



Cisco BroadWorks

Support Government Emergency Telecommunications Service (GETS)

Feature Description

Release 23.0

Document Version 1.1

SupportGETSForASFD-R230

Market Request Number 4897

Feature Request Number 11930

Copyright Notice

Copyright© 2020 Cisco Systems, Inc. All rights reserved.

Trademarks

Any product names mentioned in this document may be trademarks or registered trademarks of Cisco or their respective companies and are hereby acknowledged.

Table of Contents

1	Requirements	8
1.1	Requirements	8
1.1.1	Mandatory Requirements.....	8
1.1.2	Conditional Requirements.....	17
1.2	Additional Security Requirements	20
1.3	Mapping of Requirements to Document	20
2	Feature Purpose and Overview	21
2.1	Purpose.....	21
2.2	Overview	21
3	Use Cases	24
3.1	Standalone Typical GETS Calls	24
3.1.1	NS/EP Call Termination	24
3.1.2	GETS-AN and GETS-NT Origination.....	24
3.1.3	GETS-FC Origination	24
3.2	IMS Mode Typical GETS Calls.....	24
3.2.1	NS/EP Call Termination	24
3.2.2	GETS-FC Origination with GETS-FC Prefix	25
3.2.3	GETS-FC Origination with no GETS-FC Prefix.....	25
3.2.4	GETS-AN Origination.....	25
3.2.5	GETS-NT Origination	25
3.2.6	GETS-FC + GETS-AN and GETS-FC + GETS NT Origination	26
4	Provisioning Description.....	27
4.1	Licensing Impacts.....	27
4.2	Cisco BroadWorks Application Server Configuration.....	27
4.2.1	GETS Configuration	27
4.2.2	Emergency Distributed Denial of Service (DDoS) Protection	32
4.3	Cisco BroadWorks Network Server Configuration	34
4.3.1	GETS Configuration	34
4.3.2	Emergency Distributed Denial of Service (DDoS) Protection	35
5	Feature Operation	37
5.1	GETS and Cisco BroadWorks.....	37
5.2	Identifying GETS Calls	37
5.2.1	Standalone Mode	38
5.2.2	IMS Mode.....	40
5.2.3	Cisco BroadWorks Networks Server.....	41
5.3	Overload Controls.....	42
5.3.1	Processor Overload Control.....	42
5.3.2	Blocking Services	42
5.3.3	Emergency Call DDoS Protection	42

5.4	GETS Origination Call Flows	43
5.4.1	Standalone Mode	43
5.4.2	IMS Mode.....	47
5.4.3	GETS Call Processing for SIP 417 and 420 Error.....	49
5.5	NS/EP Termination Call Flows	51
5.5.1	Standalone Mode	52
5.5.2	IMS Mode.....	53
5.6	Downstream GETS-AS Server Support.....	54
5.6.1	Resource-Priority Changes.....	54
5.6.2	GETS Call Type Identification.....	55
5.7	SIP Interface	56
5.7.1	Resource-Priority Header (RPH).....	56
5.7.2	Require Header	59
5.7.3	SUBSCRIBE and NOTIFY Support	60
5.7.4	Supported SIP Header Support.....	60
5.8	Diameter Interface.....	60
5.8.1	Rf Interface.....	60
5.8.2	Ro Interface.....	61
5.8.3	GETS-NT Inhibited Accounting AVPs Support.....	61
5.9	DSCP Field Setting.....	62
5.9.1	Internet Protocol.....	62
5.9.2	SIP Interface	63
5.9.3	DSCP Field with Diameter Ro Interface.....	63
5.10	Ethernet COS (VLAN Priority Code Point).....	63
5.10.1	Cisco BroadWorks TAS Connected to an Untagged Port	63
5.10.2	Cisco BroadWorks TAS Connected to a Trunk Port.....	64
5.11	Prevent GETS-FC invocation via redirection	64
6	Service Interactions.....	65
6.1	Service Precedence	65
6.2	Service Interactions	65
7	System Management.....	72
7.1	Accounting	72
7.2	Monitoring and Troubleshooting	72
7.2.1	Alarms and PMs	72
7.2.2	Commands and Utilities	74
7.3	Device Management	74
8	Restrictions and Limitations.....	75
8.1	Functional Limitations.....	75
8.1.1	DSCP Field with Diameter Ro Interface.....	75
8.1.2	GETS-NT Accounting AVPs Inhibition	75
8.1.3	IMS Mode.....	75
8.2	Upgrade/Rollback Limitations	75

8.3	Enterprise Migration Restrictions	75
9	Service Patch Information	76
9.1	Functional Differences	76
9.2	Feature Activation Impacts	76
9.2.1	Method of Activation	76
9.2.2	Activatable Feature ID and Dependencies	76
10	Provisioning Interface Impacts	77
10.1	Centralized Configuration Data	77
10.1.1	executionServerSubsystem	77
10.1.2	executionServerSubsystem/gets/network	77
10.1.3	nsExecutionServerSubsystem/gets/GETSNumbers	77
10.2	CLI Impacts	78
10.2.1	Summary	78
10.2.2	Adding Application Server GETS context	79
10.2.3	Adding Application Server Numbers context	80
10.2.4	Adding Application Server Network context	83
10.2.5	Adding Application Server ReservedFACs context	84
10.2.6	Adding Application Server ResourcePriorities context	86
10.2.7	Adding Application Server SessionPriorityMap context	88
10.2.8	Adding Application Server InhibitedAVPCodes context	90
10.2.9	Adding Application Server EmergencyCallIDDoSProtection context	91
10.2.10	Adding Network Server Numbers context	93
10.2.11	Adding Network Server EmergencyCallIDDoSProtection context	95
10.3	Open Client Interface-Provisioning Impact	97
10.3.1	Application Server	97
10.4	External Authentication Impacts	115
10.5	Application Server Portal API Impacts	115
10.6	Network Server Location API Impacts	115
10.7	NSSync API Impacts	115
10.8	Application Server Dump Impacts	115
10.9	BroadCloud Dump Impacts	115
10.10	Service License Reporting Impact	115
10.11	Treatments	115
10.12	Media Announcements (Audio and Video)	116
10.13	BroadWorks Common Communication Transport Impacts	116
10.14	Device Management Impacts	116
11	Accounting Impacts	117
11.1	Summary of Changes	117
11.2	Generation of Accounting Records	117
11.3	Impact to Accounting Fields (CDR)	117
11.3.1	GETS (378)	117
11.3.2	getsOriginationType (443)	118

11.4	Original Called Reason and Redirection Reason	118
11.5	Related Call ID	118
11.6	Example	118
12	System Management Impacts	120
12.1	Performance Management Impacts	120
12.1.1	New Counters	120
12.1.2	Modified Counters	177
12.1.3	Deleted Counters or Module	177
12.1.4	Counters Polled by Network Monitoring	177
12.2	Fault Management Impacts	177
12.3	Scripts and Tools	178
12.4	EMS Integration Impacts	178
13	Execution/Call Processing Impacts.....	179
13.1	Extended Services Interface Impact.....	179
13.2	SIP/MGCP Interface Impact	179
13.2.1	Summary.....	179
13.2.2	SIP Header/MGCP Command	179
13.2.3	SIP Parameter/MGCP Signal/Event.....	180
13.2.4	Message Example.....	181
14	Client Application Impacts	183
14.1	OCI-P Impacts	183
14.2	Call Control Impacts	183
14.3	Window Impacts	183
15	Deployment/Operational Impacts	184
15.1	Configuration File Impacts	184
15.2	Security Impacts	184
15.2.1	Security Toolkit Impact	184
15.2.2	Application Server Default Hardening Impact.....	184
15.3	Scheduled Tasks	184
15.4	Third-Party Software.....	184
15.5	Server Logging Impacts	184
15.6	Client Application Impacts.....	184
16	System Engineering Impacts.....	185
16.1	Processing Impacts	185
16.1.1	New Time-Outs.....	185
16.2	Memory Impacts	185
16.3	Disk Usage Impacts	185
16.4	Port Usage Impacts.....	185
16.5	Hardware Impacts	185
16.6	Client Application Messaging Impacts.....	185
17	Service Patch Interface Impacts.....	186

17.1	Service Patch Interface Differences	186
17.2	Feature Activation Impacts.....	186
17.2.1	Behavior Impacts upon Activation	186
17.2.2	Provisioned Data Impacts on Activation.....	186
17.2.3	Provisioned Data Impacts on Deactivation	186
17.2.4	OCI Command Behavior Prior to Activation.....	186
18	Appendix A - Originating vs Terminating Calls in IMS Mode	187
	Acronyms and Abbreviations	188
	References	193

1 Requirements

1.1 Requirements

The base requirements upon which the BROADSOFT SYSTEM requirements are specified are noted by “[GIR R-x [y], ATIS [z]]”.

GIR refers to Internet Protocol (IP) Multimedia Subsystem (IMS) Core Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services, Issue 2.0, January 2013 [2].

ATIS refers to Emergency Telecommunications Service (ETS) Network Element Requirements for IMS-based Next Generation Network (NGN) Phase 2, ATIS 1000066.2016 [12].

Requirements that are struck though are not applicable to the BROADWORKS SYSTEM.

1.1.1 Mandatory Requirements

(R-1) The BROADWORKS SYSTEM shall identify an NS/EP NGN-PS call based on the presence of a Resource-Priority Header field (RPH) with either:

(R-1) a. A valid ets.x r-value and no wps namespace in a SIP INVITE request, or

(R-1) b. A valid ets.x r-value and a valid wps.y r-value in a SIP INVITE request.
[GIR R-163 [63], ATIS [63]]

(R-2) The BROADWORKS SYSTEM shall accept the ets and wps namespaces as valid with only the following resource values:

(R-2) a. for the ets namespace: ets.0, ets.1, ets.2, ets.3, or ets.4,

(R-2) b. for the wps namespace: wps.0, wps.1, wps.2, wps.3, or wps.4.
[GIR R-164 [64], ATIS [64]]

(R-3) For an NS/EP NGN-PS call, when multiple namespaces are sent, a BROADWORKS SYSTEM generating the RPH shall use one of the following formats in accordance with [RFC 4412]:

(R-3) a. Resource-Priority: namespace1.value1, namespace2.value2, ...

(R-3) b. Resource-Priority: namespace1.value1 Resource-Priority:
namespace2.value2

(R-3) c. Resource-Priority: namespace1.value1, namespace3.value3 Resource-Priority: namespace2.value2, ...
[GIR R-165 [65], ATIS [65]]

(R-4) For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall send the Supported header field with the 'resource-priority' option tag in the initial SIP INVITE request.
[GIR R-167 [501], ATIS [501]]

(R-5)When a BROADWORKS SYSTEM receives a SIP request containing a Require header field with the 'resource-priority' option tag, the BROADWORKS SYSTEM shall do one of the following:

(R-5) a. If the BROADWORKS SYSTEM does not support the SIP RPH, it shall respond with a SIP 420 (Bad Extension) response code. The FE shall list ""resource-priority"" in the Unsupported header field included in the SIP response.

(R-5) b. If the BROADWORKS SYSTEM supports RPH, but does not support the ets and wps namespaces, receives an NS/EP NGN-PS call request, then it shall reject the request with a SIP 417 (Unknown Resource-Priority) response.

(R-5) c. If the BROADWORKS SYSTEM supports RPH and supports the ets namespace, and the namespace syntax is correct, it shall process the SIP request in accordance with the requirements as specified in this Compliance Matrix."
[GIR R-168 [502]]

(R-6)For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall include the RPH when the BROADWORKS SYSTEM 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.
[GIR R-169 [67], ATIS [67]]

(R-7)For an NS/EP NGN-PS call, the BROADWORKS SYSTEM shall include the RPH when the BROADWORKS SYSTEM 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.
[GIR R-170 [68], ATIS [68]]

(R-8)For an NS/EP NGN-PS call, when a BROADWORKS SYSTEM receives a SIP 417 (Unknown Resource-Priority) response or a SIP 420 (Bad Extension) response to the initial SIP INVITE request that contains the RPH and the Require header field (including the 'resource-priority' option tag), the BROADWORKS SYSTEM shall follow the procedures specified below:

(R-8) a. The BROADWORKS SYSTEM shall resend the SIP INVITE request with the same headers, including both the RPH and Require header to another Functional Element (FE) if so configured,

(R-8) b. The BROADWORKS SYSTEM shall resend the SIP INVITE request without the Require header field, but with the RPH and a Supported header field with the 'resource-priority' option tag if every request sent per (1) receives either a SIP 417 response or a SIP 420 response with an Unsupported header field with the 'resource-priority' option tag, or if (1) is not applicable.

(R-8) c. The SIP 417 response and the SIP 420 response may contain an RPH. The BROADWORKS SYSTEM shall act as specified in items (R-8) a and (R-8) b whether or not the responses contain an RPH. The BROADWORKS SYSTEM shall generate, for each SIP 417 or SIP 420

response received, an error log entry containing the complete response received and the date and time of the error."
[GIR R-171 [69]]

(R-9) When a BROADWORKS SYSTEM receives a SIP request with an RPH with multiple instances of the ets namespace (e.g., Resource-Priority: ets.0, ets.2), the BROADWORKS SYSTEM 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 BROADWORKS SYSTEM shall generate an error log entry containing the complete SIP request received, and the date and time of the error.
[GIR R-174 [72], ATIS [72]]

(R-10) When a BROADWORKS SYSTEM 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 BROADWORKS SYSTEM 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 BROADWORKS SYSTEM shall generate an error log entry containing the complete SIP request received, and the date and time of the error.
[GIR R-175 [73], ATIS [73]]

(R-11) When a BROADWORKS SYSTEM receives a SIP request with an RPH with an invalid ets.x (e.g., Resource-Priority: ets.7), the BROADWORKS SYSTEM 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 BROADWORKS SYSTEM shall generate an error log entry containing the complete SIP request received, and the date and time of the error.
[GIR R-176 [74], ATIS [74]]

(R-12) When a BROADWORKS SYSTEM receives a SIP request with an RPH with an invalid wps.y (e.g., Resource-Priority: ets.0, wps.9), the BROADWORKS SYSTEM 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 BROADWORKS SYSTEM shall generate an error log entry containing the complete SIP request received, and the date and time of the error.
[GIR R-177 [75], ATIS [75]]

(R-13) When a BROADWORKS SYSTEM receives a SIP request with an RPH with wps.y and no ets.x (e.g., Resource-Priority: wps.4), the BROADWORKS SYSTEM 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 BROADWORKS SYSTEM shall generate an error log entry containing the complete SIP request received, and the date and time of the error.
[GIR R-178 [76], ATIS [76]]

(R-14) When a BROADWORKS SYSTEM receives a SIP ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, or UPDATE request or a SIP response with an RPH including an ets namespace for a call that was not initially recognized as an NS/EP NGN-PS call, the BROADWORKS SYSTEM shall:

(R-14) a. Use neither the ets nor wps namespaces in SIP requests and SIP responses associated with this call.

- (R-14) b.** Process the SIP requests and SIP responses associated with this call as for a normal call.
- (R-14) c.** The BROADWORKS SYSTEM 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."
[GIR R-179 [77], ATIS [77]]
- (R-15)** A Diameter-capable BROADWORKS SYSTEM FE that provides a Cx, Dx, Sh, Dh, or A3 interface shall support the Session-Priority AVP for NS/EP NGN-PS call processing. The Session-Priority AVP is type 8 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.
[GIR R-181 [503], ATIS [503]]
- ~~**(R-16)** For an NS/EP NGN-PS call, a BROADWORKS SYSTEM H.248-capable FE shall include the Priority indicator in the H.248 Add-Request command to indicate the Service User's priority level. See the Priority Values Mapping Table for appropriate mapping.
[GIR R-184 [81], ATIS [81]]~~
- ~~**(R-17)** A BROADWORKS SYSTEM 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.
[GIR R-185 [82], ATIS [82]]~~
- (R-18)** A BROADWORKS SYSTEM shall provide priority treatment (e.g., exemption from Machine Congestion Controls (MCC)) for the following SIP requests related to an NS/EP NGN-PS call: INVITE, ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.
[GIR R-186 [83], ATIS [83]]
- (R-19)** A BROADWORKS SYSTEM shall provide priority treatment (e.g., exemption from MCC) for the following SIP responses related to an NS/EP NGN-PS call: 1xx, 2xx, 3xx, 4xx, 5xx and 6xx, except for SIP 100 (Trying) and SIP 403 (Forbidden).
[GIR R-187 [84], ATIS [84]]
- (R-20)** When a BROADWORKS SYSTEM is waiting for resources external to the BROADWORKS SYSTEM (e.g., transport resources) to process a SIP INVITE request for an NS/EP NGN-PS call and has queued the request, the BROADWORKS SYSTEM shall send a SIP 182 (Queued) response.
[GIR R-188 [85], ATIS [85]]
- (R-21)** When an NS/EP NGN-PS call request is queued and the queue timer expires, the BROADWORKS SYSTEM shall send a SIP 408 (Request Timeout) response. The response shall include the Reason header field with the provisioned [Q.850] cause value.
[GIR R-189 [86], ATIS [86]]
- (R-22)** When a BROADWORKS SYSTEM receives a SIP CANCEL request for an NS/EP NGN-PS call request that it has queued, it shall remove the request from the queue and process the SIP CANCEL request as for a normal call, but with priority.
[GIR R-190 [87], ATIS [87]]

(R-23) When a BROADWORKS SYSTEM attempts to queue an NS/EP NGN-PS call 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).
[GIR R-191 [88], ATIS [88]]

(R-24) A BROADWORKS SYSTEM shall set the IP header DSCP value to the provisioned DSCPx value for the IP packets it generates to carry SIP messages that are related to an NS/EP NGN-PS call and that are provided priority treatment per R-18 and R-19.
[GIR R-192 [89], ATIS [89]]

~~**(R-25)** A BROADWORKS SYSTEM Diameter-capable FE shall set the IP header DSCP value to the provisioned DSCPx value for the IP packets it generates to carry Diameter messages that are related to an NS/EP NGN-PS call.
[GIR R-193 [90], ATIS [90]]~~

~~**(R-26)** An BROADWORKS SYSTEM H.248-capable FE shall set the IP header DSCP value to the provisioned DSCPx value for the IP packets it generates to carry H.248 messages that are related to an NS/EP NGN-PS call.
[GIR R-195 [92], ATIS [92]]~~

~~**(R-27)** An RTP-capable BROADWORKS SYSTEM FE shall set the IP header DSCP value to the provisioned DSCP_y value for the IP packets it generates to carry RTP media packets that are related to an NS/EP NGN-PS call.
[GIR R-196 [93], ATIS [93]]~~

(R-28) The BROADWORKS SYSTEM shall recognize that a received SIP INVITE request is associated with an NS/EP NGN-PS call by:

(R-28) a. The presence of an RPH with a valid ets.x and no wps, or with a valid ets.x and a valid wps.y, or

(R-28) b. Within the Request-URI, the presence of a provisioned GETS string as specified in R-29.
[GIR R-198 [95], ATIS [95]]

(R-29) The BROADWORKS SYSTEM 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-AN string (of length [m]), a successful match is detected when:

(R-29) a. The received user string contains at least ten digits, and

(R-29) b. The provisioned GETS-AN string matches the first [m] of the last ten digits of the received user string.

(R-29) c. When any of the above matches is successful, the BROADWORKS SYSTEM shall treat that call as an NS/EP NGN-PS call."
[GIR R-199 [96], ATIS [96]]

- (R-30)** When a BROADWORKS SYSTEM receives a SIP INVITE request from the direction of a UE that includes a GETS-AN within the Request-URI, and the BROADWORKS SYSTEM sends a corresponding SIP INVITE request to a FE, it shall include an RPH with the provisioned ets.x.
[GIR R-202 [99], ATIS [99]]
- (R-31)** When a BROADWORKS SYSTEM 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-AN, within the Request-URI:
- (R-31) a.** When the received RPH includes only an ets namespace or only ets and wps namespaces, the BROADWORKS SYSTEM 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.
 - (R-31) b.** Otherwise, when the received RPH includes other namespaces, the BROADWORKS SYSTEM 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-NS/EP NGN-PS request with other namespaces).
 - (R-31) c.** The BROADWORKS SYSTEM 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.
[GIR R-204 [504], ATIS [504]]
- (R-32)** For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall include RPH with the provisioned ets.x, and if available the wps.y based on R-36 in the following SIP requests it sends to an FE or, based on local policy, to an enterprise network: ACK, BYE, CANCEL, INFO, NOTIFY, PRACK, REFER, SUBSCRIBE, UPDATE.
[GIR R-207 [103], ATIS [103]]
- (R-33)** For an NS/EP NGN-PS call, based on local policy, a BROADWORKS SYSTEM shall include RPH with the provisioned ets.x, and if available the wps.y based on R-36 in SIP INVITE request it sends to an enterprise network.
[GIR R-209 [505], ATIS [505]]
- (R-34)** For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall exclude ets and wps namespaces from any RPH that is sent in SIP requests and responses to a UE.
[GIR R-210 [506], ATIS [506]]
- (R-35)** For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall include the RPH in 1xx, 2xx, 3xx, 4xx, 5xx and 6xx responses it sends to an FE 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 R-36, 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 or, based on local policy, to an enterprise network, even if the received response does not include an RPH.
[GIR R-211 [105], ATIS [105]]

- (R-36)** For an NS/EP NGN-PS call, a BROADWORKS SYSTEM shall retain the wps.y resource value most recently received within the SIP dialog from an FE. Any wps.y value received from a UE shall not be retained.
[GIR R-212 [106], ATIS [106]]
- (R-37)** ~~When the BROADWORKS SYSTEM sends a Diameter AA-Request (AAR) message to the PCRF for an NS/EP NGN-PS call, the BROADWORKS SYSTEM shall include the MPS-Identifier and Reservation-Priority AVPs [TS The BROADWORKS SYSTEM shall populate the MPS-Identifier AVP with a value of 'NS/EP NGN-PS'. If the originating Service User's priority level is available, the BROADWORKS SYSTEM shall populate the Reservation-Priority AVP with a value that corresponds to the originating Service User's priority level, consistent with the Priority Values Mapping Table. The Reservation-Priority AVP shall be populated with a default value if the originating Service User's priority level is unknown.~~
[GIR R-219 [507], ATIS [507]]
- (R-38)** ~~When the BROADWORKS SYSTEM receives a SIP INVITE request from an originating UE, that corresponds to an NS/EP NGN-PS call request, the BROADWORKS SYSTEM shall send a Diameter AAR message to the PCRF.~~
[GIR R-220 [508], ATIS [508]]
- (R-39)** ~~When the BROADWORKS SYSTEM receives a SIP INVITE request, destined for a terminating UE, that corresponds to an NS/EP NGN-PS call request, the BROADWORKS SYSTEM shall send a Diameter AAR message to the PCRF.~~
[GIR R-221 [509], ATIS [509]]
- (R-40)** When a BROADWORKS SYSTEM receives a SIP message with an RPH associated with an NS/EP NGN-PS call, the BROADWORKS SYSTEM shall include the same RPH in any corresponding SIP requests or responses that it sends, with the exception of the cases identified in R-7.
[GIR R-225 [115], ATIS [115]]
- (R-41)** When the user string in the Request-URI in the received SIP INVITE request contains at least ten digits, the BROADWORKS SYSTEM 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.
[GIR R-262 [142], ATIS [142]]
- (R-42)** When there is a match between the received user string in the Request-URI and a provisioned GETS-AN string per R-41, the BROADWORKS SYSTEM shall recognize the SIP INVITE request as a GETS-AN request, shall give priority treatment in all subsequent processing of the call, and shall mark all subsequent signaling for the call with appropriate NS/EP NGN-PS markings.
[GIR R-264 [143], ATIS [143]]
- (R-43)** ~~Upon receipt of an RPH in a SIP message associated with an NS/EP NGN-PS call, a BROADWORKS SYSTEM 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 R-7.~~
[GIR R-323 [170], ATIS [170]]
- (R-44)** For each NS/EP NGN-PS call, a CDR shall be generated. The CDR shall include an indicator that identifies the call as GETS.

- (R-44) a.** The BROADWORKS SYSTEM shall not record, nor produce to be recorded, the Service User's priority level.
- (R-44) b.** The BROADWORKS SYSTEM shall not include in the CDR the Service User's priority level.
- (R-44) c.** The BROADWORKS SYSTEM CDR shall identify the UE or user for a GETS-AN invoked call, as for normal calling."
[GIR R-415 [240], ATIS [240]]
- (R-45)** A BROADWORKS SYSTEM 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.
[GIR R-417 [242], ATIS [242]]
- (R-46)** A BROADWORKS SYSTEM 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.
[GIR R-451 [576], ATIS [576]]
- ~~**(R-47)** A BROADWORKS SYSTEM 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.
[GIR R-452 [276], ATIS [276]]~~
- (R-48)** The BROADWORKS SYSTEM shall allow configuration of the DSCP value ("DSCPx" value) to be used for the IP packets it generates to carry SIP, Diameter, and H.248 signaling messages related to an NS/EP NGN-PS call. The range of allowable values shall be 000000 to 111111 (0 to 63). The (factory) default "DSCPx" value shall be 101100 (44) (VOICE-ADMIT).
[GIR R-453 [277], ATIS [277]]
- (R-49)** A BROADWORKS SYSTEM shall allow configuration of the queue timer (identified in R-21) expiration value. The range of allowable values shall be 0 to 90 seconds. The (factory) default value shall be 30 seconds.
[GIR R-455 [279], ATIS [279]]
- (R-50)** A BROADWORKS SYSTEM shall allow configuration of the "provisioned [Q.850] cause value" identified in R-21. The range of allowable values shall be all values defined by [Q.850]. The (factory) default value shall be 102 (recovery on timer expiry).
[GIR R-456 [280], ATIS [280]]
- (R-51)** The BROADWORKS SYSTEM shall support the provisioning of at least twenty GETS-AN strings with a range of 3 – 10 digits to be used as matching criteria when processing an address contained within the Request-URI.
[GIR R-458 [282], ATIS [282]]
Note: R-51 expands the base requirement from 10 strings to 20 strings to support both TDM and IP GETS 8yy numbers
- ~~**(R-52)** A BROADWORKS SYSTEM shall allow configuration of the "default value" to be included in the Diameter Reservation Priority AVP in support of R-37. The range of allowable values shall be 11 – 15. The (factory) default value shall be 13.
[GIR R-488 [587]]~~

- (R-53)** The BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests received that attempt to establish a SIP dialog.
[GIR R-494 [589], ATIS [589]]
- (R-54)** The BROADWORKS SYSTEM shall count the number of initial SIP INVITE requests for NS/EP NGN-PS calls sent to a subsequent FE or sent to a UNI.
[GIR R-495 [590], ATIS [590]]
- (R-55)** The BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “service forbidden” is generated.
[GIR R-502 [597], ATIS [597]]
- (R-56)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “answered” is received.
[GIR R-496 [591], ATIS [591]]
- (R-57)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “caller abandoned” or “ringing but not answered” is received. The BROADWORKS SYSTEM shall also count the number of calls/sessions assumed abandoned due to the expiration of an appropriate timer or other changes in the call state.
[GIR R-497 [592], ATIS [592]]
- (R-58)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “destination busy” is received.
[GIR R-498 [593], ATIS [593]]
- (R-59)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “service unavailable” is received.
[GIR R-499 [594], ATIS [594]]
- (R-60)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “timed out of queue” is received.
[GIR R-500 [595], ATIS [595]]
- (R-61)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “service unavailable” is generated.
[GIR R-501 [596], ATIS [596]]
- (R-62)** A BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS call requests for which signaling indicating “service forbidden” is generated.
[GIR R-502 [597], ATIS [597]]
- (R-63)** A BROADWORKS SYSTEM shall count the number of messages sent to a log file during a dialog identified with an NS/EP NGN-PS call request. These messages include: (1) receipt of SIP 417 and SIP 420 responses (R-8); (2) transmission of SIP 400 responses (R-9 through R-13); and (3) messages received with an RPH with an ets namespace during a SIP dialog not initially being recognized as NS/EP NGN-PS (R-14).
[GIR R-503 [598], ATIS [598]]
- (R-64)** For an NS/EP NGN-PS call, it is desirable that a BROADWORKS SYSTEM shall provide priority treatment at the IP layer (L3) to the SIP, Diameter, and H.248 messages as applicable to the BROADWORKS SYSTEM, based on the provisioned NS/EP NGN-PS marking (e.g., DSCP value (DSCPx), IP address) for an NS/EP NGN-

PS call.
[GIR O-28 [390], ATIS [390]]

~~(R-65) For an NS/EP NGN-PS call, it is desirable that the BROADWORKS SYSTEM shall provide priority treatment to the RTP (media) packets at the IP layer (L3) based on the provisioned IP header DSCP value (DSCPv) for an NS/EP NGN-PS call.
[GIR O-29 [391], ATIS [391]]~~

(R-66) It is desirable that the BROADWORKS SYSTEM's overload controls shall permit message prioritization, based on local policy. It shall permit the prioritization of messages based on the content of the Resource-Priority header field.
[GIR O-31 [393]]

(R-67) The BROADWORKS SYSTEM shall provide the capability for BroadSoft to control activation of the NGN GETS FEATURE.

(R-68) The BROADWORKS SYSTEM shall provide the capability to control access to the NGN GETS FEATURE parameters.

1.1.2 Conditional Requirements

~~(CR-1) If the BROADWORKS SYSTEM H.248-capable controller FE support [H.248.52] and NS/EP NGN-PS call requires a specific NS/EP NGN-PS DSCP marking, an H.248-capable FE shall include the DiffServ Code Point in the H.248 Add_Request command to allow a gateway to apply a specific NS/EP NGN-PS DSCP marking to the signaling and bearer packets.
[GIR CR-23 [671], ATIS [671]]~~

(CR-2) If a BROADWORKS SYSTEM supports the Ethernet COS capabilities on an Ethernet interface between the FE and an IP router/Ethernet switch, the BROADWORKS SYSTEM shall set the Ethernet Frame Header COS parameter on the Ethernet interface to the provisioned "NS/EP" COS value for an NS/EP NGN-PS call.
[GIR CR-24 [326], ATIS [326]]

~~(CR-3) If a BROADWORKS SYSTEM sends to an SLF a Diameter User-Data-Request (UDR) message, the BROADWORKS SYSTEM shall include the Session-Priority AVP in the Diameter UDR message.
[GIR CR-25 [672], ATIS [672]]~~

~~(CR-4) If the Service-User subscription information is maintained in an HSS, the BROADWORKS SYSTEM shall send a Diameter User-Data-Request (UDR) message with the Session-Priority AVP to the HSS. The BROADWORKS SYSTEM 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.
[GIR CR-26 [673], ATIS [673]]~~

(CR-5) If the BROADWORKS SYSTEM SIP-capable FE implements an internal or external MCC overload control based on a "high/low watermark" MCC mechanism, then either messages/packets identified as being associated with NS/EP NGN-PS call requests shall be exempt from the MCC overload control, or there shall be a separate, higher, "high water mark" for NS/EP NGN-PS call requests. This "high water mark" shall be configurable.
[GIR CR-40 [335]]

- (CR-6)** — If the MCC Overload Control Algorithm causes the BROADWORKS SYSTEM SIP-capable FE to apply a static or dynamic percent blocking to limit the BROADWORKS SYSTEM's offered load, then identified NS/EP NGN-PS call requests shall be exempt from the percent blocking, until the percent to be blocked reaches a specific NS/EP NGN-PS Threshold. This NS/EP NGN-PS Threshold shall be configurable.
[GIR CR-41 [336]]
- (CR-7)** — If a BROADWORKS SYSTEM SIP-capable FE implements an internal or external MCC overload control based on a “leaky bucket” approach, then there shall be a separate NS/EP NGN-PS Token Bucket Size applicable to identified NS/EP NGN-PS call requests. This NS/EP NGN-PS Bucket Size shall be configurable.
[GIR CR-42 [337]]
- (CR-8)** — If the BROADWORKS SYSTEM Diameter-capable FE implements an internal or external MCC overload control based on a “high/low watermark” MCC mechanism, then either messages/packets identified as being associated with NS/EP NGN-PS call requests shall be exempt from the MCC overload control, or there shall be a separate, higher, “high water mark” for NS/EP NGN-PS call requests. This “high water mark” shall be configurable.
[GIR CR-43 [338]]
- (CR-9)** — If a BROADWORKS SYSTEM Diameter-capable FE implements an internal or external MCC overload control based on percent blocked, then messages/packets identified as being associated with NS/EP NGN-PS call requests shall be exempt from the “percent blocked”, until the percent to be blocked reaches a specific NS/EP NGN-PS threshold (default 100%). This NS/EP NGN-PS Threshold shall be configurable.
[GIR CR-44 [339]]
- (CR-10)** — If a BROADWORKS SYSTEM Diameter-capable FE implements an internal or external MCC overload control based on a “leaky bucket” approach, then there shall be a separate NS/EP NGN-PS Token Bucket Size applicable to messages/packets identified as being associated with NS/EP NGN-PS call requests. This NS/EP NGN-PS Bucket Size shall be configurable.
[GIR CR-45 [340]]
- (CR-11)** — If a BROADWORKS SYSTEM H.248-capable FE implements an internal or external MCC overload control based on a “high/low watermark” MCC mechanism, then either messages/packets identified as associated with NS/EP NGN-PS call requests shall be exempt from the external MCC overload control, or there shall be a separate, higher, “high water mark” for NS/EP NGN-PS call requests. This “high water mark” shall be configurable.
[GIR CR-46 [341]]
- (CR-12)** — If a BROADWORKS SYSTEM H.248-capable FE implements an internal or external MCC overload control based on percent blocked, then messages/packets identified as being associated with NS/EP NGN-PS call requests shall be exempt from the “percent blocked”, until the percent to be blocked reaches a specific NS/EP NGN-PS threshold (default 100%). This NS/EP NGN-PS Threshold shall be configurable.
[GIR CR-47 [339]]
- (CR-13)** — If a BROADWORKS SYSTEM H.248-capable FE implements an internal or external MCC overload control based on a “leaky bucket” approach, then there shall be a separate NS/EP NGN-PS Token Bucket Size applicable to messages/packets identified as being associated with NS/EP NGN-PS call requests. This NS/EP NGN-PS Bucket Size

shall be configurable.
[GIR CR-48 [340]]

(CR-14) If a BROADWORKS SYSTEM SIP-capable FE can support multiple routing of an NS/EP NGN-PS call request to a destination, then the routing list shall be configurable in support of R-8.
[GIR CR-61 [356]]

(CR-15) If a BROADWORKS SYSTEM 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 CR-2. The range of allowable values shall be 0 through 7. The (factory) default value shall be 5.
[GIR CR-70 [361], ATIS [361]]

(CR-16) If a BROADWORKS SYSTEM FE implements an internal or external MCC overload control based on a “high/low watermark” MCC mechanism (as specified in CR-5, CR-8, or CR-11), then the “high water mark” for NS/EP NGN-PS call requests shall be configurable in terms of a percent above the normal “high water mark.” The range shall be 0% (same as normal) to 100% (twice normal) with a default of 20%.
[GIR CR-71 [362]]

~~**(CR-17)** If the MCC Overload Control Algorithm causes a BROADWORKS SYSTEM FE to apply a static or dynamic percent blocking to limit the FE’s offered load (as specified in CR-6, CR-9, or CR-12), then the specific GETS Threshold shall be configurable, with a range of 0% to 100%, with the additional constraint that the GETS Threshold must be greater than the normal threshold. The default shall be 100% (i.e., NS/EP NGN-PS call requests are not blocked).
[GIR CR-72 [363]]~~

~~**(CR-18)** If a BROADWORKS SYSTEM FE implements an internal or external MCC overload control based on a “leaky bucket” approach (as specified in CR-7, CR-10, or CR-13), then the NS/EP NGN-PS Token Bucket Size shall be configurable. The range shall be 0% (same as normal) to 100% (twice normal) with a default of 20%.
[GIR CR-73 [364]]~~

~~**(CR-19)** If the BROADSOFT SYSTEM limits or throttles NS/EP NGN-PS calls/session requests via call admission controls (CAC) or other mechanisms, the BROADWORKS SYSTEM shall count the number of NS/EP NGN-PS calls/session requests rejected due to call admission controls and other NS/EP NGN-PS throttling mechanisms.
[GIR CR-74 [683]]~~

~~**(CR-20)** If the BROADWORKS SYSTEM supports exemption from packet flow controls, it is desirable that the NS/EP NGN-PS AS count the number of NS/EP NGN-PS calls/session requests exempted from packet flow controls including ACC.
[GIR CO-7 [720], ATIS [720]]~~

1.2 Additional Security Requirements

There are no additional requirements.

