls shall be exempt from ACC cancel-to control action. This implies that the call will be routed on the trunk group even if the ACC cancel-to control is set at 100%.**

[349] **If ACC is implemented at the MGCF/SGW, GETS calls shall be subject to ACC skip control**

action set at 100% but otherwise shall be exempt.

[350] If TR controls are implemented at the MGCF/SGW, GETS calls shall be exempt from TR cancel-to control action. This implies that the call will be routed on the trunk group even if the TR cancel-to control is set at 100%.

[351] If TR controls are implemented at the MGCF/SGW, GETS calls shall be subject to TR skip control action set at 100% but otherwise shall be exempt.

[352] If reroute controls are implemented at the MGCF/SGW, GETS calls shall be subject to control action by reroute controls.

[353] If cancel-from controls are implemented at the MGCF/SGW, GETS calls shall be subject to control action by cancel-from controls set at 100% but otherwise shall be exempt.

[354] If pre-hunt trunk group controls are implemented at the MGCF/SGW, they shall be processed before trunk queuing when they are active on the same trunk group.

[355] If post-hunt trunk group controls are implemented at the MGCF/SGW, trunk queuing shall be processed before post-hunt trunk group controls when they are active on the same trunk group.

5.3.12.4 Other MGCF/SGW Requirements

[191] An MGCF/SGW shall be able to identify an NGN GETS call/session based on the:

- **Presence of RPH with a valid ets.x in a SIP INVITE request,**
- **Presence of Called Party Number parameter with a GETS-AN or GETS-NT in an ISUP IAM, or**
- **Presence of Calling Party's Category parameter coded as "NS/EP Call" in an ISUP IAM.**

An MGCF/SGW may receive a Request-URI with GETS-AN or GETS-NT from an FE within the IMS Core Network if the Service Provider network does not perform authorization for a GETS-AN or GETS-NT-invoked call/session.

[192] When the Nature of address indicator subfield in the Called Party Number parameter in a received ISUP IAM is set to national (significant) number, an MGCF/SGW shall be able to perform string matches between the address digits carried in the Address signal subfield of the Called Party Number parameter and the provisioned GETS-AN or GETS-NT strings. The MGCF/SGW shall match the received address digits starting the match with the leading digit of the received address digits.

[193] For an NGN GETS call/session routed to a PSN, the MGCF/SGW shall map the Calling Party's Category and Precedence parameters in the ISUP IAM from the received SIP INVITE request as shown in Table 5.4.

Table 5.4. Mapping of SIP INVITE request header fields to corresponding ISUP IAM message parameters

Incoming SIP INVITE Request Header Fields			Outgoing ISUP IAM Message Parameters		
Request-URI	**RPH – ets namespace**	**RPH – wps namespace**	**Called Party Number**	**Calling Party's Category**	**Precedence**
GETS-AN or GETS-NT	ets.x	wps.y	GETS-AN or GETS-NT	"NS/EP Call" *	Level 'Y' **
		None		"NS/EP Call" *	None
	None	wps.y	< This is an error condition - Call/session rejected >		
		None	GETS-AN or GETS-NT	"NS/EP Call" *	None
DN (not GETS-AN or GETS-	ets.x	wps.y	DN	"NS/EP Call" *	Level 'Y' **
		None			None

Incoming SIP INVITE Request Header Fields			Outgoing ISUP IAM Message Parameters		
Request-URI	**RPH – ets namespace**	**RPH – wps namespace**	**Called Party Number**	**Calling Party's Category**	**Precedence**
NT)	None	wps.y	< This is an error condition - Call/session rejected >		
		None	DN	Not "NS/EP Call"	None

* Note that outgoing ISUP IAM messages with the CPC parameter set to value "NS/EP Call" are sent with MTP priority 1.

** The above Precedence = Level 'Y' ** entries imply that the Precedence parameter should be included (with a Precedence Level value that is mapped from the 'y' value of the wps namespace and with a corresponding MLPP Service Domain value [mapped from the 'Y' value]). Further details are provided in Clause 4.3.5.2.2.

[194] For an NGN GETS call/session routed to a PSN, the ISUP IAM sent by the MGCF/SGW shall be the same as the corresponding ISUP IAM for a non-GETS call [ATIS-1000679] except with the following GETS-specific coding:

- **The Calling Party's Category parameter shall be coded with a value of "NS/EP Call".**
- **The Precedence parameter, if included, shall be coded as shown in Table 4.6, in particular with the Precedence Level field populated with a value of 0 through 4, as appropriate for the Service User.**
- **The MTP message priority of the IAM shall be set to 1.**

[195] The MGCF/SGW shall implement all GETS priority treatment features applicable to a PSN switch (e.g., trunk queuing, exemption from network management control such as Automatic Congestion Control (ACC) and apply these features to the NGN GETS call/session that is routed to a PSN.

[196] When no outgoing trunk is available at an MGW controlled by this MGCF/SGW for an NGN GETS call/session that needs to be routed to a PSN, the MGCF/SGW shall queue the NGN GETS call/session request. The MGCF/SGW shall send a SIP 182 (Queued) response. When an outgoing trunk becomes available, the MGCF/SGW shall progress the NGN GETS call/session by sending an ISUP IAM. If the MGCF/SGW is unable to queue the NGN GETS call/session request, the MGCF/SGW shall return a SIP 503 (Service Unavailable) response. This response shall include a Reason header field [Q.850] cause value of 34 (no circuit available).

[197] When an NGN GETS call/session request is queued and the queue timer expires, the MGCF/SGW shall remove the NGN GETS call/session request from the queue and send a SIP 408 (Request Timeout) response. This response shall include a Reason header field with the provisioned [Q.850] cause value.

[198] When the MGCF/SGW receives an ISUP Address Complete Message (ACM) or Call Progress (CPG) indicating that a GETS call is queued in the PSN (with a Called Party Status indicator in the Backward Call Indicators parameter set to binary value 11 ("excessive delay")), the MGCF/SGW shall send a SIP 182 (Queued) response.

The MGCF/SGW receives a SIP CANCEL request if the calling party abandons the NGN GETS call/session while the NGN GETS call/session is queued for a trunk at the MGCF/SGW or in the PSN.

The following requirements apply to a GETS/WPS call from a PSN that is routed to a Service Provider network.

[199] When the MGCF/SGW receives a GETS call from a PSN and routes it to a Service Provider network, the MGCF/SGW shall map the Calling Party's Category parameter and the Precedence parameter (if included) in the received ISUP IAM to the SIP INVITE request sent as shown in Table 5.5.

Table 5.5 – Mapping of ISUP IAM message parameters to corresponding SIP INVITE request header fields

Incoming ISUP IAM Message Parameters			Outgoing SIP INVITE Request Header Fields		
Called Party Number	**Calling Party's Category**	**Precedence**	**Request-URI**	**RPH – ets namespace**	**RPH – wps namespace**
GETS-AN or GETS-NT	"NS/EP Call"	Level 'Y'	GETS-AN or GETS-NT	ets.x **	wps.y *
		None		ets.x **	None
	Not "NS/EP Call"	Level 'Y' (not expected to occur.)	GETS-AN or GETS-NT	ets.x **	wps.y *
		None	GETS-AN or GETS-NT	ets.x **	None
DN (not GETS-AN or GETS-NT)	"NS/EP Call"	Level 'Y'	DN	ets.x **	wps.y *
		None		ets.x **	None
	Not "NS/EP Call"	Level 'Y' (not expected to occur - Call/session is processed normally.)	DN	None	None
		None	DN	None	None

* Note that the 'y' value in the above wps.y namespace is based on the Precedence Level 'Y' value.

** "ets.x" refers to the "provisioned ets.x" in Table 5.5.

[200] When the MGCF/SGW receives a GETS call request from a PSN that enters the Service Provider network, but the MGCF/SGW queues the call/session request due to lack of processing or transport resources, the MGCF/SGW shall send an ISUP ACM or a CPG indicating queuing (see [201]).

[201] When the MGCF/SGW receives a SIP 182 (Queued) response subsequent to sending an NGN GETS call/session request on to another FE for a GETS call request from a PSN, the MGCF/SGW shall determine if an ISUP ACM message has already been sent for this NGN GETS call/session request, and shall do one of the following:

1. **If an ISUP ACM message was not previously sent, the MGCF/SGW shall send an ISUP ACM message with a Called Party's Status indicator in the Backward Call Indicators parameter set to binary value 11 ("excessive delay"), or**
2. **If an ISUP ACM message was previously sent, the MGCF/SGW shall send an ISUP CPG message with a Called Party's Status indicator in the Backward Call Indicators parameter set to binary value 11 ("excessive delay").**

[568] If the MGCF/SGW determines that an H.248 context needs to be created on receipt of a SIP INVITE request with RPH including ets.x and wps.y, it shall include the Priority indicator with the appropriate priority value in the H.248 Add_Request command sent to an MGW. The mapping of the Service User's priority level value (y) in the wps namespace to the Service User's priority level value carried in the Priority indicator shall be as shown in Table 4.5.

