Internet Engineering Task Force
INTERNET-DRAFT
draft-polk-sip-resource-03.ps
Schulzrinne/Polk
Columbia U./Cisco
March 2, 2003
Expires: August 2003

Communications Resource Priority for the Session Initiation Protocol (SIP)

Status of this Memo

Copyright Notice

Abstract

This document defines a new SIP header field for communications resource priority, called "Resource-Priority". This header field can influence the behavior of SIP UAs, such as GSTN gateways, and SIP proxies. It does not influence the forwarding behavior of IP routers.

Contents

1 Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

2 Introduction

During emergencies, communications resources including telephone circuits, IP bandwidth and gateways between the circuit-switched and IP networks may become congested. Congestion can occur due to heavy usage, loss of resources caused by the natural or man-made disaster and attacks on the network during man-made emergencies. This congestion may make it difficult for persons charged with emergency assistance, recovery or law enforcement to coordinate their efforts. As IP networks become part of converged or hybrid networks along with public and private circuit-switched (telephone) networks, it becomes necessary to ensure that these networks can assist during such emergencies.

Also, users of end systems may want to be interrupted in their lower-priority communications activities if such an emergency communications requests arrives.

There are many IP-based services that can assist during emergencies. This memo only covers requirements for real-time communications applications involving SIP, including voice-over-IP, multimedia conferencing and instant messaging/presence.

Session Initiation Protocol (SIP) [2] applications involve at least five different resources that may become scarce and congested during emergencies. These resources include gateway resources, circuit-switched network resources, IP network resources, receiving end system resources and SIP proxy resources. IP network resources are beyond the scope of SIP signaling and are therefore not considered here.

In order to improve emergency response, it may become necessary to prioritize access to SIP-signaled resources during periods of emergency-induced resource scarcity. We call this "resource prioritization".

Currently, SIP does not include a mechanism that allows a request originator to indicate to SIP element that it wishes the request to invoke such resource prioritization. To address this need, this document adds a SIP protocol element that labels certain SIP requests.

This document defines (Section 3) a new SIP [2] header field for communications resource priority, called Resource-Priority. This header field MAY be used by SIP user agents, including GSTN gateways and terminals, and SIP proxy servers to influence their treatment of SIP requests, including the priority afforded to GSTN calls. For GSTN gateways, the behavior translates into analogous schemes in the GSTN, for example the ITU Recommendation Q.735.3 [3] prioritization mechanism, in both the GSTN-to-IP and IP-to-GSTN directions.

The Resource-Priority header field may be used in several situations. A SIP request with such an indication can be treated differently in several situations:

1. The request can be given elevated priority for access to GSTN gateway resources such as trunk circuits.

2. The request can interrupt lower-priority requests at a user terminal, such as an IP phone.

3. The request can carry information from one multi-level priority domain in the telephone network, e.g., using the facilities of Q.735.3 [3], to another, without the SIP proxies themselves inspecting or modifying the header field.

4. In SIP proxies and back-to-back user agents, requests of higher priorities may displace existing signaling requests or bypass GSTN gateway capacity limits in effect for lower priorities.

This header is related to, but differs in semantics from, the Priority header field (RFC 3261 [2], Section 20.26). The Priority header field describes the priority that the SIP request should have to the receiving human or its agent. For example, it may be factored into decisions about call routing and acceptance. It does not influence the use of communications resources such as packet forwarding priority in routers.

The mechanism described here can be used for emergency preparedness in emergency telecommunications systems (ETS), but is only a small part of an emergency preparedness network.

The mechanism is structured so that it works in all SIP/RTP transparent networks [11], i.e., all network elements and SIP proxies let valid SIP requests pass through unchanged. This is important since it is likely that this mechanism will often be deployed in networks where the edge networks are unaware of the resource priority mechanism and provide no special privileges to such requests. The request then reaches a PSTN gateway or set of SIP elements that are aware of the mechanism.

For conciseness, we refer to SIP proxies and user agents that act on the Resource-Priority header field as an *RP actor*.

We define the header field syntax in Section 3 and then describe the behavior of user agents and proxies in Sections 4.3 through 4.5. Section 6 briefly describes how this feature affects existing systems that do not support it. Third-party authentication is discussed in Section 5, while general security issues are enumerated in Section 8. This specification does not propose any new SIP security mechanisms. Examples can be found in Section 7.