1.3 Mapping of Requirements to Document

SOW: Statement of Work requirements.

SECT: Main section in this document that describes the requirement.

BASE: Part of AS base functionality and not specifically documented in this document.

SOW	SECT	SOW	SECT	SOW	SECT	SOW	SECT	SOW	SECT
R-1	5.2	R-21	BASE	R-41	5.2.1.2.1	R-61	7.2.1	CR-13	N/A
R-2	5.7.1	R-22	BASE	R-42	5.2.1.2.1	R-62	7.2.1	CR-14	5.4.3
R-3	5.7.1	R-23	BASE	R-43	NA	R-63	7.2.1	CR-15	5.10
R-4	5.7.4	R-24	5.9	R-44	7.1	R-64	5.9, 8.1.1	CR-16	5.3
R-5	BASE, 5.7.1	R-25	N/A	R-45	4.1.1	R-65	N/A	CR-17	N/A
R-6	5.7.1	R-26	N/A	R-46	4.1.1, 5.8.2.1	R-66	5.3	CR-18	N/A
R-7	5.7.1	R-27	N/A	R-47	N/A	R-67	4.1	CR-19	N/A
R-8	5.4.3	R-28	5.2.1	R-48	Partial, 5.99	R-68	4.1	CR-20	N/A
R-9	5.7.1	R-29	5.2.1	R-49	BASE	CR-1	N/A		
R-10	5.7.1	R-30	5.4.1, 5.2.1.2	R-50	BASE	CR-2	5.10		
R-11	5.7.1	R-31	5.2.1.2 5.7.1	R-51	4.1.1.4	CR-3	N/A		
R-12	5.7.1	R-32	5.4.1, 5.6.1, 5.7.1	R-52	N/A due to R-37	CR-4	N/A		
R-13	5.7.1	R-33	5.4.1, 5.7.1	R-53	7.2.1	CR-5	5.3		
R-14	5.7.1	R-34	5.4.1	R-54	7.2.1	CR-6	N/A		
R-15	5.8.2	R-35	5.4.1, 5.7.1	R-55	7.2.1	CR-7	N/A		
R-16	N/A	R-36	5.7.1	R-56	7.2.1	CR-8	5.3		
R-17	N/A	R-37	N/A	R-57	7.2.1	CR-9	N/A		
R-18	5.3, 5.7.1	R-38	N/A	R-58	7.2.1	CR-10	N/A		
R-19	5.7.1	R-39	N/A	R-59	7.2.1	CR-11	N/A		
R-20	BASE	R-40	5.7.1	R-60	7.2.1	CR-12	N/A		

2 Feature Purpose and Overview

Applicable Telephony Application Server (TAS)

Application Server (AS)

2.1 Purpose

Government Emergency Telecommunications Service (GETS) is a set of requirements aimed at significantly increasing the likelihood of successful voice communication completion in times of crisis (natural or man-made disasters), when communication networks are expected to be overloaded.

2.2 Overview

This document describes how Cisco BroadWorks Telephony Application Server (TAS) supports GETS functionality in Internet Protocol Multimedia Subsystem (IMS) networks and as a Next Generation Network (NGN) standalone server.

The standalone mode allows the Cisco BroadWorks TAS to communicate directly with devices and network elements (Session Border Controllers (SBC), network gateways, proxies, and so on). Basic services and call processing for originating and terminating sessions are applied for Cisco BroadWorks users.

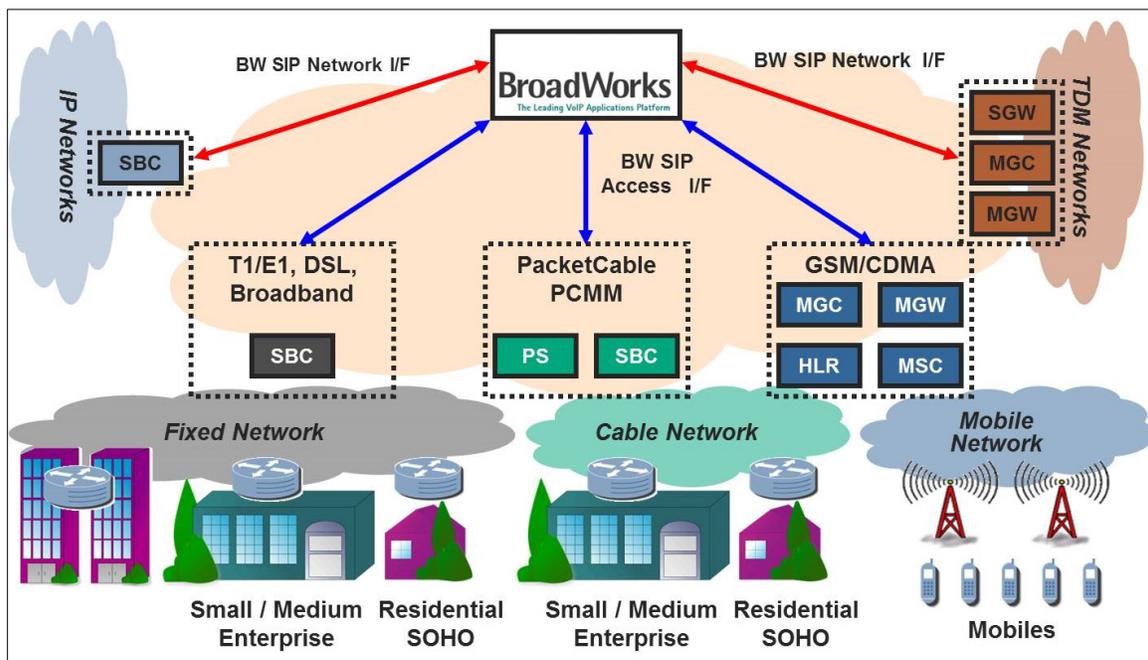


Figure 1 Cisco BroadWorks NGN Standalone Architecture

The IMS mode allows integration of the Cisco BroadWorks TAS in an IMS architecture framework. The IP Media Subsystem (IMS) is a unified service delivery architecture for next generation converged voice and data services. The Cisco BroadWorks TAS is an IMS Session Initiation Protocol (SIP) Application Server located within the IMS application layer. The Cisco BroadWorks TAS no longer interacts directly with the devices and the network, but with a Call Session Control Function (CSCF); for example, devices now register with the Serving-Call Session Control Function (S-CSCF). The basic services and call processing are the same as in the standalone mode, but special signaling options and service logic are also applied.

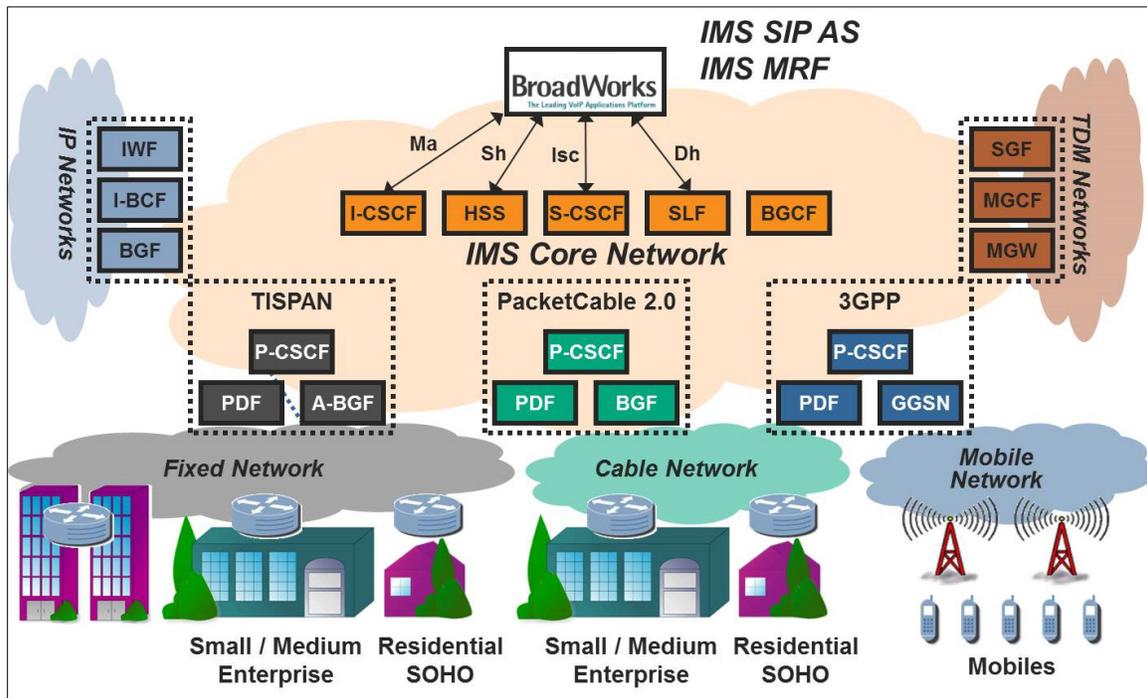


Figure 2 Cisco BroadWorks IMS Architecture

In the context of this document, Cisco BroadWorks TAS refers to functional elements Application Server (AS) and/or Network Server (NS).

An important distinction to be made is that the Cisco BroadWorks TAS does **not** implement the GETS-FC (Feature Code) AS, GETS-NT (Number Translation) AS, or GETS-AN (Access Number) AS FE behavior. As such, it does **not** authenticate GETS FC users, and it does not communicate with the GETS Personal Identification Number (PIN) and/or translation databases; however, it executes originating, mid-call, and terminating services while honoring the GETS priority. There are functional differences between when the Cisco BroadWorks TAS is running as part of an IMS network or as a standalone server. This document highlights the difference when applicable.

This feature supports the Government Emergency Telecommunications Service (GETS) and supported functionality includes:

- Promotes an originating call with a provisioned GETS-AN in the Request-URI to a GETS call (standalone mode).
- Support of GETS-FC, GETS-AN, and GETS-NT originating calls (IMS mode)
- Support of National Security and Emergency Preparedness (NS/EP) calls (both modes)

- GETS calls bypass overload controls and some originating blocking services (both modes).
- Provide strict enforcement of Next-Generation Network (NGN)-GETS requirements that pertain to the *Resource-Priority* header (RPH) validation (both modes)
- GETS feature code (GETS-FC) prefix stripping (IMS mode)
- GETS call type identification (both modes)
- Call scenarios where a GETS Application Server (GETS-AS) is located between the originating and terminating sessions (IMS mode)
- Call priority indication handling on the Diameter Online Charging Reference Point (Ro) interface (both modes)
- Privacy features that inhibit certain (configurable) attribute value pairs (AVP) in the Diameter accounting interface for GETS number translation (GETS-NT) calls. This allows for the ability not to include personally identifiable information (PII) in call detail records (CDRs) produced by external billing applications (both modes)
- System option enabling the bypass of the credit control function on the Diameter Ro interface for GETS call sessions. (both modes)
- Performance counters for all GETS call types both successful and attempted GETS calls (both modes).

Throughout this document, terminating GETS calls are referred to as terminating NS/EP calls.

3 Use Cases

3.1 Standalone Typical GETS Calls

3.1.1 NS/EP Call Termination

A Public Switched Telephone Network (PSTN) user initiates a GETS call to a Cisco BroadWorks user, by using one of the supported ways to invoke the GETS services. When it reaches the Cisco BroadWorks TAS, the SIP INVITE message is identified as GETS using its *Resource-Priority* header, allowing the call to bypass any overload controls and congestion management systems. A priority session is created for this call, which causes every outgoing message to also be labeled as GETS and handled with priority. On the network side, termination proceeds with the *Resource-Priority* header contents set in outgoing requests and responses. On the access side, Cisco BroadWorks TAS can be configured to remove GETS resource values (r-values) in outgoing requests and responses.

3.1.2 GETS-AN and GETS-NT Origination

Cisco BroadWorks GETS identifier mode is set to "Request-URI". Cisco BroadWorks User A initiates a GETS-AN/GETS-NT call by dialing a GETS-AN/GETS-NT number. A SIP INVITE request without a *Resource-Priority* header reaches the Cisco BroadWorks TAS. The user string portion of the Request-URI is compared against the provisioned list of GETS strings. When a match occurs, the request bypasses the Cisco BroadWorks TAS overload controls and the call is identified as a GETS-AN /GETS-NT call. Typical origination proceeds with the *Resource-Priority* header contents set in outgoing requests and responses. When the initial INVITE response reaches the Cisco BroadWorks TAS's originating session, the session's *Resource-Priority* header values are updated from the response (*Resource-Priority* header contents may have been changed by a median GETS-AS.)

3.1.3 GETS-FC Origination

Cisco BroadWorks GETS identifier mode is set to "Request-URI". A Cisco BroadWorks-hosted User A initiates a GETS-FC call by dialing a GETS-FC prefix (e.g. *272) and the directory number of a PSTN User B. A SIP INVITE request without a *Resource-Priority* header reaches the Cisco BroadWorks TAS. The user string portion of the Request-URI is compared against the provisioned list of GETS strings. No match occurs and the request does not bypass the Cisco BroadWorks TAS overload controls and the call is not identified as a GETS call. The call proceeds with normal call processing and fails as the GETS feature code is not recognized.

3.2 IMS Mode Typical GETS Calls

3.2.1 NS/EP Call Termination

A Public Switched Telephone Network (PSTN) user initiates a GETS call to a Cisco BroadWorks user, by using one of the supported ways to invoke the GETS services. When it reaches the Cisco BroadWorks TAS, the SIP INVITE message is identified as GETS using its *Resource-Priority* header, allowing the call to bypass any overload controls and congestion management systems. A priority session is created for this call, which causes every outgoing message to also be labeled as NS/EP and handled with priority. Typical termination proceeds with the *Resource-Priority* header contents set in outgoing requests and responses.

3.2.2 GETS-FC Origination with GETS-FC Prefix

A Cisco BroadWorks-hosted User A initiates a GETS-FC call by dialing a GETS-FC prefix and the directory number of a PSTN User B. A SIP INVITE request with valid GETS r-value(s) in its *Resource-Priority* header reaches the Cisco BroadWorks TAS servers with the GETS-FC prefix not stripped from the Request-URI. Based on the *Resource-Priority* header contents, the request also bypasses the Cisco BroadWorks TAS overload controls. After detecting the GETS-FC prefix, it is stripped from the Request-URI and the SIP endpoint is marked as a GETS-FC call. Typical origination then proceeds with the *Resource-Priority* header contents set in outgoing requests and responses.

3.2.3 GETS-FC Origination with no GETS-FC Prefix

A Cisco BroadWorks-hosted User A initiates a GETS-FC call by dialing a GETS-FC prefix and the directory number of a PSTN User B. An IMS Network Element authorizes the GETS call, removes the GETS-FC prefix in the Request-URI and includes the *Resource-Priority* header in the SIP INVITE.

A SIP INVITE request with valid GETS r-value(s) in its *Resource-Priority* header reaches the Cisco BroadWorks TAS servers with no GETS-FC prefix in the Request-URI. Based on the *Resource-Priority* header content, the request bypasses the Cisco BroadWorks TAS overload controls. No exact GETS call type can be identified and the call is marked as a GETS call. Typical origination then proceeds with the *Resource-Priority* header contents set in outgoing requests and responses.

3.2.4 GETS-AN Origination

Cisco BroadWorks User A initiates a GETS-AN call by dialing one of the GETS-AN numbers (710-NCS-GETS or one of the specific toll-free numbers in the 8YY-NXX-XXXX range). A SIP INVITE request with valid GETS r-value(s) in its *Resource-Priority* header reaches the Cisco BroadWorks TAS. Based on the *Resource-Priority* header contents, the request also bypasses the Cisco BroadWorks TAS overload controls. Since the dialed digits correspond to a network call, an enhanced network translation is triggered that causes the Cisco BroadWorks TAS to set the call type to GETS-AN based on the Network Server dial plan. The Cisco BroadWorks TAS uses this call type to identify the call as a GETS-AN call. Typical origination proceeds with the *Resource-Priority* header contents set in outgoing requests and responses. When the initial INVITE response reaches the Cisco BroadWorks TAS's originating session, the session's *Resource-Priority* header values are updated from the response. (*Resource-Priority* header contents may have been changed by a median GETS-AS.)

3.2.5 GETS-NT Origination

Cisco BroadWorks User A initiates a GETS-NT call by dialing a GETS-NT number (usually a number in the 710-NXX-XXXX range). A SIP INVITE request with valid GETS r-value(s) in its *Resource-Priority* header reaches the Cisco BroadWorks TAS. Based on the *Resource-Priority* header contents, the request also bypasses the Cisco BroadWorks TAS overload controls. Since the dialed digits correspond to a network call, an enhanced network translation is triggered that causes the Cisco BroadWorks TAS to set the call type to GETS-NT based on its dial plan. The Cisco BroadWorks TAS uses this call type to identify the call as a GETS-NT call. Typical origination proceeds with the *Resource-Priority* header contents set in outgoing requests and responses. When the initial INVITE response reaches the Cisco BroadWorks TAS's originating session, the session's *Resource-Priority* header values are updated from the response. (*Resource-Priority* header contents may have been changed by a median GETS-AS.)

3.2.6 GETS-FC + GETS-AN and GETS-FC + GETS NT Origination

A Cisco BroadWorks user initiates a GETS-FC call by dialing the GETS-FC prefix and one of the GETS-AN/GETS-NT numbers. This creates a combination of GETS-FC and GETS-AN/GETS-NT that causes the Cisco BroadWorks TAS to categorize this call as GETS-FC + GETS-AN/GETS-NT. After the prefix is stripped as in the use case in section [3.2.2 GETS-FC Origination with GETS-FC Prefix](#), the usual GETS-AN/GETS-NT handling applies. For more information about how a GETS-AN/GETS-NT communication is established, see the use case in section [3.2.4 GETS-AN Origination](#) or [3.2.5 GETS-NT Origination](#).

4 Provisioning Description

4.1 Licensing Impacts

This feature is a system service.

Official License Name	Government Emergency Telecommunications Service
License Type	System
Service Name	Government Emergency Telecommunications Service
Service Description	Increase the likelihood of successful voice communication completion in times of crisis, when communication networks are expected to be overloaded.
Service Quantity Type	Not applicable

Warning:

The use of GETS functionality is restricted in the U.S. and U.S. Territories to NS/EP users authorized by the Department of Homeland Security (DHS), Office of Emergency Communications (OEC).

Telecommunications deployment of GETS functionality must be coordinated with the OEC at the following address:

Office of Emergency Communications
 Attn: PTS Program Office
 245 Murray Lane
 Arlington, VA 20598-0615
 Email: gets@dhs.gov

4.2 Cisco BroadWorks Application Server Configuration

The Cisco BroadWorks application server is augmented with a GETS section that contains the system parameters for the GETS requirements.

4.2.1 GETS Configuration

Name	Description
<i>enabled</i>	This parameter controls whether the GETS feature is enabled. Default value is "false".
<i>enableRequireResourcePriority</i>	This parameter controls whether the outgoing first GETS call SIP INVITE request contains a <i>Require</i> header with the "resource-priority" option tag. Default value is "false".
<i>sendAccessResourcePriority</i>	This parameter controls whether GETS Resource Priority values are included in SIP traffic sent to the access side. Default value is "false". This parameter is ignored in IMS mode as IMS mode always includes GETS r-values to the access side.

Name	Description
<i>callIdentifierMode</i>	For standalone mode only, this parameter identifies the method used to identify GETS calls. This parameter is only used when creating a call session while processing an originating SIP INVITE. The possible modes are "RPH", "Request-URI", or "RPH-Request-URI". Default value is "RPH-Request-URI". This parameter is ignored in IMS mode as IMS mode only runs in "RPH" mode.
<i>priorityAVP</i>	This parameter determines the Diameter interface Session-Priority Attribute Value Pair (AVP) used when no session priority mapping are defined for the GETS call (see 4.1.1.2). The value "0" is the highest priority and "4" is the lowest. Default is "0".
<i>signalingDSCP</i>	This parameter specifies the signaling Differentiated Services Code Point (DSCP) value to identify GETS SIP traffic. Default is "44".
<i>COSPriority</i>	This parameter specifies the socket priority value that is used for GETS SIP traffic. It is used to set the Ethernet Frame Header Class of Service (COS) on the Ethernet interface. Valid values are 0 to 7. The default value is "1".
<i>outgoingSipUdpPort</i>	This parameter specifies the <i>From</i> port for outgoing GETS SIP UDP signaling.
<i>outgoingSipTcpPort</i>	This parameter specifies the <i>From</i> port for outgoing GETS SIP TCP signaling.
<i>defaultRValue</i>	This parameter specifies the <i>GETS-Mandatory</i> (e.g. ets.0) r-value that is used to promote a call to GETS when a SIP INVITE is received with a GETS-AN or GETS-NT within the Request-URI. It is also used in a SIP 400 response when no <i>GETS-Mandatory</i> class r-values have been received in a request. Default is "ets.0". See section 5.7.1.1 for details on GETS-Mandatory class definitions.
<i>bypassRoRelease</i>	When Cisco BroadWorks is configured to use Diameter Ro interface for credit control access, and this parameter is set to true, the GETS session is not terminated after receiving one of the following Diameter messages: <ul style="list-style-type: none"> - Abort-Session-Requests (ASR) or - Credit-Control-Answer (CCA) that contains the <i>Final-Unit-Indication</i> attribute-value pair (AVP) and a <i>Final-Unit-Action</i> AVP set to "TERMINATE" or "REDIRECT". Default is "false".
<i>resourcePriorities</i>	This group of parameters specifies the list of Cisco BroadWorks supported GETS r-values in a <i>Resource-Priority</i> SIP header. See 4.1.1.1 Resource Priorities Sub-Element Configuration for details.
<i>sessionPrioritiesMapping</i>	This group of parameters specifies mappings between a service user's priority level and a Diameter Session-Priority Attribute Value Pair (AVP) value. See 4.1.1.2 Session Priority Mappings Sub-Element Configuration for details.

Name	Description
<i>featureCodes</i>	This group of parameters specifies a list of GETS reserved feature access codes. See 4.1.1.3 Feature Codes Sub-Element Configuration for details.
<i>numbers</i>	This group of parameters specifies a list of provisioned GETS-AN and GETS-NT strings. See 4.1.1.4 GETS Numbers Sub-Element Configuration for details.

4.2.1.1 Resource Priorities Sub-Element Configuration

The new elements defined in the following table are added to the *resourcePriorities* collection. *RFC 4412* specifies the syntax (token-nodot + "." + token-nodot). The values are validated accordingly. The following shows how the token-nodot is defined in the document. See section 5.7.1.1 for detailed resource priorities definitions.

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

Name	Description
<i>priorityValue</i>	This parameter specifies a unique recognized r-value and a priority value used in the <i>Resource-Priority</i> SIP header, as defined in the <i>RFC 4412</i> specification. Values are case-insensitive and composed of a namespace, a dot, and a priority value. Only "ets" and "wps" namespaces are valid. For example, "ets.0."
<i>priorityLevel</i>	The session priority-level value that is attached to a session receiving this r-value. The effective priority level of a call session is the lowest <i>priorityLevel</i> of all received r-value(s). Valid values are 1 through 5, where 1 is the highest priority level. This is used to determine the value of the Session-Priority AVP.
<i>priorityClass</i>	Class the r-value belongs to. Affects how <i>Resource-Priority</i> header content is validated when invoking priority services. Choice of: <ul style="list-style-type: none"> ▪ <i>GETS-Mandatory</i>: Triggers NGN GETS priority services. At least one is required in this class to invoke GETS priority services (ets) ▪ <i>GETS</i>: Triggers NGN GETS <i>Resource-Priority</i> header validation (wps). See section 5.7.1.1 Resource Priority Header Handling for detailed description of GETS-Mandatory and GETS.

4.2.1.2 Session Priority Mappings Sub-Element Configuration

Since the Cisco BroadWorks TAS needs to add the Session-Priority AVP to outgoing Ro interface Diameter requests associated with GETS calls, it has to provide a mechanism to specify a mapping between a service user's priority and Session-Priority AVP values. The following *SessionPriority* table provides that mechanism.

Name	Description
<i>priorityLevel</i>	A session priority level as defined on the <i>ResourcePriorities</i> list.
<i>sessionPriorityValue</i>	The value of the Session-Priority AVP for outgoing Ro Diameter requests that result from INVITEs containing the associated resource priority values. According to <i>3GPP TS 29.229 [5]</i> , the value of this field can be one of the following digits where "0" has the highest priority and "4" has the lowest priority: <ul style="list-style-type: none"> ▪ 0 (PRIORITY-0) ▪ 1 (PRIORITY-1) ▪ 2 (PRIORITY-2) ▪ 3 (PRIORITY-3) ▪ 4 (PRIORITY-4)

4.2.1.3 Feature Codes Sub-Element Configuration

A list of reserved feature access codes can be configured for the Cisco BroadWorks TAS. This configuration is used only when in IMS Mode. A single such entry is defined as follows.

Name	Description
<i>Code</i>	This parameter specifies a unique reserved feature access code for GETS calls. Valid values consist of characters 0 through 9, *, #. The code must always start with character *.
<i>Description</i>	This parameter specifies the reason for reserving this feature access code.

4.2.1.4 GETS Numbers Sub-Element Configuration

A list of provisioned GETS AN or NT strings that are used in standalone mode to identify a SIP INVITE message as a GETS call when its Request-URI user part matches one of the strings in this list. This configuration is used only when in standalone mode.

Name	Description
<i>Type</i>	GETS-AN or GET-NT

Name	Description
<i>Number</i>	<p>The parameter represents a unique GETS-AN or GETS-NT string. This string matches with the Request-URI received user string to promote a regular call to a GETS call. 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). This parameter accepts a string of 4 to 10 characters, which may consists of 10 digits or 3 to 9 digits completed by a wildcard star character (*). Note that if the Request-URI received is a SIP:URI without user=phone, user=phone error correction can be done depending on the <i>userPhoneErrorCorrection</i> parameter and that the E.164 format is supported.</p> <p>For matching against a provisioned GETS-AN/NT string , a successful match is detected when:</p> <ul style="list-style-type: none"> • The received user string contains at least ten digits. • If the provisioned GETS-AN/NT has a wildcard, it matches the digits before the wildcard with the first digits of the received user string. For example a provisioned GETS-AN/NT value of "710*" will produce a positive match for all received user string "710xxxxxx". • If the provisioned GETS-AN/NT doesn't have a wildcard, it matches all ten digits of the received user string.
<i>Description</i>	This parameter specifies a brief description of the GETS-AN/NT number.

4.2.1.5 GETS-NT Inhibited AVP Code List Configuration

For billing purposes, a configurable list of inhibited Diameter Attribute Value Pair (AVP) is added to the Cisco BroadWorks TAS. The AVP Code, combined with the Vendor-Id field, uniquely identifies a Diameter attribute (see [8] *Diameter Base Protocol* for more info). The AVPs contained on this list are omitted while building outgoing billing Diameter requests (ACR on Rf and CCR on Ro), resulting from originating GETS-NT or GETS-FC + GETS-NT call sessions. See section 5.8.3 *GETS-NT Inhibited Accounting AVPs Support* for more information.

Name	Description
<i>avpCode</i>	The code of the Diameter AVP to be inhibited.
<i>vendorId</i>	The vendor ID for the Diameter AVP to be inhibited.

4.2.1.6 Web Impacts

There are no impacts.

4.2.1.7 Help Pages Impacts

There are no impacts.

4.2.1.8 CLI Impacts

System administrators can modify and view the GETS-related system parameters. The parameters are accessed and modified via the following CLI context:

```
AS_CLI/System/CallP/GETS> get; set
```

```
AS_CLI/System/CallP/GETS/Numbers> add; get; delete; set, clear
```

```

AS_CLI/System/CallP/GETS/InhibitedAVPCodes> add; get; delete
AS_CLI/System/CallP/GETS/Network> get; set;
AS_CLI/System/CallP/GETS/ResourcePriorities> add; get; delete; set
AS_CLI/System/CallP/GETS/SessionPriorityMap> add; get; delete; set
AS_CLI/System/CallP/GETS/ReservedFACs> add; get; delete; set, clear

```

4.2.1.9 Public Interface Impacts

The following OCI-P commands are added to configure the GETS-related parameters:

- SystemGETSGetRequest
- SystemGETSModifyRequest
- SystemGETSReservedFeatureAccessCodeAddRequest
- SystemGETSReservedFeatureAccessCodeDeleteRequest
- SystemGETSReservedFeatureAccessCodeGetListRequest
- SystemGETSReservedFeatureAccessCodeModifyRequest
- SystemGETSNumberAddRequest
- SystemGETSNumberDeleteRequest
- SystemGETSNumberGetListRequest
- SystemGETSNumberModifyRequest
- SystemGETSResourcePriorityAddRequest
- SystemGETSResourcePriorityDeleteRequest
- SystemGETSResourcePriorityGetListRequest
- SystemGETSResourcePriorityModifyRequest
- SystemGETSSessionPriorityMapAddRequest
- SystemGETSSessionPriorityMapDeleteRequest
- SystemGETSSessionPriorityMapGetListRequest
- SystemGETSSessionPriorityMapModifyRequest
- SystemGETSAvpCodeMapAddRequest
- SystemGETSAvpCodeMapDeleteRequest
- SystemGETSAvpCodeMapGetListRequest

4.2.2 Emergency Distributed Denial of Service (DDoS) Protection

Name	Description
<i>enabled</i>	<p>This parameter enables the emergency DDoS Protection mechanism. The default value is "False".</p> <p>Note that the parameter <i>protectionRate</i> needs to be set (non Null) before <i>enabled</i> can be set to 'True', otherwise an error is returned.</p>

Name	Description
<i>protectionRate</i>	<p>This is the emergency calls per second rate that the server accepts before any new emergency calls are dropped. An incoming emergency call is dropped if the current emergency calls per second exceeds this configured threshold value.</p> <p>The default value is Null. This parameter needs to be non Null before the variable <i>enabled</i> can be set to "True". Valid values are 1 to 10000.</p> <p>For a service provider concerned about the potential of a very high emergency call rate, the emergency <i>protectionRate</i> could be set around 1X of the AS capacity.</p>
<i>sampleIntervalInSeconds</i>	<p>The number of seconds used to calculate the emergency calls per second. The emergency calls per second is the average for this interval. Measuring the average call rate over the sample interval allows amortizing the effect of sporadic variations that may occur over shorter time interval.</p> <p>Valid values are 1 to 30. Default value is 5 seconds.</p>
<i>protectionAction</i>	<p>Specifies the action to be performed when an emergency call is declined by the emergency DDoS Protection mechanism. The possible actions are:</p> <p>"Redirect" (Respond to the message with "302 Moved Temporarily"), "Error" (Respond to the message with "503 Service Unavailable"), "Decline" (Respond to the message with 603 + Retry-After), "Drop" (Do not respond) or "Unavailable" (Respond to the message with 480 + Retry-After. Default value is "Error"</p>

4.2.2.1 Web Impacts

There are no impacts.

4.2.2.2 Help Pages Impacts

There are no impacts.

4.2.2.3 CLI Impacts

System administrators can modify and view the Emergency Call DDoS Protection system parameters. The parameters are accessed and modified via the following CLI context:

```
AS_CLI/System/CallP/EmergencyCallDDoSProtection> get; set; clear;
```

Warning Message:

The following warning message is returned when the *enabled* flag is set to "true" or when the protection rate is changed:

"WARNING: The Protection Rate is a critical configuration parameter. Ensure that the value chosen meets your requirements for processing number of emergency calls per second and protecting the system from entering severe overload.

Do you want to proceed with your changes? (yes/no)"

4.2.2.4 Public Interface Impacts

The following OCI-P commands are added to configure the Emergency Call DDoS Protection parameters:

- SystemEmergencyCallDDoSProtectionGetRequest

- SystemEmergencyCallIDDoSProtectionModifyRequest

4.3 Cisco BroadWorks Network Server Configuration

The existing GETS section of the Cisco BroadWorks Network server is augmented with new system parameters for the GETS AS support. Note that for adequate feature handling, all Network Servers that are part of the same replication cluster should be configured with the same GETS attributes.

4.3.1 GETS Configuration

Name	Description
<i>GETSNumbers</i>	This parameter specifies a list of provisioned GETS-AN and GETS-NT strings.

4.3.1.1 GETS Numbers Sub-Element Configuration

A list of provisioned GETS AN or NT strings that are used to identify a SIP INVITE message as a GETS call when its Request-URI user part matches one of the strings in this list.

Name	Description
<i>Type</i>	GETS-AN or GET-NT
<i>Number</i>	<p>The parameter represents a GETS-AN or GETS-NT string. This string matches with the Request-URI received user string to promote a regular call to a GETS call. 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). This parameter accepts a string of 4 to 10 characters, which may consist of 10 digits or 3 to 9 digits completed by a wildcard star character (*). Note that if the Request-URI received is a SIP:URI without user=phone, user=phone error correction can be done depending on the <i>userPhoneErrorCorrection</i> parameter and that the E.164 format is supported.</p> <p>For matching against a provisioned GETS-AN/NT string , a successful match is detected when:</p> <ul style="list-style-type: none"> • The received user string contains at least ten digits. • If the provisioned GETS-AN/NT has a wildcard, it matches the digits before the wildcard with the first digits of the received user string. For example a provisioned GETS-AN/NT value of "710*" will produce a positive match for all received user string "710xxxxxx". • If the provisioned GETS-AN/NT doesn't have a wildcard, it matches all ten digits of the received user string.
<i>Description</i>	This parameter specifies a brief description of the GETS-AN/NT value.

4.3.1.2 Web Impacts

There are no impacts.

4.3.1.3 Help Pages Impacts

There are no impacts.

4.3.1.4 CLI Impacts

System administrators can modify and view the GETS-related system parameters. The parameters are accessed and modified via the following CLI context:

```
NS_CLI/System/CallP/GETS/GETSNumbers> add; get; delete; set
```

4.3.1.5 Public Interface Impacts

There are no impacts.