[569] If the MGCF/SGW determines that an H.248 context needs to be created on receipt of an ISUP IAM with a Precedence parameter, it shall include the Priority indicator with the appropriate priority value in the H.248 Add_Request command sent to an MGW. The mapping of the Service User's priority level value carried in the ISUP Precedence parameter to the Service

User's priority level value carried in the Priority indicator shall be as shown in Table 4.4.

[570] **For an NGN GETS call/session request, if the MGCF/SGW determines that an H.248 context needs to be created, it shall include the Priority indicator with a default priority value in the H.248 Add_Request command sent to an MGW if:**

- **A SIP INVITE request with RPH including ets.x but without wps.y was received, or**
- **An ISUP IAM without a Precedence parameter was received.**

The default value to be included in the H.248 Priority indicator should be based on Authorized Agency policy, and provisioned in the MGCF.

Configuration requirement to set the default value is specified in [276].

If an NGN GETS call/session originating in the PSN that transverses the IMS Core Network is queued for available resources in the Terminating Network, e.g., Radio Access Network, a queuing indicator from the Radio Access Network may be propagated into the IMS Core Network (resulting in a SIP 182 Queued response in the IMS Core Network) and the interworking timer (T_{OIW2}), as specified in [ATIS-1000679] expires, early ringing is provided to the originating UE. This early ringing gives the impression that the NGN GETS call/session has been offered to the called party, when in fact it has not. To avoid early ringing upon expiry of the interworking timer for which an MGCF/SGW has previously received a SIP 182 Queued response, a ringing tone is not provided to the originating UE.

[571] **Upon expiry of the interworking timer (TOIW2), as defined in [ATIS-1000679], for an NGN GETS call/session for which an MGCF/SGW has previously received a SIP 182 Queued response, the MGCF/SGW shall not send a ringing tone towards the originating UE. No ISUP ACM or CPG message shall be generated.**

5.3.13 MGW

This Clause specifies requirements associated with MGW processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic MGW functionality as defined in 3GPP Release 11 specifications.

[572] **An MGW shall apply the procedures of [H.248.1] for the processing of the Priority indicator in the H.248 Add_Request command. Based on the presence of the Priority indicator populated with a value as indicated in Table 4.5 in the H.248 Add_Request command, an MGW shall mark the contexts accordingly, and apply the priority treatment specified in Clauses 5.2.4.4 (H.248-Related Priority Treatment), 5.2.4.5 (RTP-Related Priority Treatment), and 5.2.4.6 (General Priority Treatment) for an NGN GETS call/session routed from the Service Provider network to a PSN, and for a GETS call received from a PSN.**

[207] **For NGN GETS call/session user interactions, the MGW shall support Table 3, Section 3.2 and Sections 2.2, 2.3, and 3.2 of [RFC 4733] for all codecs that the MGW supports. For G.711 codecs, in addition to supporting [RFC 4733], the MGW shall be capable of receiving and sending DTMF in the Clearmode payload type.**

5.3.14 SLF

This Clause specifies requirements associated with SLF processing. Only NGN GETS-specific requirements are included, reflecting incremental requirements that extend beyond basic SLF functionality as defined in 3GPP Release 11 specifications.

5.3.14.1 Diameter Processing

The SLF is a Diameter-capable FE. An SLF provides the address of the HSS that contains the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by a Service Provider.

An SLF is only required if a Service Provider Network has more than one HSS. The SLF may be queried during an NGN GETS call/session in the following scenarios:

- The SLF may optionally be queried by an NGN GETS AS via a Diameter User-Data-Request (UDR) message.
- For NGN GETS call/session terminations, the SLF may be queried by the I-CSCF via a Diameter Location-Info-Request (LIR) message.
- For NGN GETS call/session terminations to an unregistered called party, the SLF may be queried by the S-CSCF via a Diameter Server-Assignment-Request (SAR) message.

The SLF supports the common set of Diameter message processing capabilities for NGN GETS, as discussed in Clause 5.2.2.

5.3.14.2 Other SLF Requirements

This Clause specifies the resolution mechanism, which enables an I-CSCF, S-CSCF, or NGN GETS AS to find the address of the HSS that contains the subscriber data for a given user when multiple and separately addressable HSSs have been deployed by the Service Provider.

An NGN GETS AS may query an SLF to determine the HSS serving the calling party.

[573] When an SLF receives a Diameter User-Data-Request (UDR) message with the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the SLF shall initiate procedures with priority processing to determine the HSS serving the calling party.

When [573] applies, the SLF sends to the NGN GETS AS a Diameter User-Data-Answer (UDA) message that includes the HSS address serving the calling party.

For call/session termination, an I-CSCF may query an SLF to determine the HSS serving the called party.

[574] When an SLF receives a Diameter Location-Info-Request (LIR) message with the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the SLF shall initiate procedures with priority processing to determine the HSS serving the called party.

When [574] applies, the SLF sends to the I-CSCF a Diameter Location-Info-Answer (LIA) message that includes the HSS address serving the called party.

For call/session termination to an unregistered called party, an S-CSCF may query an SLF to progress the call/session.

[575] When an SLF receives a Diameter Server-Assignment-Request (SAR) message with the DRMP AVP with a value of 4 or less and/or the Session-Priority AVP, the SLF shall initiate procedures with priority processing.

When [575] applies, the SLF sends to the S-CSCF a Diameter Server-Assignment-Answer (SAA) message.

5.3.14.3 Priority Treatment Requirements

The SLF applies priority treatment when processing signaling messages related to an NGN GETS call/session (e.g., allocating local resources with priority), as discussed in Clause 5.2.4. Corresponding requirements related to Diameter-capable FEs (Clause 5.2.4.2) are applicable to the SLF, beyond the general priority treatment requirements (Clause 5.2.4.6).

5.3.15 Access Session Border Gateway (A-SBG)

The A-SBG anchors NGN GETS media streams from an originating UE, and provides a Back-to-Back User Agent (B2BUA) capability to mask the originating UE's IP address.

6 OAM&P Requirements

This Clause specifies operations requirements to support NGN GETS. Like any other technology and service, NGN GETS will need to be managed for Operations, Administration, Maintenance, and Provisioning (OAM&P).

This Clause only includes OAM&P requirements related to the Service Provider's IMS-based Core Network that are specific to NGN GETS.

This Clause is subdivided as follows:

- Clause 6.1 specifies requirements for the Service Provider network. These are broad *service management function* requirements that need to be supported by the IMS Core Network as a whole. Operations System (OS) requirements are not addressed and are beyond the scope of this Standard.
- Clauses 6.2 and 6.3 specify requirements for specific OAM&P support features that need to be incorporated into the FEs, i.e., an expansion of the FE requirements specified in Clause 5. Common and FE specific requirements are provided in separate subclauses.

6.1 Service Management Functions

The following subclauses correspond to the ITU defined Telecommunication Management Network (TMN) Management Functional Areas (MFAs), namely Fault, Configuration, Accounting, Performance, and Security (FCAPS) [M.3400] [M.3060].

6.1.1 Configuration Management

FE configuration requirements focus on the identification of data elements that a Service Provider network must support and allow to be configurable by a Service Provider. Configuration Management requirements for specific FEs are provided in Clause 6.3.

The additional configuration management requirements for carrier selection and alternate carrier routing are a subject for future study. These would apply to scenarios in which a Service Provider network supports user selection of a desired IXC Service Provider on a per call/session basis (analogous to using a Carrier Access Code with PSTN Equal Access capabilities).

6.1.2 Performance Management

In order to verify the performance of NGN GETS calls/sessions, two kinds of metrics are needed:

- Operational measurements are generated by individual FEs, and report on the performance at that device, e.g., the "percentage of queued calls that were eventually served".
- Per Call Records are generated by the network, and report on the end-to-end disposition of each NGN GETS call/session attempt, whether successful or not. For instance, these records are used to calculate the percent of call/ session attempts that are successful. This should not be confused with the Charging Data Records described in Clause 6.1.5, which only account for billable (i.e., successful) calls/sessions, and may not account for failed or unsuccessful calls/sessions.

In Clause 6.2, the term "operational measurements" is used to refer to underlying FE requirements.

6.1.2.1 Operational Measurements – General Approach

In Clause 6.2, Operational Measurement (OM) requirements are specified for specific NGN GETS SIP-capable FEs. All peg counts should utilize existing collection intervals (used for existing peg counts), e.g., 30-minute intervals. Table 6.1 summarizes the OMs and designates the particular NGN GETS SIP-capable FEs to which each applies.