The mechanism aims to satisfy the requirements in [11]. We present a detailed analysis in Section A.

3 The Resource-Priority and Allow-Resource-Priority SIP Header Fields

This document defines the Resource-Priority and Allow-Resource-Priority SIP header fields. The Resource-Priority header field marks a SIP request as desiring prioritized resource access, as described in the introduction. In responses, it indicates the actual resource priority that was granted to the request.

Implementations MAY change the value offered in the request; in some environments, the response value is known to be the same as in the request.

The SIP element behavior is described for UACs in Section 4.3, for UAS in Section 4.4, for proxies in Section 4.5. The syntax of the Resource-Priority header field is as follows:

```
Resource-Priority  =  "Resource-Priority" HCOLON Resource-value
Resource-value     =  namespace "." priority
namespace          =  alphanum / "-"
priority           =  alphanum / "-"
```

```
Resource-Priority: dsn.priority
```

The Resource-value parameter in the Resource-Priority header indicates the resource priority desired by the request originator. The resource value is formatted as “namespace” “.” “priority value”. The value is drawn from the namespace identified by the namespace token. Namespaces and priorities are case-independent ASCII. Each namespace has at least one priority value. Namespaces and priority values within each namespace are registered with IANA (Section 12); some initial namespaces are described in Section B.

> We require that even namespaces with only one priority value list that value to avoid problems if additional priority values are added later.

The Allow-Resource-Priority response header field indicates what resource values the SIP element supports. The syntax of the Allow-Resource-Priority header field is as follows:

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

Example:

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

Header field	where	proxy	INV	MES	OPT	NOT	SUB
Resource-Priority	R	amd	o	o	-	o	o
Resource-Priority	200	-	o	o	-	o	o
Accept-Resource-Priority	200	-	o	-	o	-	-
Accept-Resource-Priority	417	-	m	m	-	m	m
Accept-Resource-Priority	420	-	m	m	-	m	m

The header fields have no defined meaning in ACK, BYE, CANCEL, INFO, PRACK and REGISTER requests and MUST be ignored by recipients of such requests. Accept-Resource-Priority is only returned in 420 (Not Supported) responses if the element supports the resource priority mechanism, but does not support the particular namespace or priority value.

4 Behavior of SIP Elements that Receive Prioritized Requests

4.1 General Rules

All user agent servers and proxy servers that receive SIP requests share certain common behavior, which we describe below. Behavior that is specific to user agent servers is covered in Section 4.4, while Section 4.5 deals with proxy behavior.

A SIP element supporting this specification MUST be able to interpret the Resource-Priority header field in INVITE, MESSAGE [4], UPDATE [5], SUBSCRIBE [6] and NOTIFY [6] requests. It ignores the header field in other requests unless the request definition defines behavior for the particular method.

If an element receives a request with a namespace or priority value that it does not recognize, it MAY serve the request if the request would succeed and experience treatment no different than a non-labeled request. Namespaces MAY require implementations to enforce strict behavior where unknown priority values cause the request to be rejected with 417 (Resource-Priority failed) instead.

If the request would fail due to lack of resources if the resource priority indication is ignored or would get a different treatment, the element MUST reject the request with response code 417 (Resource-Priority failed) so that the originator can re-attempt with a more appropriate resource priority. (An example of "different treatment" would be the priority labeling of the circuit-switched network call in a gateway or the routing to a different gateway.)

If a request is rejected with response code 417 (Resource-Priority failed), the response MUST include a Accept-Resource-Priority header field enumerating all the resource values that the server is willing to process. Note that the user may not be authorized to use all of these resource values. The response MAY list only those values that the user is authorized to use, but this is not required.

A SIP server MAY return status code 503 (Service Unavailable) if there are insufficient resources at the resource priority level specified. The response MAY also include a Warning header with warning code 370 (Insufficient Bandwidth) if the request failed due to insufficient capacity for the media streams, rather than insufficient signaling capacity.