4.3.2 Emergency Distributed Denial of Service (DDoS) Protection

Name	Description
<i>enabled</i>	This parameter enables the emergency DDoS Protection mechanism. The default value is "False". Note that the parameter <i>protectionRate</i> needs to be set (non Null) before <i>enabled</i> can be set to 'True', otherwise an error is returned.
<i>protectionRate</i>	This is the emergency calls per second rate that the server accepts before any new emergency calls are dropped. An incoming emergency call is dropped if the current emergency calls per second exceeds this configured threshold value. The default value is Null. This parameter needs to be non Null before the variable <i>enabled</i> can be set to "True". Valid values are 1 to 10000. For a service provider concerned about the potential of a very high emergency call rate, the emergency <i>protectionRate</i> could be set around 1X of the AS capacity.
<i>sampleIntervalInSeconds</i>	The number of seconds used to calculate the emergency calls per second. The emergency calls per second is based on the average for this interval. Measuring the average call rate over the sample interval allows amortizing the effect of sporadic variations that may occur over shorter time interval. Valid values are 1 to 30. Default value is 5 seconds.
<i>protectionAction</i>	Specifies the action to be performed when an emergency call is declined by the emergency DDoS Protection mechanism. The possible actions are: "Error" (Respond to the message with "503 Service Unavailable") "Drop" (Do not respond). Default value is "Error"

4.3.2.1 Web Impacts

There are no impacts.

4.3.2.2 Help Pages Impacts

There are no impacts.

4.3.2.3 CLI Impacts

System administrators can modify and view the Emergency Call DDoS Protection related system parameters. The parameters are accessed and modified via the following CLI context:

```
NS_CLI/System/CallP/EmergencyCallDDoSProtection> get; set; clear;
```

Warning Message:

The following warning message is returned when the *enabled* flag is set to “true” or when the protection rate is changed:

“WARNING: The Protection Rate is a critical configuration parameter. Ensure that the value chosen meets your requirements for processing number of emergency calls per second and protecting the system from entering severe overload.

Please confirm (Yes, Y, No, N)”

4.3.2.4 Public Interface Impacts

There are no impacts.

5 Feature Operation

5.1 GETS and Cisco BroadWorks

Cisco BroadWorks implements the following functions (in relation to this activity, since Cisco also has servers for provisioning, database, and so on):

- Telephony Application Servers. This architecture consists of a Network Server (NS) and/or Application Server (AS).

IMPORTANT: Cisco BroadWorks does not implement the GETS AS. This means that Cisco BroadWorks does **not** collect the GETS PIN and GETS-AN destination numbers.

Although the call flows in this document are GETS-specific as implemented in the United States, the same principles apply in other countries/regions that have similar requirements and as specified by the *Multimedia Priority Service* [6] and *Enhancements for Multimedia priority service* [7]. Cisco BroadWorks supports these instances as well, provided that GETS AS functionality or preemption is not required.

5.2 Identifying GETS Calls

Once a call is identified as GETS, services that create additional call legs (such as call forwarding or forked to multiple destinations) are also created with GETS priority. Services interactions with other servers also contain GETS priority.

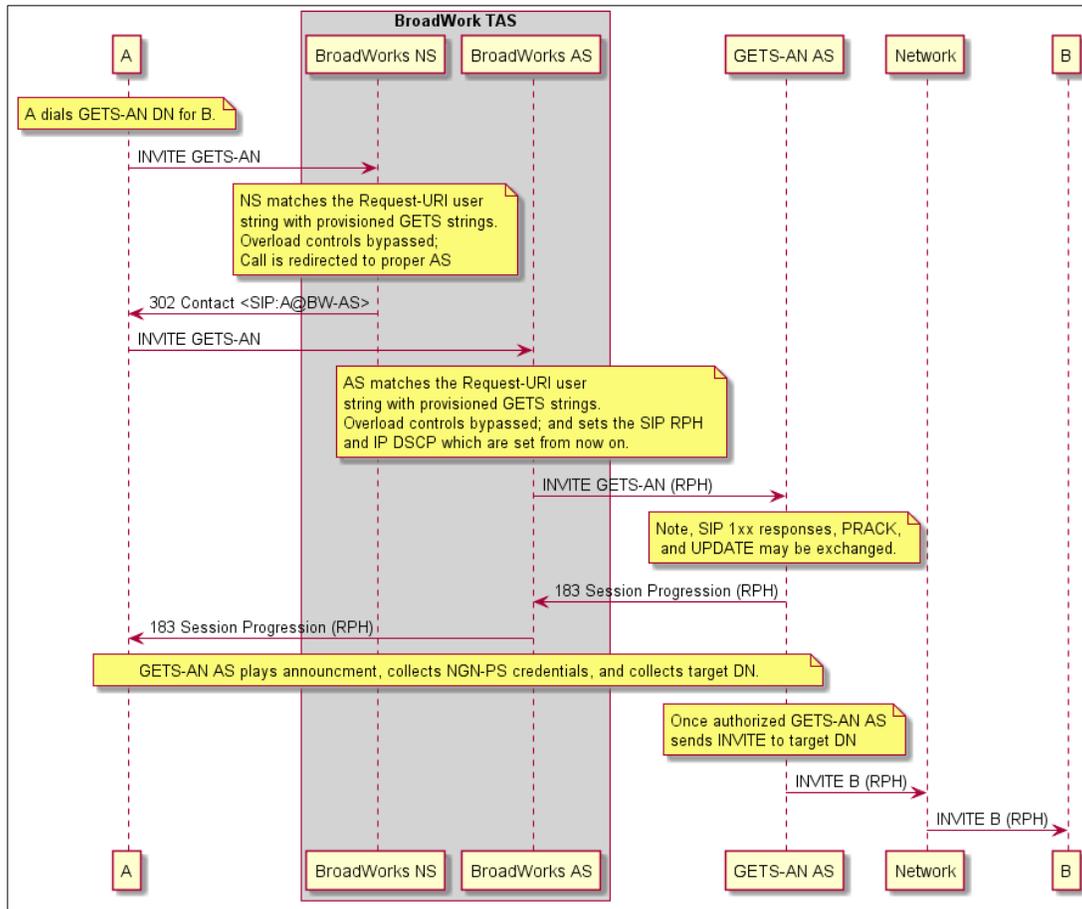


Figure 3 Identifying GETS-AN Call

5.2.1 Standalone Mode

Complete call flows for standalone are described in section 5.4 *GETS Origination Call Flows* and 5.5 *NS/EP Termination Call Flows*.

5.2.1.1 NS/EP Calls

Terminating calls are identified as a GETS call by the presence of a valid *Resource-Priority* header, in its initial SIP INVITE message. Similarly, the header is proxied for future messages and other server/services interactions for the GETS call.

This header is added in SIP messages and responses related to the GETS call. If the call is forwarded or forked to multiple destinations before or after that the communication has been established (such as BroadWorks Anywhere, Simultaneous Ringing), it is included in each additional call leg. Also, the header is sent to other servers that are associated with the GETS call.

5.2.1.2 Originating Calls

The Cisco BroadWorks AS supports different modes of identifying GETS originating calls:

- *Request-URI Mode* – Based only on the Request-URI, the Cisco BroadWorks AS is the functional element that recognizes an originating SIP INVITE as a GETS call and adds the RPH for the rest of the call session.

- *RPH Mode* – In this mode, it is assumed that call was identified as a GETS call upstream by another functional element. Only with the presence of an RPH in the originating SIP INVITE is the call given GETS priority.
- *RPH-Request-URI Mode* – This mode combines the other two modes with RPH mode having precedence over the Request-URI mode. This is the default mode at server installation.

Since the Cisco BroadWorks NS is usually accessed prior to the Cisco BroadWorks AS (as a proxy, or to perform a AS lookup), it only supports the *RPH-Request-URI* mode.

5.2.1.2.1 Request-URI Mode

In this mode, GETS number strings are provisioned for GETS call identification during call processing. Both the Cisco BroadWorks NS and Cisco BroadWorks AS must be provisioned with the same list of numbers for a call to have priority across Cisco BroadWorks.

Originating calls are only identified as GETS calls when the received user string from the *Request-URI* is set to a GETS provisioned string in Cisco BroadWorks. 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).

When matched, a Resource-Priority header with provisioned value defined in *defaultRValue* parameter (i.e. ets.0) is added to the GETS call and is proxied in all future messages with the network side.

A provisioned GETS string should pursue the following rules:

- The string must start with 710 or 8xx.
- A wildcard character (*) is supported as long as it the last character in the string.
- The string must be 10 digits long when no wildcard character exists (*) and must be 4 to 10 character when a wildcard is present.
- When a Request-URI matches more than one provisioned numbers then the most restrictive one is used.

For example:

Consider the following provisioned numbers.

<i>number</i>	<i>type</i>
7106274387	GETS-AN
710*	GETS-NT
8882884387	GETS-AN
8002578373	GETS-AN
8009004387	GETS-AN
8776464387	GETS-AN
8553334387	GETS-AN
8554004387	GETS-AN
8008184387	GETS-AN
8666272255	GETS-AN

Based on the user strings received (from Request-URI):

User String	Call Identified as
7106275555	GETS-NT
7106274387	GETS-AN
8776464387	GETS-AN
8884564387	Non-GETS
8882884387	GETS-AN
7104563333	GETS-NT

When in this mode and the Cisco BroadWorks TAS receives a SIP INVITE with a *Resource-Priority* header with GETS r-values and no GETS-AN/GETS-NT in the request URI the call is not considered to be GETS and no special priority is given to the call. Furthermore, if only GETS namespaces are in the RPH, a SIP 403 messages is returned to calling UE. If other namespaces are present in the header, the GETS r-values are stripped from the message leaving only the other namespace before the call is allowed to proceed.

Due to the nature of the Request-URI mode, an originating SIP INVITE message with “*Require:resource-priority*” header results in a SIP 417 error response sent to the UE regardless of the contents of the resource priority header.

5.2.1.2.2 RPH Mode

A standalone Cisco BroadWorks TAS configured with “RPH” call identifier mode behaves similar to IMS mode. That is, it is assumed that the GETS call is identified upstream in the call flow and a *Resource-Priority* header is inserted in the SIP interface message before it is sent to Cisco BroadWorks TAS. Only with this *Resource-Priority* header in its initial SIP INVITE, is the Cisco BroadWorks TAS able to detect that a call is a GETS call.

This header is proxied and added in SIP messages and responses related to the GETS call. If the call is forwarded or forked to multiple destinations (such as, BroadWorks Anywhere, Simultaneous Ringing), it is included in each additional call leg. Also, the header is also sent to other server interactions that are associated with the GETS call.

5.2.1.2.3 RPH-Request-URI Mode

A standalone Cisco BroadWorks TAS configured in this mode combines the other two modes with the RPH identifier having precedence. That is, if there is an RPH with valid GETS values in the initial originating SIP INVITE, then these values are proxied and used for the rest of the call. If no RPH GETS values exist, the Request-URI mode call identifier processing is applied.

5.2.2 IMS Mode

In an IMS network topology, a GETS call is identified upstream in the call flow and inserts a *Resource-Priority* header in the SIP interface message. Only with this *Resource-Priority* header in their initial SIP INVITE are the Cisco BroadWorks TAS servers able to detect that a call is a GETS call (both for originating and terminating calls). See the Cisco BroadWorks AS Mode ISC documentation for the detailed description of how originating and terminating calls are determined for IMS mode [10].

See Appendix A - Originating vs Terminating Calls in IMS Mode for a summary description of how originating and terminating calls are determined for IMS mode

This header is proxied and added in SIP messages and responses related to the GETS call.

Complete call flows for IMS mode are described in section 5.4 *GETS Origination Call Flows* and 5.5 *NS/EP Termination Call Flows*.

5.2.3 Cisco BroadWorks Networks Server

Since the Cisco BroadWorks Network Server is usually accessed prior to the Cisco BroadWorks AS (as a proxy server or to perform an AS lookup), it also has a mechanism to identify GETS calls in order to bypass overload controls. To support the new "Request-URI" and "RPH-Request-URI" call identification modes of the Cisco BroadWorks AS, the existing GETS validation of the Cisco BroadWorks NS is slightly modified to allow SIP INVITE requests having a GETS number in their Request-URI to bypass overload controls as illustrated in this figure:

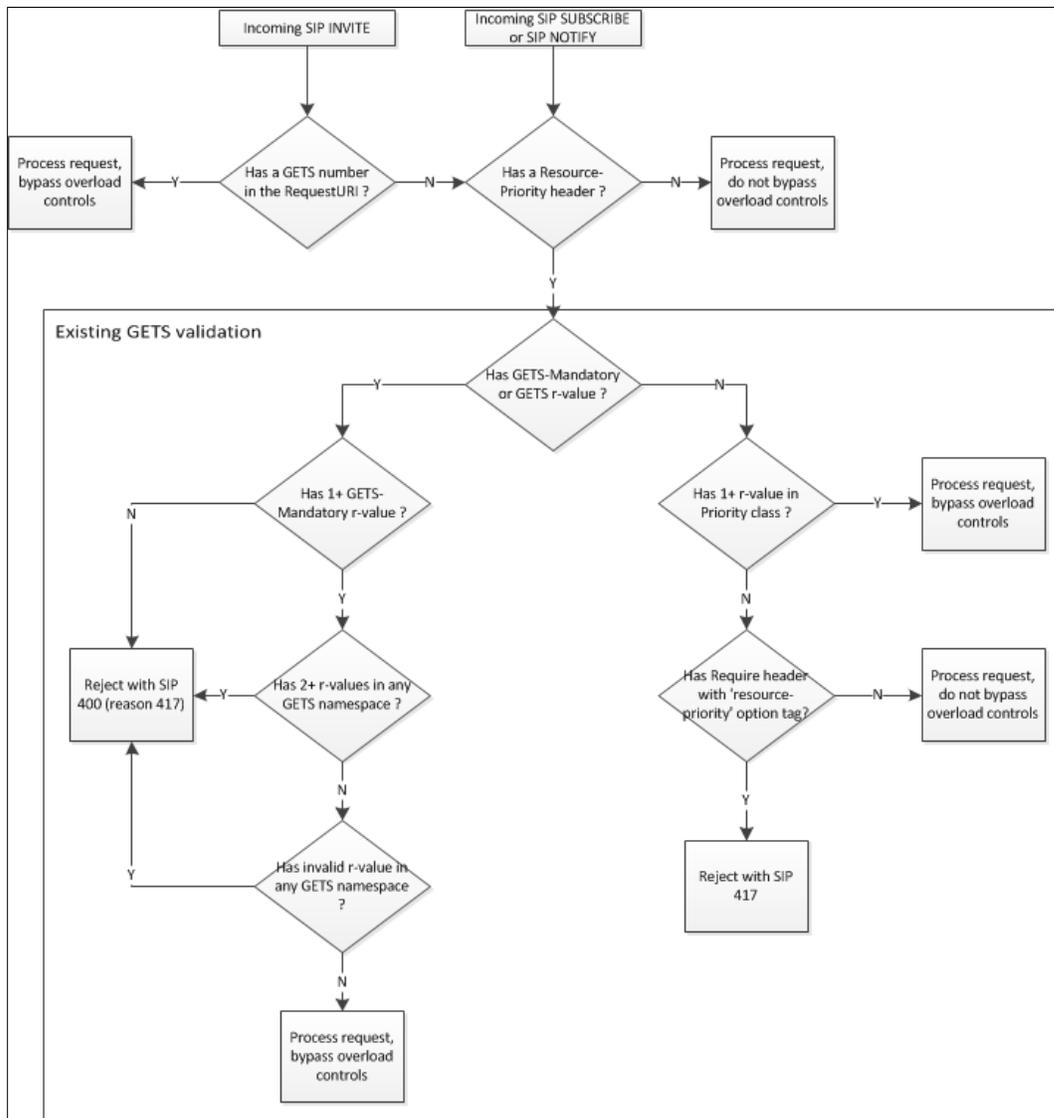


Figure 4 Cisco BroadWorks Network Server GETS validation

Note that the Priority class is used by other Cisco products that are out of the scope of this document and that it should not be used in AS deployments.

5.3 Overload Controls

5.3.1 Processor Overload Control

When the Cisco BroadWorks TAS is in overload condition (yellow or red), GETS calls are still accepted when a normal call might be denied. Note that overload controls only apply to an initial SIP request. Subsequent SIP requests and responses are not subject to overload controls and are always accepted, whether or not the call is a GETS call.

An incoming GETS SIP INVITE is put at the end of the message-processing queue, that is, the queuing order is not affected by the fact that a call is a GETS call. Since the amount of time messages spend in the message-processing queue is precisely what overload controls monitor, this still ensures that GETS messages have a very high probability of being processed (and without undue delay).

However, if the system reaches an extreme overload condition (which is usually prevented by conventional overload controls), even GETS calls are denied. This occurs for messages that have been in the queue for longer than a configured maximum packet age.

Note: GETS and emergency calls are treated equally under processor overload conditions.

5.3.2 Blocking Services

GETS calls bypass blocking and capacity services that would otherwise prevent normal calls to be completed.

Examples of blocking and capacity services are Call Capacity Management, Call Processing Policies, Concurrent Call Licensing and Trunk Capacity.

For the complete list of blocking services that are bypassed by GETS calls, refer to section 6 Service Interactions.

5.3.3 Emergency Call DDoS Protection

Under exceptionally intense emergency calling, it is possible that Cisco BroadWorks AS and/or NS servers are overloaded with emergency calls which are not rejected by the overload controls in the yellow or the red overload state. Under this intense calling, the servers may enter severe overload condition where emergency or GETS calls cannot be processed by the servers.

To avoid reaching this severe overload condition, the Emergency Call DDoS Protection mechanism can be enabled and configured to allow the servers to drop emergency calls prior to servers entering this condition. This extra protection keeps resources available for processing GETS calls. The Emergency Call DDoS Protection mechanism can be enabled independent of GETS.

Once enabled, a threshold for the number of emergency calls per second is required to be configured along with a sampling period (default value is 5 seconds). For each incoming emergency call, the current average number of emergency calls per seconds is compared with the configured threshold. When the current average calls per second rate exceeds the configured threshold, the configured protection action is executed and the emergency call is dropped.

Because the *bwCallpEmergencyCallsPerSecond* gauge uses a different sampling technique and sampling period than the Emergency DDoS protection mechanism, it displays a different value than the configured protection rate during low traffic. However, when the traffic is high, the *bwCallpEmergencyCallsPerSecond* gauge displays a rate approximatively similar to the call rate calculated by the Emergency DDoS protection mechanism.

5.4 GETS Origination Call Flows

Cisco BroadWorks supports the following GETS origination calls:

- GETS-FC (IMS mode only) - The user has a GETS service subscription and activates the GETS functionality by dialing a feature code (FC) prior to dialing the called party number.
- GETS-AN (standalone and IMS mode) - A user dials a GETS Access Number, the user is then prompted for a PIN and destination number in order to activate the GETS call.
- GETS-NT (standalone and IMS mode) - A user dials a GETS Network Translation number. The user is prompted for a PIN. Once the PIN is accepted, the call terminates to a target DN that is mapped to that GETS-NT number. The calling and called parties do not have any information of each other.

5.4.1 Standalone Mode

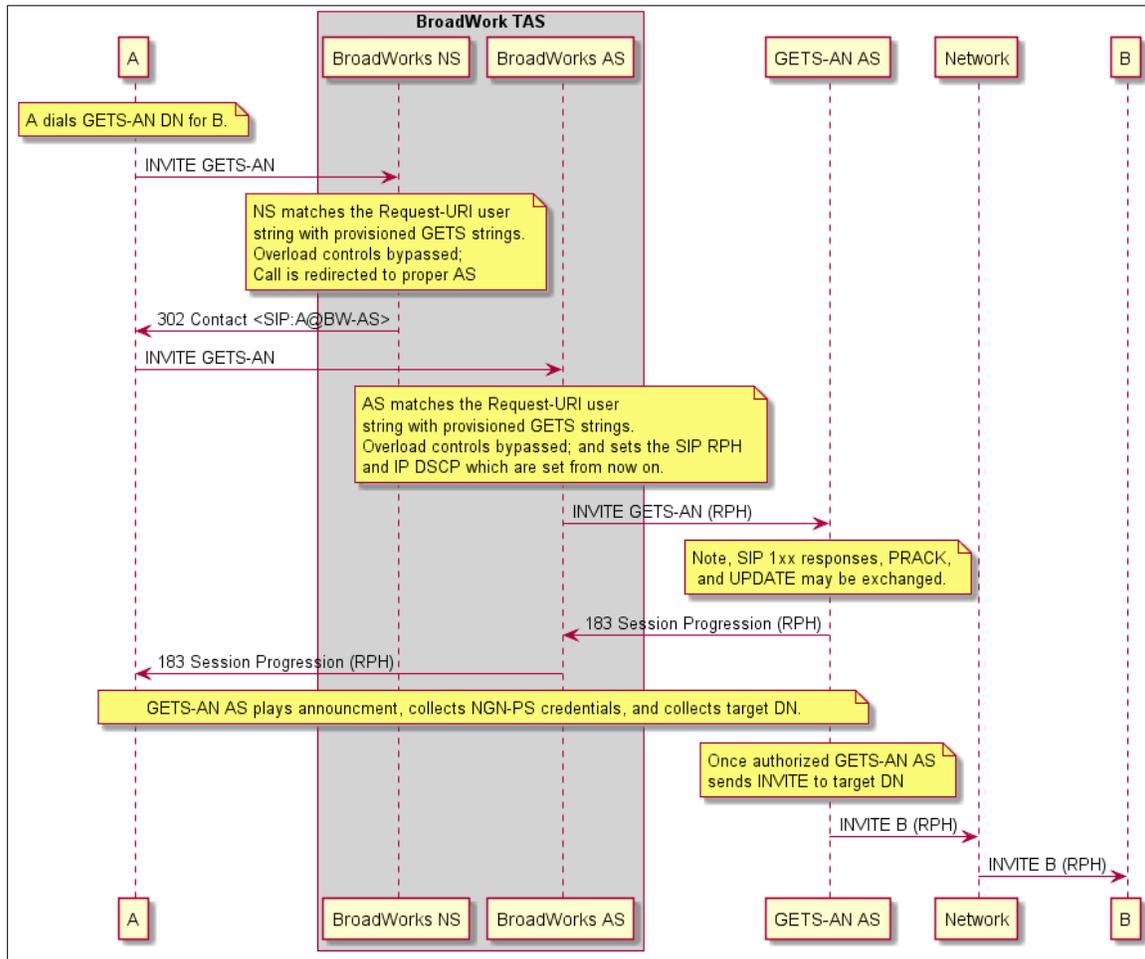
In a Cisco BroadWorks TAS standalone mode, GETS-AN and GETS-NT originations are supported. GETS-AN and GETS-NT are identified as specified in *5.2.1 Standalone Mode*. *GETS-FC* is not supported for standalone Cisco BroadWorks TAS.

This section specifies Cisco BroadWorks TAS behavior when it is configured to identify GETS calls with the *Request-URI*. When RPH is used to identify the GETS call, the behavior is the same as IMS Mode behavior (see 5.4.2 IMS Mode).

5.4.1.1 GETS-FC Origination

Not supported in standalone mode.

5.4.1.2 GETS-AN Origination



5 Standalone GETS-AN Origination Call

Key components of call flow:

- Cisco BroadWorks NS receives a GETS-AN in the SIP INVITE request URI for the origination call.
- Cisco BroadWorks NS matches the Request-URI user string against provisioned GETS strings and allows the call to bypass overload controls.
- The call is redirected to the Cisco BroadWorks AS without an RPH in origination calls.
- The Cisco BroadWorks AS considers the call a GETS-AN call when the Request-URI user string is successfully matched against provisioned GETS strings.
- Once matched, the Cisco BroadWorks AS sets the RPH and IP DSCP in SIP INVITE and in all future session messages. The Cisco BroadWorks TAS bypasses overload controls and originating services are executed.
- After originating services are applied the call continues to the GETS-AN for PIN collection and authentication.

5.4.1.3 GETS-NT Origination

For a GETS-NT call, the call flow is similar to GETS-AN with the following main differences:

- The GETS-AN AS is replaced with a GETS-NT AS (these are, however, typically collocated).
- After PIN collection, GETS-NT AS also performs a translation of the GETS-NT DN to a destination UE.

5.4.1.4 Sending GETS Resource Priority to User Equipment

For the standalone mode GETS calls, there exists the option of sending the *Resource-Priority* GETS namespaces to the user equipment (on the access side only). This is set via a system wide configuration as specified in 4.1.1 *GETS*. With *sendAccessResourcePriority* enabled, *Resource-Priority* headers with GETS values are sent to the access side user equipment.

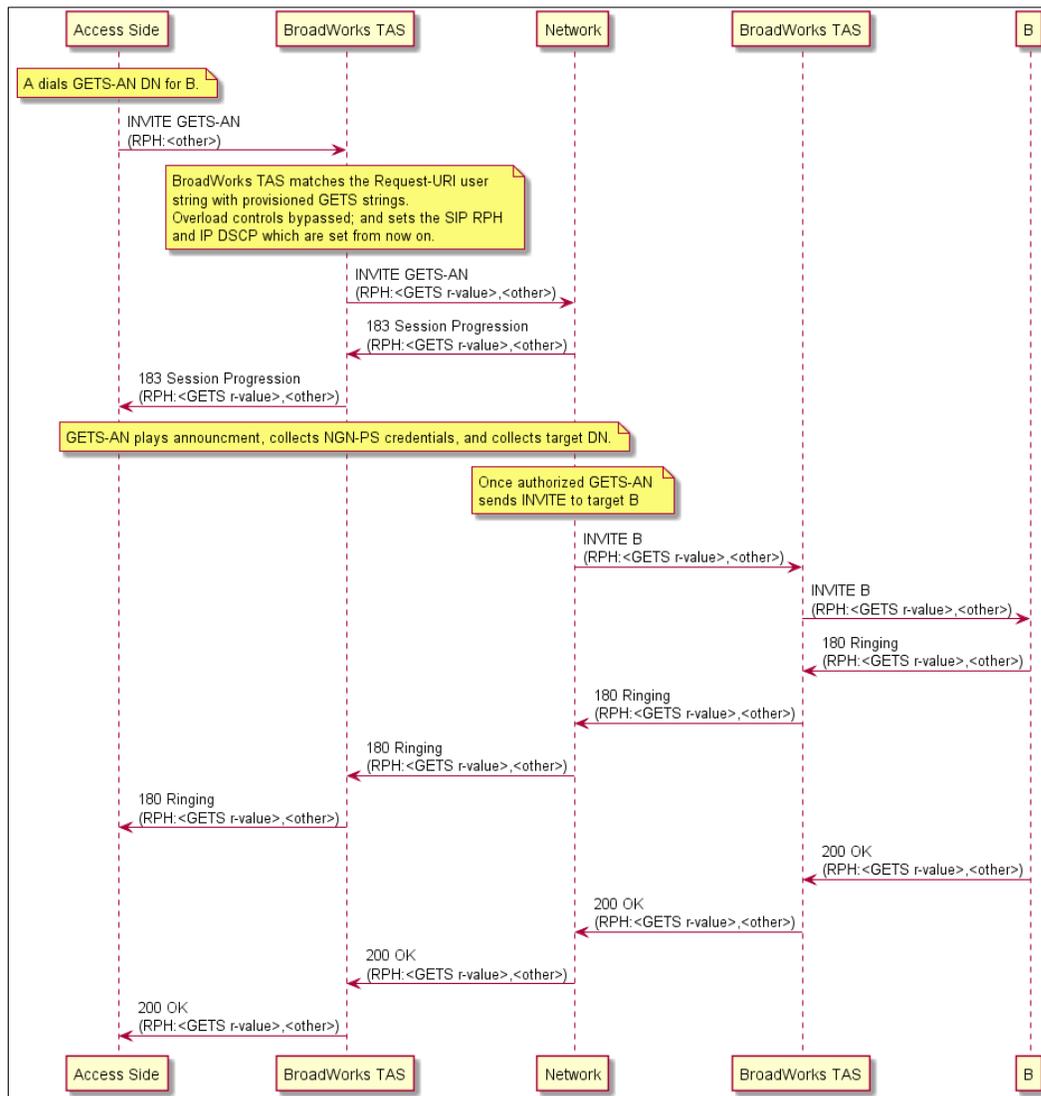


Figure 6 Standalone Sending RPH to UE

When *sendAccessResourcePriority* is disabled, GETS values are stripped from *Resource-Priority* sent to the access side user equipment. Only GETS values are stripped any other *Resource-Priority* value is left untouched.

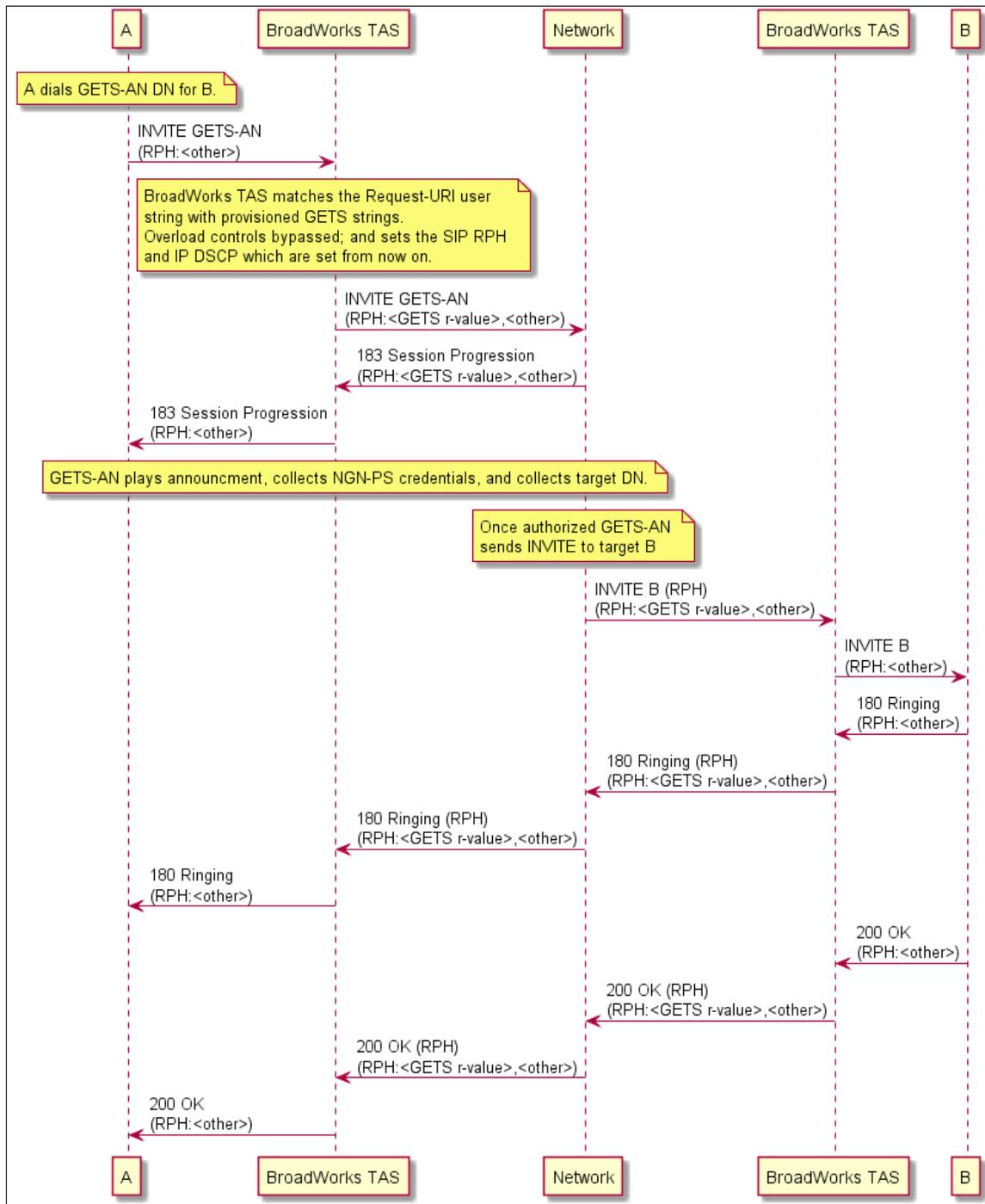


Figure 7 Standalone No RPH sent to UE

5.4.2 IMS Mode

In IMS Mode, an external functional element identifies the call as a GETS call and inserts a RPH in the SIP message. This is usually performed by the proxy call session control function (P-CSCF). Once the SIP message reaches any of the Cisco BroadWorks TAS functional elements (AS and/or NS), they validate the RPH and going forward the call is handled with GETS priority.

5.4.2.1 GETS-FC Origination

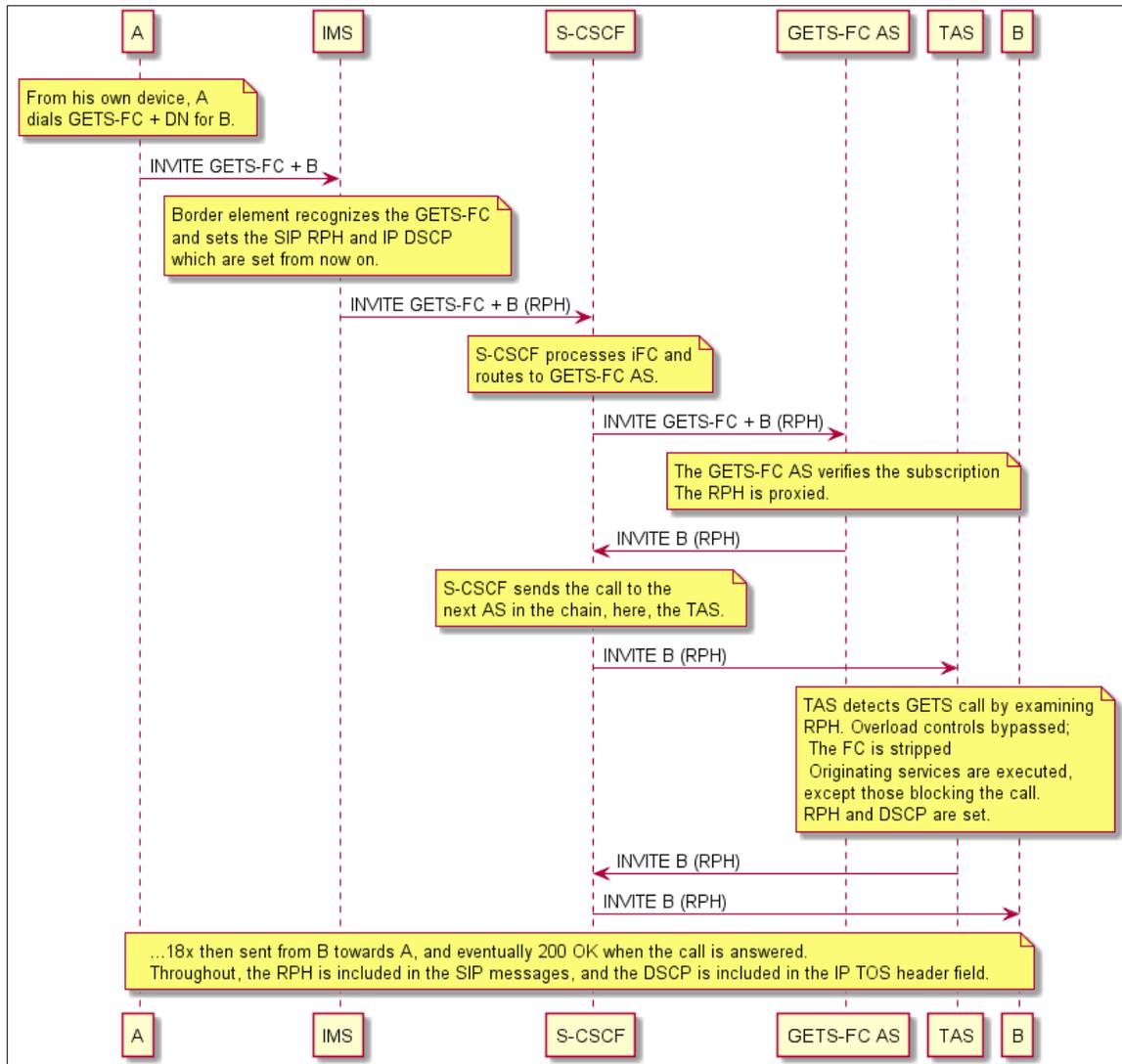


Figure 8 IMS Mode GETS-FC Origination Call

Key components of call flow:

- IMS Border elements (P-CSCF) recognize the GETS-FC feature code and add the *Resource-Priority* header (RPH) to the SIP message. Furthermore, all subsequent messaging still has the *Resource-Priority* SIP header (RPH), and both SIP signaling and Real-Time Transport Protocol (RTP) media have the Differentiated Services

Code Point (DSCP) set in the *IP Type of Service (TOS)* header so that packets can be routed with higher priority.

