Internet Engineering Task Force
Internet Draft
draft-mills-sip-access-network-info-03.txt

Duncan Mills
Vodafone

Date: June 2002
Expires: December 2002

Private Session Initiation Protocol Extension for Access Network Information

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

The distribution of this memo is unlimited.

1. Abstract

This mechanism is useful in SIP networks that provide layer 2/layer 3 connectivity through different access technologies.
This document defines the private SIP extension header P-Access-Network-Info. SIP User Agents may use this header to relay information about the access technology to serving proxies in their home network. The serving proxy may then use this information to optimize services for the UA. For example, a 3GPP terminal uses this header to pass information about the access network such as radio access technology and cell ID to its home service provider.

2. Applicability Statement

This draft is appropriate in environments where SIP services are dependent on SIP elements knowing details about the IP and lower layer technologies used by a UA to connect to the SIP network. Specifically, the extension requires that the UA know the access technology it is using, and that a proxy desires such information to provide services. Generally, SIP is built on the "Everything over IP and IP over everything" principle, where the access technology is not relevant for the operation of SIP. Since SIP systems generally should not care or even know about the access technology, this draft is not for general SIP usage.

The information revealed in the P-Access-Network-Info header is potentially very sensitive. Proper protection of this information depends on the existence of specific business and security relationships amongst the proxies that will see messages containing this header. It also depends on explicit knowledge of the UA of the existence of those relationships. Therefore, this mechanism is only suitable in environments where the appropriate relationships are in place, and the UA has explicit knowledge that they exist.

3. Conventions used in this document

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [1] and indicate requirement levels for compliant implementations.

4. Table of Contents

5. Introduction

There are many cases where a user is accessing their home network

services via a particular access network. An example is a 3GPP wireless terminal that accesses a SIP server via the UMTS Radio Access Network.

In this document we define an access network as the network providing the layer 2/layer 3 IP connectivity which in turn provides a user with access to the SIP capabilities or services provided by the home network of that user.

In some cases, the home network may wish to know information about the type of access network that the UA is currently using. Some services are more suitable or less suitable depending on the access type, and some services are of more value to subscribers if the access network details are known in the home network.

In other cases, the home network may simply wish to know crude location information in order to provide certain services to the user. For example, many of the location based services available in wireless networks today require the home network to know the identity of the cell the user is being served by.

Some regulatory requirements exist mandating that for cellular radio systems, the identity of the cell where an emergency call is established is made available to the emergency authorities.

The home network may desire knowledge about the access network. This is achieved by defining a new private SIP extension header as defined in [3], P-Access-Network-Info. This header carries information relating to the access network between the UAC and its serving proxy in the home network.

6. Overview of Operation

When a user agent generates a SIP request or response which it knows is going to be securely sent to its home network, it inserts a P-Access-Network-Info header into the message. This header contains information on the access network that the UA is using to get IP connectivity. The header is ignored by intermediate proxies between the UA and the home proxy. The home proxy can inspect the header and make use of the information contained there to provide services. Before proxying the request onwards, the home proxy strips the header from the message.

7. The P-Access-Network-Info header

The P-Access-Network-Info header is used to transport a set of parameters associated with the access characteristics of a particular network.

The information in the P-Access-Network-Info is privacy sensitive.

It is intended for use between the UA and proxies in the home network.

The P-Access-Network-Info header is described using ABNF syntax. The following description of the ABNF syntax is based on the ABNF used for SIP [3]:


```
P-Access-Network-Info              ="P-Access-Network-Info" HCOLON
                                   access-network-information

access-network-information         = access-type
                                   *(SEMI access-info]

access-type                        ="IEEE-802.11a" /
                                   "IEEE-802.11b" / "3GPP-GERAN" /
                                   "3GPP-UTRAN-FDD" /
                                   "3GPP-UTRAN-TDD" /
                                   "3GPP-CDMA2000" / token

access-info                        = cgi-3gpp /
                                   utran-cell-id-3gpp /
                                   extension-access-info

extension-access-info              = gen-value

cgi-3gpp                           = "cgi-3gpp" EQUAL (token /
                                   quoted-string)

utran-cell-id-3gpp                 = "utran-cell-id-3gpp" EQUAL
                                   (token / quoted string)
```

Access-info could contain additional information relating to the access network. The values for "cgi-3gpp" and "utran-cell-id-3gpp" are defined in 3GPP TS 24.229 [5]

The following table expands on tables 2 and 3 in [3].

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-Access-Network-Info	dr		-	o	-	o	o	o

PRA	UPD	SUB	NOT	INF	REF
o	o	o	o	o	o

Comparisons follow the case-sensitivity rules defined by SIP [3].

8. Handling of the P-Access-Network-Info header

8.1 UAC behavior

A UAC that supports this extension and is willing to disclose the related parameters MAY insert the P-Access-Network-Info header in any SIP message request.