4.2 Restricting Default Request Handling

In some cases, the UAC wants to ensure that only UAS that understand the resource priority mechanism, the namespace and the priority value handle the request, while all others reject the request. A UAC MAY insert a Require header with the Resource-Priority option tag in a request to achieve this behavior. Following standard behavior (Section 8.2.2.3 of [2]), a UAS MUST then reject the request with response code 420

(Bad Extension) if it does not understand the mechanism, the namespace or the priority value. If the UAS is capable of the resource priority indication in general, but does not understand the namespace or priority value, it MUST also include a Accept-Resource-Priority header field indicating the namespace-priority combinations it can accept.

The use of the Resource-Priority option tag with Proxy-Require is NOT RECOMMENDED.

For example, a gateway that is unaware of a resource priority namespace might accept a request at non-elevated priority, but then the request could later be preempted by other requests. Also, use of the Require restriction ensures that in parallel forking, only branches that support the resource priority mechanism succeed.

4.3 User Agent Client Behavior

SIP UACs supporting this specification MUST be able to generate the Resource-Priority header field for requests that require elevated resource access priority. The UAC MUST only include at most one Resource-Priority header field in the request.

If the request is returned with 417 (Resource-Priority failed), the UAC MAY retry the request with a different namespace or priority value, drawing from the values returned by the Accept-Resource-Priority header field in the response.

4.4 User Agent Server Behavior

The OPTIONS request can be used to determine if a UAS supports the mechanism. A compliant implementation SHOULD return a Accept-Resource-Priority header field in OPTIONS responses enumerating all valid resource values. An implementation MAY reveal this capability only to authorized UACs.

If the UAS understands the resource value, but refuses to honor the request with elevated priority for this particular user, it returns the 403 (Forbidden) response code. It MAY include the list of resource values that the user is allowed to use in the Accept-Resource-Priority response header field.

The lookup of the authorized values may take significant resources since it may involve an AAA interaction. Thus, it seems imprudent to require that the list is customized to the user. In general, legitimate users know their highest resource value that they are entitled to.

The precise effect of the Resource-Priority indication depends on the type of UAS, the namespace and local policy. For example, a circuit-switched telephony gateway might move requests with elevated priority to the front of the queue of requests waiting for outbound lines, it may utilize additional resources or it may preempt existing calls. For a terminal, such as a SIP phone, requests with elevated priority might trigger a special alert tone or preempt other, lower-priority ongoing calls. The generic protocol mechanism described here does not mandate the particular element behavior, but namespace definitions, such as the ones in Section B, need to spell out the desired behavioral properties of user agents and proxy servers.

4.5 Proxy Behavior

SIP proxies may ignore, inspect, insert and modify the Resource-Priority header field. SIP proxies MAY downgrade the Resource-Priority of or reject unauthenticated requests. Details are a matter of local policy.

This behavior is similar to that for any header field, as a UA can decide to reject a request for the presence, absence or value of any information in the request.

A SIP proxy MAY use the Resource-Priority indication in its routing decisions, e.g., to find a next hop that is reserved for a particular resource priority.

There do not appear to be any special considerations when forking requests containing a resource priority indication.

Otherwise, the proxy behavior is the same as for user agent servers (Section 4.4).

5 Third-Party Authentication

In some case, the RP actor may not be able to authenticate the requestor or determine whether an authenticated user is authorized to make such a request. In these circumstances, the SIP entity may avail itself of general SIP mechanisms that are not specific to this application. The authenticated identity management mechanism [7] allows a third party to verify the identity of the requestor and certify this towards an RP actor. In networks with mutual trust, the SIP asserted identity mechanism [13] can help the RP actor determine the identity of the requestor.

6 Backwards Compatibility

The resource priority mechanism described in this document is fully backwards compatible with SIP systems following RFC 3261 [2]. Naturally, systems not understand the mechanism can only deliver standard, not elevated, service priority. User agent servers and proxies can ignore any Resource-Priority header field just like any other unknown header field and then treat the request like any other request. Naturally, the request may still succeed.

Introducing Require or Proxy-Require would not help, as systems that do not support the mechanism will not improve by rejecting the request due to feature failure. Since the intent of resource priority indications is to increase the probability of call completion, adding failure modes appears counterproductive.

7 Examples

The SDP message body and the BYE and ACK exchanges are the same as in [8] and omitted for brevity.