- Prior to Cisco BroadWorks TAS, the GETS-FC AS is invoked by the S-CSCF. The GETS-FC AS validates the subscription and strips the feature code from the request URI before proceeding.
- The TAS servers detect the GETS call by the appearance of the RPH. The TAS bypasses overload controls and originating services are executed.

5.4.2.2 GETS-FC Origination with FC Not Stripped

To allow the TAS's originating call session to properly mark the call as GETS-FC, Cisco BroadWorks also supports call flows where the GETS-FC feature access code is not stripped by the IMS core, but instead is forwarded to the TAS as is, as shown in the following figure.

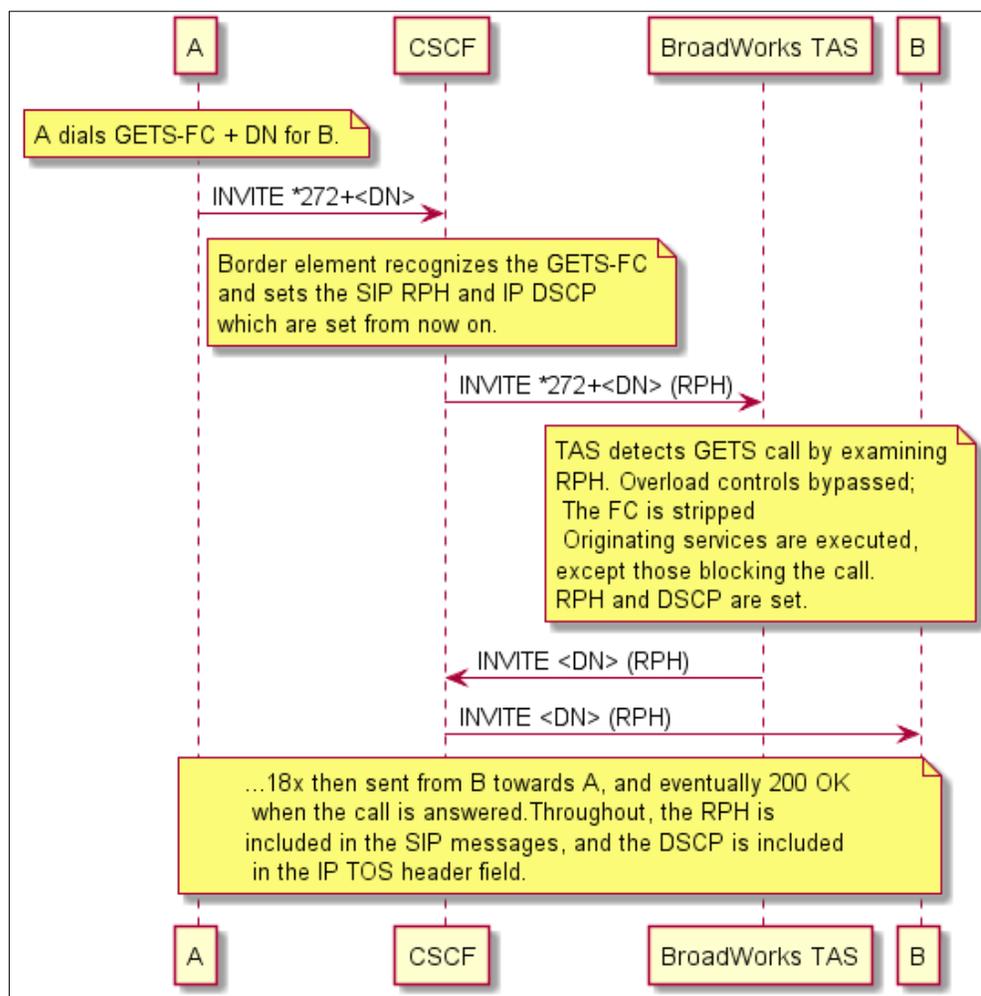


Figure 9 IMS Mode GETS-FC Not Stripped Origination Call

Key components of call flow:

- IMS (CSCF) core does not strip the FC from the request URI.

- Cisco BroadWorks TAS is provisioned with FC and is able to match/detect the GETS-FC call. The Cisco BroadWorks TAS bypasses overload controls and originating services are executed.

5.4.2.3 GETS-AN and GETS-NT Origination

For a GETS-AN call and a GETS-NT call, the call flow is similar to GETS-FC with the following main differences:

- The GETS-FC AS is replaced with a GETS-AN AS or a GETS-NT AS (these are, however, typically collocated).
- User A is prompted for a PIN.
- Following a GETS-AN, after PIN collection, user A is prompted for a DN.
- Following a GETS-NT, after PIN collection, GETS-NT AS performs a translation of the GETS-NT DN to a destination UE.
- Cisco BroadWorks TAS receives the INVITE with proper destination and RPH set.

5.4.3 GETS Call Processing for SIP 417 and 420 Error

5.4.3.1 Route Advance

When an originating GETS SIP INVITE network translation results in multiple contacts for destination functional element, Cisco BroadWorks TAS supports re-routing a GETS SIP INVITE to another functional element when a SIP 417 or 420 is received for an attempt. See Section 5.3 in the *Cisco BroadWorks Treatment Guide* for general route advancing details [11].

Cisco BroadWorks sends another SIP INVITE with the same header (including RPH and Require header) to the next destination. If all destinations return a SIP 417/420, then the Cisco BroadWorks TAS sets the final response to SIP 417 or 420 depending on the last message received.

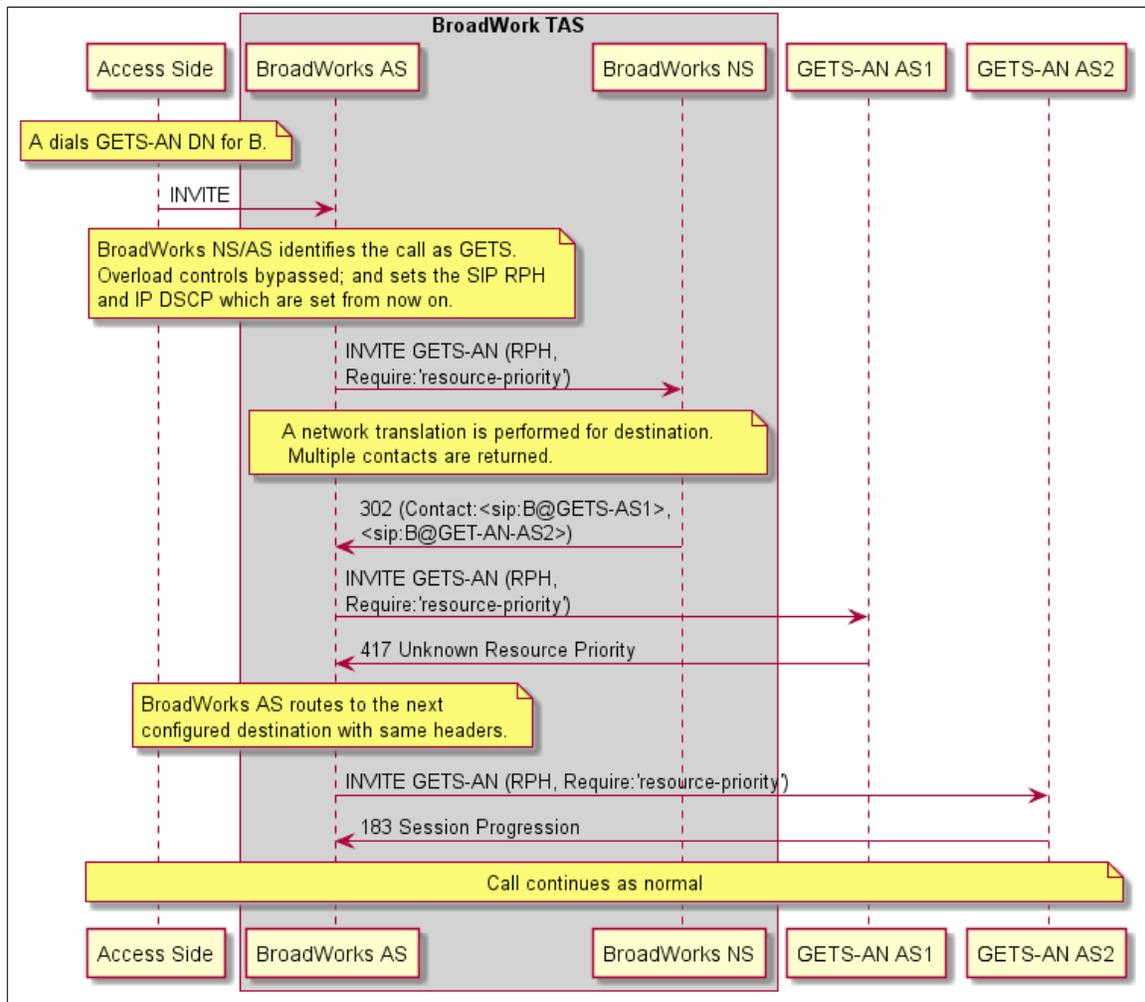


Figure 10 GETS Call Route Advance for SIP 417

5.4.3.2 Resending SIP INVITE

The Cisco BroadWorks TAS resends a GETS SIP INVITE when all the Network Server returned contacts respond with a SIP 417 or 420 with an Unsupported:'resource-priority' to each SIP INVITE contact attempt.

In this case, the Cisco BroadWorks TAS resends the SIP INVITE to the last destination attempted. The Require Header is removed from the SIP INVITE, and it is sent with the same RPH and with a Supported header field with tag 'resource-priority' as described in RFC-3261 (See [4])

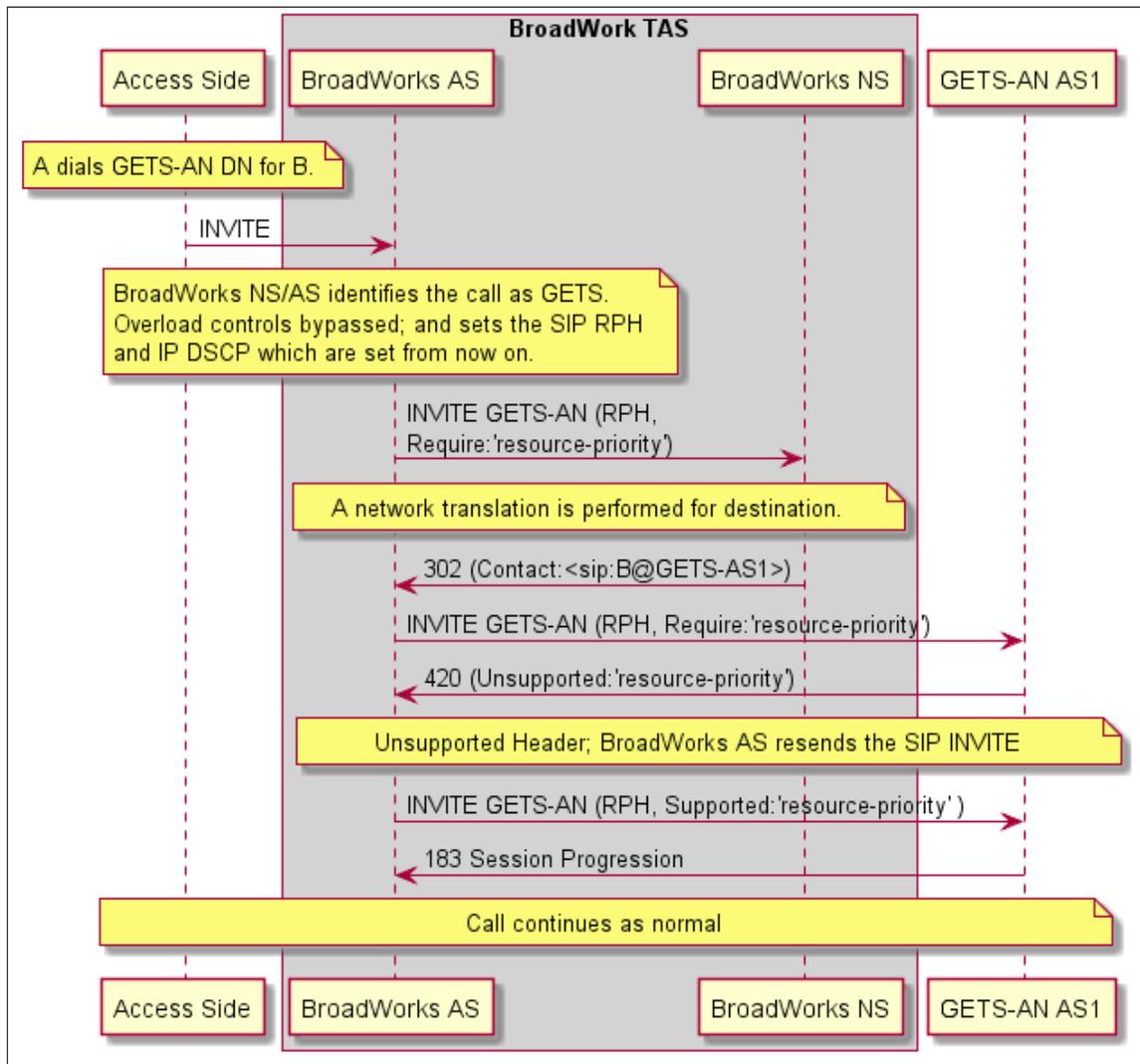


Figure 11 GETS Call Resending SIP INVITE

5.5 NS/EP Termination Call Flows

Terminations are more straightforward in that a GETS AS is not involved, since GETS processing (processing the feature code, collecting the GETS PIN and destination number for GETS-AN, and so on) is done on the originating side.

5.5.1 Standalone Mode

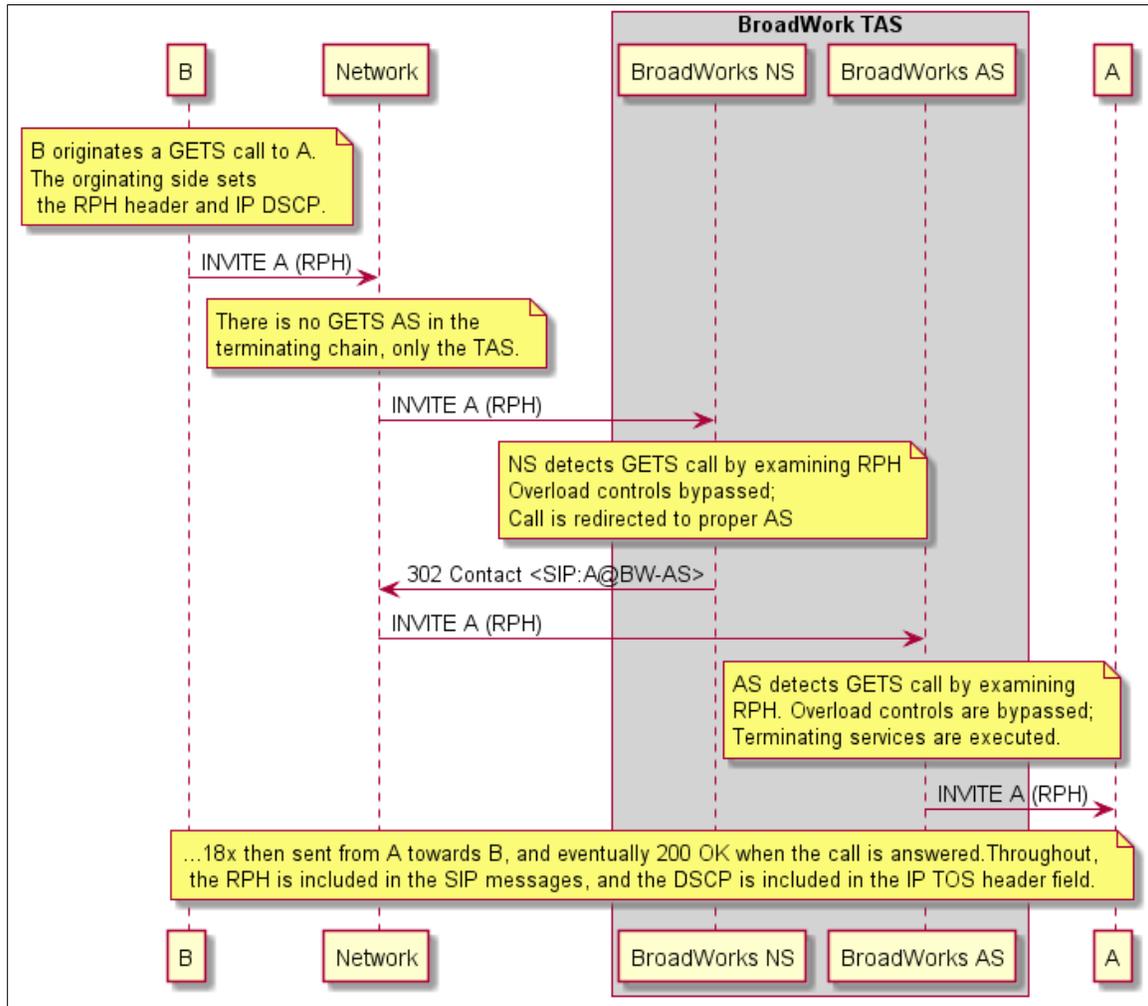


Figure 12 Standalone NS/EP Termination Call

Key components of call flow:

- The call is tagged as GETS on the origination side. The termination side only bypasses overload controls and bypasses some blocking services for a GETS call (RPH header).
- For the standalone mode GETS calls, based on a configurable parameter the *Resource-Priority* GETS values are sent to the user equipment (access side) or are removed before sending to user equipment. This is set via configuration as specified in 4.1.1 GETS. See 5.4.1.4 Sending GETS Resource Priority to User Equipment for a detailed call flow.

5.5.2 IMS Mode

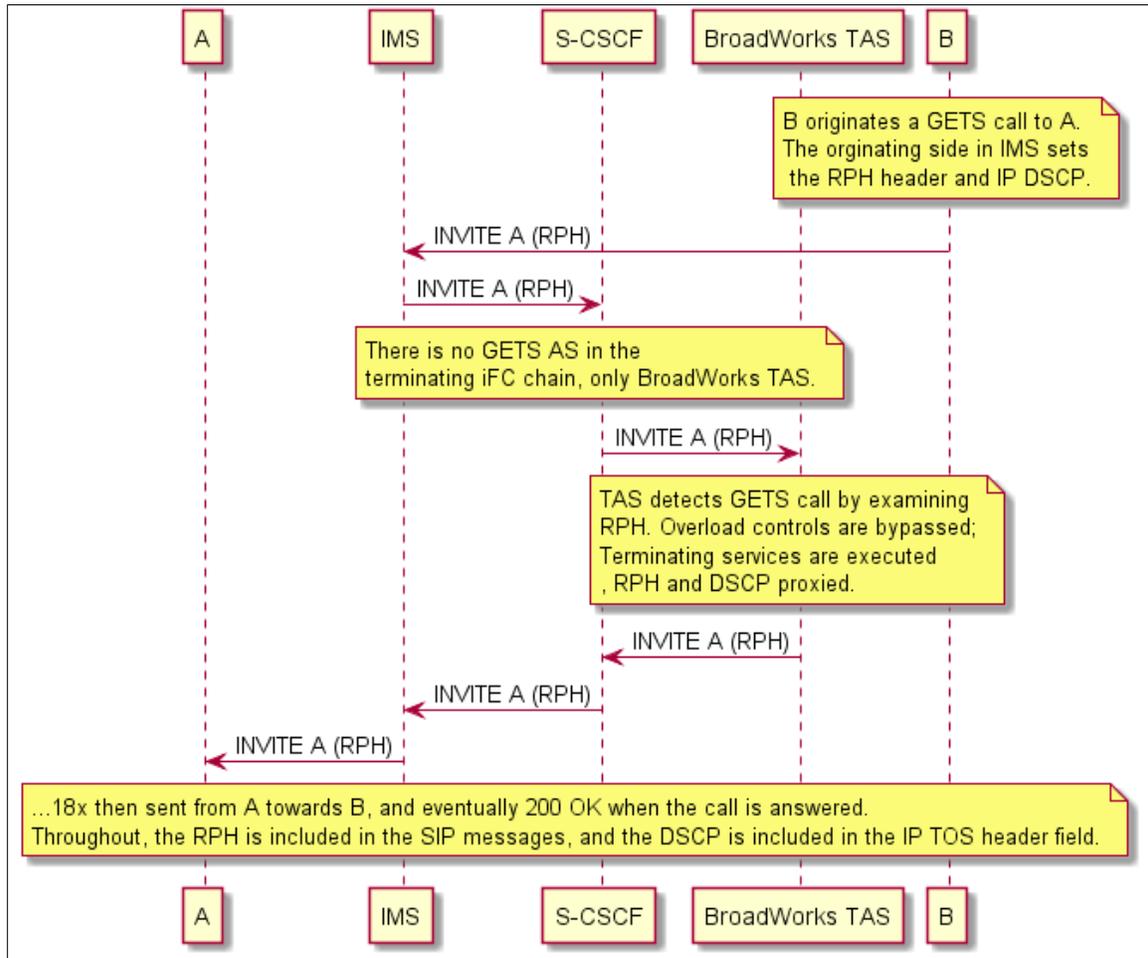


Figure 13 IMS Mode NS/EP Termination Call

Key components of call flow:

- The call is only tagged as GETS on the origination side. The termination side only bypasses overload controls and bypasses some blocking services for a GETS call (RPH header).

5.6 Downstream GETS-AS Server Support

5.6.1 Resource-Priority Changes

In some call flows, a third-party GETS Application Server (GETS-AS) is encountered between the Cisco BroadWorks TAS origination server and the termination server. This is the case for standalone mode and can also be configured as such in IMS networks. In these network configurations, the original call session does not receive the final r-values for the GETS call in the initial origination INVITE. Since the Cisco BroadWorks TAS is located upstream from the GETS-AS in the signaling flow, it needs to import the r-values it receives in 1xx and 2xx responses coming from the Network Side. From this point on, outgoing requests and responses use the new r-values. Note that if a 1xx or 2xx response is received without a Resource-Priority Header, the r-values of the ongoing session are not cleared.

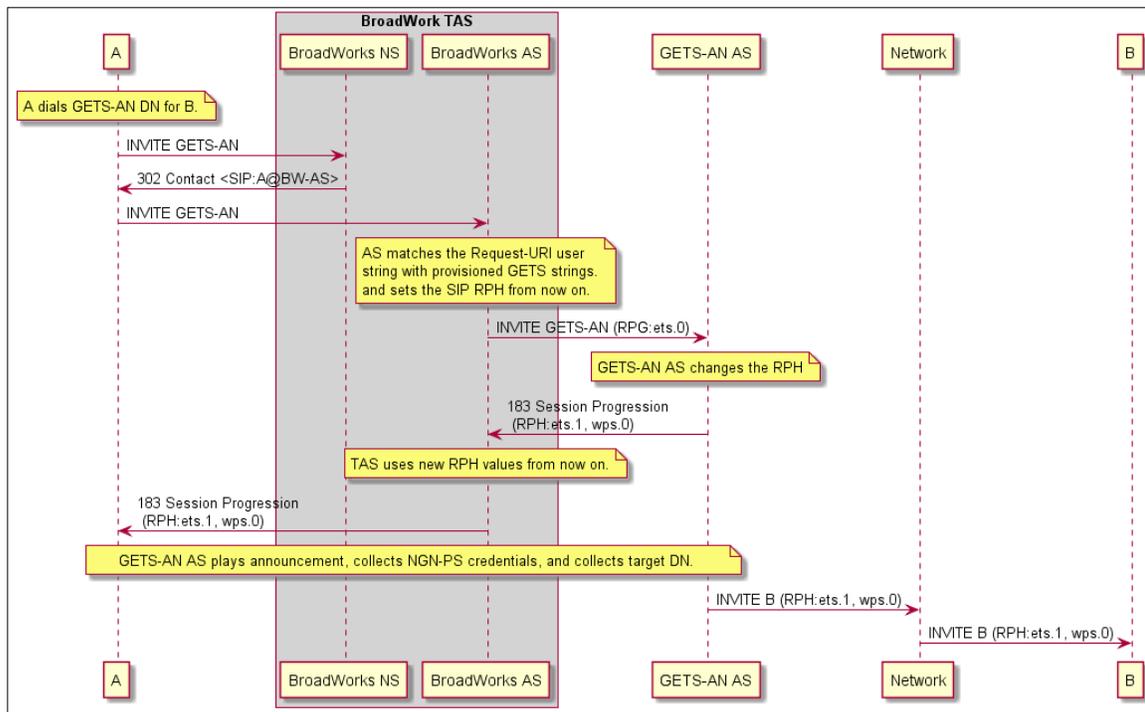


Figure 14 RPH Update on SIP 1xx Message

5.6.2 GETS Call Type Identification

In certain scenarios, with a downstream GETS Application Server, the Cisco BroadWorks TAS is not always able to properly identify the GETS call variant employed for the call. This may be required for billing records and or statistics collecting. The Cisco BroadWorks TAS can be provisioned with GETS-AN and/or GETS-NT numbers to determine a more granular GETS call type.

5.6.2.1 Request-URI mode Call Type identification

If the *callIdentifierMode* is set to “Request-URI”, an originating call is only considered a GETS call when a GETS-AN/NT provisioned string is identified in the *Request-URI* (see 5.2 *Identifying GETS Calls*). Therefore based on the match, GETS calls are identified as call type “GETS-AN” or “GETS-NT”.

For terminating sessions, the only indication that a SIP request is a GETS request is taken from the *Resource-Priority* header r-values received. Terminating session call types are set to “NS/EP”.

5.6.2.2 RPH mode Call Type Identification

If the *callIdentifierMode* is set to “RPH”, Cisco BroadWorks TAS uses enhanced network translation to identify GETS call types. By default a RPH with valid GETS values results in the call type to be identified as “GETS”. This applies to both originating and terminating sessions.

Furthermore for originating sessions, a Cisco BroadWorks TAS can be configured to perform network translations for DNs. The TAS can be configured to use enhanced network translation to perform a lookup which allows the Cisco BroadWorks TAS to determine whether the dialed number is a GETS-AN or GETS-NT number. GETS calls have no impact on translation results, that is, policies impacting call translations process GETS calls similar to normal calls.

The call types returned by network translation results (the *ct* parameter of the contact header in a 302 response from the Network Server) are used to determine the GETS call type as described here:

The GETS-FC, GETS-AN, and GETS-NT flags are used to determine the GETS call type based on the information in the following table.

GETS-FC	GETS-AN	GETS-NT	GETS Call Type
0	0	0	GETS
0	0	1	GETS-NT
0	1	0	GETS-AN
1	0	0	GETS-FC
1	0	1	GETS-FC + GETS-NT
1	1	0	GETS-FC + GETS-AN

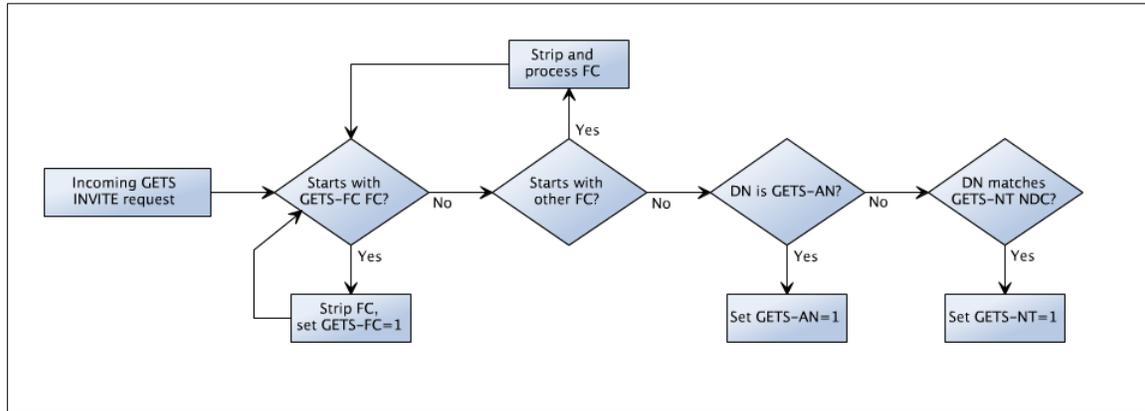


Figure 15 GETS Call Type Identification Processing

Individual GETS-AN numbers have precedence over GETS-NT national destination code (NDC) matches. For instance, a system may have provisioned “710-NCS-GETS” (“710-627-4387”) as a GETS-AN number and 710 as a GETS-NT NDC. In this case, the destination number “710-627-4387” would result in GETS-AN=1, GETS-NT=0, and the number 710-123-4567 would result in GETS-AN=0, GETS-NT=1.

As the table suggests, the GETS origination type is not known to the terminating session and the only indication that a SIP request is a GETS request is taken from the *Resource-Priority* header r-values received. Also note that GETS call type identification is only possible with a GETS-AN/NT AS located midway through the signaling path and an initial GETS-FC INVITE that does not have the GETS-FC prefix stripped. If this is not the case, the call is detected as a plain GETS call in the originating session.

The GETS-FC flag defaults to “0” and is set when a GETS prefix is detected and stripped. The GETS-AN and GETS-NT flags default to “0” and are calculated only when the original destination corresponds to a network destination. An enhanced network translation, which must be enabled to provide GETS call typing, is then invoked and its response is received by the TAS with a GETS AN (GAN) call type set for GETS-AN numbers and a GETS NT (GNT) call type set for GETS-NT numbers.

To accomplish this, *GAN* and *GNT* need to be defined as new call types on the Network Server and the dial plans need to be modified to set the appropriate call types when a destination DN matches a GETS-AS/NT number. Typically, GETS-AN entries are matching exact DNs and GETS-NT entries match the NDCs (710 for NGN GETS).

5.7 SIP Interface

5.7.1 Resource-Priority Header (RPH)

The main interface impacted by GETS is the SIP interface used for call processing signaling. In particular, the *Resource-Priority* header is used by the Cisco BroadWorks TAS to detect that a call is a GETS call and should be handled with priority when the header is present in an initial SIP INVITE request. Also, when a GETS call is detected through a *Request-URI* match with a provisioned value, a *Resource-Priority* header is added by the Cisco BroadWorks TAS for the rest of the call. The *Resource-Priority* SIP header can be present in any SIP request or response, except for 100 Trying and 403 Forbidden. Cisco BroadWorks inserts the header in most messages with the exceptions being 100 Trying and 403 Forbidden response for invalid GETS r-values.

This header is proxied and added in SIP messages and responses related to the GETS call. If the call is forwarded or forked to multiple destinations (such as, BroadWorks Anywhere, Simultaneous Ringing), it is included in each additional call leg.

This also includes messages and responses sent to other servers when these are associated with the GETS call.

The following shows how the *Resource-Priority* header is present in all these SIP messages and responses. For example:

```
Resource-Priority: ets.0
```

Note that it is also possible to receive several *Resource-Priority* headers in the same SIP message or response. The received priorities are proxied and included in subsequent requests and responses for the duration of the session.

It is important to note that the Cisco BroadWorks TAS does not actually use the specific priority values for any other purpose than identifying GETS calls. GETS calls are handled the same (for example, with overload controls bypassed) regardless of their actual priority r-values (namespace or priority value).

If a SIP request or response without a *Resource-Priority* Header is received in an already established GETS dialog, the message is still handled with priority since overload controls only apply to initial session-creating SIP requests. In this situation, initial priorities continue to be included in subsequent requests and responses.

5.7.1.1 Resource Priority Header Handling

The Cisco BroadWorks TAS handling and validation of *Resource-Priority* headers closely adheres to the NGN GETS standard. The Cisco BroadWorks TAS is provisioned with a list of resource priority values that are to be used to validate GETS calls. There are two classes of priority values: *GETS (wps)* or *GETS-Mandatory (ets)*. When provisioned with *GETS-Mandatory (ets)* class resource priorities, the GETS call RPH must contain one and only one of the *GETS-Mandatory (ets)* resource priorities. The provisioned *GETS* class resource priorities (*wps*) are supported by Cisco BroadWorks TAS but are not required in every GETS call RPH.

First, the handling of the *Resource-Priority* header respects *RFC 4412* and NGN GETS related to error handling. Any validation error that is GETS-related, that is, an invalid set of r-values from the *GETS-Mandatory(ets)* and *GETS (wps)* r-value priority classes, results in a SIP 400 (*Bad Request*) response with a 417 code in the *Reason* header, regardless of the presence of the *resource-priority* option in a *Require* header, in the request. The *Resource-Priority* header of this response does not contain the “wps.y” r-value received, and in the case where “GETS” (*wps*) class r-value(s) have been received without a “GETS-Mandatory” value (*ets*) or if multiple “GETS-Mandatory” values (e.g. *ets.0*, *ets.1*) have been received, the response contains a default system-configurable *GETS-Mandatory* r-value (*ets*). The error, along with the SIP request, is logged at the *Notice* level in the execution log.

The handling of requests with *Resource-Priority* header(s) is summarized in the following figure.