FEs should be capable of providing such OMs, however a Service Provider may choose to disable OMs for specific FEs and thus FEs must allow such a procedure. Furthermore, if FEs are combined into an NE (e.g., PSTN Gateway), then the corresponding OMs are only required once. An attempt has been made to minimize the number of OMs required (to be cost-effective), and to only require OMs that can be justified (e.g., who will use the OM, what will it be used for, etc.). In general, OMs are considered most useful at the edge of the network and at the AS, however OMs at other nodes may be useful for determining the amount of use and effectiveness (e.g., percentage of queued calls that were eventually served) of NGN GETS priority treatments. The specifics of which additional FEs need to provide OMs will depend on the deployment details, where specific priority treatments are implemented, and which FEs have knowledge of NGN GETS call/session attempts. The desire is that each NGN GETS call/session attempt failure will be recorded (directly or indirectly) by OMs.

Some other considerations made when defining OM requirements are:

- If knowledge of call state/processing is needed to compute the OM, then that OM would only be required at an FE that had such knowledge (i.e., AS or MGCF for PSN interworking).
- OMs triggered by NGN GETS user behavior (e.g., entry of an invalid DN that causes a call to not complete) are useful so that such failure types can be factored out when computing call completion rates.
- Although OMs may be useful in supporting functions beyond performance management (e.g., usage data management and/or security management), such applications were not considered as part of determining the current set of required OMs.

Table 6.1 – Summary of Operational Measurements Applicable to Particular NGN GETS SIP-capable FEs

OM	P-CSCF	I-CSCF	S-CSCF	IBCF	BGCF	NGN GETS AS	MRFC	MGCF
INCOMING NGETS	[579]			[583]		[589]		[627]
OUTGOING NGETS	[580]			[584]		[590]		[628]
RCVD ANSWER						[591]		[629]
CALLER ABANDONED						[592]		[630]
RCVD BUSY						[593]		[631]
RVCD SVC UNAVL						[594]		[632]
RCVD Q TO						[595]		[633]
SENT SVC UNAVL						[596]		[634]
SENT FORBIDDEN	[581]			[585]		[597]		[635]
MEDIA QD								[692]
MEDIA Q TO								[693]
MEDIA Q OVFL								[694]
GETS ERROR LOG						[598]		
NMC EXEMPTIONS	[718]			[719]		[720]		[721]
GETS LIMIT EXCEEDED	[683]			[684]		[686]		[695]
RCVD GETS NANP						[603]		
RCVD AN E164						[610]		
GETS NANP AUTH SUCCESS						[604]		
AN E164 AUTH SUCCESS						[612]		
GETS AUTH FAIL OPEN						[605]		
GETS AUTH FAIL INVLD PIN						[606]		
GETS AUTH FAIL ~PRIV						[607]		
GETS AUTH FAIL INVLD DN						[608]		
RCVD FC NANP						[617]		

OM	P-CSCF	I-CSCF	S-CSCF	IBCF	BGCF	NGN GETS AS	MRFC	MGCF
RCVD FC E164						[618]		
FC NANP AUTH SUCCESS						[619]		
FC E164 AUTH SUCCESS						[620]		
FC AUTH FAIL ~PRIV						[621]		
FC AUTH FAIL INVLD DN						[622]		
GETS DN						[599]		
GETS FC						[600]		
GETS FC+DN						[601]		
GETS NOFC NODN						[602]		

6.1.2.2 Per Call Records – General Approach

Per Call Records are a key means for the Authorized Agency to evaluate NGN GETS call/session effectiveness, both within an individual Service Provider and end-to-end. Per Call Records are similar in structure to Charging Data Records with two notable differences:

- Per Call Records are generated for every NGN GETS call/session attempt, whether or not completed, or billable, and whether or not it reaches the NGN GETS AS;
- Per Call Records include a field, or fields, which indicate the disposition of the call/session.

It is recognized that the specific disposition, or “cause” codes will vary by FE vendor and Service Provider. At a minimum, these disposition codes should allow all NGN GETS call/session attempts to be categorized as:

1. Successfully Answered (whether by a human or a machine);
2. Successful but NOT Answered (including the equivalent of “User Busy” and “Ring No Answer”);
3. User Error (including the equivalent of non-routable number, error in entering the PIN or DN, if appropriate, and user abandon);
4. Failures to establish the requested call/session (these may be further subdivided to indicate, to the extent possible, where, and what kind of, failure occurred).

The Per Call Records should include:

- Originating FE (may be redacted for GETS-NT calls/sessions);
- Originating UE (may be redacted for GETS-NT calls/sessions);
- Originating location (City, State) (may be redacted for GETS-NT calls/sessions);
- Timestamps for call/session origination, call/session completion (if applicable), call/session release;
- Call/session duration;
- Called number, or URI (may be redacted for GETS-NT calls/sessions);
- Terminating/Destination FE (may be redacted for GETS-NT calls/sessions);
- Terminating/Destination UE (may be redacted for GETS-NT calls/sessions);
- Terminating/Destination location (City, State) (may be redacted for GETS-NT calls/sessions);
- Indications of whether it was a GETS-AN, GETS-FC, or GETS-NT call/session;
- Disposition/Cause code or codes.

The precise format and structure of the Per Call Records is likely to vary for different vendors and Service Providers. To the extent possible, the objective is to take advantage of data the Service Provider is already collecting for internal use, rather than requiring completely new functionality.

6.1.3 Fault Management

Fault Management includes functions which enable the detection, isolation and correction of abnormal operation of the IMS Core Network. The essential fault management capabilities do not change with NGN GETS, i.e., they are the same as those for normal calls/sessions. The requirements specific to NGN GETS and related to fault management that are specified in Clause 6.2 are intended to be extensions of existing capabilities.

6.1.4 Security Management

Security Management includes functions such as prevention, detection, containment of security violations and recovery, and security administration. Beyond the authentication and authorization procedures as described in previous Clauses and provisioning of the NGN GETS Credentials, there are no other security management requirements specified. NGN GETS Credentials and GETS Translation security issues are subject to individual agreements between the Authorized Agency and the Service Provider.

6.1.5 Accounting Management

This Clause focuses on the identification of data elements that the Service Provider network must support and allow to be collected for use in the accounting management processes.

Billing for an NGN GETS call/session will rely on the Charging Data Records (CDRs) normally generated in the Service Provider's network. With two exceptions, the conditions for generating a CDR for NGN GETS are the same as those for a normal call/session. The exceptions are that CDRs for a GETS-NT-invoked call/session and for GETS-PDN will not contain location information for the calling and called party. For a GETS-NT and GETS-PDN-invoked call/session, the information to be recorded in Billable Event records that are used to produce a CDR is restricted.

[240] For each NGN GETS call/session, a CDR shall be generated. The CDR shall include an indicator that identifies the call/session as GETS. The indicator shall identify the call/session origination as either a) GETS-FC, b) GETS-AN, c) GETS-NT, d) GETS-FC + GETS-AN, or e) GETS-FC + GETS-NT.

1. **An FE that records, or produces information to be recorded, for a Billable Event shall record the DN for a GETS-AN or GETS-FC call/session origination, unless the DN is a GETS-NT or GETS-PDN.**
2. **An FE that translates a GETS-NT or GETS-PDN and that records, or produces information to be recorded, for a Billable Event shall not record the GETS-NT or GETS-PDN or translated number, originating number, city, or state, or other details that can be used to derive such originating caller's information.**
3. **An FE that records, or produces information to be recorded, for a Billable Event shall record only the first eight digits of the PIN for GETS-AN or GETS-NT call/session origination.**
4. **An FE that records, or produces information to be recorded, for a Billable Event shall not record, nor produce to be recorded, the Service User's priority level.**
5. **An FE that produces a CDR for a GETS-AN-invoked call/session, using PIN authorization, shall include only the first eight digits of the PIN for Service User identification.**
6. **An FE that produces a CDR shall not include in the CDR the Service User's priority level.**
7. **An FE that produces a CDR shall identify the UE or user for a GETS-FC or GETS-AN-invoked call/session, as for normal calling.**

[240] identifies Billable Event records and CDRs as separate record types. An FE may send a Billable Event record to another FE, which will use the information in the Billable Event record to produce a CDR.

[241] The IMS Charge Control Function shall purge all location information (including number, city, state, or other details that can be used to derive location) on the calling and called parties from all Billable Event records and CDRs associated with an NGN GETS session known (by the network) to be associated with a GETS-NT or GETS-PDN.