7.1 Simple Call

```
User A                  User B
  |                        |
  |       INVITE F1        |
  |----------------------->|
  |    180 Ringing F2      |
  |<-----------------------|
  |                        |
  |       200 OK F3        |
  |<-----------------------|
  |         ACK F4         |
  |----------------------->|
  |   Both Way RTP Media   |
  |<======================>|
  |                        |
```

In this scenario, User A completes a call to User B directly. The call from A to B is marked with a resource priority indication.

```
F1 INVITE User A -> User B

INVITE sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Resource-Priority: dsn.flash
Contact: <sip:UserA@client.atlanta.com;transport=tcp>

Content-Type: application/sdp
Content-Length: ...

...

F2 180 Ringing User B -> User A

SIP/2.0 180 Ringing
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Contact: <sip:UserB@client.biloxi.com;transport=tcp>
Content-Length: 0


F3 200 OK User B -> User A

SIP/2.0 200 OK
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Resource-Priority: dsn.flash
Contact: <sip:UserB@client.biloxi.com;transport=tcp>
Content-Type: application/sdp
```

```
Content-Length: ...

...
```

7.2 Receiver Does Not Understand Namespace

In this example, the receiving UA does not understand the “dsn” namespace and thus returns a 417 (Resource-Priority failed) status code. We omit the message details for messages F5 through F7 since they are essentially the same as in the first example.

```
User A                  User B
   |                        |
   |       INVITE F1        |
   |----------------------->|
   | 417 R-P failed F2      |
   |<-----------------------|
   |         ACK F3         |
   |----------------------->|
   |                        |
   |       INVITE F4        |
   |----------------------->|
   |    180 Ringing F5      |
   |<-----------------------|
   |       200 OK F6        |
   |<-----------------------|
   |         ACK F7         |
   |----------------------->|
   |                        |
   |   Both Way RTP Media   |
   |<======================>|

F1 INVITE User A -> User B

INVITE sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Resource-Priority: dsn.flash
Contact: <sip:UserA@client.atlanta.com;transport=tcp>

Content-Type: application/sdp
Content-Length: ...
```

```
...

F3 417 Resource-Priority failed  User B -> User A

SIP/2.0 417 Resource-Priority failed
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Allow-Resource-Priority: q735.0, q735.1, q735.2, q735.3, q735.4
Contact: <sip:UserB@client.biloxi.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 0

F3 ACK User A -> User B

ACK sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bd5
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 ACK
Content-Length: 0

F4 INVITE User A -> User B

INVITE sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 2 INVITE
Resource-Priority: q735.3
Contact: <sip:UserA@client.atlanta.com;transport=tcp>

Content-Type: application/sdp
Content-Length: ...
...
```

8 Security Considerations

Any resource priority mechanism can be abused to obtain resources and thus deny service to other users. An adversary may be able to take over a particular gateway, cause additional congestion during PSTN during emergencies or deny service to legitimate ETS users.

While the indication itself does not have to provide separate authentication, any SIP request carrying such information has higher authentication requirements than regular requests. Below, we describe authentication and authorization aspects, confidentiality and privacy requirements, protection against denial of service attacks and anonymity requirements. Naturally, the general discussion in RFC 3261 [2] applies.

8.1 Authentication and Authorization

Prioritized access to network and end system resources imposes particularly stringent requirements on authentication and authorization mechanisms since access to prioritized resources may impact overall system stability and performance, not just result in theft of, say, a single phone call.

Under certain emergency conditions, the network infrastructure, including its authentication and authorization mechanism, may be under attack.

Given the urgency during emergency events, normal statistical fraud detection may be less effective, thus placing a premium on reliable authentication.

Common requirements for authentication mechanisms apply, such as resistance to replay, cut-and-paste and bid-down attacks.

Authentication MAY be SIP-based or use other mechanisms. Use of Digest authentication and/or S/MIME is RECOMMENDED for UAS authentication, but it requires that the parties share a common secret. SIP systems employing resource priority MUST implement S/MIME at least for integrity, as described in Section 23 of [2]. Section 5 describes third-party authentication.

8.2 Confidentiality and Integrity

All aspects of Emergency Telecommunications Systems (ETS) are likely to be sensitive and must be protected from intercept and alteration. In particular, requirements for protecting the confidentiality of communications relationships may be higher than for normal commercial service. For SIP, the To, From, Organization, Subject and Via header fields are examples of particularly sensitive information. Systems MUST provide for encryption at the transport level using TLS and MAY implement other transport-layer or network-layer security mechanisms. UACs SHOULD use the "sips" URI to request a secure transport association to the destination.