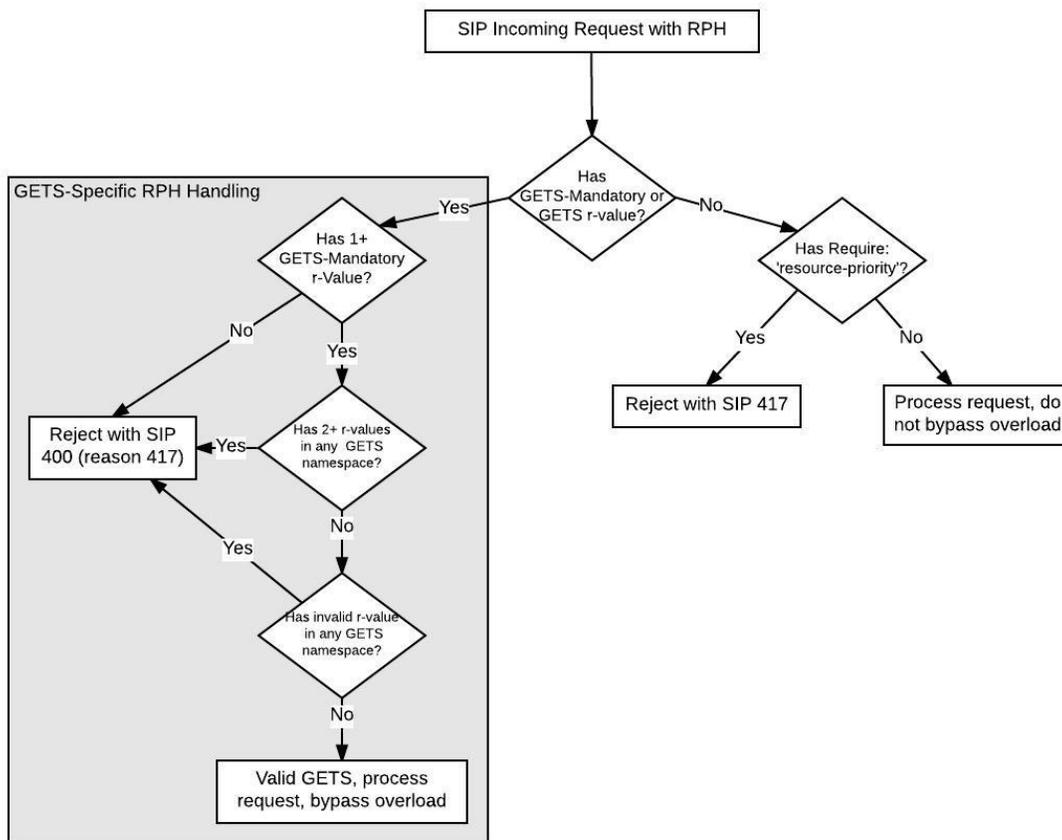


Figure 16 SIP Resource-Priority Processing

Valid GETS SIP requests that target existing dialogs incur additional validation. If the target dialog is not a GETS dialog, the Cisco BroadWorks TAS does not use or forward the request's r-values. The request does not bypass overload controls and is output with an error message in the logs, at the *Notice* level.

For existing GETS dialogs, Cisco BroadWorks TAS does not use or forward r-values from requests other than the initial session creating request. If a re-INVITE without a resource-priority header targeting an existing GETS dialog is received, the message is handled with priority and the session's r-values remain the same. If the re-INVITE has different r-values then the session that it targets, the resource-priority header is ignored and the message is also handled with priority.

If an incoming initial SIP INVITE contains *Resource-Priority* header(s) that contain only unknown namespaces (that is, which are not configured on the server) and the *Require* header contains the *resource-priority* option tag, then the Cisco BroadWorks TAS rejects the request with a SIP 417 (*Unknown Resource-Priority*) response. This response contains an *Accept-Resource-Priority* header with the configured resource priorities.

Note that the aforementioned error codes may not be returned if the system is in overload condition and overload controls returns its own error code, since this error code has priority. For example, when in overload conditions, a call that is normally evaluated (as seen in diagram) to return a SIP 400 or SIP 417 error will be blocked by overload controls and will return a SIP 503 error to the UE instead of a SIP 400 or SIP 417 error.

5.7.1.2 Resource Priority Examples

Consider the example:

For NGN GETS compatibility, the Cisco BroadWorks TAS has been configured with the following Resource Priorities.

<i>priorityValue</i>	<i>priorityLevel</i>	<i>priorityClass</i>
wps.0	1	GETS
wps.1	2	GETS
wps.2	3	GETS
wps.3	4	GETS
wps.4	5	GETS
ets.0	1	GETS-Mandatory
ets.1	1	GETS-Mandatory
ets.2	1	GETS-Mandatory
ets.3	1	GETS-Mandatory
ets.4	1	GETS-Mandatory

Following the SIP Resource-Priority Processing flow chart the following Resource-Priority header examples would result in:

<i>Sample Incoming Resource-Priority Header</i>	<i>Resulting TAS Server Behavior</i>
ets.0	GETS call, bypass overload controls, allowed to proceed.
ets.1	GETS call, bypass overload controls, allowed to proceed.
ets.0, ets.1	Rejected with SIP 400 (code 417 in reason header)
ets.0, wps.1	GETS call, bypass overload controls, allowed to proceed.
wps.1, ets.0	GETS call, bypass overload controls, allowed to proceed.
ets.0, wps.0, wps.1	Rejected with SIP 400 (code 417 in reason header)
ets.5	Rejected with SIP 400 (code 417 in reason header)
ets.0, wps.5	Rejected with SIP 400 (code 417 in reason header)
wps.0	Rejected with SIP 400 (code 417 in reason header)

5.7.2 Require Header

On the Cisco BroadWorks TAS, if so configured (via the *enableRequireResourcePriority* system parameter), the outgoing initial INVITEs of a call identified as a GETS call contains the *Require* header with the *resource-priority* option tag. This tag is added even if the incoming message did not itself contain such a tag.

Following is how the outgoing INVITE appears.

```
INVITE sip:user@host.com SIP/2.0
(...)
Require: resource-priority
Resource-Priority: ets.0, wps.3
(...)
```

If the incoming initial GETS INVITE contained a *Require* header with the *resource-priority* option tag, the TAS does not proxy it to the outgoing INVITE (though it is added, as previously mentioned, if the *enableRequireResourcePriority* system parameter is set).

If a SIP INVITE is resent because every downstream network elements are responding with SIP 417 or 420, the “*resource-priority*” option tag is removed from the *Require* header field (see [5.4.3.2 Resending SIP INVITE](#)).

5.7.3 SUBSCRIBE and NOTIFY Support

In IMS Mode, the GETS feature bypasses overload for SIP SUBSCRIBE and NOTIFY dialog/sessions that have valid GETS *Resource-Priority* header(s).

Incoming and outgoing requests and responses are subject to the same validation and rules as INVITE-created sessions.

In standalone mode, when configured to identify the GETS call with the Resource-Priority header (*callIdentifierMode* set to “*RPH*” or “*RPH-Request-URI*”), the GETS feature bypasses the overload controls similar to IMS mode.

In Standalone mode, with *callIdentifierMode* configured to *Request-URI*, SIP SUBSCRIBE and NOTIFY do not bypass overload controls. Furthermore, in this configuration the Cisco BroadWorks TAS ignores the presence of a Resource-Priority header, a ‘resource-priority’ *Require* option tag or a GETS number in the Request-URI of SIP SUBSCRIBE and SIP NOTIFY messages.

5.7.4 Supported SIP Header Support

Cisco BroadWorks TAS forwards initial SIP INVITEs with the *resource-priority* option in the *Supported* header, for GETS sessions. The *resource-priority* option is also added to the *Supported* header when responding to SIP OPTIONS requests targeting existing GETS sessions.

5.8 Diameter Interface

The Cisco BroadWorks TAS uses the Diameter protocol for the following purposes:

- The Rf reference point for offline billing
- The Ro reference point for online billing

The following new Cisco vendor AVPs are provided in ACR/CCR messages (if configured for Cisco AVPs):

- GETS – Only present when call is a GETS call
- GETS Origination Type – For GETS originating calls, specifies the type of GETS origination call.

5.8.1 Rf Interface

The Rf interface is not impacted by GETS since call setup is not impacted by offline billing.

5.8.2 Ro Interface

The Ro interface for online billing is modified to have the Session-Priority AVP (with the configurable *priorityAVP* system parameter value) in the Diameter Credit Control Request (CCR) asking for credits. This AVP is part of the IMS-Information group AVP in the CCR. GETS users are not expected to subscribe to the Prepaid service and terminations to prepaid users are handled as usual. However, treatment of the requests by the Online Charging System (OCS) can be made with priority, and the OCS has the option to allow the call despite the lack of credits.

5.8.2.1 Session Priority Value

The value of the Session-Priority is different for each session and depends on a system-configurable mapping to the GETS service user priority level. For example, to comply with NGN GETS, the settings in the following table can be used in addition to those in section 5.7.1 *Resource-Priority Header (RPH)*.

<i>priorityLevel</i>	<i>sessionPriorityValue</i>
1	0
2	1
3	2
4	3
5	4

If no mapping is defined for a GETS call's priority level, the default priority AVP value is used. If the call is not flagged as GETS, no Session-Priority AVP is emitted.

5.8.2.2 Ro Interface Bypass

A new Cisco BroadWorks TAS configurable parameter allows bypassing responses and requests that would otherwise trigger the termination of a GETS call session, allowing a non-GETS-aware ECF to interoperate properly with GETS call sessions.

With this setting enabled, incoming CCA messages that have a Final-Unit-Indication AVP and a Final-Unit-Action AVP set to "TERMINATE" or to "REDIRECT" are processed but do not result in the termination or redirection of the call session for GETS sessions. CCA messages for GETS sessions with Result-Code AVP set to 4010 (DIAMETER END USER SERVICE DENIED) or 4012 (DIAMETER_CREDIT_LIMIT_REACHED) also do not result in session termination. ASRs are also ignored for GETS call sessions.

GETS call sessions ignore a received Credit-Control-Failure-Handling AVP and use CONTINUE instead to prevent a charging system malfunction to cause premature termination of a GETS call.

5.8.3 GETS-NT Inhibited Accounting AVPs Support

In GETS-originating call sessions, a configurable list of AVPs to be inhibited from GETS-NT ACRs has been added. When issuing ACRs or CCRs that are associated with an originating GETS-NT call session, any AVP that appears on the list is removed from the outgoing request, allowing the personally identifiable information (PII) to be hidden from the CDRs produced by external billing applications.

All AVPs not defined in that list continue to appear in the Diameter requests for originating GETS-NT or GETS-FC + GETS-NT call sessions.

Here is a non-exhaustive list of AVPs that could be included in the GETS-NT Inhibited AVP Code List:

- BWAS-Called-Number (*avp code 9, vendor ID 6431*)
- BWAS-Dialed-Digits (*avp code 18, vendor ID 6431*)
- BWAS-Original-Called-Number (*avp code 36, vendor ID 6431*)
- BWAS-UserID (*avp code 121, vendor ID 6431*)

Vendor ID is a unique identification number attributed by the Internet Assigned Numbers Authority (IANA). Cisco's Vendor ID is 6431.

Refer to [13] *Cisco BroadWorks Accounting Call Detail Record Interface Specification* to get the list of Cisco BroadWorks-specific attributes used in Diameter requests.

Note that this list of inhibited AVPs is not considered in a GETS-NT terminating session or GETS-AN + GETS-NT and GETS-AN + GETS-PDN calls. The reason for this is that dialed digits are received by the GETS-AN Application Server and they are not seen by the Cisco BroadWorks Telephony Application Server, which is not able to further qualify the GETS call type.

Also note that some AVPs that are used to identify Diameter sessions are mandatory and cannot be inhibited. The complete list of AVPs restricted from being added in the GETS-NT Inhibited AVP Code List is as follows:

- Session ID (AVP=263)
- Destination Realm (AVP=283)
- Origin Host (AVP=264)
- Origin Realm (AVP=296)
- Account Record Type (AVP=480)
- Account Record Number (AVP=485).

5.9 DSCP Field Setting

5.9.1 Internet Protocol

GETS SIP signaling (TAS) is given higher priority at the transport level (which is useful if the network supports it and can reduce delays and packet loss for this traffic). The *Differentiated Services Code Point (DSCP)* field is set to the configured value (the *signalingDSCP* system parameter for SIP) in the *IP* header.

For IPv4, the *DSCP* field is in the six most significant bits of the second byte of the *IPv4* header, with the two remaining bits representing the *Explicit Congestion Notification (ECN)* field. The *DSCP* field was originally defined as the *Type of Service (TOS)* field.

Inside the *IPv6* header, the *DSCP* field is part of the *Traffic Class* field, using its six most significant bits, again with the *ECN* field occupying the two remaining bits. The *Traffic Class* field is split between the first and second bytes of the header.

5.9.2 SIP Interface

For the SIP interface, both UDP and TCP can be used.

For outgoing UDP SIP GETS traffic on the TAS, the port configured by the *sipUdpPort* system parameter is used as the “from” port.

For outgoing TCP SIP GETS traffic, the *sipTcpPort* is used.

Since the DSCP cannot be set for each packet on a given TCP connection, it is possible that two TCP connections may need to be set up between the Cisco BroadWorks server and the remote SIP server or device: one for normal traffic and one for GETS traffic with a different DSCP value. This is not expected to be an issue unless firewalls or remote devices have particular restrictions.

5.9.2.1 TCP and UDP Ports for GETS Traffic

The outgoing GETS SIP traffic is sent from a specific port (one for User Datagram Protocol [UDP] and another one for Transmission Control Protocol [TCP]). This allows the setting of the DSCP IP flag for these messages.

Cisco BroadWorks TAS can be configured with SIP symmetric signaling enabled. That is, the Cisco BroadWorks AS sends SIP messages on the same source tuple (protocol, IP address, port) as it uses to receive. For messages that use the configured GETS port, the symmetric signaling parameter is ignored; signaling is not symmetrical even if *symmetricSignaling* is enabled on the Application Server or Network Server. This is because the server must use a different connection for DSCP.

Remote servers and devices must accept (for example, if using SIP TCP transport) at least two ports for the same host (Cisco BroadWorks TAS).

5.9.3 DSCP Field with Diameter Ro Interface

Although the Session-Priority AVP is added to the Ro interface requests made for GETS calls, the *IP* header’s *DSCP* field is not set for the query. This is because the Java platform does not support setting the *DSCP* field for individual packets on a given TCP connection. Working around this would require setting up additional TCP connections with the OCS, requiring additional configuration both on the Cisco BroadWorks TAS and OCS sides, to add additional Diameter peers.

5.10 Ethernet COS (VLAN Priority Code Point)

When a Cisco BroadWorks TAS is connected to a switch that carries network traffic to multiple VLANs, it might be useful to set the Priority code point (PCP) field of the 802.1Q VLAN tag to an increased value for Ethernet frames transporting GETS SIP signaling. This field is used by switches, routers and other network equipment to differentiate traffic at data-link level and thus enforce QoS.

5.10.1 Cisco BroadWorks TAS Connected to an Untagged Port

If a Cisco BroadWorks TAS is deployed in a network where VLAN tagging is handled by a switch and then stripped from Ethernet frames, the Priority Code Point value can be customized by adding a new entry in a DSCP-to-CoS map that most switches have. This entry should map the value of the *signalingDSCP* system parameter with the expected Ethernet COS value. This is done with the following command in a Cisco switch:

```
Router# configure terminal
Router(config)# mls qos map dscp-cos 56 to 7
```

5.10.2 Cisco BroadWorks TAS Connected to a Trunk Port

If a Cisco BroadWorks TAS is deployed in a network where VLAN support is expected to be handled directly by the Cisco BroadWorks TAS, the Priority Code Point value can be customized by using a similar method as for DSCP field setting.

- 1) For outgoing UDP and TCP GETS traffic, specific ports are used to allow iptables to filter GETS IP packets (see [TCP and UDP Ports for GETS Traffic](#)).
- 2) When an IP packet is filtered as GETS by the iptables utility, the “CLASSIFY” target extension is used to set the Linux kernel socket priority value (skb->priority) according to the provisioned *socketPriority*.
- 3) Finally, Linux network stack uses the VLAN egress priority mapping to map the socket priority to an egress priority that is used to populate the PCP value of the VLAN tag. This mapping can be configured with *vconfig*, by running the following command:

```
vconfig set_egress_map ethX.Y skbpriority vlanpcp
```

5.11 Prevent GETS-FC invocation via redirection

In order to comply with NS/EP IMS Core Network IR NGN GETS [3], Cisco BroadWorks TAS has the ability to prevent users from setting a GETS-FC number as a forwarded-to number. Since the GETS feature code can be combined with multiple other feature codes, the Cisco BroadWorks TAS has no way to detect that the provided dialed number is a GETS-FC without running the complete translation and call typing process.

The Validation of Configured Digits feature (provisioning validation), introduced in Release 14.0, can be used to address this issue. If a user attempts to provision a new destination number for a call forwarding/redirection service while Provisioning Validation is enabled, the Cisco BroadWorks TAS uses the Provisioning Validation Protocol to simulate the entire translation and call typing process with the forwarded number to verify if this number is allowed. This feature enhances the Provisioning Validation framework to always reject GETS-FC numbers.

When provisioning a forwarding number, the Cisco BroadWorks TAS rejects numbers prefixed by a GETS-FC feature access code (example: *272) by comparing the destination DN with the reserved digit map that contains reserved call type mappings and reserved feature access codes. Rejecting a DN that contains a GETS-FC feature access code at any other position (for example, *67*2721112223333) requires the intervention of Provisioning Validation. Note that the Provisioning Validation feature is not enabled by default and has to be activated for this requirement to be fully met.

6 Service Interactions

6.1 Service Precedence

There is no impact.

6.2 Service Interactions

This section describes the GETS interactions with various Cisco BroadWorks services. Only services impacted by GETS are documented here. A complete list of all Cisco BroadWorks services and their description can be found in the *Cisco BroadWorks Service Guide* (see [9]).

Note that the general philosophy for blocking services is to allow originating GETS calls and prevent them from being blocked, because GETS calls can be originated from a device not owned by the GETS Service User.

However, terminating blocking services usually work as expected since a termination (whether or not it is GETS) is inherently made to the intended user's device. Note that there is an exception for Anonymous Call Rejection, as described in section [6.2.1.2 Anonymous Call Rejection](#).

Once a call is identified as GETS, services that create additional call legs (such as call forwarding or forked to multiple destinations) are also created with GETS priority. Services interactions with other servers also contain GETS priority.

6.2.1.1 Authorization/Account Codes

The Authorization/Account Codes (AAC) feature does not block a GETS origination, nor does it even prompt for an authorization or account code. The feature is completely bypassed for GETS calls.

6.2.1.2 Anonymous Call Rejection

The Anonymous Call Rejection (ACR) service is bypassed for GETS calls. Anonymous GETS calls or GETS calls without a display name are allowed to complete even though the ACR service is enabled. One reason for this behavior is that GETS-NT calls are always anonymous due to their requirements, which are that they are not to be traceable. Therefore, this behavior ensures that they can terminate properly to ACR users.

6.2.1.3 Automatic Callback

When Automatic Callback is requested by a user during a GETS call, the callback SIP INVITE from the AS to the originator is sent with the same priority as the one associated with the previous session. When the originator answers the callback, the resulting call between the originator and terminator is also a GETS call.

6.2.1.4 BroadWorks Anywhere

If the incoming call is GETS, the call continues to be GETS throughout the redirections to the BroadWorks Anywhere locations.

Furthermore, for a standalone Cisco BroadWorks TAS configured to identify GETS calls by *Request-URI* and the BroadWorks Anywhere portal redirects to a provisioned GETS-AN or GETS-NT number, the outgoing SIP INVITE (to the network) will contain GETS priority for downstream processing.

6.2.1.5 BroadWorks Mobility

Mobile originations and terminations are promoted to GETS and treated with priority if the initial SIP INVITE that was used to anchor the call was flagged as GETS. For instance, if a Cisco BroadWorks TAS receives an IP Multimedia Routing Number (IMRN) allocation request via Xsi from a BroadWorks Anywhere Location to establish a call to a GETS-AN or GETS-NT number, the subsequent SIP INVITE targeting this IMRN from the Media Gateway Controller (MGC) is implicitly considered as GETS and is not subject to overload controls.

The *Deny Call Originations* flag is ignored for GETS for mobile originations.

6.2.1.6 Call Capacity Management

Although a GETS call counts toward Call Capacity Management (CCM) group usage computations, no GETS calls are blocked because a CCM group is at (or above) capacity.

6.2.1.7 Call Forwarding Always

A forwarding leg is handled with priority (and contains the *Resource-Priority* SIP header and *DSCP IP* header field) when the incoming call is GETS.

Furthermore, for a standalone Cisco BroadWorks TAS configured to identify GETS calls by *Request-URI* and the call forwarded to number is a provisioned GETS-AN or GETS-NT number, the outgoing SIP INVITE (to the network) will contain GETS priority for downstream processing.

6.2.1.8 Call Forwarding Always Secondary

Interaction is the same for all call forwarding services. See description for [6.2.1.7 Call Forwarding Always](#)

6.2.1.9 Call Forwarding Busy

Interaction is the same for all call forwarding services. See description for [6.2.1.7 Call Forwarding Always](#)

6.2.1.10 Call Forwarding No Answer

Interaction is the same for all call forwarding services. See description for [6.2.1.7 Call Forwarding Always](#)

6.2.1.11 Call Forwarding Not Reachable

Interaction is the same for all call forwarding services. See description for [6.2.1.7 Call Forwarding Always](#)

6.2.1.12 Call Forwarding Selective

Interaction is the same for all call forwarding services. See description for [6.2.1.7 Call Forwarding Always](#)

6.2.1.13 Call Processing Policies

The following are the Call Processing Policies that are bypassed for GETS calls:

- Maximum number of concurrent calls
- Maximum number of video calls

6.2.1.14 Call Transfer

An originating GETS call is handled with priority when transferred (blind transfer). For terminating NS/EP calls, a blind transfer is handled similar to a forwarded call, and is therefore handled with priority.

For Consultation (through the Xsi-Actions interface or device initiated), when a subsequent call is made while the user was already in a GETS originating call (presumably not initiated via the client so that it could be flagged as a GETS call), the transfer origination is also made with priority (it has the *Resource-Priority* header and DSCP set).

If the existing call was a terminating NS/EP call, the origination is not made with priority. This is consistent with the requirements in *NS/EP IMS Core Network IR NGN GETS [2]*. However, in standalone mode configured to identify GETS calls by *Request-URI*, if the destination number is a GETS-AN or GETS-NT provisioned number, the call is recognized as a GETS call and the origination also treated with priority.

6.2.1.15 City-Wide Centrex

In standalone mode configured to identify GETS calls by *Request-URI*, a CWC GETS extension call will not be identified a GETS call and maybe stopped by overload controls. However, if the translated extension matches a provisioned GETS-AN or GETS-NT number the outgoing SIP INVITE (to the network) will contain GETS priority for downstream processing.

6.2.1.16 Click To Dial

Click-To-Dial originations are **not** handled with priority for the first leg to the Cisco BroadWorks user's device if no other calls exist for the user. However, in standalone mode configured to identify GETS calls by *Request-URI*, if the destination number is a GETS-AN or GETS-NT provisioned number, the call is recognized as a GETS call and first leg to the Cisco BroadWorks user's device is also treated with priority.

If the Click To Dial is for a consultation and an existing call was a GETS origination, then the Click-To-Dial call is also handled with priority. See section *6.2.1.14 Call Transfer* for consultation details..

6.2.1.17 Collaborate

Each new call leg between a user's device and a Collaborate Bridge keeps their individual GETS status and does not affect the interaction between the AS and other participants. When a user joins a Collaborate Room via a GETS call, the conference is marked as GETS with the user's Resource-Priority header r-values. When multiple users join a Collaborate Room via GETS calls, the conference is also marked as GETS and the Resource-Priority header r-values it uses are those of the call with the highest priority as provided by the configurable mapping section. The GETS Resource-Priority r-values of the conference are used for the interactions between the Cisco BroadWorks Application Server (AS) and the Cisco BroadWorks Video Server (UVS). If Cisco BroadWorks receives an OCI-C request to outdial a participant, the r-values of the conference are used to populate the Resource-Priority header of the SIP INVITE that is sent to the new participant.

6.2.1.18 Communication Barring - Fixed

Communication Barring originating call rules are bypassed for GETS calls.

6.2.1.19 Communication Barring User-Control

Communication Barring originating call rules are bypassed for GETS calls.

6.2.1.20 Concurrent Call Licensing

A GETS call is counted toward the total number of calls. However GETS calls are not blocked by Concurrent Call Licensing.

6.2.1.21 Congestion Management

GETS calls bypass Congestion Management restricted servers and sends the message to the server regardless of whether the server is in congestion control.

6.2.1.22 Custom Ringback

Any custom ringback invocation in a GETS terminating session is prevented. The video and call waiting variants are blocked as well.

6.2.1.23 Emergency Zones

GETS calls bypass this service altogether. Even if the Emergency Zone service is assigned, enabled and configured to reject all call originations, GETS calls from outside of the home zone proceed normally.

6.2.1.24 Enterprise Trunk

Unscreened GETS calls are allowed, regardless of the value of the *Allow Unscreened Calls* or *Allow Unscreened Emergency Calls* flags. GETS calls are allowed even if an enterprise or group has no available business trunking license units. Enterprise Trunk Capacity is ignored for GETS calls except when the maximum active incoming calls allowed is set to 0 for all trunks of the Enterprise Trunk. In this case, the restriction implies that the Enterprise Trunk is not to be used for incoming calls at all.

6.2.1.25 Expensive Call Notification

Expensive Call Notification (ECN) is bypassed for GETS calls. Therefore, no announcement is played to the originating user.

6.2.1.26 External Custom Ringback

Any custom ringback invocation in a GETS terminating session is prevented.

6.2.1.27 Intercept Group/User

Intercept group and intercept user services do not block an originating GETS call. However, for a GETS calls terminating to an intercepted group/user, the call is handled (blocked or redirected) normally.

6.2.1.28 Legacy Automatic Callback

Legacy Automatic Callback service invocations are not possible for GETS calls.

6.2.1.29 Meet-Me Conferencing

Each new call leg between a user's device and a Meet-Me Conference Bridge keeps their individual GETS status and does not affect the interaction between the AS and other participants. When a user joins a Meet-Me Conference via a GETS call, the conference is marked as GETS with the user's Resource-Priority header r-values. When multiple users join a Meet-Me Conference via GETS calls, the conference is also marked as GETS and the Resource-Priority header r-values it uses are those of the call with the highest priority as provided by the configurable mapping section. The GETS Resource-Priority r-values of the conference are used for the interactions between the Cisco BroadWorks Application Server (AS) and the Cisco BroadWorks Media Server (MS). If Cisco BroadWorks receives an OCI-C request to outdial a participant, the r-values of the conference are used to populate the Resource-Priority header of the SIP INVITE that is sent to the new participant. If a participant requests to be transferred to an operator, the outgoing SIP INVITE to the operator has the same GETS status as the initial SIP INVITE that was received to connect this user to the Meet Me Conference Bridge.

6.2.1.30 N-Way Call

Cisco BroadWorks supports GETS conferences when they are initiated by the owner of at least one origination GETS call. This is supported for device initiated conferences and conferences initiated through Xsi-Actions interfaces. The GETS conference imported priority level is set to that of the highest involved GETS-originating call session.

For device-initiated conferences where a device sends an INVITE to a conference-creation URI and subsequently refers remote parties to the newly created conference URI, support for implicit GETS priority has been added. If the conference-creating user is the originator of any GETS call, the conference is marked as GETS and the *Resource-Priority* header r-values it uses are those of the call with the highest priority as provided by the configurable mapping section.

Also, for a device-initiated conference, the new dialog that connects the originating party to the conference bridge is authorized only if Cisco BroadWorks TAS is not in overload condition (Green). Once the call to the conference bridge is established, it is marked as GETS and further requests are handled based on priority.

While Cisco BroadWorks TAS does not reject requests targeting already established non-GETS call sessions, external functional elements may reject those requests since they are not marked with GETS *Resource-Priority* header r-values.

6.2.1.31 Number Portability Announcement

This service is bypassed for GETS calls.

6.2.1.32 Outgoing Calling Plan

GETS originating calls are not blocked by Outgoing Calling Plan (OCP) for GETS calls.

If Enhanced Outgoing Calling Plan (EOCP) is set to "No", a GETS call still goes through normally. If set to "Auth Code", a GETS call goes through normally without being prompted for an authorization code. If EOCP is set to "Xfer T1", a GETS call goes through without being transferred.

6.2.1.33 Overload Controls

Even when the Cisco BroadWorks server is in overload condition, a new GETS call is still processed and thus bypasses overload controls that would otherwise (that is, for a non-GETS call) have blocked the call. See 5.3 *Overload Controls* for more details.

6.2.1.34 Prepaid

When configuration *bypassRoRelease* is disabled, prepaid has priority over GETS calls. If a prepaid GETS origination or termination does not have sufficient credits at call setup or during the call, the call is released normally. Note that *3GPP TS 22.952* describes interactions between priority services and the Prepaid service.

When configuration *bypassRoRelease* is enabled then the call is allowed to setup or continue regardless when the user has sufficient credits or not.

6.2.1.35 Remote Office

Terminations to a Remote Office user are handled with priority if the incoming call is a GETS call.

6.2.1.36 Session Admission Control

Restrictions of Session Admission Control are bypassed for GETS calls.

6.2.1.37 Shared Call Appearance

Terminating NS/EP calls forked to several devices have all the parallel legs alerted with priority.

GETS originations are handled as expected no matter which device originates it. GETS originations from devices not allowed to make calls are allowed.

Shared Call Appearance Retrieve or Bridging can be made as usual to retrieve or bridge a GETS call (originating or terminating).

Each new call leg between an SCA Location and an SCA Bridge keeps their individual GETS status and does not affect the interaction between the AS and other participants.

If the initial call is GETS and an SCA location creates an SCA bridge via a non-GETS call the conference is marked as GETS and inherits the Resource-Priority header r-values of the initial call.

When an SCA location joins a non-GETS SCA bridge via a GETS call, the conference is marked as GETS with the SCA location's Resource-Priority header r-values.

When an SCA location joins a GETS SCA bridge via a GETS call, the conference remains GETS and the Resource-Priority header r-values it uses are those of the call with the highest priority as provided by the configurable mapping section.

The GETS Resource-Priority r-values of the conference are only used for the interactions between the Cisco BroadWorks Application Server (AS) and the Cisco BroadWorks Media Server (MS).

6.2.1.38 Three-Way Call

Same interaction as N-Way Call service, see [6.2.1.30 N-Way Call](#).

6.2.1.39 Treatments

Configurable treatments for SIP error codes 417 (Unknown Resource-Priority) and 420 (Bad Extension) are bypassed for GETS calls. If a downstream network element responds with SIP 417 or 420 after receiving a GETS SIP INVITE, the Cisco BroadWorks TAS ignores the configured treatment and proceeds with the Route Advancing and SIP INVITE resending as described in [5.4.3 GETS Call Processing for SIP 417 and 420 Error](#).

6.2.1.40 Trunk Group

Trunk Group capacity restriction is bypassed for GETS calls and the GETS priority applies, except when the maximum active incoming calls allowed is set to 0 for the trunk. In this case, the restriction implies that the trunk is not to be used for incoming calls at all.

Refer to Section 13 of the *Cisco BroadWorks SIP Trunking Solution Guide* [14] for the detailed description of Trunk Group Capacity Management.

6.2.1.41 Verify Translation and Routing (VTR)

GETS is transparent to VTR service. The VTR output is changed to identify GETS calls.

6.2.1.42 Zone Calling Restrictions

GETS calls bypass Zone Calling Restrictions.

7 System Management

7.1 Accounting

The GETS feature requires a few accounting changes.

- This GETS feature adds a new CDR Field called *GETS*. For originating and terminating CDRs, this field is set to “Yes” when a call is a GETS call. This field is only present for GETS calls. If present, its value is “Yes”.
- This feature adds CDR field *GETSOriginationType* to originating CDRs. *GETSOriginationType* records the type of GETS originating call and its value is either
 - “GETSAN”,
 - “GETSNT”,
 - “GETSFC”, (IMS Mode only)
 - “GETSFCAN”, (IMS Mode only)
 - “GETSFCNT”, (IMS Mode only)
 - “GETS”
- This feature modifies the value of the Session-Priority AVP in outgoing Ro interface Diameter messages associated with a GETS call. This AVP is used by the billing systems to identify the priority level assigned to a call.
- A *SessionPriority* table is created to map possible session priority-level values to a Diameter Session-Priority AVP value. When a new originating session is created, the Cisco BroadWorks TAS uses the session’s priority level to look up the corresponding session priority value in this table and the Diameter requests involved in the accounting of this call are augmented with this Session-Priority AVP containing this value.
- This feature adds a way to obfuscate Diameter AVPs that can provide sensitive information when a Cisco BroadWorks user originates a GETS-NT or GETS-FC + GETS-NT call. As explained in section 5.8.3 a *GETSNTInhibitedAVPCodeList* table is added to this feature. When a GETS-NT or GETS-FC + GETS-NT originating session is created, all AVPs present in this table are removed from any outgoing billing (ACR, CCR) Diameter messages associated with this GETS call.
- To support the usage control mechanism using Diameter Ro (online billing), this feature also allows for the bypassing of session termination after a Credit-Control-Failure. This feature allows for the bypassing termination of any GETS call after receiving an ASR message or a CCA message with a Final-Unit-Indication AVP and a Final-Unit-Action AVP set to “TERMINATE” or “REDIRECT”.

7.2 Monitoring and Troubleshooting

7.2.1 Alarms and PMs

This feature introduces some basic statistics counters for originating and terminating GETS calls.

The Cisco Performance Measurements (PMs) may also be known as Operational Measurements (OMs).

7.2.1.1 Originating GETS Call Counters

For originating call there are separate counters for each of the following originating GETS call types:

- GETSFC (IMS Mode only)
- GETSFCAN (IMS Mode only)
- GETSFCNT (IMS Mode only)
- GETSAN
- GETSNT
- GETS

These counters are added at the system, service provider, and group level. The following counters are defined for each call type:

- Counter for each attempted GETS call. That is, a call with an RPH header with valid or invalid GETS namespaces or a call with GETS Request URI.
- Counter for each attempted GETS call that passes RPH namespace validation or Request-URI GETS call identification and is sent to the next destination (see 5.2 Identifying GETS Calls and 5.7.1 Resource-Priority Header (RPH) for more details).
- Counter for each GETS call that results in being answered (SIP 200).
- Counter for each GETS call that is ringing but not answered (SIP 18x) and a SIP CANCEL is received from end users or from the network.
- Counter for each GETS call that is ringing but not answered (SIP 18x) and is timed out by Cisco BroadWorks TAS. Because the ring timeout mechanism does not apply to calls terminating to a PSTN network, originating ringing timeout counters are impossible to increment in IMS mode where all calls are routed to the network.
- Counter for each GETS call that is declined by the called user (SIP 603).
- Counter for each GETS call that fails as forbidden (SIP 403).
- Counter for each GETS call that fails as destination busy (SIP 486 and 600).
- Counter for each GETS call that fails as service unreachable (SIP 503).
- Counter for each GETS call that fails timed-out (SIP 408, 504).
- Counter for each GETS call that Cisco BroadWorks TAS generates a SIP 400 due to invalid *Resource-Priority* header as specified in 5.7.1.1 Resource Priority Header Handling.
- Counter for each time Cisco BroadWorks TAS receives a SIP 417 or a SIP 420 response from a downstream functional element.
- Count the number of times a SIP request contains a valid *Resource-Priority* header but the call session initially was not recognized as a GETS call.