6.2 Common Requirements

This Clause specifies requirements that are applicable to multiple FEs within the IMS Core Network. FE-specific requirements are specified in Clause 6.3. When a Network Element (NE) implements multiple FEs:

- If the same requirement applies to each FE, the NE may need to implement the requirement only once;
- If the FEs have a set of requirements that are non-overlapping, all the requirements in the set should apply to the NE.

6.2.1 Common Requirements Applicable to NGN GETS SIP-capable FEs

The FEs as enumerated in Clause 5.2.1 are NGN GETS SIP-capable FEs. The common OAM&P requirements in this subclause address OAM&P associated with the general processing related to SIP RPH with the namespaces associated with NGN GETS. These requirements apply to multiple NGN GETS SIP-capable FEs within the IMS Core Network. FE-specific modifications or exceptions to the common requirements are identified where applicable.

6.2.1.1 Configuration Management

Clause 5.1.1 identifies the term “provisioned ets.x” to refer to the ets resource value that is provisioned in accordance with Authorized Agency policy.

[242] An NGN GETS SIP-capable FE shall allow configuration of the “provisioned ets.x” r-priority value. The range of allowable r-priority values shall be 0, 1, 2, 3, or 4. The (factory) default r-priority value shall be 0.

6.2.1.2 Fault Management

One of the key fault management tools is that of logging error conditions that occur in the network. Detailed error conditions related to NGN GETS that will trigger fault management log records to be created are identified within Clause 5. A summary of these error conditions detectable by an NGN GETS SIP-capable FE is provided in Table 6.2 below.

Table 6.2. Summary of Error Conditions to be Logged

Triggering Events for FE Logging	Detailed Triggering Requirements
SIP request with an RPH with multiple instances of ets namespace	Clause 5.2.1.4
SIP request with an RPH with multiple instances of wps namespace	Clause 5.2.1.4
SIP request with an RPH with invalid ets resource value	Clause 5.2.1.4
SIP request with an RPH with invalid wps resource value	Clause 5.2.1.4
SIP request with an RPH with a wps resource value and no ets resource value.	Clause 5.2.1.4
SIP message with an RPH with an ets namespace for a call/session not initially recognized as NGN GETS	Clause 5.2.1.4

6.2.2 Common Diameter Functional Entity Requirements

Diameter-capable FEs support the following Diameter requirement.

[723] A Diameter-capable FE shall allow configuration of the "default value" to be included in the DRMP AVP for an NGN GETS call/session. The range of allowable values shall be 0 - 4. The (factory) default value shall be 2.

[723] should be interpreted in relation to requirements in Clause 5.2.2.

The I-CSCF, S-CSCF, GETS-FC AS, GETS-AN AS, and GETS-NT AS support the following Diameter requirement.

[576] A Diameter-capable FE shall allow configuration of the "default value" to be included in the Diameter Session-Priority AVP. The range of allowable values shall be 0 – 4. The (factory) default value shall be 2.

[576] should be interpreted in relation to requirements in Clause 5.2.2.

6.2.3 Common H.248 Functional Entity Requirements

The IBCF, MGCF/SGW, and MRFC support the following H.248 requirement.

[276] An H.248-capable FE shall allow configuration of the default value for the Priority indicator included in the H.248 Add_Request command to indicate the Service User's priority level. The range of allowable values shall be 11 – 15. The (factory) default value shall be 11.

[276] should be interpreted in relation to requirements in Clause 5.2.3.

6.2.4 Priority Treatment Requirements

The following requirements should be interpreted in relation to requirements in Clause 5.2.4:

[277] All FEs in the IMS Core Network for NGN GETS shall allow configuration of the DSCP value to be used for the IP packets it generates to carry SIP, Diameter, HTTP, and H.248 signaling messages related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).

[679] If either the MRFC or MRFP do not support [H.248.52], an MRFP shall allow configuration of the DSCP value to be used for the IP packets the MRFP generates to carry RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).

[680] If either the MGCF or MGW do not support [H.248.52], an MGW shall allow configuration of the DSCP value to be used for the IP packets the MGCF generates to carry RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).

[681] If both the MRFC and MRFP support [H.248.52] and NGN GETS call/session requires a specific NGN GETS DSCP marking for the media packets, the MRFC shall allow configuration of the DSCP value to be used for the IP packets the MRFP generates to carry RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).

[682] If both the MGCF and MGW support [H.248.52] and NGN GETS call/session requires a specific NGN GETS DSCP marking for the media packets, the MGCF shall allow configuration of the DSCP value to be used for the IP packets the MGW generates to carry RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).

Note that requirements similar to [679], [680], [681], and [682] that apply to a TrGW are specified in Clause 6.3.11.

The following requirements should be interpreted in relation to requirements in Clause 5.2.4.1:

[279] **An NGN GETS SIP-capable FE shall allow configuration of the queue timer (identified in [86] and [197] of Clause 5) expiration value. The range of allowable values shall be 0 to 90 seconds. The (factory) default value shall be 30 seconds.**

[280] **An NGN GETS SIP-capable FE shall allow configuration of the "provisioned [Q.850] cause value" identified in [86] and [197] of Clause 5. The range of allowable values shall be all values defined by [Q.850]. The (factory) default value shall be 102 (recovery on timer expiry).**

The following requirement should be interpreted in relation to requirements in Clause 5.2.4.6:

[361] **If an NGN GETS FE supports the Ethernet Class Of Service (COS) capabilities on the Ethernet interface between the FE and an IP router/Ethernet switch, then the FE shall allow configuration of the "NS/EP" COS value specified by [326] of Clause 5.2.4.6. The range of allowable values shall be 0 through 7. The (factory) default value shall be 5.**

Note that the value of 5 is currently used for normal VoIP traffic. It is expected that the "NS/EP" COS value is set to provide an NGN GETS call/session with the highest priority treatment on the Ethernet interface.

NOTE: MCC, as described in Clause 5.2.4.7 may require associated configuration parameters. Specific configuration requirements concerning MCC are for further study.

6.3 FE Specific Requirements

6.3.1 P-CSCF

The common requirements specified in Clause 6.2 are applicable to the P-CSCF.

6.3.1.1 Configuration Requirements

The following requirements should be interpreted in relation to requirements in Clause 5.3.1.2. Note that according to [95] and [96], one of the mechanisms by which a P-CSCF recognizes that a received SIP INVITE request is associated with an NGN GETS call/session is by the presence of a GETS string (GETS-FC, GETS-AN, or GETS-NT) within the Request-URI.

[282] **A P-CSCF shall support the provisioning of at least ten GETS-AN or GETS-NT strings with a range of 3 – 10 digits to be used as matching criteria when processing an address contained within the Request-URI, in support of a GETS-AN or GETS-NT-invoked call/session.**

[283] **A P-CSCF shall support the provisioning of the GETS-FC.**

The values for the GETS-ANs will be agreed as part of the anticipated SLAs between the Service Providers and the Authorized Agency. The GETS-ANs will be the same for all Service Providers.

The following requirements should be interpreted in relation to requirements in Clause 5.3.1.4.

[286] **The first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall support a minimum of 100 configured IP addresses in support of [287] and [288].**

[287] **For each configured IP address (as specified in [286]), the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall support the configuration of the following parameters to support a throttling mechanism that controls the number of NGN GETS call/session requests received from the configured IP address (associated with the UNI)**

in support of [108]:

- **THROTTLE-MAX-RATE – maximum number of NGN GETS call/session requests (range is 1 to 100 (per interval minute) with a default of 10);**
- **THROTTLE-INTERVAL – time interval for which the number of NGN GETS call/session requests are counted (the interval is configurable within a range of 1 to 30 minutes with a default value of 5 minutes);**
- **THROTTLE-MAX-CONCURRENT – maximum number of concurrent (as defined in Clause 5.3.1.4) NGN GETS calls/sessions; the maximum number allowed is configurable within a range of 1 to 1000 with a default value of 50.**

[288] The first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) shall allow configuration of a binary parameter (on a per configured IP address basis as per [286]) to allow or block incoming NGN GETS call/session requests across the UNI. The (factory) default value shall be "allow".

[396] It is desirable that the first NGN GETS SIP-capable FE at the UNI (e.g., P-CSCF or an SBC implementation) support the following configurable parameters to support a throttling mechanism that controls the number of NGN GETS call/session requests originating from any IP address that is not configured as in [286]:

- **Parameter 1 – maximum number of NGN GETS call/session requests (range is 1 to 100 (per interval minute) with a default of 10);**
- **Parameter 2 – time interval for which the number of NGN GETS call/session requests are counted (the interval is configurable within a range of 1 to 30 minutes with a default value of 5 minutes);**
- **Parameter 3 – maximum number of concurrent (as defined in Clause 5.3.1.4) NGN GETS calls/sessions; the maximum number allowed is configurable within a range of 1 to 1000 with a default value of 50.**

For [396], the value for each parameter applies to all UNIs supported by the FE. For [287], note that "0" is not an allowable value when setting THROTTLE-MAX-RATE or THROTTLE-MAX-CONCURRENT to implement [288].