The Resource-Priority header field can be carried in the SIP message header or can be encapsulated in a message fragment carried in the SIP message body [9]. Encapsulation allows to protect this header field against inspection or modification by proxies, using S/MIME. However, in many cases, proxies will need to authenticate and authorize the request, so that encapsulation is undesirable.

8.3 Anonymity

Some users may wish to remain anonymous to the request destination. For the reasons noted earlier, users have to authenticate themselves towards the SIP elements carrying the request where they desire resource priority treatment. The authentication may be based on capabilities and noms, not necessarily their civil name. Clearly, they may remain anonymous towards the request destination, using the network-asserted identity and general privacy mechanisms [16, 13].

8.4 Denial-of-Service Attacks

As noted, ETS systems are likely to be subject to deliberate denial- of-service attacks during certain types of emergencies. DOS attacks may be launched on the network itself as well as its authentication and authorization mechanism. As noted, systems should minimize the amount of state, computation and network resources that an unauthorized user can command. The system must not amplify attacks by causing the transmission of more than one packet to a network address whose reachability has not been verified.

9 IANA Registration of Resource-Priority and Accept-Resource-Priority Header Fields

The following is the registration for the Resource-Priority header field:

RFC number: RFCxxxx

Header name: Resource-Priority

Compact form: none

The following is the registration for the Accept-Resource-Priority header field:

RFC number: RFCxxxx

Header name: Accept-Resource-Priority

Compact form: none

10 IANA Registration for Option Tag Resource-Priority

RFC number: RFCxxxx

Name of option tag: Resource-Priority

Descriptive text: Indicates or requests support for the resource priority mechanism.

11 IANA Registration for Response Code 417

RFC number: RFCxxxx

Response code: 417

Default reason phrase: Resource-Priority failed

12 IANA Considerations

Additional namespaces and priority values are registered with IANA. Within each namespace, The registration may indicate the relative precedence levels, expressed as an ordered list. The registration must indicate the default level to be assumed in the absence of the priority value or if an implementation does not understand a level from the namespace. New labels should not be added to existing namespaces; as noted above, implementations predating the addition will ignore such values. The registration MUST describe how SIP elements should treat requests from that namespace, e.g., whether preemption or only preferential queueing are allowed. Namespaces MAY also impose particular authentication or authorization consideration that are stricter than the baseline described here. Namespaces MAY disallow default treatment of priority values not understood by an implementation. If a namespace calls for "strict" interpretation, an implementation that does not support a priority value MUST reject requests with unknown priority values with a 417 (Resource-Priority failed) response.

A Addressing the IEPREP Requirements

Below, we describe how the mechanism in this memo as well as plausible alternatives address the requirements in [11]. For each requirement, we indicate what existing mechanism can be used or what candidate extensions might be suitable. In general, none of the currently standardized or proposed SIP features indicate whether a request makes special claims to SIP-mediated resources or not. (The Priority header indicates the urgency to the human recipient of the request and is orthogonal to this issue.)

In general, SIP offers four mechanisms to convey protocol semantics: URIs scheme (US) or parameter (UP), header fields (H), request methods (M), caller preferences (C) and body content (B).

Thus, there are three choices:

Deduce: Information in U, H, M, C or B is used to deduce the resource priority demand.

New: A new H, M, C or B is added.

Out-of-band: Some other protocol indicates the choice.

Where applicable, we indicate which of these three approaches and which element might be suitable.

A.1 General Requirements

REQ-1: Not specific to one scheme or country: This requirement implies that any SIP indication is flexible enough to accommodate a variety of namespaces. There currently is no indication, so current SIP cannot satisfy the requirement.

REQ-2: Independent of particular network architecture: This requirement rules out use of a new URI type (U), since all SIP-addressable resources need to be included. It also makes an out-of-band protocol difficult, as that typically pre-supposes support from network elements such as firewalls.

REQ-3: Invisible to network (IP) layer: This requirement makes use of out-of-band mechanisms difficult. Out-of-band mechanisms also would have to be directed to the all the same locations that the SIP request travels, adding difficulty.