7.2.1.2 Terminating NS/EP Call Counters

For terminating calls there are only GETS call type counters. These counters are added at the system, service provider, and group level:

- Counter for each attempted GETS call. That is, a call with an RPH header with valid or invalid GETS namespaces.
- Counter for each attempted GETS call that passes RPH namespace validation and is sent to the next destination (see 5.2 Identifying GETS Calls and 5.7.1 Resource-Priority Header (RPH) for more details).
- Counter for each GETS call that results in being answered (SIP 200).
- Counter for each GETS call that is ringing but not answered (SIP 18x) and a SIP CANCEL is received from end users or from the network.
- Counter for each GETS call that is ringing but not answered (SIP 18x) and is timed out by Cisco BroadWorks TAS.
- Counter for each GETS call that is declined by the called user (SIP 603).
- Counter for each GETS call that fails as forbidden (SIP 403).
- Counter for each GETS call that fails as destination busy (SIP 486 and 600).
- Counter for each GETS call that fails as service unreachable (SIP 503).
- Counter for each GETS call that fails timed-out (SIP 408, 504).
- Counter for each GETS call that Cisco BroadWorks TAS generates a SIP 400 due to invalid *Resource-Priority* header as specified in 5.7.1.1 Resource Priority Header Handling.
- Counter for each time Cisco BroadWorks TAS receives a SIP 417 or a SIP 420 response from a downstream functional element.
- Count the number of times a SIP request contains a valid *Resource-Priority* header but the call session initially was not recognized as a GETS call.

7.2.1.3 Emergency Call DDoS Protection Counters

These PMs are added at system level to monitor the operation of the Emergency DDoS protection mechanism:

- A counter that tracks the number of times that the server rejects an emergency call due the emergency call throttling mechanism.
- A gauge that measures the rate at which emergency origination attempts occur.

7.2.2 Commands and Utilities

There is no impact.

7.3 Device Management

There is no impact.

8 Restrictions and Limitations

8.1 Functional Limitations

8.1.1 DSCP Field with Diameter Ro Interface

Although the Session-Priority AVP is added to the Ro interface requests made for GETS calls, the *IP* header's *DSCP* field is not set for the query. This is because the Java platform does not support setting the *DSCP* field for individual packets on a given TCP connection. Working around this would require setting up additional TCP connections with the OCS, requiring additional configuration on the Application Server and OCS sides, to add additional Diameter peers.

8.1.2 GETS-NT Accounting AVPs Inhibition

As specified in section [5.8.3 GETS-NT Inhibited Accounting AVPs Support](#) some mandatory AVPs cannot be added in the *getsNTInhibitedAVPCodeList*. Indeed, system administrators are prevented from inhibiting certain specific AVPs from GETS-NT ACRs or responses for confidentiality reasons..

8.1.3 IMS Mode

8.1.3.1 Out-of-the-Blue GETS Originations

In some situations (such as ClickTo-Dial), the Cisco BroadWorks AS may send Out of the Blue (OOTB) requests to the S-CSCF. An OOTB request is a request that originates from the Application Server and is not directly associated with a request from the S-CSCF. Out-of-the-Blue GETS originations from the Cisco BroadWorks TAS are not fully supported by this feature. The Cisco BroadWorks TAS, having no means to authenticate the request, does **not** add a *Resource-Priority* header by itself. New SIP dialogs originated from the Cisco BroadWorks TAS do not have a *Resource-Priority* header until requests reach IMS core elements and/or a GETS-AS. Until one such element authenticates the GETS request and adds the *Resource-Priority* header, no priority treatment occurs in the Cisco BroadWorks TAS, and overload controls in place on the Cisco BroadWorks TAS may cause rejection of the request before authentication can take place.

8.1.3.2 Click To Dial

Click-To-Dial originations, along with Voice Portal Calling, are not flagged as GETS calls until the S-CSCF has sent the OOTB call to the GETS AS (assuming it is configured to do so), which is after the Cisco BroadWorks TAS has processed the origination. This still allows the terminating side to handle the call with high priority, for example, bypassing call admission controls. However, the originating device has not been invited with priority and does not transmit RTP media with the DSCP flag.

8.2 Upgrade/Rollback Limitations

There are no limitations.

8.3 Enterprise Migration Restrictions

There are no restrictions.

9 Service Patch Information

This feature is patched in the following:

- Release 21.sp1
- Release 22.0

9.1 Functional Differences

The *GETS* enabled flag cannot be set to true if the feature is not activated.

9.2 Feature Activation Impacts

9.2.1 Method of Activation

This feature is activated using the following CLI command:

```
AS_CLI/System/ActivatableFeature> activate 11930
```

9.2.2 Activatable Feature ID and Dependencies

The feature ID is 11930 and there are no dependencies.

10 Provisioning Interface Impacts

10.1 Centralized Configuration Data

10.1.1 executionServerSubsystem

The ExecutionServerSubsystem, is augmented with a GETS/Network section that contains the system parameters for the GETS requirements on the Execution Server.

Name	Type	Content Restrictions	Default Value	Description
<i>GETS/Network</i>	Not applicable			Provides the ability to manage GETS system-level network attributes.

10.1.2 executionServerSubsystem/gets/network

The following table illustrates the GETS configuration modifications.

Name	Type	Content Restrictions	Default Value	Description
<i>outgoingSipUdpPort</i>	Integer	1025 through 65535, nillable	nil	This parameter specifies the <i>From</i> port for outgoing GETS SIP UDP signaling.
<i>outgoingSipTcpPort</i>	Integer	1025 through 65535, nillable	nil	This parameter specifies the <i>From</i> port for outgoing GETS SIP TCP signaling.
<i>COSPriority</i>	Integer	0 to 7	5	This parameter specifies the socket priority value that is used for GETS SIP traffic. It is used to set the Ethernet Frame Header Class of Service (COS) on the Ethernet interface.

10.1.3 nsExecutionServerSubsystem/gets/GETSNumbers

The nsExecutionServerSubsystem, is augmented with a GETS/GETSNumber section that contains the list of numbers to be considered as GETSNumbers. The following table illustrates the GETS configuration modifications..

Name	Type	Content Restrictions	Default Value	Description
<i>Type</i>	Token	AN, NT		This parameter specifies whether the number is considered as GETS-AN or GET-NT.

Name	Type	Content Restrictions	Default Value	Description
<i>Number</i>	String	4 to 10 characters, which must be 10 digits or 3 to 9 digits completed by a wildcard star character (*). The number must start with 710 or 8.		<p>The parameter represents a GETS-AN or GETS-NT string. This string matches with the Request-URI received user string to promote a regular call to a GETS call. 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). This parameter accepts a string of 4 to 10 characters, which may consist of 10 digits or 3 to 9 digits completed by a wildcard star character (*). Note that if the Request-URI received is a SIP:URI without user=phone, user=phone error correction can be done depending on the <i>userPhoneErrorCorrection</i> parameter and that the E.164 format is supported.</p> <p>For matching against a provisioned GETS-AN/NT string, a successful match is detected when:</p> <ul style="list-style-type: none"> ▪ The received user string contains at least ten digits. ▪ If the provisioned GETS-AN/NT has a wildcard, it matches the digits before the wildcard with the first digits of the received user string. For example a provisioned GETS-AN/NT value of "710*" will produce a positive match for all received user string "710xxxxxx". ▪ If the provisioned GETS-AN/NT doesn't have a wildcard, it matches all ten digits of the received user string.
<i>Description</i>	String	1 to 80 characters, nillable		This parameter specifies a brief description of the GETS-AN/NT number.

10.2 CLI Impacts

10.2.1 Summary

The Application Server and Network Server CLI are modified by this feature.

The following CLI contexts are added:

- *AS_CLI/System/CallP/GETS*
- *AS_CLI/System/CallP/GETS/Numbers*
- *AS_CLI/System/CallP/GETS/InhibitedAVPCodes*
- *AS_CLI/System/CallP/GETS/Network*
- *AS_CLI/System/CallP/GETS/ResourcePriorities*
- *AS_CLI/System/CallP/GETS/SessionPriorityMapping*
- *AS_CLI/System/CallP/GETS/ReservedFACs*

- AS_CLI/System/CallP/EmergencyCallDDoSProtection
- NS_CLI/System/CallP/GETS/Numbers
- NS_CLI/System/CallP/EmergencyCallDDoSProtection>

```
.AS_CLI
...System
....CallP
.....GETS [get set]
.....Numbers [add delete get set clear]
.....InhibitedAVPCodes [add delete get]
.....Network [get set clear]
.....ReservedFACs [add delete get set clear]
.....ResourcePriorities [add delete get set]
.....SessionPriorityMap [add delete get set]
..... EmergencyCallDDoSProtection [get set clear]
```

Figure 17 Application Server CLI Hierarchy Changes

```
.NS_CLI
...System
....CallP
.....GETS
.....Numbers [add delete get set clear]
..... EmergencyCallDDoSProtection [get set clear]
```

Figure 20 Network Server CLI Hierarchy Changes

10.2.2 Adding Application Server GETS context

Location
AS_CLI/System/CallP/GETS
Description
This level is used to configure Government Emergency Telecommunications Service (GETS) system-level attributes related to call processing.

10.2.2.1 Command get

Location
AS_CLI/System/CallP/GETS
Description
This command is used to view Government Emergency Telecommunications Service (GETS)-related attributes.
Syntax
get get takes no parameter
Example
AS_CLI/System/CallP/GETS> get enabled = true enableRequireResourcePriority = false sendAccessResourcePriority = false callIdentifierMode = rph defaultPriorityAVP = 2 signalingDSCP = 45 defaultRValue = ets.0 bypassRoRelease = true

10.2.2.2 Command set

Location	
AS CLI/System/CallP/GETS	
Description	
This command is used to modify Government Emergency Telecommunications Service (GETS)-related attributes.	
Syntax	
<pre>set <attribute>, Multiple Choice = {enabled, enableRequireResourcePriority, sendAccessResourcePriority, callIdentifierMode, priorityAVP, signalingDSCP, defaultRValue, bypassRoRelease} <enabled>, Choice = {false, true} <enableRequireResourcePriority>, Choice = {false, true} <sendAccessResourcePriority>, Choice = {false, true} <callIdentifierMode>, Choice = {rph, requestUri, rphRequestUri} <defaultPriorityAVP>, Integer {0 to 4} <signalingDSCP>, Integer {0 to 63} <defaultRValue>, String {5 to 80 characters} <bypassRoRelease>, Choice = {false, true}</pre>	
Parameters	
attribute:	The name of an attribute to modify.
enabled:	This parameter controls whether Government Emergency Telecommunications Service (GETS) is enabled.
enableRequireResourcePriority:	This parameter controls whether the outgoing first Government Emergency Telecommunications Service (GETS) call SIP INVITE request contains a <i>Require</i> header with the resource-priority option tag.
sendAccessResourcePriority:	This parameter controls whether Government Emergency Telecommunications Service (GETS) Resource Priority values are included in SIP traffic sent to the access-side.
callIdentifierMode:	This parameter specifies the method used to identify Government Emergency Telecommunications Service (GETS) calls.
defaultPriorityAVP:	This parameter determines the Diameter interface Session-Priority Attribute-Value Pair (AVP) used when no session priority mappings are defined.
signalingDSCP:	This parameter specifies the signaling Differentiated Services Code Point (DSCP) value to identify Government Emergency Telecommunications Service (GETS) SIP traffic.
defaultRValue:	This parameter specifies the Government Emergency Telecommunications Service (GETS)-Mandatory r-value to use when no GETS-Mandatory class r-values are provided.
bypassRoRelease:	This parameter determines whether a Government Emergency Telecommunications Service (GETS) call session is terminated after receiving one of the following diameter messages:
	- ASR
	- CCA that contains the Final-Unit-Indication Attribute-value pair (AVP) and a Final-Unit-Action AVP value set to "TERMINATE" or "REDIRECT".
Example	
<pre>\$ AS_CLI/h /CallP/GETS> set defaultRValue ets.0 ...Done \$ AS_CLI/System/CallP/GETS> set bypassRoRelease true ...Done</pre>	

10.2.3 Adding Application Server Numbers context

Location	
AS CLI/System/CallP/GETS/Numbers	

Description
This level is used to configure GETS Access Number (GETS-AN) and GETS Number Translation (GETS-NT) numbers.

10.2.3.1 Command add

Location
AS CLI/System/CallP/GETS/Numbers
Description
This command is used to define a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) number.
Syntax
<pre> add <number>, String {4 to 10 characters} <type>, Choice = {AN, NT} [<attribute>, Multiple Choice = {description}] <description>, String {1 to 80 characters} </pre>
Parameters
<p>number: The parameter represents a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) string. This string matches with the Request-URI received user string to promote a regular call to a Government Emergency Telecommunications Service (GETS) call. 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). This parameter accepts a string of four to 10 characters, which may consists of 10 digits or three to 9 digits completed by a wildcard star character (*). Note that if the Request-URI received is a SIP:URI without user=phone, user=phone error correction can be done depending on the userPhoneErrorCorrection parameter and that the E.164 format is supported. For matching against a provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) string, a successful match is detected when:</p> <ul style="list-style-type: none"> -The received user string contains at least ten digits. -If the provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) has a wildcard, it matches the digits before the wildcard with the first digits of the received user string. For example a provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) value of "710*" will produce a positive match for all received user string "710xxxxxxx" -If the provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) does not have a wildcard, it matches all ten digits of the received user string. <p>type: This parameter determines whether the number is considered as GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT).</p> <p>attribute: This parameter specifies an additional attribute for the GETS Access Number (GETS-AN)/Number Translation (GETS-NT) number.</p> <p>description: This parameter specifies a brief description of the GETS Access Number (GETS-AN)/GETS Number Translation (GETS-NT) number.</p>
Example
<pre> \$ AS_CLI/System/CallP/GETS/Numbers> add 7106274387 AN ...Done </pre>

10.2.3.2 Command delete

Location
AS CLI/System/CallP/GETS/Numbers
Description
This command is used to delete an existing GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) number.

Syntax
delete <number>, String {4 to 10 characters}
Parameters
number: The Government Emergency Telecommunications Service (GETS) number to delete.
Example
<pre>\$ AS_CLI/System/CallP/GETS/Numbers> delete 7106274387 ...Done</pre>

10.2.3.3 Command set

Location
AS CLI/System/CallP/GETS/Numbers
Description
This command is used to modify an existing GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) number.
Syntax
set <number>, String {4 to 10 characters} <attribute>, Multiple Choice = {type, description} <type>, Choice = {AN, NT} <description>, String {1 to 80 characters}
Parameters
number: This parameter specifies the Government Emergency Telecommunications Service (GETS) number to modify. attribute: This parameter specifies the name of an attribute to modify. type: This parameter specifies the new type for the existing Government Emergency Telecommunications Service (GETS) number. description: This parameter specifies a new description for the existing Government Emergency Telecommunications Service (GETS) number.
Example
<pre>\$ AS_CLI/System/CallP/GETS/Numbers> set 7106274387 type NT ...Done</pre>

10.2.3.4 Command get

Location
AS CLI/System/CallP/GETS/Numbers
Description
This command is used to display all existing GETS Access Numbers (GETS-AN)/GETS Number Translations (GETS-NT).
Syntax
get Get takes no parameter.
Example
<pre>\$ AS_CLI/System/CallP/GETS/Numbers> get Number Type Description ===== 710665555 NT GETS-NT number 7106274387 AN 2 entries found.</pre>

10.2.3.5 Command clear

Location	
AS CLI/System/CallP/GETS/Numbers	
Description	
This command is used to clear Government Emergency Telecommunications Service (GETS) number-related attributes.	
Syntax	
<pre>clear <number>, String {4 to 10 characters} <attribute>, Multiple Choice = {description}</pre>	
Parameters	
number:	This parameter specifies the GETS number for which an attribute is to be cleared.
attribute:	The name of an attribute to clear.
Example	
<pre>\$ AS_CLI/System/CallP/GETS/Numbers> clear 7106665555 description ...Done</pre>	

10.2.4 Adding Application Server Network context

Location	
AS CLI/System/CallP/GETS/Network	
Description	
This level is used to configure Government Emergency Telecommunications Service (GETS) call processing network-related attributes.	

10.2.4.1 Command set

Location	
AS CLI/System/CallP/GETS/Network	
Description	
This command is used to modify Government Emergency Telecommunications Service (GETS) call processing network-related attributes.	
Syntax	
<pre>set <attribute>, Multiple Choice = {outgoingSipUdpPort, outgoingSipTcpPort, COSPriority} <outgoingSipUdpPort>, Integer {1025 to 65535} <outgoingSipTcpPort>, Integer {1025 to 65535} <COSPriority>, Integer {0 to 7}</pre>	
Parameters	
attribute:	This parameter specifies the name of an attribute to modify.
outgoingSipUdpPort:	This parameter specifies the <i>From</i> port for outgoing Government Emergency Telecommunications Service (GETS) SIP UDP signaling.
outgoingSipTcpPort:	This parameter specifies the <i>From</i> port for outgoing Government Emergency Telecommunications Service (GETS) SIP TCP signaling.
COSPriority:	This parameter specifies the socket priority value that is used for Government Emergency Telecommunications Service (GETS).
Example	
<pre>\$ AS_CLI/System/CallP/GETS/Network> set outgoingSipUdpPort 8099 COSPriority 6 ...Done</pre>	

10.2.4.2 Command get

Location
AS CLI/System/CallP/GETS/Network
Description
This command is used to view Government Emergency Telecommunications Service (GETS) call processing network-related attributes.
Syntax
get Get takes no parameter.
Example
AS_CLI/System/CallP/GETS/Network> get outgoingSipUdpPort = 8099 outgoingSipTcpPort = 8091 COSPriority = 6

10.2.4.3 Command clear

Location
AS CLI/System/CallP/GETS/Network
Description
This command is used to clear Government Emergency Telecommunications Service (GETS) call processing network-related attributes.
Syntax
clear <attribute>, Multiple Choice = { outgoingSipUdpPort, outgoingSipTcpPort }
Parameters
attribute: The name of an attribute(s) to clear.
Example
\$ AS_CLI/System/CallP/GETS/Numbers> clear outgoingSipUdpPort ...Done

10.2.5 Adding Application Server ReservedFACs context

Location
AS CLI/System/CallP/GETS/ReservedFACs
Description
This level is used to configure Feature Access Codes reserved for Government Emergency Telecommunications Service (GETS).

10.2.5.1 Command add

Location
AS CLI/System/CallP/GETS/ReservedFACs
Description
This command is used to define a Government Emergency Telecommunications Service Feature access code (GETS-FAC).
Syntax
add <code>, String {2 to 5 characters} [<description>, String {1 to 80 characters}]
Parameters

code: The Feature Access Code to identify a Government Emergency Telecommunications Service (GETS) call.
 description: A description of the Government Emergency Telecommunications Service Feature access code (GETS-FAC).

Example

```
$ AS_CLI/System/CallP/GETS/ReservedFACs> add *272 "FAC for GETS"
...Done
```

10.2.5.2 Command delete

Location
AS CLI/System/CallP/GETS/ReservedFACs
Description
This command is used to delete an existing Government Emergency Telecommunications Service Feature access code (GETS-FAC).
Syntax
delete <code>, String {2 to 5 characters}
Parameters
code: The Government Emergency Telecommunications Service Feature access code (GETS-FAC) to delete.
Example
\$ AS_CLI/System/CallP/GETS/ReservedFACs> delete *272 ...Done

10.2.5.3 Command set

Location
AS CLI/System/CallP/GETS/ReservedFACs
Description
This command is used to modify an existing Government Emergency Telecommunications Service Feature access code (GETS-FAC).
Syntax
set <code>, String {2 to 5 characters} <attribute>, Multiple Choice = {newCode, description} <newCode>, String {2 to 5 characters} <description>, String {1 to 80 characters}
Parameters
code: This parameter specifies the Government Emergency Telecommunications Service Feature access code (GETS-FAC) to modify. Attribute: This parameter specifies the name of an attribute to modify. newCode: This parameter specifies a new feature access code (FAC) to replace the existing Government Emergency Telecommunications Service Feature access code (GETS-FAC). description: This parameter specifies a new description for the existing Government Emergency Telecommunications Service Feature access code (GETS-FAC).
Example
\$ AS_CLI/System/CallP/GETS/ReservedFACs> set *272 newCode *273 ...Done

10.2.5.4 Command get

Location

AS CLI/System/CallP/GETS/ReservedFACs
Description
This command is used to display all existing Government Emergency Telecommunications Service Feature access codes (GETS-FACs).
Syntax
get Get takes no parameter.
Example
<pre>\$ AS_CLI/System/CallP/GETS/ReservedFACs> get Code Description ===== *273 *277 FAC for GETS 2 entries found.</pre>

10.2.5.5 Command clear

Location
AS CLI/System/CallP/GETS/ReservedFACs
Description
This command is used to clear Government Emergency Telecommunications Service Feature access code (GETS-FAC)-related attributes.
Syntax
clear <code>, String {2 to 5 characters} <clearAttribute>, Multiple Choice = {description}
Parameters
code: This parameter specifies the Government Emergency Telecommunications Service Feature access code (GETS-FAC) for which an attribute is to be cleared. clearAttribute: The attribute to clear.
Example
<pre>\$ AS_CLI/System/CallP/GETS/ReservedFACs> clear *277 description ...Done</pre>

10.2.6 Adding Application Server ResourcePriorities context

Location
AS CLI/System/CallP/GETS/ResourcePriorities
Description
This level is used to configure Government Emergency Telecommunications Service (GETS) ResourcesPriorities.

10.2.6.1 Command add

Location
AS CLI/System/CallP/GETS/ResourcePriorities
Description
This command is used to add a recognized resource-priority value and additional Next Generation Network (NGN) Government Emergency Telecommunications Service (GETS)-related attributes.
Syntax

<pre>add <priorityValue>, String {5 to 80 characters} <priorityLevel>, Integer {1 to 5} <priorityClass>, Choice = {GETS-Mandatory, GETS}</pre>
<p>Parameters</p> <p>priorityValue: This parameter specifies a Resource-Priority r-value, which is constructed with a namespace, a dot, and a priority value, as per RFC 4412. For example, "ets.2". Values are case-insensitive.</p> <p>priorityLevel: This parameter specifies the maximum session priority level that is attached to a session receiving this r-value. The effective priority level of a call session is the lowest 'priorityLevel' of all received r-value(s). Used to determine the value of the Session-Priority AVP.</p> <p>priorityClass: This parameter determines which class the r-value belongs to. The value affects how RPH content is validated when invoking priority services. The values are:</p> <ul style="list-style-type: none"> -"GETS-Mandatory": Triggers Next-Generation Network (NGN) Government Emergency Telecommunications Service (GETS) priority services. At least one is required in this class to invoke GETS priority services. -"GETS": Triggers NGN Government Emergency Telecommunications Service (GETS) RPH validation.
<p>Example</p> <pre>\$ AS_CLI/System/CallP/GETS/ResourcePriorities> add ets.0 5 GETS-Mandatory ...Done</pre>

10.2.6.2 Command delete

<p>Location</p> <pre>AS_CLI/System/CallP/GETS/ResourcePriorities</pre>
<p>Description</p> <p>This command is used to delete a recognized resource-priority value.</p>
<p>Syntax</p> <pre>delete <priorityValue>, String {5 to 80 characters}</pre>
<p>Parameters</p> <p>priorityValue: This parameter specifies a Resource-Priority r-value, which is constructed with a namespace, a dot, and a priority value, as per RFC 4412. For example, "ets.2". Values are case-insensitive.</p>
<p>Example</p> <pre>\$ AS_CLI/System/CallP/GETS/ResourcePriorities> delete ets.1 ...Done</pre>

10.2.6.3 Command set

<p>Location</p> <pre>AS_CLI/System/CallP/GETS/ResourcePriorities</pre>
<p>Description</p> <p>This command is used to modify a recognized resource-priority-related attributes.</p>
<p>Syntax</p> <pre>set <priorityValue>, String {5 to 80 characters} <attribute>, Multiple Choice = {newPriorityValue, priorityLevel, priorityClass} <newPriorityValue>, String {5 to 80 characters} <priorityLevel>, Integer {1 to 5} <priorityClass>, Choice = {GETS-Mandatory, GETS}</pre>

Parameters
<p>priorityValue: This parameter specifies a Resource-Priority r-value, which is constructed with a namespace, a dot, and a priority value, as per RFC 4412. For example, "ets.2". Values are case-insensitive.</p> <p>Attribute: The name of an attribute to modify.</p> <p>newPriorityValue: This parameter specifies the new Resource-Priority r-value.</p> <p>priorityLevel: This parameter specifies the maximum session priority level value that is attached to a session receiving this r-value. The effective priority level of a call session is the lowest 'priorityLevel' of all received r-value(s). It is used to determine the value of the Session-Priority AVP.</p> <p>priorityClass: This parameter determines which class the r-value belongs to. The value affects how RPH content is validated when invoking priority services. The values are:</p> <ul style="list-style-type: none"> - "GETS-Mandatory": Triggers Next-Generation Network (NGN) Government Emergency Telecommunications Service (GETS) priority services. At least one is required in this class to invoke GETS priority services. - "GETS": Triggers NGN Government Emergency Telecommunications Service (GETS) RPH validation.
Example
<pre>\$ AS_CLI/System/CallP/GETS/ResourcePriorities> set ets.0 priorityLevel 4 priorityClass GETS-Mandatory ...Done</pre>

10.2.6.4 Command get

Location
AS_CLI/System/CallP/GETS/ResourcePriorities
Description
This command is used to display all recognized resource-priority values and additional Next Generation Network (NGN) Government Emergency Telecommunications Service (GETS) related attributes.
Syntax
get Get takes no parameter.
Example
<pre>\$ AS_CLI/System/CallP/GETS/ResourcePriorities> get Priority Value Priority Level Priority Class ===== ets.2 2 GETS-Mandatory wps.1 1 GETS 2 entries found.</pre>

10.2.7 Adding Application Server SessionPriorityMap context

Location
AS_CLI/System/CallP/GETS/SessionPriorityMap
Description
This level is used to configure Government Emergency Telecommunications Service (GETS) Session Priority Map.

10.2.7.1 Command add

Location
AS_CLI/System/CallP/GETS/SessionPriorityMap
Description
This command is used to add a mapping between a service user's priority level and a Diameter Session-Priority Attribute Value Pair (AVP) value.

Syntax
<pre>add <priorityLevel>, Integer {1 to 5} <sessionPriorityValue>, Integer {0 to 4}</pre>
Parameters
<p>priorityLevel: This parameter specifies the session priority level.</p> <p>sessionPriorityValue: This parameter specifies the value of the Session-Priority AVP for outgoing Ro Diameter requests that result from INVITEs containing the associated resource priority values.</p>
Example
<pre>\$ AS_CLI/System/CallP/GETS/SessionPriorityMap> add 2 4 ...Done</pre>

10.2.7.2 Command delete

Location
AS_CLI/System/CallP/GETS/SessionPriorityMap
Description
This command is used to delete a mapping between a service user's priority level and a Diameter Session-Priority Attribute-Value Pair (AVP) value.
Syntax
<pre>delete <priorityLevel>, Integer {1 to 5}</pre>
Parameters
priorityLevel: This parameter specifies the session priority level to delete.
Example
<pre>\$ AS_CLI/System/CallP/GETS/SessionPriorityMap> delete 1 ...Done</pre>

10.2.7.3 Command set

Location
AS_CLI/System/CallP/GETS/SessionPriorityMap
Description
This command is used to modify an existing a mapping between a service user's priority level and a Diameter Session-Priority Attribute-Value Pair (AVP) value.
Syntax
<pre>set <priorityLevel>, Integer {1 to 5} <attribute>, Multiple Choice = {sessionPriorityValue} <sessionPriorityValue>, Integer {0 to 4}</pre>
Parameters
<p>priorityLevel: This parameter specifies the session priority level to modify.</p> <p>attribute: The name of an attribute to modify.</p> <p>sessionPriorityValue: This parameter specifies a new Session-Priority AVP for this priorityLevel.</p>
Example
<pre>\$ AS_CLI/System/CallP/GETS/SessionPriorityMapping> set 2 3 ...Done</pre>

10.2.7.4 Command get

Location
AS CLI/System/CallP/GETS/SessionPriorityMap
Description
This command is used to display all existing mappings between a service user's priority level and a Diameter Session-Priority Attribute-Value Pair (AVP) value.
Syntax
get Get takes no parameter.
Example
<pre> \$ AS_CLI/System/CallP/GETS/SessionPriorityMap> get Priority Level Session Priority Value ===== 2 4 1 3 2 entries found. </pre>

10.2.8 Adding Application Server InhibitedAVPCodes context

Location
AS CLI/System/CallP/GETS/InhibitedAVPCodes
Description
This level is used to configure Government Emergency Telecommunications Service (GETS) inhibited Attribute-Value Pair (AVP) codes.

10.2.8.1 Command add

Location
AS CLI/System/CallP/GETS/InhibitedAVPCodes
Description
This command is used to add a Diameter Attribute-Value Pair (AVP) combination to inhibit for Government Emergency Telecommunications Service (GETS)-NT calls. The AVP combination includes a diameter AVP and a vendor ID.
Syntax
<pre> add <avpCode>, Integer {0 to 2147483647} <vendorId>, Integer {0 to 2147483647} </pre>
Parameters
<pre> avpCode : This parameter specifies the diameter Attribute-Value Pair (AVP) code to inhibit. vendorId: This parameter specifies the vendor ID of the Diameter Attribute- Value Pair (AVP) to inhibit. </pre>
Example
<pre> \$ AS_CLI/System/CallP/GETS/InhibitedAVPCodes> add 121 6431 ...Done </pre>

10.2.8.2 Command delete

Location
AS CLI/System/CallP/GETS/InhibitedAVPCodes

Description
This command is used to remove an inhibited Diameter Attribute-Value Pair (AVP) combination for Government Emergency Telecommunications Service (GETS)-NT calls. The AVP combination includes a vendor ID and a diameter AVP.
Syntax
<pre>delete <avpCode>, Integer {0 to 2147483647} <vendorId>, Integer {0 to 2147483647}</pre>
Parameters
<p>avpCode : This parameter specifies the diameter Attribute-Value Pair (AVP) code to remove.</p> <p>vendorId: This parameter specifies the vendor ID of the Diameter Attribute-Value Pair (AVP).</p>
Example
<pre>\$ AS_CLI/System/CallP/GETS/InhibitedAVPCodes> delete 121 6431 ...Done</pre>

10.2.8.3 Command get

Location
AS_CLI/System/CallP/GETS/InhibitedAVPCodes
Description
This command is used to view the list of Diameter Attribute-Value Pairs (AVPs) that are inhibited for Government Emergency Telecommunications Service (GETS)-NT calls.
Syntax
<pre>get Get takes no parameter.</pre>
Example
<pre>\$ AS_CLI/System/CallP/GETS/InhibitedAVPCodes> get avpCode vendorId ===== 121 6431 874 10415 2 entries found.</pre>

10.2.9 Adding Application Server EmergencyCallDDoSProtection context

Location
AS_CLI/System/CallP/EmergencyCallDDoSProtection
Description
This level is used to view and modify the Emergency Call DDoS Protection mechanism. Under exceptionally intense emergency calling, it is possible that BroadWorks AS and/or NS servers are overloaded with emergency calls which are not rejected by the overload controls in the yellow or the red overload state. Under this intense calling, the servers may enter severe overload condition where emergency or GETS calls cannot be processed by the servers. To avoid reaching this severe overload condition, the Emergency Call DDoS Protection mechanism can be enabled and configured to allow the servers to drop emergency calls prior to servers entering this condition.

10.2.9.1 Command get

Location
AS_CLI/System/CallP/EmergencyCallDDoSProtection

Description
This command is used to view the Emergency Call DDoS Protection related attributes.
Syntax
get Get takes no parameter.
Example
<pre>AS_CLI/System/CallP/EmergencyCallDDoSProtection> get enabled = true protectionRate = 10 sampleInterval = 5 protectionAction = error</pre>

10.2.9.2 Command set

Location
AS_CLI/System/CallP/EmergencyCallDDoSProtection
Description
This command is used to modify the Emergency Call DDoS Protection related attributes.
Syntax
<pre>set <attribute>, Multiple Choice = {enabled, protectionRate, sampleInterval, protectionAction} <enabled>, Choice = {false, true} <protectionRate>, Integer {1 to 10000} <sampleInterval>, Integer {1 to 30} <protectionAction>, Choice = {error, decline, drop, redirect, unavailable}</pre>
Parameters
<pre>attribute : This parameter specifies the name of an attribute to modify. enabled : This parameter enables the emergency DDoS Protection mechanism. protectionRate : This parameter specifies the emergency calls per second rate that the server accepts before any new emergency calls are dropped. An incoming emergency call is dropped if the current emergency calls per second exceeds this configured threshold value. For a service provider concerned about the potential of a very high emergency call rate, the emergency protectionRate could be set around 1X of the AS capacity. sampleInterval : This parameter specifies the number of seconds used to calculate the emergency calls per second. The emergency calls per second is the average for this interval. Measuring the average call rate over the sample interval allows amortizing the effect of sporadic variations that may occur over shorter time interval. protectionAction: This parameter specifies the action to be performed when an emergency call is declined by the emergency DDoS Protection mechanism. The possible actions are: "redirect" (Respond to the message with "302 Moved Temporarily"), "error" (Respond to the message with "503 Service Unavailable"), "decline" (Respond to the message with 603 + Retry-After), "drop" (Do not respond) or "unavailable" (Respond to the message with 480 + Retry-After).</pre>
Example
<pre>AS_CLI/System/CallP/EmergencyCallDDoSProtection> set enabled true protectionRate 10 sampleInterval 10 protectionAction error</pre>

WARNING: The Protection Rate is a critical configuration parameter. Ensure that the value chosen meets your requirements for processing number of emergency calls per second and protecting the system from entering severe overload.

Do you wish to continue?

Please confirm (Yes, Y, No, N): y
...Done

10.2.9.3 Command clear

Location
AS_CLI/System/CallP/EmergencyCallDDoSProtection
Description
This command is used to clear the Emergency Call DDoS Protection protection rate.
Syntax
clear <attribute>, Multiple Choice = {protectionRate}
Parameters
attribute : This parameter specifies the name of an attribute to clear.
Example
AS_CLI/System/CallP/EmergencyCallDDoSProtection> clear protectionRate ...Done

10.2.10 Adding Network Server Numbers context

Location
NS_CLI/System/CallP/GETS/Numbers
Description
This level is used to configure GETS Access Number (GETS-AN) and GETS Number Translation (GETS-NT) numbers.