The following requirement should be interpreted in relation to requirements in Clause 5.3.1.5:

[578] A P-CSCF shall allow configuration of the "default value" to be included in the Diameter Reservation-Priority AVP in support of [507]. The range of allowable values shall be 11 – 15. The (factory) default value shall be 13.

6.3.1.2 Fault Management

In addition to the logging of error conditions shown in Table 6.2, an additional error condition detectable by a P-CSCF that needs to be logged (as specified in [504]) is as follows:

- SIP INVITE request received from a UE that contains an RPH with an ets namespace but that does not include a GETS-FC, GETS-AN, or GETS-NT within the Request-URI.

6.3.1.3 Operational Measurements

In addition to the collection of OMs, the P-CSCF also performs additional performance management functions. [110] and [111] specify performance-related conditions (detectable by a P-CSCF) that will trigger the generation of performance monitoring alerts and logging of events that trigger the alerts. These should be considered as extensions of existing performance management logging and alerting capabilities already provided by the P-CSCF as part of its normal operations capabilities. It should be possible for the Service Provider to inhibit the generation of these alerts.

The remainder of this Clause addresses specific OM requirements for the P-CSCF.

[579] The P-CSCF, designated for INCOMING NGETS in Table 6.1, shall count the number of NGN GETS call/session requests received that attempt to establish a SIP dialog.

[579] is pegged upon receipt of an NGN GETS call/session request in the IP domain used to establish a SIP dialog between the originating UE and the terminating UE. The request may contain a GETS-AN, GETS-NT, or GETS-FC and no NGN GETS marking, or some indication that the request is an NGN GETS call/session request (e.g., an RPH with an ets namespace). Note that [579] would peg the initial SIP INVITE request associated with a call/session request (since this establishes a SIP dialog), but not subsequent SIP (re)INVITE requests associated with the same SIP dialog.

[580] The P-CSCF, designated for OUTGOING NGETS in Table 6.1, shall count the number of initial SIP INVITE requests for NGN GETS call/sessions sent to a subsequent network FE or sent to a UNI.

[580] is pegged upon transmission of a message in the IP domain (SIP INVITE request). The message being sent should contain the appropriate NGN GETS markings. Note that [580] pegs the initial SIP INVITE request associated with an NGN GETS call/session request, but not subsequent SIP (re)INVITE requests associated with the same call/session.

[581] The P-CSCF, designated for SENT FORBIDDEN in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating “service forbidden” is generated.

[581] is pegged after generation of a SIP 403 response associated with the initial SIP INVITE request.

[718] If the P-CSCF, designated for NMC EXEMPTIONS in Table 6.1, supports exemption from packet flow controls, it is desirable that the P-CSCF count the number of NGN GETS calls/session requests exempted from packet flow controls including ACC.

[683] If the P-CSCF, designated for GETS LIMIT EXCEEDED in Table 6.1, limits or throttles NGN GETS calls/session requests via call admission controls (CAC) or other mechanisms, the P-CSCF shall count the number of NGN GETS calls/session requests rejected due to call admission controls and other NGN GETS throttling mechanisms.

[683] is pegged when an NGN GETS call/session is rejected due to throttling constraints at the P-CSCF (e.g., the P-CSCF will not allow more than 1,000 simultaneous NGN GETS calls), or when the call is rejected due to Call Admission Control constraints.

6.3.2 I-CSCF

The common requirements specified in Clause 6.2 are applicable to the I-CSCF.

6.3.3 S-CSCF

The common requirements specified in Clause 6.2 are applicable to the S-CSCF.

6.3.4 IBCF

The common requirements specified in Clause 6.2 are applicable to the IBCF. An IBCF uses the configured DSCP value (per requirement [277]) for the IP packets that it sends to an FE within its IMS Core Network and that carry SIP and H.248 messages related to an NGN GETS call/session. An IBCF uses the DSCP value 101100 (44) (VOICE-ADMIT) for the IP packets that it sends to an FE outside its IMS Core Network and that carry SIP messages related to an NGN GETS call/session, per requirement [135].

6.3.4.1 Configuration Requirements

The following requirements should be interpreted in relation to requirements in Clause 5.3.4.2. Note that according to [118], one of the mechanisms by which an IBCF recognizes that a received SIP INVITE request is associated with an NGN GETS call/session is by the presence of a GETS string (GETS-FC, GETS-AN, or GETS-NT) within the Request-URI.

[293] An IBCF shall support the provisioning of at least ten GETS-AN or GETS-NT strings with a range of 3 – 10 digits to be used as matching criteria when processing an address contained within the Request-URI, in support of a GETS-AN, or GETS-NT-invoked call/session.

[294] An IBCF shall support the provisioning of the GETS-FC.

See Clause 6.3.1.1 for additional information about GETS-AN and GETS-NT string values.

The following requirement should be interpreted in relation to requirements in Clause 5.3.4.3.1:

[295] An IBCF shall allow configuration (on a per external entity basis, where an external entity may be identified by an IP address or FQDN) to select one of the options listed in [122]. The (factory) default shall be Option 1.

The following requirement should be interpreted in relation to requirements in Clause 5.3.4.3.2:

[296] An IBCF shall allow configuration to select one of the options listed in [125]. The (factory) default shall be Option 1.

The following requirements should be interpreted in relation to requirements in Clause 5.3.4.4.

[297] An IBCF shall allow a minimum of 100 external entities to be identified using configured IP addresses and FQDNs for the purpose of applying the capabilities described in [298] and [299].

[298] An IBCF shall support per identified external entity (as specified in [297]) the configuration of the following parameters to support a throttling mechanism that controls the number of NGN GETS call/session requests received from the external entity in support of [128].

- **THROTTLE-MAX-RATE – maximum number of NGN GETS call/session requests (range is 1 to 100 (per interval minute) with a default of 10);**
- **THROTTLE-INTERVAL – time interval for which the number of NGN GETS call/session requests are counted (the interval is configurable within a range of 1 to 30 minutes with a default value of 5 minutes);**
- **THROTTLE-MAX-CONCURRENT – maximum number of concurrent (as defined in Clause 5.3.1.4) NGN GETS calls/sessions; the maximum number allowed is configurable within a range of 1 to 1000 with a default value of 50.**

[299] An IBCF shall allow configuration of a binary parameter (on a per external entity basis as per [297]) to allow or block incoming NGN GETS call/session requests across the NNI to external entities. The (factory) default value shall be "allow".

For [298], note that "0" is not an allowable value when setting THROTTLE-MAX-RATE or THROTTLE-MAX-CONCURRENT.

[276] applies to the IBCF.

6.3.4.2 Operational Measurements

In addition to the collection of OMs, the IBCF also performs additional performance management functions. [130] and [131] specify performance-related conditions (detectable by an IBCF) that will trigger the generation of performance monitoring alerts and the logging of events that trigger the alerts. These should be considered as extensions of existing performance management logging and alerting capabilities already provided by the IBCF as part of its normal operations capabilities. It should be possible for the Service Provider to inhibit the generation of these alerts.

The remainder of this Clause addresses specific OM requirements for the IBCF.

[583] The IBCF, designated for INCOMING NGETS in Table 6.1, shall count the number of NGN GETS call/session requests received that attempt to establish a SIP dialog.

[583] is pegged upon receipt of an NGN GETS call/session request in the IP domain used to establish a SIP dialog between the originating UE and the terminating UE. The request may contain a GETS-AN, GETS-NT, or GETS-FC and no NGN GETS marking, or some indication that the request is an NGN GETS call/session request (e.g., an RPH with an ets namespace). Note that [583] would peg the initial SIP INVITE request associated with a call/session request (since this establishes a SIP dialog), but not subsequent SIP (re)INVITE requests associated with the same SIP dialog.

[584] The IBCF, designated for OUTGOING NGETS in Table 6.1, shall count the number of initial SIP INVITE requests for NGN GETS call/sessions sent to a subsequent network FE.

For [584], the “subsequent network FE” may either be within, or external to, the Service Provider’s network.

[584] is pegged upon transmission of a message in the IP domain (SIP INVITE request). The message being sent should contain the appropriate NGN GETS markings. Note that [584] pegs the initial SIP INVITE request associated with an NGN GETS call/session request, but not subsequent SIP (re)INVITE requests associated with the same call/session.

[585] The IBCF, designated for SENT FORBIDDEN in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating “service forbidden” is generated.