REQ-4: Mapping of existing schemes: This requirement has similar implications as REQ-1. It calls for the ability to accommodate multi-valued enumerations of priority levels.

REQ-5: No loss of information: This requirement stipulates that there cannot be a many-to-one mapping, e.g., from some scheme to a set of integers, since information about the original scheme would be lost.

REQ-6: Extensibility: This requirement indicates the need for an IANA registry to add additional items later.

REQ-7: Separation of policy and mechanism: The mechanism must be labels, not prescriptions for detailed call handling.

REQ-8: Method-neutral: This rules out adding a new method that calls for prioritized handling.

REQ-9: Default behavior: This requirement only indicates that the specification of any such scheme needs to address default behavior in elements that expect to receive such an indication.

REQ-10: Address-neutral: This requirement rules out the use of special URIs or a new URI type. It may, however, be satisfied with a new URI parameter on all URI schemes that may be carried in SIP. This requirement is satisfied by H, M, B, and C.

REQ-11: Identity-independent: This rules out the use of a special From value.

REQ-12: Independent of network location: This requirement rules out the use of the Contact header or Via information.

REQ-13: Multiple simultaneous schemes: This requirement mandates that the indication allow a list of names.

REQ-14: Discovery: This requirement argues for the use of standard SIP negotiation mechanisms to determine the capabilities of the other side, such as Require, Proxy-Require or OPTIONS.

REQ-15: Testing: It does not appear that this adds additional protocol requirements.

REQ-16: 3PCC: All mechanisms indicated appear to satisfy this requirement.

REQ-17: Proxy-visible: This requirement rules out the use of message bodies, since these are not meant to be inspected or modified by proxies.

Given REQ-8, REQ-10, REQ-11, there does not appear to be an existing indication from which a recipient can reliably deduce resource priority. In addition, mechanisms B, M, and US fail one or more requirements, leaving mechanisms H, C and UP.

UP requires that all SIP schemes be fitted with this parameter and thus may make satisfying REQ-10 difficult.

Caller preferences describe desired capabilities and properties of the end system and are used to select among a set of candidate locations. This does not match the semantics desired here.

Thus, we will focus our attention below on the H and UP mechanisms.

The information that needs to be conveyed according to REQ-1, REQ-4, REQ-5, REQ-10, REQ-11, and REQ-12 appears to be more suitable for a request header. It logically does not describe the destination or source, but rather a property of the request. URI parameters are meant to describe properties of the

Also, there is currently no mechanism in place to negotiate support for URI parameters.

A.2 Security Requirements

SEC-1: More rigorous: SIP-related mechanisms, such as Digest authentication and hop-by-hop authentication, offer suitably strong authentication mechanisms.

However, Digest authentication can currently only provide integrity of the method, request URI and body, not header fields. Thus, an adversary could remove the indication header without detection. However, that is not likely to be more disruptive than simply removing the whole request or modifying the destination address.

Modification of the indication is not likely to be useful to an adversary unless some form of trust domain [14] is used where one element authenticates the request at a lower priority, the adversary modifies it to a higher one and then abuses those privileges in later SIP elements that trust the first element. Otherwise, increasing the priority will only incur additional authentication requirements and likely cause the request to fail.

The discussion in [15] investigates how signed SIP message bodies may be used to address this issue.

SEC-2: Attack protection: This is a generic SIP requirement. Denial of service issues are discussed at length in [2]. The reader is referred to that document for further details.

SEC-3: Independent of mechanism: The candidate mechanisms work with all existing SIP security techniques.

SEC-4: Non-trusted end systems: This requirement suggests the use of one-time passwords in SIP. This may be implementable on top of the existing Digest mechanism, but no such specification exists.

SEC-5: Replay: The approved SIP authentication mechanisms address this concern.

SEC-6: Cut-and-paste: The approved SIP authentication mechanisms address this concern.

SEC-7: Bid-down: This concern is addressed by [stalled Digest draft].

SEC-8: Confidentiality: If H or UP are used, body encryption is not effective, so that channel security is called for. Currently, SIP offers the use of IPsec and TLS.

SEC-9: Anonymity: The network-asserted identity and general privacy mechanisms [16, 13] are applicable.

SEC-10: Denial-of-service: See SEC-2.

SEC-11: Minimize resource use by unauthorized users: See SEC-2.