10.2.10.1 Command add

Location
NS_CLI/System/CallP/GETS/Numbers
Description
This command is used to define a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) numbers.
Syntax
add <number>, String {4 to 10 characters} <type>, Choice = {AN, NT} [<attribute>, Multiple Choice = {description}] <description>, String {1 to 80 characters}
Parameters

<p>number: The parameter represents a GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) string. This string matches with the Request-URI received user string to promote a regular call to a Government Emergency Telecommunications Service (GETS) call. 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). This parameter accepts a string of four to 10 characters, which may consist of 10 digits or three to nine digits completed by a wildcard star character (*). Note that if the Request-URI received is a SIP:URI without user=phone, user=phone error correction can be done depending on the userPhoneErrorCorrection parameter and that the E.164 format is supported. For matching against a provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) string, a successful match is detected when:</p> <ul style="list-style-type: none"> -The received user string contains at least ten digits. - The provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) has a wildcard, it matches the digits before the wildcard with the first digits of the received user string. For example a provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) value of "710*" will produce a positive match for all received user string "710xxxxxxx". -If the provisioned GETS Access Number (GETS-AN)/Number Translation (GETS-NT) does not have a wildcard, it matches all ten digits of the received user string. <p>type: This parameter specifies whether the number is considered as GETS Access Number (GETS-AN) or GET-NT.</p> <p>attribute: The GETS Access Number (GETS-AN)/Number Translation (GETS-NT) number.</p> <p>description: This parameter specifies a brief description of the GETS Access Number (GETS-AN)/Number Translation (GETS-NT) number.</p>
<p>Example</p> <pre>\$ NS_CLI/System/CallP/GETS/Numbers> add 7106274387 AN ...Done</pre>

10.2.10.2 Command delete

Location
NS CLI/System/CallP/GETS/Numbers
Description
This command is used to delete an existing GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) number.
Syntax
delete <number>, String {4 to 10 characters}
Parameters
number: This parameter specifies the Government Emergency Telecommunications Service (GETS) number to delete.
Example
<pre>\$ NS_CLI/System/CallP/GETS/Numbers> delete 7106274387 ...Done</pre>

10.2.10.3 Command set

Location
NS CLI/System/CallP/GETS/Numbers
Description
This command is used to modify an existing GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) number.
Syntax
set <number>, String {4 to 10 characters} <attribute>, Multiple Choice = {type, description}

<code><type>, Choice = {AN, NT}</code>	
<code><description>, String {1 to 80 characters}</code>	
Parameters	
number:	This parameter specifies the Government Emergency Telecommunications Service (GETS) number to modify.
attribute:	This parameter specifies the name of an attribute to modify.
type:	This parameter specifies the new type of the existing Government Emergency Telecommunications Service (GETS) number.
description:	This parameter specifies a new description for the existing Government Emergency Telecommunications Service (GETS) number.
Example	
<pre>\$ NS_CLI/System/CallP/GETS/Numbers> set 7106274387 newNumber 7106274388 type nt ...Done</pre>	

10.2.10.4 Command get

Location	
NS CLI/System/CallP/GETS/Numbers	
Description	
This command is used to display all existing GETS Access Number (GETS-AN) or GETS Number Translation (GETS-NT) numbers.	
Syntax	
get Get takes no parameter.	
Example	
<pre>\$ NS_CLI/System/CallP/GETS/Numbers> get Number Type Description ===== 7106665555 NT GETS-NT number 7106274387 AN GETS-AN number 2 entries found.</pre>	

10.2.10.5 Command clear

Location	
NS CLI/System/CallP/GETS/Numbers	
Description	
This command is used to clear (set to no value) GETS number-related attributes.	
Syntax	
<pre>clear <number>, String {4 to 10 characters} <attribute>, Multiple Choice = {description}</pre>	
Parameters	
number:	The directory number for which an attribute is to be cleared.
attribute:	The name of an attribute to clear.
Example	
<pre>\$ NS_CLI/System/CallP/GETS/Numbers> clear 7106665555 description ...Done</pre>	

10.2.11 Adding Network Server EmergencyCallIDDoSProtection context

Location	
NS CLI/System/CallP/EmergencyCallIDDoSProtection	

Description
This level is used to view and modify the Emergency Call DDoS Protection mechanism. Under exceptionally intense emergency calling, it is possible that BroadWorks AS and/or NS servers are overloaded with emergency calls which are not rejected by the overload controls in the yellow or the red overload state. Under this intense calling, the servers may enter severe overload condition where emergency or GETS calls cannot be processed by the servers. To avoid reaching this severe overload condition, the Emergency Call DDoS Protection mechanism can be enabled and configured to allow the servers to drop emergency calls prior to servers entering this condition.

10.2.11.1 Command get

Location
NS CLI/System/CallP/EmergencyCallDDoSProtection
Description
This command is used to view the Emergency Call DDoS Protection related attributes.
Syntax
get Get takes no parameter.
Example
NS_CLI/System/CallP/EmergencyCallDDoSProtection> get enabled = false protectionRate = 5 sampleInterval = 5 protectionAction = error

10.2.11.2 Command set

Location
NS CLI/System/CallP/EmergencyCallDDoSProtection
Description
This command is used to modify the Emergency Call DDoS Protection related attributes.
Syntax
Set <attribute>, Multiple Choice = {enabled, protectionRate, sampleInterval, protectionAction} <enabled>, Choice = {false, true} <protectionRate>, Integer {1 to 10000} <sampleInterval>, Integer {1 to 30} <protectionAction>, Choice = {drop, error}
Parameters
attribute : This parameter specifies the name of an attribute to modify. enabled : This parameter enables the emergency DDoS Protection mechanism. protectionRate : This parameter specifies the emergency calls per second rate that the server accepts before any new emergency calls are dropped. An incoming emergency call is dropped if the current emergency calls per second exceeds this configured threshold value. For a service provider concerned about the potential of a very high emergency call rate, the emergency ` could be set around 1X of the NS capacity. sampleInterval : This parameter specifies the number of seconds used to calculate the emergency calls per second. The emergency calls per second is the average for this interval. Measuring the average call rate over the sample interval allows amortizing the effect of sporadic variations that may occur over shorter time interval.

<p>protectionAction: This parameter specifies the action to be performed when an emergency call is declined by the emergency DDoS Protection mechanism. The possible actions are: "error" (Respond to the message with "503 Service Unavailable") or "drop" (Do not respond)</p>
<p>Example</p> <pre>NS_CLI/System/CallP/EmergencyCallDDoSProtection> set enabled true protectionRate 10 sampleInterval 10 protectionAction drop</pre> <p>WARNING: The Protection Rate is a critical configuration parameter. Ensure that the value chosen meets your requirements for processing number of emergency calls per second and protecting the system from entering severe overload.</p> <p>Do you wish to continue?</p> <p>Please confirm (Yes, Y, No, N): y ...Done</p>

10.2.11.3 Command clear

<p>Location</p>
<p>NS_CLI/System/CallP/EmergencyCallDDoSProtection</p>
<p>Description</p>
<p>This command is used to clear the Emergency Call DDoS Protection protection rate.</p>
<p>Syntax</p>
<pre>clear <attribute>, Multiple Choice = {protectionRate}</pre>
<p>Parameters</p>
<p>attribute : This parameter specifies the name of an attribute to clear.</p>
<p>Example</p>
<pre>NS_CLI/System/CallP/EmergencyCallDDoSProtection> clear protectionRate ...Done</pre>

10.3 Open Client Interface-Provisioning Impact

10.3.1 Application Server

10.3.1.1 Summary

The following new data types are created:

- GETSNumber
- GETSNumberDescription
- GETSNumberType
- GETSPriorityValue
- GETSPriorityClass
- GETSSignalingDSCP
- GETSCallIdentifierMode
- GETSPriorifyAVP

- GETSPriorityLevel
- GETSSessionPriority
- GETSReservedFeatureAccessCodeDescription
- SampleIntervallInSeconds
- ProtectionRate
- ProtectionAction

The following OCI commands are created:

- SystemGETSGetRequest
- SystemGETSModifyRequest
- SystemGETSReservedFeatureAccessCodeAddRequest
- SystemGETSReservedFeatureAccessCodeDeleteRequest
- SystemGETSReservedFeatureAccessCodeGetListRequest
- SystemGETSReservedFeatureAccessCodeModifyRequest
- SystemGETSNumberAddRequest
- SystemGETSNumberDeleteRequest
- SystemGETSNumberGetListRequest
- SystemGETSNumberModifyRequest
- SystemGETSResourcePriorityAddRequest
- SystemGETSResourcePriorityDeleteRequest
- SystemGETSResourcePriorityGetListRequest
- SystemGETSResourcePriorityModifyRequest
- SystemGETSSessionPriorityMapAddRequest
- SystemGETSSessionPriorityMapDeleteRequest
- SystemGETSSessionPriorityMapGetListRequest
- SystemGETSSessionPriorityMapModifyRequest
- SystemGETSAvpCodeMapAddRequest
- SystemGETSAvpCodeMapDeleteRequest
- SystemGETSAvpCodeMapGetListRequest
- SystemEmergencyCallDDoSProtectionGetRequest
- SystemEmergencyCallDDoSProtectionModifyRequest

10.3.1.2 Command Impacts

10.3.1.2.1 *GETSNumber*

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSNumber">
```

```

<xs:annotation>
  <xs:appinfo>
  </xs:appinfo>
  <xs:documentation>
    A string that represents a GETS-AN or GETS-NT number. It is composed of
    up to 10 digits or a minimum of 3 digits with a wildcard *.
  </xs:documentation>
</xs:annotation>
<xs:restriction base="xs:token">
  <xs:minLength value="4"/>
  <xs:maxLength value="10"/>
</xs:restriction>
</xs:simpleType>

```

10.3.1.2.2 GETSNumberDescription

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="GETSNumberDescription">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      GETS Reserved Number Description
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <xs:minLength value="1"/>
    <xs:maxLength value="80"/>
  </xs:restriction>
</xs:simpleType>

```

10.3.1.2.3 GETSCallIdentifierMode

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="GETSCallIdentifierMode">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      The GETS Call Identifier Mode.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <xs:enumeration value="Request-URI"/>
    <xs:enumeration value="RPH"/>
    <xs:enumeration value="RPH-Request-URI"/>
  </xs:restriction>
</xs:simpleType>

```

10.3.1.2.4 GETSNumberType

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="GETSNumberType">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      The GETS Reserved Number type.
      AN - GETS-AN
      NT - GETS-NT
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">

```

```
<xs:enumeration value="AN"/>
<xs:enumeration value="NT"/>
</xs:restriction>
</xs:simpleType>
```

10.3.1.2.5 GETSPriorityAVP

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSPriorityAVP">
  <xs:annotation>
    <xs:appinfo>
      </xs:appinfo>
    <xs:documentation>
      The GETS Diameter interface Session-Priority Attribute Value Pair (AVP).
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="0"/>
    <xs:maxInclusive value="4"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.6 GETSPriorityLevel

XML Schema file: *OCISchemaDataTypes.xsd*

```
<xs:simpleType name="GETSPriorityLevel">
  <xs:annotation>
    <xs:appinfo>
      </xs:appinfo>
    <xs:documentation>
      The GETS Priority level.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="5"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.7 GETSPriorityValue

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSPriorityValue">
  <xs:annotation>
    <xs:appinfo>
      </xs:appinfo>
    <xs:documentation>
      The GETS Priority value. It is composed of an r-value followed by a dot and a
      priority value.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <xs:minLength value="3"/>
    <xs:maxLength value="80"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.8 GETSPriorityClass

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSPriorityClass">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      The GETS r-value.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <xs:enumeration value="GETS-Mandatory"/>
    <xs:enumeration value="GETS"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.9 GETSSignalingDSCP

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSSignalingDSCP">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      The GETS signaling Differentiated Services Code Point (DSCP) value.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="0"/>
    <xs:maxInclusive value="63"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.10 GETSSessionPriority

XML Schema file: *OCISchemaDataTypes.xsd*

```
<xs:simpleType name="GETSSessionPriority">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
    <xs:documentation>
      The GETS Session Priority AVP value.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="0"/>
    <xs:maxInclusive value="4"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.1.2.11 GETSReservedFeatureAccessCodeDescription

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:simpleType name="GETSReservedFeatureAccessCodeDescription">
  <xs:annotation>
    <xs:appinfo>
    </xs:appinfo>
```

```

<xs:documentation>
  GETS Reserved FAC Description
</xs:documentation>
</xs:annotation>
<xs:restriction base="xs:token">
  <xs:minLength value="1"/>
  <xs:maxLength value="80"/>
</xs:restriction>
</xs:simpleType>

```

10.3.1.2.12 SampleIntervalInSeconds

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="SampleIntervalInSeconds">
  <xs:annotation>
    <xs:documentation>
      The number of seconds used to calculate the emergency calls per second.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="30"/>
  </xs:restriction>
</xs:simpleType>

```

10.3.1.2.13 ProtectionRate

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="ProtectionRate">
  <xs:annotation>
    <xs:documentation>
      This is the emergency calls per second rate that the server accepts before any new
      emergency calls are dropped.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:int">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="10000"/>
  </xs:restriction>
</xs:simpleType>

```

10.3.1.2.14 ProtectionAction

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:simpleType name="ProtectionAction">
  <xs:annotation>
    <xs:documentation>
      The action to take for SIP messages that are not processed during Emergency DDos.
      Decline      = Respond to the message with 603 + Retry-After
      Drop        = Do not respond
      Error       = Respond to the message with 503
      Redirect    = Respond to the message with 302
      Unavailable = Respond to the message with 480 + Retry-After
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <xs:enumeration value="Decline"/>
    <xs:enumeration value="Drop"/>
    <xs:enumeration value="Error"/>
  </xs:restriction>
</xs:simpleType>

```

```

<xs:enumeration value="Redirect"/>
<xs:enumeration value="Unavailable"/>
</xs:restriction>
</xs:simpleType>

```

10.3.1.2.15 SystemGETSGetRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSGetRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get the GETS system settings.
      The response is either SystemGETSGetResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSGetResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSGetRequest.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="enabled" type="xs:boolean"/>
        <xs:element name="enableRequireResourcePriority" type="xs:boolean"/>
        <xs:element name="sendAccessResourcePriority" type="xs:boolean"/>
        <xs:element name="callIdentifierMode" type="GETSCallIdentifierMode"/>
        <xs:element name="defaultPriorityAVP" type="GETSPriorifyAVP"/>
        <xs:element name="signalingDSCP" type="GETSSignalingDSCP"/>
        <xs:element name="defaultRValue" type="GETSPriorityValue"/>
        <xs:element name="bypassRoRelease" type="xs:boolean"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.16 SystemGETSModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
    </xs:appinfo>
  </xs:annotation>

```

```

    <xsDataModeSupported>>false</xsDataModeSupported>
  </xs:appinfo>
  <xs:documentation>
    Modify GETS system settings.
    The following elements are only used in AS data mode and ignored in the Amplify data
    mode:
      callIdentifierMode
    The response is either SuccessResponse or ErrorResponse.
  </xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="core:OCIRequest">
    <xs:sequence>
      <xs:element name="enabled" type="xs:boolean" minOccurs="0"/>
      <xs:element name="enableRequireResourcePriority" type="xs:boolean" minOccurs="0"/>
      <xs:element name="sendAccessResourcePriority" type="xs:boolean" minOccurs="0"/>
      <xs:element name="callIdentifierMode" type="GETSCallIdentifierMode" minOccurs="0"/>
      <xs:element name="defaultPriorityAVP" type="GETSPriorifyAVP" minOccurs="0"/>
      <xs:element name="signalingDSCP" type="GETSSignalingDSCP" minOccurs="0"/>
      <xs:element name="defaultRValue" type="GETSPriorityValue" minOccurs="0"/>
      <xs:element name="bypassRoRelease" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

```

10.3.1.2.17 SystemGETSReservedFeatureAccessCodeAddRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSReservedFeatureAccessCodeAddRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>true</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Add a GETS reserved FAC.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="code" type="FeatureAccessCode"/>
        <xs:element name="description" type="GETSReservedFeatureAccessCodeDescription"
minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.18 SystemGETSReservedFeatureAccessCodeDeleteRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSReservedFeatureAccessCodeDeleteRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>true</xsDataModeSupported>

```

```

</xs:appinfo>
<xs:documentation>
  Delete a GETS reserved FAC.
  The response is either SuccessResponse or ErrorResponse.
</xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="core:OCIRequest">
    <xs:sequence>
      <xs:element name="code" type="FeatureAccessCode"/>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

```

10.3.1.2.19 SystemGETSReservedFeatureAccessCodeGetListRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSReservedFeatureAccessCodeGetListRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>true</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get a list of GETS reserved FAC.
      The response is either SystemGETSReservedFeatureAccessCodeGetListResponse or
      ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSReservedFeatureAccessCodeGetListResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>true</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSReservedFeatureAccessCodeGetListRequest.
      The table columns are: "Code" and "Description".
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="reservedCodeTable" type="core:OCITable"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.20 SystemGETSReservedFeatureAccessCodeModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSReservedFeatureAccessCodeModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>true</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Modify a GETS reserved FAC.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="code" type="FeatureAccessCode"/>
        <xs:element name="newCode" type="FeatureAccessCode" minOccurs="0"/>
        <xs:element name="description" type="GETSReservedFeatureAccessCodeDescription"
nillable="true" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.21 SystemGETSNumberAddRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSNumberAddRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Add a GETS reserved Number.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="number" type="GETSNumber"/>
        <xs:element name="type" type="GETSNumberType"/>
        <xs:element name="description" type="GETSNumberDescription" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.22 SystemGETSNumberDeleteRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSNumberDeleteRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>

```

```

    <xsDataModeSupported>>false</xsDataModeSupported>
  </xs:appinfo>
  <xs:documentation>
    Delete a GETS reserved Number.
    The response is either SuccessResponse or ErrorResponse.
  </xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="core:OCIRequest">
    <xs:sequence>
      <xs:element name="number" type="GETSNumber"/>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

```

10.3.1.2.23 SystemGETSNumberGetListRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSNumberGetListRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get a list of GETS reserved Numbers.
      The response is either SystemGETSNumberGetListResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSNumberGetListResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSNumberGetListRequest.
      The table columns are: "Number", "Type" and "Description".
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="reservedNumberTable" type="core:OCITable"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.24 SystemGETSNumberModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSNumberModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Modify a GETS reserved Number.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="number" type="GETSNumber"/>
        <xs:element name="type" type="GETSNumberType" minOccurs="0"/>
        <xs:element name="description" type="GETSNumberDescription" nillable="true"
minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.25 SystemGETSResourcePriorityAddRequest

Authorization level: System

XML Schema file: OCISchemaSystem.xsd

```

<xs:complexType name="SystemGETSResourcePriorityAddRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Add a GETS Resource Priority.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="priorityValue" type="GETSPriorityValue"/>
        <xs:element name="priorityLevel" type="GETSPriorityLevel"/>
        <xs:element name="priorityClass" type="GETSPriorityClass"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.26 SystemGETSResourcePriorityDeleteRequest

Authorization level: System

XML Schema file: OCISchemaSystem.xsd

```

<xs:complexType name="SystemGETSResourcePriorityDeleteRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>

```

```

    <xsDataModeSupported>>false</xsDataModeSupported>
  </xs:appinfo>
  <xs:documentation>
    Delete a GETS Resource Priority.
    The response is either SuccessResponse or ErrorResponse.
  </xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="core:OCIRequest">
    <xs:sequence>
      <xs:element name="priorityValue" type="GETSPriorityValue"/>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

```

10.3.1.2.27 SystemGETSResourcePriorityGetListRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemGETSResourcePriorityGetListRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get a list of GETS Resource Priorities.
      The response is either SystemGETSResourcePriorityGetListResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSResourcePriorityGetListResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>>true</asDataModeSupported>
      <amplifyDataModeSupported>>true</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSResourcePriorityGetListRequest.
      The table columns are: "Priority Value", "Priority Level" and "Priority Class".
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="resourcePriorityTable" type="core:OCITable"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.28 SystemGETSResourcePriorityModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSResourcePriorityModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Modify a GETS reserved Resource Priority.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="priorityValue" type="GETSPriorityValue"/>
        <xs:element name="newPriorityValue" type="GETSPriorityValue" minOccurs="0"/>
        <xs:element name="priorityLevel" type="GETSPriorityLevel" minOccurs="0"/>
        <xs:element name="priorityClass" type="GETSPriorityClass" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.29 SystemGETSSessionPriorityMapAddRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSSessionPriorityMapAddRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Add a GETS Session Priority map. It maps a priority level with a session priority AVP value.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="priorityLevel" type="GETSPriorityLevel"/>
        <xs:element name="sessionPriority" type="GETSSessionPriority"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.30 SystemGETSSessionPriorityMapDeleteRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSSessionPriorityMapDeleteRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Delete a GETS Session Priority map.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="priorityLevel" type="GETSPriorityLevel"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.31 SystemGETSSessionPriorityMapGetListRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSSessionPriorityMapGetListRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get a list of GETS Session Priority maps.
      The response is either SystemGETSSessionPriorityMapGetListResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSSessionPriorityMapGetListResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSSessionPriorityMapGetListRequest.
      The table columns are: "Priority Level" and "Session Priority Value".
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="sessionPriorityTable" type="core:OCITable"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

```
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

10.3.1.2.32 SystemGETSSessionPriorityMapModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSSessionPriorityMapModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Modify a GETS Session Priority Map.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="priorityLevel" type="GETSPriorityLevel"/>
        <xs:element name="sessionPriority" type="GETSSessionPriority" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.33 SystemGETSAvpCodeMapAddRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSAvpCodeMapAddRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Add a GETS AVP Code map at the system level. It maps a Diameter AVP Code with a
      vendor ID for.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="avpCode" type="xs:int"/>
        <xs:element name="vendorId" type="xs:int"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.34 SystemGETSAvpCodeMapDeleteRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSAvpCodeMapDeleteRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Delete a system GETS AVP Code map.
      The response is either SuccessResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
        <xs:element name="avpCode" type="xs:int"/>
        <xs:element name="vendorId" type="xs:int"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

10.3.1.2.35 SystemGETSAvpCodeMapGetListRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```
<xs:complexType name="SystemGETSAvpCodeMapGetListRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get a list of GETS AVP Code Maps at the system level.
      The response is either SystemGETSAvpCodeMapGetListResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest"/>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemGETSAvpCodeMapGetListResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>true</amplifyDataModeSupported>
      <xsDataModeSupported>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to SystemGETSAvpCodeMapGetListRequest.
      The table columns are: "AVP Code" and "Vendor ID".
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="avpCodeTable" type="core:OCITable"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

```

</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

```

10.3.1.2.36 SystemEmergencyCallDDoSProtectionGetRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemEmergencyCallDDoSProtectionGetRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>>false</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Get the system Emergency Call DDos Protection configurations.
      The response is either SystemEmergencyCallDDoSProtectionGetResponse or ErrorResponse.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIRequest">
      <xs:sequence>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="SystemEmergencyCallDDoSProtectionGetResponse">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>>false</amplifyDataModeSupported>
      <xsDataModeSupported>>false</xsDataModeSupported>
    </xs:appinfo>
    <xs:documentation>
      Response to the SystemEmergencyCallDDoSProtectionGetRequest.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="core:OCIDataResponse">
      <xs:sequence>
        <xs:element name="enabled" type="xs:boolean"/>
        <xs:element name="sampleIntervalSeconds" type="SampleIntervalInSeconds"/>
        <xs:element name="protectionRate" type="ProtectionRate" minOccurs="0"/>
        <xs:element name="protectionAction" type="ProtectionAction"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

10.3.1.2.37 SystemEmergencyCallDDoSProtectionModifyRequest

Authorization level: System

XML Schema file: *OCISchemaSystem.xsd*

```

<xs:complexType name="SystemEmergencyCallDDoSProtectionModifyRequest">
  <xs:annotation>
    <xs:appinfo>
      <asDataModeSupported>true</asDataModeSupported>
      <amplifyDataModeSupported>>false</amplifyDataModeSupported>

```

```
<xsDataModeSupported>>false</xsDataModeSupported>
</xs:appinfo>
<xs:documentation>
  Modify the Emergency Call DDos Protection settings.
  The response is either SuccessResponse or an ErrorResponse.
</xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="core:OCIRequest">
    <xs:sequence>
      <xs:element name="enabled" type="xs:boolean" minOccurs="0"/>
      <xs:element name="sampleIntervalSeconds" type="SampleIntervalInSeconds"
minOccurs="0"/>
      <xs:element name="protectionRate" type="ProtectionRate" nillable="true"
minOccurs="0"/>
      <xs:element name="protectionAction" type="ProtectionAction" minOccurs="0"/>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>
```

10.3.1.3 Deprecated Commands

There is no impact.

10.3.1.4 Reporting Impacts

There is no impact.

10.4 External Authentication Impacts

There is no impact.

10.5 Application Server Portal API Impacts

There is no impact.

10.6 Network Server Location API Impacts

There is no impact.

10.7 NSSync API Impacts

There is no impact.

10.8 Application Server Dump Impacts

There is no impact.

10.9 BroadCloud Dump Impacts

There is no impact.

10.10 Service License Reporting Impact

There is no impact.

10.11 Treatments

There is no impact..

10.12 Media Announcements (Audio and Video)

There is no impact.

10.13 BroadWorks Common Communication Transport Impacts

There is no impact.

10.14 Device Management Impacts

There is no impact.

11 Accounting Impacts

11.1 Summary of Changes

This feature uses Accounting interface changes introduced by Execution Server (XS) feature implementations.

These existing CDR Fields are now used for the Application Server:

- 378 gets
- 443 getsOriginationType

The Session-Priority AVP value sent over the Diameter Ro interface in the CCR requests for GETS calls is modified. The value of the Session-Priority AVP is now derived from the Session Priority Mappings configuration as described in [5.8.2.1 Session Priority Value](#).

A new option has been added to bypass the release of GETS/eMPS calls, effectively ignoring any indication received in an ASR or CCA that would result in the release of the call (see section [5.8.2.2 Ro Interface Bypass](#)).

11.2 Generation of Accounting Records

There is no impact.

11.3 Impact to Accounting Fields (CDR)

The fields described in this section already exist and are now used by the Application Server.

11.3.1 GETS (378)

Field ID	378
Failover ID	N/A
Module	IP
Feature	191436
Release	Release 20.0
Radius Dictionary	BWAS-Gets
CLI Name	gets
XML Tag	gets
Service Name	N/A
Length	3
Example Data	Yes
Description	This field is only present for GETS calls. If present, its value is "Yes".

11.3.2 getsOriginationType (443)

Field ID	443
Failover ID	N/A
Module	IP
Feature	8290
Release	R22.0
Radius Dictionary	BWAS-GETS-OriginationType
CLI Name	getsOriginationType
XML Tag	getsOriginationType
Service Name	N/A
Length	15
Example Data	GETSFCAN
Description	This field captures the GETS origination type ("GETSFC", "GETSAN", "GETSNT", "GETSFCAN", "GETSFCNT", "UnknownGETS", "GETS") of a GETS origination session. "UnknownGETS" is not used by Application Server deployments. "GETS" is not used by Execution Dataless deployments.

11.4 Original Called Reason and Redirection Reason

This is not applicable.

11.5 Related Call ID

This is not applicable.

11.6 Example

The following is an XML example that highlights the *GETS* fields in **bold**.

```

<cdrData>
  <headerModule>
    <recordId>
      <eventCounter>21</eventCounter>
      <systemId>DEFAULT</systemId>
      <date>20050225000257.327</date>
      <systemTimeZone>0-050000</systemTimeZone>
    </recordId>
    <serviceProvider>MtlASDev</serviceProvider>
    <type>Normal</type>
  </headerModule>
  <basicModule>
    <userNumber>+15146982500</userNumber>
    <direction>Originating</direction>
    <callingNumber>+15146982500</callingNumber>
  <callingPresentationIndicator>Public
    </callingPresentationIndicator>
    <dialedDigits>3331111603</dialedDigits>
    <calledNumber>3331111603</calledNumber>
  <networkTranslatedNumber>+13331111603
    </networkTranslatedNumber>
    <startTime>20050225000257.327</startTime>
    <userTimeZone>0-050000</userTimeZone>

```