[585] is pegged after generation of a SIP 403 response associated with the initial SIP INVITE request.

[719] If the IBCF, designated for NMC EXEMPTIONS in Table 6.1, supports exemption from packet flow controls, it is desirable that the IBCF count the number of NGN GETS calls/session requests exempted from packet flow controls including ACC.

[684] If the IBCF, designated for GETS LIMIT EXCEEDED in Table 6.1, limits or throttles NGN GETS calls/session requests via call admission controls (CAC) or other mechanisms, the IBCF shall count the number of NGN GETS calls/session requests rejected due to call admission controls and other NGN GETS throttling mechanisms.

[684] is pegged when an NGN GETS call/session is rejected due to throttling constraints at the IBCF (e.g., the IBCF will not allow more than 1,000 simultaneous NGN GETS calls), or when the call is rejected due to Call Admission Control constraints.

6.3.5 Application Server

The common requirements specified in Clause 6.2 are applicable to GETS-FC AS, GETS-AN AS, and GETS-NT AS.

6.3.5.1 Configuration Requirements

[300] A GETS-FC AS shall support the provisioning of the GETS-FC value to be used by the AS to identify a GETS-FC call/session request.

[365] If a Service Provider has chosen to store GETS-FC subscription information at a GETS-FC AS instead of at an HSS, then the GETS-FC AS shall have the capability to be provisioned with each Service User's priority level (for each Service User with a subscription with the Service Provider).

[301] A GETS-AN AS shall allow provisioning of at least nine GETS-AN 10-digit strings to be used as matching criteria when processing an address contained within the Request-URI, in support of a GETS-AN-invoked call/session.

[302] In support of [143] and [525], the GETS-AN AS or GETS-NT AS shall be configurable for:

- **Number of attempts to access the candidate MRFCs over a range of 1 to 100, with a default of 10, and**
- **Time interval between attempts for each MRFC over a range of 100 ms to 1 sec, and a default of 200 ms.**

[303] A GETS-AN AS or GETS-NT AS shall allow configuration of a time interval (over a range of 1 to 10 seconds, with a default of 5 seconds) which shall be used to instruct the AS how long to:

- **Wait for the calling party to respond to a prompt for PIN collection as specified in [519], and**
- **Wait for the calling party to respond to the prompt to enter the DN before proceeding with processing in terminating the call/session as indicated in [156] (not applicable to GETS-NT AS).**

Note that for [303], a single value is set that applies to both waiting intervals.

[304] A GETS-NT AS shall provide the capability to allow the PIN bypass option to be configured as 'on' or 'off', as described in [165]. The default setting shall be 'off'.

[588] A GETS-NT AS shall allow provisioning of at least two GETS-NT 3-digit strings to be used as primary filters or matching criteria for potential GETS-NT requests. It shall also allow the provisioning of at least two NOT-GETS-NT 10 digit strings to be used as secondary negative filters or NOT-matching criteria to ensure that GETS-AN requests are not mis-categorized as GETS-NT requests. Both these filters or matching criteria will be used when processing an address contained within the Request-URI, in support of a GETS-NT-invoked call/session.

6.3.5.2 Fault Management

In addition to the logging of error conditions shown in Table 6.2, additional error conditions detectable by an AS that need to be logged (as specified in [139], [144], [159], and [536]) are as follows:

- GETS-FC AS receives a SIP INVITE request including a GETS-FC but without an RPH with the ets namespace;
- GETS-AN AS receives a user string in the Request-URI that matches none of the provisioned GETS-AN strings, or the user string in the Request-URI contains less than ten digits;
- GETS-NT AS receives a user string in the Request-URI for which the first three digits of the last ten digits match none of the provisioned GETS-NT strings, or the user string in the Request-URI contains less than ten digits.

6.3.5.3 Operational Measurements (NGN GETS AS)

The Operational Measurement (OM) requirements in this Clause apply to GETS-AN AS, GETS-NT AS, and GETS-FC AS.

[589] An NGN GETS AS, designated for INCOMING NGETS in Table 6.1, shall count the number of NGN GETS call/session requests received that attempt to establish a SIP dialog.

[589] is pegged upon receipt of an NGN GETS call/session request in the IP domain used to establish a SIP dialog between the originating UE and the terminating UE. The request may contain a GETS-AN, GETS-NT, or GETS-FC and no NGN GETS marking, or some indication that the request is an NGN GETS call/session request (e.g., an RPH with an ets namespace). Note that [589] would peg the initial SIP INVITE request associated with a call/session request (since this establishes a SIP dialog), but not subsequent SIP (re)INVITE requests associated with the same SIP dialog.

[590] An NGN GETS AS, designated for OUTGOING NGETS in Table 6.1, shall count the number of initial SIP INVITE requests for NGN GETS call/sessions sent to a subsequent network FE.

[590] is pegged upon transmission of a message in the IP domain (SIP INVITE request). The message being sent should contain the appropriate NGN GETS markings. Note that [590] pegs the initial SIP INVITE request associated with an NGN GETS call/session request, but not subsequent SIP (re)INVITE requests associated with the same call/session.

[591] An NGN GETS AS, designated for RCVD ANSWER in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "answered" is received.

Note that for [591], this measurement is pegged after receipt of the 200 response associated with the initial SIP INVITE request. The NGN GETS AS needs to have the logic to ensure that only the 200 response that corresponds to the end user is used to peg the OM, and that it only pegs once for each call attempt.

[592] An NGN GETS AS, designated for CALLER ABANDONED in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "caller abandoned" or "ringing but not answered" is received. The NGN GETS AS shall also count the number of calls/sessions assumed abandoned due to the expiration of an appropriate timer or other changes in the call/session state.

One condition for which [592] is pegged is the receipt of a SIP CANCEL request associated with the initial SIP INVITE request.

[593] An NGN GETS AS, designated for RCVD BUSY in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "destination busy" is received.

[593] is pegged after receipt of a SIP 486 or a SIP 600 response associated with the initial SIP INVITE request.

[594] An NGN GETS AS, designated for RCVD SVC UNAVL in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "service unavailable" is received.

[594] is pegged when the received message is a SIP 4xx (except 403, 408 or 486), 5xx or 6xx (except 600) response.

[595] An NGN GETS AS, designated for RCVD Q TO in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "timed out of queue" is received.

[595] is pegged after receiving a SIP 408 response.

[596] An NGN GETS AS, designated for SENT SVC UNAVL in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "service unavailable" is generated.

[596] is pegged upon generation of a SIP 4xx (except 403, 408, or 486), 5xx or 6xx (except 600) response associated with the initial SIP INVITE request.

[597] An NGN GETS AS, designated for SENT FORBIDDEN in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "service forbidden" is generated.

[597] is pegged after generation of a SIP 403 response associated with the initial SIP INVITE request.

[598] An NGN GETS AS, designated for GETS ERROR LOG in Table 6.1, shall count the number of messages sent to a log file during a dialog identified with an NGN GETS call/session request. Based on the Clause 5 requirements, these messages include: (1) transmission of SIP 400 responses ([72] through [76]); and (2) messages received with an RPH with an ets namespace during a SIP dialog not initially being recognized as NGN GETS ([77]).

[598] counts the number of NGN GETS call/session requests where an error occurred due to the SIP RPH. Detailed information is captured in a log file for further analysis.

[720] If an NGN GETS AS, designated for NMC EXEMPTIONS in Table 6.1, supports exemption from packet flow controls, it is desirable that the NGN GETS AS count the number of NGN GETS calls/session requests exempted from packet flow controls including ACC.

[686] If an NGN GETS AS, designated for GETS LIMIT EXCEEDED in Table 6.1, limits or throttles NGN GETS calls/session requests via call admission controls (CAC) or other mechanisms, the NGN GETS AS shall count the number of NGN GETS calls/session requests rejected due to call admission controls and other NGN GETS throttling mechanisms.

[686] is pegged when an NGN GETS call/session is rejected due to throttling constraints at an NGN GETS AS (e.g., the NGN GETS AS will not allow more than 1,000 simultaneous NGN GETS calls), or when the call is rejected due to Call Admission Control constraints.

6.3.5.4 Operational Measurements (NGN GETS AS, NGN GETS Multi-AS System)

The term "NGN GETS multi-AS system" is used below to refer to a system that implements a combination of the GETS-AN AS, GETS-NT AS, and GETS FC AS FEs. The OMs specified in this Clause are unique to a "NGN GETS multi-AS system" since they rely on a combined knowledge of GET-AN, GETS-NT, and GETS-FC calls. Computation of these OMs is not feasible when the GETS-AN AS, GETS-NT AS, and GET FC AS are deployed as separate FEs.