SEC-12: Avoid amplification: See SEC-2.

B Initial Namespace Registrations

B.1 Namespace dsn

This document defines the namespace “dsn”. The namespace “dsn” (Defense Switched Network), contains the priority values “critic-ecp”, “flash-override”, “flash”, “immediate”, “priority”, “routine”, with “critic-ecp” as the highest priority value and “routine” as the lowest.

The values are adopted from RFC 791 [10], omitting the levels "network control" and "internetwork control", as these are inappropriate here.

The value "critic-ecp" stands for "Critical and Emergency Call Processing" [10]. This value SHOULD only be used for authorized emergency communications, for example in the United States Government Emergency Telecommunications Service (GETS) [17], the United Kingdom Government Telephone Preference Scheme (GTPS) and similar government emergency preparedness or reactionary implementations elsewhere.

B.2 Namespace q735

This document also defines the namespace "q735". The namespace "q735" supports interworking with Q.735.3 (or equivalent) GSTN (ISDN) entities; this allows, for example, carrying information between Q.735.3 entities without loss of information. One or both of the SIP endpoints might be PSTN gateways. The namespace contains the priority values "0", "1", "2", "3" and "4", with "4" representing the lowest priority and "0" the highest. The default is "4".

B.3 Namespace ECS

Emergency Communication System. TBD (or moved to a separate document depending on timing). authorized emergency calls - emergency calls by the public ("911/112") - commercial priority - other non-priority calls.

C References

Normative References

[1] S. Bradner, "Key words for use in rfcs to indicate requirement levels," RFC 2119, Internet Engineering Task Force, Mar. 1997.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002.

[3] International Telecommunication Union, "Stage 3 description for community of interest supplementary services using signalling system no. 7: Multi-level precedence and preemption," Recommendation Q.735.3, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, Mar. 1993.

[4] B. Campbell, J. Rosenberg, and H. Schulzrinne, eds., "Session initiation protocol (SIP) extension for instant messaging," RFC 3428, Internet Engineering Task Force, Dec. 2002.

[5] J. Rosenberg, "The session initiation protocol (SIP) UPDATE method," RFC 3311, Internet Engineering Task Force, Oct. 2002.

[6] A. B. Roach, "Session initiation protocol (sip)-specific event notification," RFC 3265, Internet Engineering Task Force, June 2002.

[7] J. Peterson, "Enhancements for authenticated identity management in the session initiation protocol (SIP)," internet draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[8] A. R. Johnston *et al.*, “Session initiation protocol basic call flow examples,” internet draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[9] R. Sparks, “Internet media type message/sipfrag,” RFC 3420, Internet Engineering Task Force, Nov. 2002.

[10] J. B. Postel, “Internet protocol,” RFC 791, Internet Engineering Task Force, Sept. 1981.

Informative References

[11] H. Schulzrinne, “Requirements for resource priority mechanisms for the session initiation protocol,” internet draft, Internet Engineering Task Force, Dec. 2002. Work in progress.

[12] R. Sparks, “The SIP referred-by mechanism,” internet draft, Internet Engineering Task Force, Feb. 2003. Work in progress.

[13] C. Jennings, J. Peterson, and M. Watson, “Private extensions to the session initiation protocol (SIP) for asserted identity within trusted networks,” RFC 3325, Internet Engineering Task Force, Nov. 2002.

[14] M. Watson, “Short term requirements for network asserted identity,” RFC 3324, Internet Engineering Task Force, Nov. 2002.

[15] R. Mahy, “Discussion of suitability: S/MIME instead of digest authentication in the session initiation protocol (SIP),” internet draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[16] J. Peterson, “A privacy mechanism for the session initiation protocol (SIP),” RFC 3323, Internet Engineering Task Force, Nov. 2002.

[17] K. Carlberg and I. Brown, “Framework for supporting IEPS in IP telephony,” internet draft, Internet Engineering Task Force, Oct. 2001. Work in progress.

D Acknowledgments

Mike Pierce and Rohan Mahy provided helpful comments.

E Authors’ Addresses

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA
electronic mail: schulzrinne@cs.columbia.edu

James Polk
Cisco Systems
2200 East President George Bush Turnpike
Richardson, TX 75082 USA
electronic mail: jmpolk@cisco.com