The UAC inserting this information MUST trust the home network proxy to protect its privacy by deleting the header before forwarding the message outside of the home proxyÆs domain. In order to do this it must also have transitive trust in intermediate proxies between it and the home network proxy. This trust is established by business agreements between the home network and the access network, and generally supported by the use of standard security mechanisms, e.g. IPsec, AKA, and TLS.

This document does not define either the nature of the information or the messages where the P-Access-Network-Info needs to be inserted.

Some systems may require that the P-Access-Network-Info header is only sent by the UAC when a secure connection to the proxy in the home network is present. For example, in 3GPP systems, the UAC MUST NOT send this header in the initial unauthenticated REGISTER request.

8.2 Proxy behavior

A proxy MUST NOT insert or modify the P-Access-Network-Info header.

The proxy in the home network may act upon any information in the P-Access-Network-Info header if it is present, to provide a different service depending on the network through which the UA is accessing the server. For example, for cellular radio access networks the home network may use the cell ID to provide basic localised services.

A proxy, typically located in the home network, and therefore trusted, MUST delete the header when the SIP signaling is forwarded to a SIP server located in a non-trusted administrative network domain. The access network information is used by a home network and is of no interest to the destination network.

9. Security considerations

This extension assumes that the access network is trusted by the UA

(because the UAÆs home network has a trust relationship with the access network), as described in section 7.

This extension assumes that the information added to the header by the UAC should be sent only to trusted entities and should not be used outside of the trusted administrative network domain.

The home network uses the information contained in this header to provide additional services and UAs are expected to provide correct information. However, there are no security problems resulting from a UAC inserting incorrect information. Networks providing services based on the information carried in the P-access-network-info header will therefore need to trust the UAC sending the information. A rogue UAC sending false access network information will do no more harm than to restrict the user from using certain services.

The mechanism provided in this document is designed primarily for private systems like 3GPP. Most security requirements are met by way of private standardised solutions.

For instance, 3GPP will use the P-Access-Network-Info header to carry relatively sensitive information like the cell ID. Therefore the information MUST NOT be sent outside of the 3GPP domain. Section 8.2 of this document satisfies this requirement.

The UAC is aware - if it is a 3GPP UAC - that it is operating within a trusted domain.

The 3GPP UAC is aware of whether or not a secure connection to the home network domain for transporting SIP signalling, is currently available, and as such the sensitive information carried in the P-Access-Network-Info header should not be sent in any initial unauthenticated and unprotected requests (e.g. REGISTER). This is stated in section 8.1 of this document.

Any UAC that is using this extension and is not part of a private trusted domain should not consider the mechanism as secure and as such SHOULD NOT send sensitive information in the P-Access-Network-Info header.

Any proxy that is operating in a private trust domain where the P-Access-Network-Info header is supported is required to delete the header, if it is present, from any message prior to forwarding it outside of the trusted domain. This is stated in section 8.2.

Therefore, a home network that requires its UACs to send information in the P-access-network-info header must ensure that either that information is not of a sensitive nature or that the information is not sent outside of the trust domain.

A proxy receiving a message containing the P-Access-Network-Info header from a non-trusted entity is not able to guarantee the validity of the contents.

10. IANA Considerations

This document defines the SIP extension header field "P-Access-Network-Info" which should be included in the registry of SIP headers defined in SIP RFC 3261 [3]. As required by the SIP change process draft-tsvarea-sipchange [6] the SIP extension header name "Access-Network-Info" should also be registered in association with this extension. However, "Access-Network-Info" MUST NOT be used until documented by a standards-track RFC. Expert reveiw as required for this process is to be provided by the SIP Working Group.

The following is the registration for the P-Access-Network-Info header field:

RFC Number: RFCXXXX [Note to IANA: Fill in with the RFC number of this specification.]

Header Field Name: P-Access-Network-Info

Compact Form: None

11. References

Normative References

1. Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2. Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

3. Rosenberg, J. et al, "SIP, Session Initiation Protocol", RFC 3261, May 2002.

4. D. Crocker, Ed., and P. Overell, "Augmented BNF for syntax specifications: ABNF," RFC 2234, November 1997.

5. 3rd Generation Partnership Project; Technical Specification Group Core Network; "IP Multimedia Call Control Protocol based on SIP and SDP;" Stage 3 (Release 5)

Non-Normative References

6. Mankin, A., "SIP Change Process draft-tsvarea-sipchange", March 2002.

7. Garcia M. et al: "3GPP requirements on SIP", draft-garcia-sipping-3gpp-reqs-03.txt, September 2002, work in progress.

12. Author's Address

Duncan Mills
The Courtyard, 2-4 London Road
Newbury
Berkshire RG14 1JX
Tel: +44 1635 676074
e-mail: duncan.mills@vf.vodafone.co.uk

Full Copyright Statement