```
<localCallId>17:0</localCallId>
<answerIndicator>Yes</answerIndicator>
<answerTime>20050225000328.111</answerTime>
<releaseTime>20050225000341.771</releaseTime>
<terminationCause>016</terminationCause>
<callCategory>private</callCategory>
<networkCallType>lo</networkCallType>
<chargeIndicator>y</chargeIndicator>
<typeOfNetwork>public</typeOfNetwork>
<b>releasingParty>remote</b><b>releasingParty>
<userId>userea@bruno-2.mtl.broadsoft.com</userId>
</basicModule>
<centrexModule>
  <group>Cisco1_as2</group>
</centrexModule>
<ipModule>
  <route>192.168.8.111:5060</route>
  <networkCallID>BW190302244240205523783712@192.168.8.111
    </networkCallID>
  <codec>PCMU/8000/1</codec>
  <b>gets>Yes</b></gets>
  <b>getsOriginationType>GETSAN</b></getsOriginationType>
  <accessDeviceAddress>192.168.13.30
    </accessDeviceAddress>
</ipModule>
</cdrData>
```

12 System Management Impacts

12.1 Performance Management Impacts

12.1.1 New Counters

12.1.1.1 AS System Counters

12.1.1.1.1 Attempted GETS Call Validation

Name:	bwCallpGETSOrigValidationAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS call with GETS namespaces or a provisioned Request-URI.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a SIP message has a resource priority header with GETS namespaces (ets, wps) and/or the request URI is a known GETS number for a user of this system.

Name:	bwCallpGETSTermValidationAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to terminate a GETS call with GETS namespaces.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a SIP INVITE has a resource priority header with GETS namespaces (ets, wps) for a user of this system.

12.1.1.1.2 Invalid Resource-Priority Sent

Name:	bwCallpGETSOrigInvalidRPHSent
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks refuses a GETS call with a SIP 400 or SIP 417 error for a user of this system has attempted to originate a GETS call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks refuses a GETS call with SIP 400 or SIP 417 for a user of this system.

Name:	bwCallpGETSTermInvalidRPHSent
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks refuses a GETS call with a SIP 400 or SIP 417 error for a terminating GETS call for a user of this system.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks refuses a GETS call with SIP 400 or SIP 417 for a user of this system.

12.1.1.1.3 Ignore Resource-Priority

Name:	bwCallpGETSOrigIgnoreRPH
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS originating call for a user of this system.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS call for a user of this system.

Name:	bwCallpGETSTermIgnoreRPH
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS terminating call for a user of this system.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS call for a user of this system.

12.1.1.1.4 Invalid Resource-Priority Received

Name: bwCallpGETSOrigFCInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSOrigANInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSOrigNTInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSOrigFCANInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSOrigFCNTInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSOrigGETSInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a unknown GETS call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

Name: bwCallpGETSTermInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times Cisco BroadWorks receives a SIP 417 or SIP 420 error for a downstream functional element for a terminating GETS call for a user of this system. This happens only for terminating call sessions.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this system.

12.1.1.1.5 Attempted GETS Calls

Name: bwCallpGETSOrigFCAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSOrigANAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSOrigNTAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSOrigFCANAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSOrigFCNTAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSOrigGETSAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS origination of unknown type is processed for a user of this system and is sent to a subsequent functional element.

Name: bwCallpGETSTermAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of terminating GETS call attempts for a user of this system.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination is successfully processed for a user of this system and is sent to a subsequent functional element.

12.1.1.1.6 Answered GETS Calls

Name: bwCallpGETSOrigFCAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this system results in the call being answered.

Name: bwCallpGETSOrigANAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this system results in the call being answered.

Name: bwCallpGETSOrigNTAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination for a user of this system results in the call being answered.

Name: bwCallpGETSOrigFCANAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being answered.

Name: bwCallpGETSOrigFCNTAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being answered.

Name: bwCallpGETSOrigAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a unknown GETS origination for a user of this system results in the call being answered.

Name:	bwCallpGETSTermAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this system results in the call being answered.

12.1.1.1.7 Cancel GETS Calls

Name:	bwCallpGETSOrigFCCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this system results in the call being answered.

Name:	bwCallpGETSOrigANCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this system results in the call being canceled.

Name:	bwCallpGETSOrigNTCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this system results in the call being canceled.

Name: bwCallpGETSOrigFCANCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being canceled.

Name: bwCallpGETSOrigFCNTCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being canceled.

Name: bwCallpGETSOrigCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a unknown GETS origination for a user of this system results in the call being canceled.

Name: bwCallpGETSTermCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this system results in the call being canceled.

12.1.1.1.8 Ringing Timeout GETS Calls

Name:	bwCallpGETSOrigFCRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this system results in the call ringing but being timed out.
Name:	bwCallpGETSOrigANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this system results in the call ringing but being timed out.
Name:	bwCallpGETSOrigNTRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this system results in the call ringing but being timed out.
Name:	bwCallpGETSOrigFCANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call ringing but being timed out.

Name: bwCallpGETSOrigFCNTRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call ringing but being timed out.

Name: bwCallpGETSOrigRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this system results in the call ringing but being timed out.

Name: bwCallpGETSTermRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this system results in the call ringing but being timed out.

12.1.1.1.9 Declined GETS Calls

Name: bwCallpGETSOrigFCDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this system results in the call being declined.

Name: bwCallpGETSOrigANDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this system results in the call being declined.

Name: bwCallpGETSOrigNTDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination for a user of this system results in the call being declined (SIP 603).

Name: bwCallpGETSOrigFCANDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being declined.

Name: bwCallpGETSOrigFCNTDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being declined.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being declined.

Name: bwCallpGETSOrigDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this system results in the call being declined (SIP 603).

Name: bwCallpGETSTermDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this system results in the call being declined.

12.1.1.1.10Forbidden GETS Calls

Name: bwCallpGETSOrigFCForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call being forbidden (SIP 403).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this system results in the call being forbidden.

Name: bwCallpGETSOrigANForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this system results in the call being forbidden.

Name: bwCallpGETSOrigNTForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination for a user of this system results in the call being forbidden.

Name: bwCallpGETSOrigFCANForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being forbidden.

Name: bwCallpGETSOrigFCNTForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being forbidden.

Name: bwCallpGETSOrigForbidden
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being forbidden (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this system results in the call being forbidden.

Name:	bwCallpGETSTermForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call being forbidden (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this system results in the call being forbidden.

12.1.1.1.11 Busy GETS Calls

Name:	bwCallpGETSOrigFCBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this system results in the call being busy.

Name:	bwCallpGETSOrigANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this system results in the call being busy.

Name:	bwCallpGETSOrigNTBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this system results in the call being busy.

Name:	bwCallpGETSOrigFCANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being busy.

Name:	bwCallpGETSOrigFCNTBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being busy.

Name:	bwCallpGETSOrigBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this system results in the call being busy.

Name:	bwCallpGETSTermBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this system results in the call being busy.

12.1.1.1.12 Unreachable GETS Calls

Name:	bwCallpGETSOrigFCUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this system results in the call being unreachable.
Name:	bwCallpGETSOrigANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this system results in the call being unreachable.
Name:	bwCallpGETSOrigNTUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this system results in the call being unreachable.
Name:	bwCallpGETSOrigFCANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being unreachable.

Name: bwCallpGETSOrigFCNTUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being unreachable.

Name: bwCallpGETSOrigUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this system results in the call being unreachable.

Name: bwCallpGETSTermUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this system results in the call being unreachable.

12.1.1.1.13 Timed-Out GETS Calls

Name: bwCallpGETSOrigFCTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSOrigANTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSOrigNTTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSOrigFCANTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSOrigFCNTTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSOrigTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this system results in the call being timed out by destination.

Name: bwCallpGETSTermTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this system has attempted to terminate a GETS call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this system results in the call being timed out by destination.

12.1.1.1.14 Emergency Call DDoS Protection Counter

Name: bwCallpEmergencyCallDropped
MIB: BW-Execution.mib
Module: enterprises.broadsoft.applicationServer.callpModule.callpStats
Description: This counter tracks the number of times that the server rejects an emergency call due the emergency call throttling mechanism.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an emergency call is rejected due to the emergency call DDoS protection mechanism.

Name: bwCallpEmergencyCallsPerSecond
MIB: BW-Execution.mib
Module: enterprises.broadsoft.applicationServer.callpModule.callpStats
Description: This gauge measures the rate at which emergency origination attempts occur. It uses the timestamps of up to the last 100 emergency origination attempts in calculating the rate.
Type: Gauge32
Access: Read-only

12.1.1.2 AS Service Provider Counters

12.1.1.2.1 Attempted GETS Call Validation

Name:	bwCallpGETSSPOrigValidationAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call with GETS namespaces or a provisioned Request-URI.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a SIP message has a resource priority header with GETS namespaces (ets, wps) and/or the request URI is a known GETS number for a user of this service provider.

12.1.1.2.2 Invalid Resource-Priority Sent

Name:	bwCallpGETSSPOrigInvalidRPHSent
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks refuses a originating GETS call with a SIP 400 or SIP 417 error for a user of this service provider has attempted to originate a GETS call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks refuses a GETS call with SIP 400 or SIP 417 for a user of this service provider.

12.1.1.2.3 Ignore Resource-Priority

Name:	bwCallpGETSSPOrigIgnoreRPH
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks ignores a valid Resource Priority header received for an established originating non-GETS call for a user of this service provider.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS call for a user of this service provider.

12.1.1.2.4 Invalid Resource-Priority Received

Name:	bwCallpGETSSPOrigFCInvalidRPHReceived
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name:	bwCallpGETSSPOrigANInvalidRPHReceived
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name:	bwCallpGETSSPOrigNTInvalidRPHReceived
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name:	bwCallpGETSSPOrigFCANInvalidRPHReceived
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name: bwCallpGETSSPOrigFCNTInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name: bwCallpGETSSPOrigGETSInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a unknown GETS call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

Name: bwCallpGETSSPTermInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times Cisco BroadWorks receives a SIP 417 or SIP 420 error for a downstream functional element for a terminating GETS call for a user of this service provider.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this service provider.

12.1.1.2.5 Attempted GETS Calls

Name: bwCallpGETSSPOrigFCAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPOrigANAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPOrigNTAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPOrigFCANAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPOrigFCNTAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPOrigGETSAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type..
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS origination of unknown type is processed for a user of this service provider and is sent to a subsequent functional element.

Name: bwCallpGETSSPTermAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of terminating GETS call attempts for a user of this service provider.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination is successfully processed for a user of this service provider.

12.1.1.2.6 Answered GETS Calls

Name: bwCallpGETSSPOrigFCAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being answered.

Name: bwCallpGETSSPOrigANAnswered
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call being answered.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPOrigNTAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPOrigFCANAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPOrigFCNTAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPOrigAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a unknown GETS origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPTermAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this service provider results in the call being answered.

12.1.1.2.7 Cancel GETS Calls

Name:	bwCallpGETSSPOrigFCCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being answered.

Name:	bwCallpGETSSPOrigANCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being canceled.

Name:	bwCallpGETSSPOrigNTCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being canceled.

Name: bwCallpGETSSPOrigFCANCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being canceled.

Name: bwCallpGETSSPOrigFCNTCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being canceled.

Name: bwCallpGETSSPOrigCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a unknown GETS origination for a user of this service provider results in the call being canceled.

Name: bwCallpGETSSPTermCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this service provider results in the call being canceled.

12.1.1.2.8 Ringing Timeout GETS Calls

Name:	bwCallpGETSSPOrigFCRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call ringing but being timed out.

Name:	bwCallpGETSSPOrigANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call ringing but being timed out.

Name:	bwCallpGETSSPOrigNTRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call ringing but being timed out.

Name:	bwCallpGETSSPOrigFCANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call ringing but being timed out.

Name: bwCallpGETSSPOrigFCNTRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call ringing but being timed out.

Name: bwCallpGETSSPOrigRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call ringing but being timed out.

Name: bwCallpGETSSPTermRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this service provider results in the call ringing but being timed out.

12.1.1.2.9 Declined GETS Calls

Name: bwCallpGETSSPOrigFCDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being declined.

Name: bwCallpGETSSPOrigANDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being declined.

Name: bwCallpGETSSPOrigNTDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being declined (SIP 603).

Name: bwCallpGETSSPOrigFCANDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being declined.

Name: bwCallpGETSSPOrigFCNTDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being declined.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being declined.

Name:	bwCallpGETSSPOrigDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call being declined (SIP 603).

Name:	bwCallpGETSSPTermDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this service provider results in the call being declined.

12.1.1.2.10Forbidden GETS Calls

Name:	bwCallpGETSSPOrigFCForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPOrigANForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPOrigNTForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPOrigFCANForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPOrigFCNTForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPOrigForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being forbidden (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call being forbidden.

Name:	bwCallpGETSSPTermForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call being forbidden (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this service provider results in the call being forbidden.

12.1.1.2.11 Busy GETS Calls

Name:	bwCallpGETSSPOrigFCBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPOrigANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPOrigNTBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPOrigFCANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPOrigFCNTBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPOrigBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call being busy.

Name:	bwCallpGETSSPTermBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this service provider results in the call being busy.

12.1.1.2.12 Unreachable GETS Calls

Name:	bwCallpGETSSPOrigFCUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being unreachable.
Name:	bwCallpGETSSPOrigANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being unreachable.
Name:	bwCallpGETSSPOrigNTUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being unreachable.
Name:	bwCallpGETSSPOrigFCANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being unreachable.

Name: bwCallpGETSSPOrigFCNTUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being unreachable.

Name: bwCallpGETSSPOrigUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call being unreachable.

Name: bwCallpGETSSPTermUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this service provider results in the call being unreachable.

12.1.1.2.13 Timed-Out GETS Calls

Name: bwCallpGETSSPOrigFCTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPOrigANTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPOrigNTTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPOrigFCANTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPOrigFCNTTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPOrigTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this service provider results in the call being timed out by destination.

Name:	bwCallpGETSSPTermTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this service provider has attempted to terminate a GETS call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this service provider results in the call being timed out by destination.

12.1.1.3 AS Group Counters

12.1.1.3.1 Attempted GETS Call Validation

Name:	bwCallpGETSGroupOrigValidationAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call with GETS namespaces or a provisioned Request-URI.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a SIP message has a resource priority header with GETS namespaces (ets, wps) and/or the request URI is a known GETS number for a user of this group.

12.1.1.3.2 Invalid Resource-Priority Sent

Name:	bwCallpGETSGroupOrigInvalidRPHSent
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks refuses an originating GETS call with a SIP 400 or SIP 417 error for a user of this group has attempted to originate a GETS call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks refuses a GETS call with SIP 400 or SIP 417 for a user of this group.

12.1.1.3.3 Ignore Resource-Priority

Name:	bwCallpGETSGroupOrigIgnoreRPH
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times Cisco BroadWorks ignores a valid Resource Priority header received for an established originating non-GETS call for a user of this group.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks ignores a valid Resource Priority header received for an established non-GETS call for a user of this group.

12.1.1.3.4 Invalid Resource-Priority Received

Name:	bwCallpGETSGroupOrigFCInvalidRPHReceived
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupOrigANInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupOrigNTInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupOrigFCANInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupOrigFCNTInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupOrigGETSInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a unknown GETS call and that it resulted in the call being rejected with a SIP 417 or SIP 420 error for a downstream functional element
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

Name: bwCallpGETSGroupTermInvalidRPHReceived
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times Cisco BroadWorks receives a SIP 417 or SIP 420 error for a downstream functional element for a terminating GETS call for a user of this group.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time Cisco BroadWorks receives a SIP 417 or a SIP SIP 420 for a GETS call for a user of this group.

12.1.1.3.5 Attempted GETS Calls

Name: bwCallpGETSGroupOrigFCAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination is processed for a user of this group and is sent to a subsequent functional element.

Name: bwCallpGETSGroupOrigANAttempts
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination is processed for a user of this group and is sent to a subsequent functional element.

Name:	bwCallpGETSGroupOrigNTAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination is processed for a user of this group and is sent to a subsequent functional element.

Name:	bwCallpGETSGroupOrigFCANAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination is processed for a user of this group and is sent to a subsequent functional element.

Name:	bwCallpGETSGroupOrigFCNTAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination is processed for a user of this group and is sent to a subsequent functional element.

Name:	bwCallpGETSGroupOrigGETSAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type..
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS origination of unknown type is processed for a user of this group and is sent to a subsequent functional element.

Name:	bwCallpGETSGroupTermAttempts
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of terminating GETS call attempts for a user of this group.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination is successfully processed for a user of this group.

12.1.1.3.6 Answered GETS Calls

Name:	bwCallpGETSGroupOrigFCAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigANAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigNTAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigFCANAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigFCNTAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a unknown GETS origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupTermAnswered
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call being answered.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this group results in the call being answered.

12.1.1.3.7 Cancel GETS Calls

Name:	bwCallpGETSGroupOrigFCCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this group results in the call being answered.

Name:	bwCallpGETSGroupOrigANCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call being canceled.

Name:	bwCallpGETSGroupOrigNTCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being canceled.

Name:	bwCallpGETSGroupOrigFCANCanceled
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being canceled by the caller.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being canceled.

Name: bwCallpGETSGroupOrigFCNTCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being canceled.

Name: bwCallpGETSGroupOrigCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a unknown GETS origination for a user of this group results in the call being canceled.

Name: bwCallpGETSGroupTermCanceled
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call being canceled by the caller.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this group results in the call being canceled.

12.1.1.3.8 Ringing Timeout GETS Calls

Name: bwCallpGETSGroupOrigFCRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this group results in the call ringing but being timed out.

Name:	bwCallpGETSGroupOrigANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call ringing but being timed out.

Name:	bwCallpGETSGroupOrigNTRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call ringing but being timed out.

Name:	bwCallpGETSGroupOrigFCANRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call ringing but being timed out.

Name:	bwCallpGETSGroupOrigFCNTRingingTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call ringing but being timed out.

Name: bwCallpGETSGroupOrigRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this group results in the call ringing but being timed out.

Name: bwCallpGETSGroupTermRingingTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call ringing but being timed out by Cisco BroadWorks.
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this group results in the call ringing but being timed out.

12.1.1.3.9 Declined GETS Calls

Name: bwCallpGETSGroupOrigFCDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this group results in the call being declined.

Name: bwCallpGETSGroupOrigANDeclined
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call being declined (SIP 603).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this group results in the call being declined.

Name:	bwCallpGETSGroupOrigNTDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being declined (SIP 603).

Name:	bwCallpGETSGroupOrigFCANDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being declined.

Name:	bwCallpGETSGroupOrigFCNTDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being declined.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being declined.

Name:	bwCallpGETSGroupOrigDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this group results in the call being declined (SIP 603).

Name:	bwCallpGETSGroupTermDeclined
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call being declined (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this group results in the call being declined.

12.1.1.3.10Forbidden GETS Calls

Name:	bwCallpGETSGroupOrigFCForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupOrigANForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupOrigNTForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupOrigFCANForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupOrigFCNTForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call being forbidden (SIP 403).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupOrigForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call being forbidden (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this group results in the call being forbidden.

Name:	bwCallpGETSGroupTermForbidden
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call being forbidden (SIP 603).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this group results in the call being forbidden.

12.1.1.3.11 Busy GETS Calls

Name:	bwCallpGETSGroupOrigFCBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC origination for a user of this group results in the call being busy.
Name:	bwCallpGETSGroupOrigANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call being busy.
Name:	bwCallpGETSGroupOrigNTBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being busy.
Name:	bwCallpGETSGroupOrigFCANBusy
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being busy.

Name: bwCallpGETSGroupOrigFCNTBusy
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being busy.

Name: bwCallpGETSGroupOrigBusy
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this group results in the call being busy.

Name: bwCallpGETSGroupTermBusy
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call destination being busy (SIP 406 or SIP 600).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this group results in the call being busy.

12.1.1.3.12 Unreachable GETS Calls

Name: bwCallpGETSGroupOrigFCUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this group results in the call being unreachable.

Name:	bwCallpGETSGroupOrigANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-AN origination for a user of this group results in the call being unreachable.

Name:	bwCallpGETSGroupOrigNTUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being unreachable.

Name:	bwCallpGETSGroupOrigFCANUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being unreachable.

Name:	bwCallpGETSGroupOrigFCNTUnreachable
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination being unreachable (SIP 503).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being unreachable.

Name: bwCallpGETSGroupOrigUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time an unknown GETS origination for a user of this group results in the call being unreachable.

Name: bwCallpGETSGroupTermUnreachable
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call destination being unreachable (SIP 503).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS termination for a user of this group results in the call being unreachable.

12.1.1.3.13 Timed-Out GETS Calls

Name: bwCallpGETSGroupOrigFCTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-FC call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-FC origination for a user of this group results in the call being timed out by destination.

Name: bwCallpGETSGroupOrigANTimeout
MIB: BW-Execution.mib
Module: enterprises.broadsoft.broadworks.executionServer.services.gets
Description: This counter tracks the number of times a user of this group has attempted to originate a GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type: Counter32
Access: read/write
Incremented: This counter is incremented each time a GETS-AN origination for a user of this group results in the call being timed out by destination.

Name:	bwCallpGETSGroupOrigNTTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-NT origination for a user of this group results in the call being timed out by destination.

Name:	bwCallpGETSGroupOrigFCANTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-AN call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-AN origination for a user of this group results in the call being timed out by destination.

Name:	bwCallpGETSGroupOrigFCNTTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS-FC + GETS-NT call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS-FC + GETS-NT origination for a user of this group results in the call being timed out by destination.

Name:	bwCallpGETSGroupOrigTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to originate a GETS call of unknown GETS type and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an unknown GETS origination for a user of this group results in the call being timed out by destination.

Name:	bwCallpGETSGroupTermTimeout
MIB:	BW-Execution.mib
Module:	enterprises.broadsoft.broadworks.executionServer.services.gets
Description:	This counter tracks the number of times a user of this group has attempted to terminate a GETS call and that it resulted in the call destination returning a timeout message (SIP 408 or SIP 504).
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time a GETS termination for a user of this group results in the call being timed out by destination.

12.1.1.4 NS System Counters

12.1.1.4.1 Emergency Call DDoS Protection Counter

Name:	bwCallpEmergencyCallDropped
MIB:	BW-NSExecution.mib
Module:	enterprises.broadsoft.nsExecutionServer.processing
Description:	This counter tracks the number of times that the server rejects an emergency call due the emergency call throttling mechanism.
Type:	Counter32
Access:	read/write
Incremented:	This counter is incremented each time an emergency call is rejected due to the emergency call DDoS protection mechanism.

Name:	bwCallpEmergencyCallsPerSecond
MIB:	BW-NSExecution.mib
Module:	enterprises.broadsoft.nsExecutionServer.processing
Description:	This gauge measures the rate at which emergency origination attempts occur. It uses the timestamps of up to the last 100 emergency origination attempts in calculating the rate.
Type:	Gauge32
Access:	Read-only

12.1.2 Modified Counters

There is no impact.

12.1.3 Deleted Counters or Module

There is no impact.

12.1.4 Counters Polled by Network Monitoring

There is no impact.

12.2 Fault Management Impacts

There are no impacts.

12.3 Scripts and Tools

There is no impact.

12.4 EMS Integration Impacts

There is no impact.

13 Execution/Call Processing Impacts

13.1 Xtended Services Interface Impact

There is no impact

13.2 SIP/MGCP Interface Impact

13.2.1 Summary

For both access and network interfaces, the Application Server parses received *Resource-Priority* SIP headers, validates them and then proxies them. In certain error responses, the *Accept-Resource-Priority* SIP header is generated. The new *resource-priority* option tag of the *Require* header is also introduced and supported. Validation was introduced to prevent *Resource-Priority* resource values from being considered if they are changed in a dialog (except in responses to an initial INVITE).

For network access, the Application Server may also generate a new *Resource-Priority* SIP header before sending a SIP INVITE to the network (this happens when a GETS call is identified by Request-URI). Also, the *Supported* header is added to outgoing initial SIP INVITE requests associated with GETS sessions.

Strict conformance with NGN GETS (see *NS/EP IMS Core Network IR NGN GETS, Phase 1, Voice Service [2]*) regarding error handling during the validation of the *Resource-Priority* header is also implemented.

When a call is blocked by the Emergency call DDoS protection mechanism, the BroadWorks Application Server responds with a *SIP 503 Service Unavailable*, a *SIP 603 Decline* with a *Retry-After* header, a *SIP 480 Temporarily Unavailable* with a *Retry-After* header, a *SIP 302 Moved Temporarily* with the alternate Application Server as contact or it silently drops the call. The value of the *Retry-After* header is a number selected randomly between *minRetryAfterInSeconds* and *maxRetryAfterInSeconds*. If the call is blocked by the Network Server Emergency call DDoS protection mechanism the Cisco BroadWorks Network Server responds with a *SIP 503 Service Unavailable* or it silently drops the call.

For more detailed explanation of SIP impacts, see **5.7 SIP Interface**.

13.2.2 SIP Header/MGCP Command

The following descriptions apply to both access and network interfaces.

13.2.2.1 Resource-Priority

The *Resource-Priority* SIP header can be present in any SIP request or response, except for 100 Trying and 403 Forbidden. The GETS specifications [2] differ from *RFC 4412* [3] in this regard, and Cisco BroadWorks follows the GETS specifications. Cisco BroadWorks inserts the header in most messages (with exceptions such as 100 Trying and responses to a BYE or a 302) sent for a GETS call.

In incoming requests, the header is used to identify GETS calls in initial SIP INVITE requests, but it is ignored in other requests.

This header is defined in *RFC 4412* [3]. For more details see **5.7.1 Resource-Priority Header (RPH)**.

Name of SIP header: Resource-Priority

Augmented Backus-Naur Form (ABNF) format

```
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 / "-" / "!" / "%" / "*"
                    / " " / "+" / "`" / "!" / "~" )
```

13.2.2.2 Accept-Resource-Priority

As stated in section **5.7.1.1 Resource Priority Header Handling**, Cisco BroadWorks may add the Accept-Resource-Priority in SIP error responses. This header is defined in *RFC 4412*[3].

Name of SIP header: Accept-Resource-Priority

ABNF format

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

13.2.2.3 Supported

As stated in section **5.7.4 Supported SIP Header Support**, Cisco BroadWorks forwards initial SIP INVITEs with the *resource-priority* option in the *Supported* header, for GETS sessions. This header is now added in outgoing initial SIP INVITEs originating from GETS sessions with the *resource-priority* option tag to indicate to the remote functional element that Cisco BroadWorks supports the *Resource-Priority* header as defined in *RFC 4412* [3].

This header is defined in *RFC 3261* [4].

Augmented Backus-Naur Form (ABNF) format

```
Supported = "Supported" HCOLON option-tag *(COMMA option-tag)
```

13.2.3 SIP Parameter/MGCP Signal/Event

13.2.3.1 *resource-priority* Option Tag in Require SIP Header

If the *enableRequireResourcePriority* system parameter is enabled, the outgoing first SIP INVITE of a GETS call contains the *resource-priority* option tag in the *Require* header. This option tag is also parsed in certain error conditions to decide on the action to take (for example, ignore or respond with error).

This parameter is defined in *RFC 4412* [3].

Name of SIP option tag: *resource-priority*

There is no further ABNF for this option tag.

For compliance with NGN GETS (see *NS/EP IMS Core Network IR NGN GETS, Phase 1, Voice Service [2]*), requests with *resource-priority* in the *Require* header that also have invalid GETS r-value(s) in their *Resource-Priority* header result in a SIP 400 *Bad Request* response with a 417 cause in its *Reason* header. Requests with no GETS r-value are unaffected by this change, where the usual *RFC 4412 [3] Resource-Priority* error handling takes place. GETS r-values are any r-values in the *GETS* or *GETS-Mandatory* classes. For a flowchart detailing the *Resource-Priority* validation and error handling algorithm, see section [5.7.1 Resource-Priority Header \(RPH\)](#).

As an illustrative example, consider the following INVITE that has an invalid *GETS* class "wps.8" r-value, with the *resource-priority* option in the *Require* header. (Note that only the request line and the *Require* and *Resource-Priority* headers are shown.)

```
INVITE sip:5146971500@operator.com;user=phone SIP/2.0
Require:resource-priority
Resource-Priority:ets.0,wps.8
```

Cisco BroadWorks responds with a SIP 400 response.

```
SIP/2.0 400 Bad request
Resource-Priority:ets.0
Reason:SIP;text="Invalid Resource-Priority";cause=417
```

If the request has unknown or invalid r-values that do not belong to the *GETS* or *GETS-Mandatory* classes, as in the following example, then Cisco BroadWorks instead responds with a SIP 417 response.

```
INVITE sip:5146971500@operator.com;user=phone SIP/2.0
Require:resource-priority
Resource-Priority:ns.1
```

SIP 417 response

```
SIP/2.0 417 Unknown Resource-Priority
```

13.2.3.2 r-value Handling in Resource-Priority SIP Header

In addition to the change described in section [13.2.3.1 resource-priority Option Tag in Require SIP Header](#), an additional validation occurs for incoming requests targeting existing endpoints where the following occurs:

- A new incoming request with no GETS r-value in the *Resource-Priority* header is processed as a GETS request if targeting an existing GETS endpoint.
- A request with a *GETS* r-value in the *Resource-Priority* header is **not** processed as a GETS request if targeting an existing non-GETS endpoint.

13.2.4 Message Example

13.2.4.1 Resource-Priority SIP Header

The following is an example of the *Resource-Priority* header.

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

13.2.4.2 Accept-Resource-Priority SIP Header

The following is an example of the *Accept-Resource-Priority* header.

```
Accept-Resource-Priority: dsn.flash-override, dsn.flash, dsn.immediate,  
dsn.priority, dsn.routine
```

13.2.4.3 *resource-priority* Option Tag

The following shows that the *Require* header can contain the *resource-priority* option tag.

```
INVITE sip:user@host.com SIP/2.0  
(...)  
Require: resource-priority  
Resource-Priority: ets.0, wps.3  
(...)
```

13.2.4.4 *resource-priority* in Supported Header

This is an example of an outgoing INVITE sent from the Application Server to the network for an initial incoming GETS INVITE highlighting the addition of the *resource-priority* option tag in the *Supported* header.

```
INVITE sip:user@host.com SIP/2.0  
(...)  
Resource-Priority: ets.0, wps.3  
Supported:100rel,resource-priority  
(...)
```

14 Client Application Impacts

14.1 OCI-P Impacts

There is no impact.

14.2 Call Control Impacts

There is no impact

14.3 Window Impacts

There is no impact.

15 Deployment/Operational Impacts

15.1 Configuration File Impacts

There is no impact.

15.2 Security Impacts

On the Application Server, an additional UDP port and an additional TCP port are used for outgoing GETS signaling traffic. For more information, see section *16.4 Port Usage Impacts*.

Since this feature requires allowing some SIP messages to bypass Cisco BroadWorks overload control mechanisms, there is a theoretical risk that the Application Server could reach an extreme overload condition. In practice, however, the number of simultaneous GETS calls should remain quite low. Note that extreme overload controls still apply, preventing instability due to an overload of incoming GETS messages.

The Emergency Call DDoS Protection mechanism addresses another theoretical vulnerability where the Cisco BroadWorks TAS receives an exceptionally high number of emergency calls causing it to enter an extreme overload condition where GETS calls cannot be processed anymore. A configurable protection rate is added to Cisco BroadWorks Application and Network Servers to protect the Cisco BroadWorks TAS from being overwhelmed with emergency calls and to ensure that sufficient resources are always available to process GETS calls.

15.2.1 Security Toolkit Impact

There is no impact.

15.2.2 Application Server Default Hardening Impact

There is no impact.

15.3 Scheduled Tasks

There is no impact.

15.4 Third-Party Software

There is no impact.

15.5 Server Logging Impacts

There is no impact.

15.6 Client Application Impacts

There is no impact.

16 System Engineering Impacts

16.1 Processing Impacts

To identify GETS call messages and sessions, minimal extra processing is executed for each SIP message. For each SIP message, the resource priority header is validated against provisioned GETS namespaces.

To identify GETS calls with the Request-URI, this feature introduces minimal extra processing for each originating call SIP INVITE. For each originating call SIP INVITE, a lookup of the received Request-URI user string to a provisioned list of DN numbers is performed when there is no Resource-priority header (or no GETS namespace in the Resource-priority header) and the call identifier mode supports request URI identification.

When the Emergency Call DDoS Protection mechanism is enabled, minimal additional processing is executed for each emergency call to verify if the current emergency call rate exceeds the configured protection rate.

16.1.1 New Time-Outs

There is no new time-out.

16.2 Memory Impacts

There is no impact.

16.3 Disk Usage Impacts

There is no impact.

16.4 Port Usage Impacts

On the Application Server, an additional UDP port and an additional TCP port are used for outgoing GETS signaling traffic (regardless of the remote address). For the connection-oriented TCP, this translates into several sockets (or connections), one for each remote address that receives GETS signaling.

16.5 Hardware Impacts

There is no impact.

16.6 Client Application Messaging Impacts

There is no impact.

17 Service Patch Interface Impacts

17.1 Service Patch Interface Differences

There is no impact.

17.2 Feature Activation Impacts

17.2.1 Behavior Impacts upon Activation

After the activation of feature 11930, administrators can enable GETS the same way as the non-patched version of this feature.

17.2.2 Provisioned Data Impacts on Activation

No impact.

17.2.3 Provisioned Data Impacts on Deactivation

When the feature is deactivated, GETS configuration fields are set back to their default value and the InhibitedAVPCodes, Numbers, ReservedFACS, ResourcePriorities and SessionPriorityMap lists are cleared.

17.2.4 OCI Command Behavior Prior to Activation

The SystemGETSModifyRequest OCI command fails if the “enabled” field is set to true and feature 11930 is not activated.

18 Appendix A - Originating vs Terminating Calls in IMS Mode

This appendix provides a high-level description of how the Cisco BroadWorks AS determines whether a SIP INVITE message should be handled as an originating or a terminating call in IMS mode.

See the Cisco BroadWorks AS Mode ISC specification documentation for the detailed and up to date description [10].

Note that this appendix is included here for convenience and might not be updated when future changes to the referenced document are made.

When receiving a SIP INVITE message, the Cisco BroadWorks Application Server determines to run the origination or the termination services based on the following:

The INVITE request contains a *Route* header that indicates that the S-CSCF expects the Application Server to execute either originating or terminating services and the Application Server recognizes the identity of a Cisco BroadWorks subscriber.

Any of the following parameters in the Route header indicate that the Application Server should execute originating services:

- call=orig
- mode=originating
- orig

Any of the following parameters in the Route header indicate that the Application Server should execute terminating services:

- call=term
- call=term_registered
- call=term_unregistered
- mode=terminating
- term

If the Route header does not contain any orig or term triggers, an attempt is made to determine whether the BW AS should execute originating or terminating services based on the following:

- The Application Server examines the *Via* headers. If it finds one of its own network addresses in a *Via* header, indicating that the INVITE request has already been routed through the Application Server, then it does not execute originating services and it executes terminating services if it finds a Cisco BroadWorks subscriber for the Request URI.
- The Application Server examines the *P-Asserted-Identity* header. If it finds a Cisco BroadWorks subscriber identity in the *P-Asserted-Identity* header, then it executes originating services for that subscriber.
- The Application Server examines the *From* header. If it finds a Cisco BroadWorks subscriber identity in the *From* header, then it executes originating services for that subscriber.
- The Application Server examines the *Request URI*. If it finds the address of a Cisco BroadWorks subscriber, then it executes terminating services for that subscriber.

Acronyms and Abbreviations

This section lists the acronyms and abbreviations found in this document. The acronyms and abbreviations are listed in alphabetical order along with their meanings.

3GPP	3rd Generation Partnership Project
AAC	Account/Authorization Code
ABNF	Augmented Backus-Naur Form
ACC	Advanced Call Control
ACD	Automatic Call Distribution
ACL	Access Control List
ACR	Anonymous Call Rejection
Admin	Administrator
AMS	Access Mediation Server
API	Application Programming Interface
AS	Application Server
AVP	Attribute-Value Pair
BCCT	BroadWorks Common Communication Transport
BLF	Busy Lamp Field
BW	BroadWorks
CBF	Communication Barring – Fixed
CCRS	Call Center Reporting Server
CDR	Call Detail Record
CDS	Call Detail Server
CFA	Call Forwarding Always
CFB	Call Forwarding Busy
CFNA	Call Forwarding No Answer
CFNR	Call Forwarding Not Reachable
CFS	Call Forwarding Selective
CLI	Command Line Interface
CLID	Calling Line ID
CNAM	Caller ID with NAME
CORBA	Common Object Request Broker Architecture
COS	Class of Service (Ethernet)
CPL	Call Processing Language
CPU	Central Processing Unit
CRS	Call Recording Server

CS	Conferencing Server
CSCF	Call Session Control Function
CSTA	Computer Supported Telecommunications Applications
CSV	Comma-Separated Value
CTI	Computer Telephony Integration
CWT	Call Waiting Tone
dBm	The power ratio in decibel (dB) of the measured power referenced to one milliwatt (mW)
dBm0	The level of a signal as specified in dBm0, is the level of that signal (in dBm) as measured at the reference point of the network.
DBS	Database Server
DDoS	Distributed Denial of Service
DGC	Distributed Group Calls
DM	Device Management
DN	Directory Number
DND	Do Not Disturb
DOS	Disk Operating System
DPUBI	Directed Call Pickup with Barge-in
DSCP	DiffServ Code Point
ECN	Explicit Congestion Notification
EMS	Element Management System
ENUM	E.164 Number Mapping
EOCP	Enhanced Outgoing Calling Plan
ETS	Emergency Telecommunications Service
FAC	Feature Access Code
FD	Feature Description
FE	Functional Element
FQDN	Fully Qualified Domain Name
FR	Feature Request
FS	Functional Specification
FTP	File Transfer Protocol
GAN	GETS-AN
GETS	Government Emergency Telecommunications Service
GETS-AS	GETS-Application Server
GETS-AN	GETS- Access Number
GETS-FC	GETS- Feature Code
GETS-NT	GETS- Number Translation
GIR	Government Industry Requirements

GNT	GETS-NT
HCB	Hierarchical Communication Barring
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
Hz	Hertz
ICP	Incoming Calling Plan
IMAP	Internet Message Access Protocol
IMRN	IP Multimedia Routing Number
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IVR	Interactive Voice Response
LI	Lawful Intercept
LO	Local
LPS	Local Premium Service
LSSGR	LATA Switching Systems Generic Requirements
MAC address	Media Access Control address
MB	Megabyte
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MOC	Microsoft Office Communications
MR	Market Request
MS	Media Server
NCOS	Network Class of Service
NE	Network Element
NFM	Network Function Manager
NGN	Next Generation Network
NS	Network Server
NS/EP	National Security and Emergency Preparedness
NSSync	Network Server Synchronization
OAM&P	Operations, Administration, Management, and Provisioning
OCI	Open Client Interface
OCI-C	Open Client Interface-Call Control
OCI-P	Open Client Interface-Provisioning
OCI-R	Open Client Interface-Reporting
OCP	Outgoing Calling Plan
OCS	Open Client Server
ODP	Outgoing Digit Plan

OID	Object Identifier
OM	Operational Measurement
OOTB	Out-of-the-Blue
OS	Operating System
OSS	Operations Support System
PAWS	Performance Analysis Working Session
PBX	Private Branch Exchange
PCV	P-Charging-Vector
PDF	Portable Document Format
PDN	Pseudo Destination Number
PIN	Personal Identification Number
PM	Performance Measurement
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
PTT	Push to Talk
PUI	Public User Identity
RAM	Random Access Memory
RFC	Request for Comments
Rf	Offline Charging Reference Point between an AS and the Event Charging Function
Ro	Online Charging Reference Point between an AS and the Event Charging Function
RPH	Resource-Priority Header
RTP	Real-Time Transport Protocol
r-value	Resource Value
SAC	Session Admission Control
SBC	Session Border Controller
SCA	Shared Call Appearance
SCA	Selective Call Acceptance
S-CSF	Serving-Call Session Control Function
SCR	Selective Call Rejection
SDR	Session Data Replication
SIP	Session Initiation Protocol
SMAP	Software Management Application Protocol
SMDI	Simplified Message Desk Interface
SMPP	Short Message Peer-to-Peer Protocol
SMS-C	Short Message Service Center
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	Service Patch
SRV	Service Locator
SSH	Secure Shell
SSL	Secure Sockets Layer
TAS	Telephony Application Server
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TO	Toll
TOS	Type of Service
TPS	Toll Premium Services
TXNS	Transactions
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VMS	Voice Mail System
VoIP	Voice Over Internet Protocol
VTR	Verify Translation and Routing
WebDAV	Web-based Distributed Authoring and Versioning
WPS	Wireless Priority Service
WS	Web Server
XML	eXtensible Markup Language
XS	Execution Server
XSD	XML Schema Definition
Xsi	Xtended Services Interface
Xsp	Xtended Services Platform

References

- [1] Cisco Systems, Inc. 2020. *GETS Support Feature Description, Release 20.0*. Available from Cisco at cisco.com.
- [2] National Communications System (NCS), *NS/EP IMS Core Network IR NGN GETS, Phase 1, Voice Service*, Issue 2.0, January 2013.
- [3] Schulzrinne, H., and Polk, J., "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, Internet Engineering Task Force, February 2006. Available from www.ietf.org.
- [4] Rosenberg, J. et al, "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force, June 2002. Available from www.ietf.org.
- [5] 3rd Generation Partnership Project. 2016. *3GPP TS 29.229*. Available from 3GPP at http://www.etsi.org/deliver/etsi_ts/129200_129299/129229/13.00.00_60/ts_129229v130000p.pdf.
- [6] 3rd Generation Partnership Project (3GPP). 2011. *3GPP TS 22.153 v11.1.0 Multimedia priority service (Release 11)*. Available from <http://www.3gpp.org/>.
- [7] 3rd Generation Partnership Project (3GPP). 2012. *3GPP TS 23.854 v11.0.0 Enhancements for Multimedia priority service (MPS) (Release 11)*. Available from <http://www.3gpp.org/>
- [8] V. Fajardo, et al. "Diameter Base Protocol", RFC 6733, Internet Engineering Task Force, October 2012. Available from www.ietf.org.
- [9] Cisco Systems, Inc. 2020. *Cisco BroadWorks Service Guide*. Available from Cisco at cisco.com.
- [10] Cisco Systems, Inc. 2020. *Cisco BroadWorks AS Mode ISC Interface*. Available from Cisco at cisco.com.
- [11] Cisco Systems, Inc. 2020. *Cisco BroadWorks Treatment Guide*. Available from Cisco at cisco.com.
- [12] Emergency Telecommunications Service (ETS) Network Element Requirements for IMS-based Next Generation Network (NGN) Phase 2, ATIS 1000066.2016. Available at www.ansi.org.
- [13] Cisco Systems, Inc. 2020. *Cisco BroadWorks Accounting Call Detail Record Interface Specification*. Available from Cisco at cisco.com.
- [14] Cisco Systems, Inc. 2020. *Cisco BroadWorks SIP Trunking Solution Guide*. Available from Cisco at cisco.com.