[599] An NGN GETS multi-AS system shall count the number of incoming NGN GETS call/session requests received with a GETS-DN (AN or NT) and no GETS-FC.

[600] An NGN GETS multi-AS system shall count the number of incoming NGN GETS call/session requests received with a GETS-FC and no GETS-DN (AN/NT).

[601] An NGN GETS multi-AS system shall count the number of incoming NGN GETS call/session requests received with both a GETS-FC and a GETS-DN (AN/NT).

[602] An NGN GETS multi-AS system shall count the number of incoming NGN GETS call/session requests received with a normal DN, no GETS-FC, and an ets RPH.

6.3.5.5 Operational Measurements (NGN GETS AS, NGN GETS Bi-AS System)

The term "NGN GETS bi-AS system" is used below to refer to a system that implements both the GETS-AN AS and GETS-NT AS FEs. The intent of NGN GETS bi-AS system measurement requirements is to not differentiate GETS-NT calls/sessions from GETS-AN calls/sessions. Peg counts for the NGN GETS bi-AS system should include both call/session types.

[603] An NGN GETS bi-AS system shall count both (1) the number of GETS-NT call/session requests, and (2) the number of GETS-AN call/session requests received for which the GETS-

AN destination is a NANP DN (including GETS-PDN). The system shall provide one RCVD GETS NANP count that includes both types of NGN GETS call/session requests.

[604] An NGN GETS bi-AS system shall count both (1) the number of GETS-AN call/session requests received with an NANP DN (including GETS-PDN) and authorized successfully, and (2) the number of GETS-NT call/session requests received and authorized successfully. The system shall provide one GETS NANP AUTH SUCCESS count that includes both types of NGN GETS call/session requests. GETS-NT call/session requests received that are authorized due to the requirement for GETS-NT PIN authorization being suspended by Authorized Agency administrative action (i.e., PIN bypass) shall be included in this count.

[603] pegs all GETS-NT call/session requests and all GETS-AN call/session requests with an NANP, GETS-PDN, or non-World Zone 1 DN, while [604] pegs only those requests that have been successfully authorized.

[605] An NGN GETS bi-AS system shall count the number of GETS-AN and GETS-NT call/session requests received which were authorized by default due to inability to access the NGN GETS Credentials information. The system shall provide one GETS AUTH FAIL OPEN count that includes both types of NGN GETS call/session requests.

[606] An NGN GETS bi-AS system shall count the number of both GETS-AN and GETS-NT call/session requests received, but not authorized due to a missing or invalid PIN. The system shall provide one GETS AUTH FAIL INVLD PIN count that includes both types of NGN GETS call/session requests.

[607] An NGN GETS bi-AS system shall count the number of both GETS-AN and GETS-NT call/session requests received, but not honored due to the entered PIN not having the requisite calling privileges. The system shall provide one GETS AUTH FAIL ~PRIV count that includes both types of NGN GETS call/session requests.

For example, [607] would be pegged if a user without international calling privileges associated with their NGN GETS Credentials attempted to make such a call/session.

[608] An NGN GETS bi-AS system shall count (1) the number of GETS-AN call/session requests received, but not honored due to the entry of an invalid DN, (2) the number of GETS-AN call/session requests received, but not honored due to an inability to translate the GETS-PDN number, and (3) the number of GETS-NT call/session requests that fail due to an inability to translate the GETS-NT number. The system shall provide one GETS AUTH FAIL INVLD DN count that includes both GETS-AN and GETS-NT call/session requests.

6.3.5.6 Operational Measurements (GETS-AN AS)

[609] A GETS-AN AS shall count the number of GETS-AN call/session requests received for which the GETS-AN destination is a NANP DN (including GETS-PDN).

[610] A GETS-AN AS shall count the number of GETS-AN call/session requests received for which the destination is a non-World Zone 1 DN.

[611] A GETS-AN AS shall count the number of GETS-AN call/session requests received with an NANP DN (including GETS-PDN) and authorized successfully.

[612] A GETS-AN AS shall count the number of GETS-AN call/session requests received with a non-World Zone 1 DN and authorized successfully.

Requirements [609] and [610] peg all GETS-NT call/session requests and all GETS-AN call/session requests with an NANP, GETS-PDN, or non-World Zone 1 DN, while [611] and [612] peg only those requests that have been successfully authorized.

[613] A GETS-AN AS shall count the number of GETS-AN call/session requests received that were

authorized by default due to inability to access the NGN GETS Credentials information.

[614] A GETS-AN AS shall count the number of GETS-AN call/session requests received, but not authorized due to a missing or invalid PIN.

[615] A GETS-AN AS shall count the number of GETS-AN call/session requests received, but not honored due to the entered PIN not having the requisite calling privileges.

For example, [615] would be pegged if a user without international calling privileges associated with their NGN GETS Credentials attempted to make such a call/session.

[616] A GETS-AN AS shall count the number of GETS-AN call/session requests received, but not honored due to the entry of an invalid DN.

[712] For each OM provided by the GETS-AN AS, it is an objective that the count be subdivided as follows:

- **Count applicable to voice sessions.**
- **Count applicable to video sessions.**

6.3.5.7 Operational Measurements (GETS-NT AS)

Operational measurements for the GETS-NT AS are for further study.

6.3.5.8 Operational Measurements (GETS-FC AS)

[617] A GETS-FC AS shall count the number of GETS-FC call/session requests received for which the destination is a NANP DN.

[618] A GETS-FC AS shall count the number of GETS-FC call/session requests received for which the destination is a non-World Zone 1 DN.

[619] A GETS-FC AS shall count the number of GETS-FC call/session requests received with an NANP DN and authorized successfully.

[620] A GETS-FC AS shall count the number of GETS-FC call/session requests received with a non-World Zone 1 DN and authorized successfully.

[621] A GETS-FC AS shall count the number of GETS-FC call/session requests received, but not honored due to the use not having the requisite privileges.

For example, [621] would be pegged if a user attempted international calling, and the privileges associated with the GETS-FC did not permit international calling.

[622] A GETS-FC AS shall count the number of GETS-FC call/session requests received, but not honored due to the entry of an invalid DN.

[713] For each OM provided by the GETS-FC AS, it is an objective that the count be subdivided as follows:

- **Count applicable to voice sessions**
- **Count applicable to video sessions.**

6.3.6 MRFC

The common requirements (except [680] and [682]) specified in Clause 6.2 are applicable to the MRFC.

The MRFC may store scripts/instructions for PIN, DN, and announcement information.

6.3.7 MRFP

[277], [679], and [681] apply with the following addition.

[306] An MRFP shall allow provisioning of GETS-specific announcements for GETS-AN AS or GETS-NT AS user interactions. The following default announcements, or their factory equivalents, shall be used:

1. **"Bong" tone to prompt for initial PIN entry.**
2. **"Please re-enter your PIN now" for case when additional PIN prompt is required.**
3. **"Please enter your destination number now" as the prompt to enter a DN after successful PIN entry.**
4. **"Your call cannot be completed as dialed. Please check your number and try again" when the PIN remains invalid through all permitted attempts at re-entry or when the DN is not entered or when the DN is recognized to be invalid.**
5. **"You are using GETS" when the call can be advanced after completion of the authentication and authorization process.**

6.3.8 PCRF

The common requirements specified in Clause 6.2 are applicable to the PCRF. Additional PCRF configuration management requirements are specified in [ATIS-1000065.2015].

6.3.9 HSS

The common requirements specified in Clause 6.2 are applicable to the HSS. In addition, the following HSS requirements apply.

[366] If a Service Provider has chosen to store GETS-FC subscription information at an HSS instead of at a GETS-FC AS, then the HSS shall have the capability to be provisioned with each Service User's priority level (for each Service User with a subscription with the Service Provider).

[307] An HSS shall have the capability to be provisioned with iFC for Service Users (as necessary) to be downloaded to the S-CSCF to allow a trigger at the S-CSCF and route the SIP INVITE request to a GETS-FC AS for processing of a GETS-FC call/session request.

6.3.10 NGN GETS Information

Provisioning requirements apply to the NGN GETS Credentials and to the GETS Translation information.

For the NGN GETS Credentials information, [626] applies.

[626] The NGN GETS Credentials information shall support provisioning of the following PIN-indexed information:

1. **PIN, as 12 numeric digits,**
2. **Service User's priority level, as integer in the range 1-5,**
3. **GETS-NT Voice calling privilege, as yes or no,**
4. **GETS-NT Video calling privilege, as yes or no,**
5. **GETS-AN Voice calling privileges,**
    a. **Domestic calling privilege, as yes or no;**
    b. **International calling privilege, as yes or no;**
    c. **GETS-PDN calling privilege, as yes or no,**

6. **GETS-AN Video calling privileges,**
    a. **Domestic calling privilege, as yes or no;**
    b. **International calling privilege, as yes or no;**
    c. **GETS-PDN calling privilege, as yes or no,**

The minimum number of PIN entries to be supported is 2,000,000.

For the GETS Translation information, [309] applies.

[309] **The GETS Translation information shall support provisioning of the following translations for:**

1. **A GETS-NT to an NPA-NXX-XXXX number,**
2. **A GETS-PDN to an NPA-NXX-XXXX number.**

The minimum number of translation entries to be supported is one million for each of the above translation types, i.e., total of 2 million entries.

For [309], the translations may be taken from anywhere in the NPA-NXX-XXXX range.

6.3.11 TrGW

[277] applies. In addition, [688] and [690] provide modifications of [679] through [682] that are applicable to a TrGW.

[688] **If an IBCF/TrGW does not support [H.248.52], a TrGW shall allow configuration of the DSCP value to be used for the IP packets that the TrGW sends to an FE within its IMS Core Network and that carries RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).**

[690] **If an IBCF/TrGW supports [H.248.52] and NGN GETS call/session requires a specific NGN GETS DSCP marking for the media packets, an IBCF shall allow configuration of the DSCP value to be used for the IP packets that the TrGW sends to an FE within its IMS Core Network and that carries RTP payload related to an NGN GETS call/session. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default DSCP value shall be 101100 (44) (VOICE-ADMIT).**

6.3.12 BGCF

The common requirements specified in Clause 6.2 are applicable to the BGCF.

6.3.13 MGCF/SGW

The common requirements (except [679] and [681]) specified in Clause 6.2 are applicable to the MGCF/SGW.

Additional operations requirements for the SS7-based interface to the PSN are beyond the scope of this Standard.

6.3.13.1 Configuration Management

[313] **An MGCF/SGW shall allow provisioning of at least ten GETS strings to be used as matching criteria when processing an address contained within the ISUP Called Party Number parameter, in support of a GETS-AN or GETS-NT-invoked call/session. The string length shall range from 3 to 10 digits. No (factory) default strings are required.**

6.3.13.2 Operational Measurements

The MGCF/SGW must support OMs across both the IP domain and the TDM domain.

[627] The MGCF, designated for INCOMING NGETS in Table 6.1, shall count the number of NGN GETS call/session requests received that attempt to establish a SIP dialog.

[627] is pegged upon receipt of an NGN GETS call/session request in the IP domain or the TDM domain. The request may contain a GETS-AN, GETS-NT, or GETS-FC and no NGN GETS marking, or some indication that the request is an NGN GETS call/session request (e.g., an RPH with an ets namespace or a CPC = "NS/EP Call" parameter in an IAM). Note that [627] would peg the initial SIP INVITE request associated with a call/session request, but not subsequent SIP (re)INVITE requests associated with the same SIP dialog.

[628] The MGCF, designated for OUTGOING NGETS in Table 6.1, shall count the number of initial SIP INVITE requests for NGN GETS call/sessions sent to a subsequent network FE. The count shall also include, for the TDM domain, the number of IAMs that contain a GETS-AN, GETS-NT or GETS-FC, or the CPC parameter with "NS/EP Call" sent into the PSN.

[628] is pegged upon transmission of a message in the IP domain (SIP INVITE request) and upon transmission of a message in the TDM domain (ISUP IAM). The message being sent should contain the appropriate NGN GETS markings. Note that, in the IP domain, [628] pegs the initial SIP INVITE request associated with an NGN GETS call/session request, but not subsequent SIP (re)INVITE requests associated with the same call/session.

[629] The MGCF, designated for RCVD ANSWER in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "answered" is received.

Note that for [629], the call/session may be completed in either the IP domain or the TDM domain. In the IP domain, this measurement is pegged after receipt of the 200 response associated with the initial SIP INVITE request. The MGCF needs to have the logic to ensure that only the 200 response which corresponds to the end user is used to peg the OM, and that it only pegs once for each call attempt. In the TDM domain, this measurement is pegged after receipt of an SS7/ISUP answer message (ANM).

[630] The MGCF, designated for CALLER ABANDONED in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "caller abandoned" or "ringing but not answered" is received. The MGCF shall also count the number of calls/sessions assumed abandoned due to the expiration of an appropriate timer or other changes in the call/session state.

[630] is pegged upon receipt of a message in the IP domain or the TDM domain. In the IP domain, this measurement is pegged after receipt of a SIP CANCEL request associated with the initial SIP INVITE request. In the TDM domain, the measurement is pegged after receipt of an ISUP release message (REL) with a cause code of 18 (no user responding) or 19 (no answer from user).

[631] The MGCF, designated for RCVD BUSY in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "destination busy" is received.

[631] is pegged upon receipt of a message in the IP domain or the TDM domain. In the IP domain, this measurement is pegged after receipt of a SIP 486 or a SIP 600 response associated with the initial SIP INVITE request. In the TDM domain, this measurement is pegged after receipt of an ISUP Release message (REL) with a cause code of 17 (user busy).

[632] The MGCF, designated for RCVD SVC UNAVL in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating "service unavailable" is received.

In the IP domain, [632] is pegged when the received message is a SIP 4xx (except 403, 408, or 486), 5xx, or 6xx (except 600) response. In the TDM domain, [632] is pegged when the received ISUP message is a REL message with a cause code other than 17, 18, or 19.

[633] The MGCF, designated for RCVD Q TO in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating “timed out of queue” is received.

In the IP domain, [633] is pegged upon receipt of a SIP 408 response. In the TDM domain, different messages may be received and cause [633] to be pegged, depending on whether the call is in a wireless or wireline domain. A typical message is an ISUP REL message with a cause code of 102.

[634] The MGCF, designated for SENT SVC UNAVL in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating “service unavailable” is generated.

[634] is pegged upon generation of an error message in the TDM domain (typically an ISUP REL message with a cause code other than values 17, 18, or 19) or in the IP domain (typically a SIP 4xx (except 403, 408, or 486), 5xx, or 6xx (except 600) response) associated with the initial SIP INVITE request.

[635] The MGCF, designated for SENT FORBIDDEN in Table 6.1, shall count the number of NGN GETS call/session requests for which signaling indicating “service forbidden” is generated.

[635] is pegged after generation of a SIP 403 response associated with the initial SIP INVITE request.

[692] If the MGCF, designated for MEDIA QD in Table 6.1, queues NGN GETS call/session requests for media resources, the MGCF shall count the number of NGN GETS call/session requests for which media resource queuing is attempted.

[692] is pegged for all queuing attempts, and thus is pegged in conjunction with [693] when the queuing attempt failed due to queue overflow.

[693] If the MGCF, designated for MEDIA Q TO in Table 6.1, queues NGN GETS call/session requests for media resources, the MGCF shall count the number of NGN GETS call/session requests which are queued for media resources and time out of the queue.

[693] is pegged for both the IP domain and for the TDM domain. In the IP domain, this measurement is pegged upon generation of a SIP 408 response. In the TDM domain, different messages may be generated and cause [693] to be pegged, depending on whether the call is in a wireless or wireline domain. A typical message is an ISUP REL message with a cause code of 102.

[694] If the MGCF, designated for MEDIA Q OVFL in Table 6.1, queues NGN GETS call/session requests for media resources, the MGCF shall count the number of NGN GETS call/session requests for which media resource queuing is attempted, but the call/session cannot be queued due to the queue being filled to its capacity.

[694] is pegged for both the IP domain and for the TDM domain. In the IP domain, [694] is pegged upon generation of a SIP 503 response for this condition. (Note that a SIP 503 response will also be generated for conditions other than a full queue.) In the TDM domain, different messages may be generated and cause [694] to be pegged, depending on whether the call is in a wireless or wireline domain. A typical message is an ISUP REL message with a cause code of 34.

[721] If the MGCF, designated for NMC EXEMPTIONS in Table 6.1, supports exemption from network management controls in the TDM domain and/or exemption from packet flow controls in the IP domain, it is desirable that the MGCF count the number of NGN GETS calls/session requests exempted (in either domain) including ACC.

[695] If the MGCF, designated for GETS LIMIT EXCEEDED in Table 6.1, limits or throttles NGN GETS calls/session requests via call admission controls (CAC) or other mechanisms, the MGCF shall count the number of NGN GETS calls/session requests rejected due to call admission controls and other NGN GETS throttling mechanisms.

[695] is pegged when an NGN GETS call/session is rejected due to throttling constraints at the MGCF (e.g., the MGCF will not allow more than 1,000 simultaneous NGN GETS calls), or when the call is rejected due to Call Admission Control constraints.

6.3.14 MGW

[277], [680], and [682] apply.

6.3.15 SLF

[576] applies.