DISPATCH Working Group
Internet-Draft
Intended status: Informational
Expires: June 6, 2014

J. van Elburg
Detecon International Gmbh
K. Drage
Alcatel-Lucent
M. Ohsugi
S. Schubert
K. Arai
NTT

December 03, 2013

The Session Initiation Protocol (SIP) P-Private-Network-Indication Private-Header (P-Header) draft-vanelburg-dispatch-private-network-ind-04

Abstract

This document specifies the SIP P-Private-Network-Indication P-header used by the 3rd-Generation Partnership Project (3GPP). The P-Private-Network-Indication indicates that the message is part of the message traffic of a private network, and identifies that private network. A private network indication allows nodes to treat private network traffic according to a different set of rules than the set applicable to public network traffic.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on June 6, 2014.

Table of Contents

1. Introduction

1.1. Overview

ETSI TISPAN defined Next Generation Networks (NGN) which uses the 3rd-Generation Partnership Project (3GPP) IMS (IP Multimedia Subsystem) which in turn uses SIP (RFC3261 [RFC3261]) as its main signaling protocol. For more information on the IMS, a detailed description can be found in 3GPP TS 23.228 [3GPP.23.228] and 3GPP TS 24.229 [3GPP.24.229]. 3GPP and ETSI TISPAN have identified a set of requirements that can be met by defining a new optional SIP header, according to the procedures in RFC 5727 [RFC5727].

1.2. Applicability

According to RFC 3427 [RFC3427], P-headers have a limited applicability. Specifications of P-headers such as this RFC need to clearly document the useful scope of the proposal, and explain its limitations and why it is not suitable for the general use of SIP on the Internet.

The P-Private-Network-Indication header field is intended to be used in controlled closed networks like 3GPP IMS and ETSI TISPAN NGN networks. The P-Private-Network-Indication header is not intended for the general internet environment and is probably not suitable for such an environment.

1.3. Backgrounds

The P-Private-Network-Indication header field has been referred by 3GPP IMS specifications and has already been used in some networks as an indicator for a specific capability. The header field has been already implemented in some vendors' equipment in some countries. RFC 5727 [RFC5727] prohibits the new proposal of P-header "unless existing deployments or standards use the prefix already." The P-Private-Network-Indication header field is already used by existing deployments and 3GPP standards, therefore, this is exactly the case where the P-header is allowed as an exception.

1.4. Business communication

ETSI TISPAN has identified a framework [ETSI.181.019] for the support of business communication capabilities by the NGN. As well as the direct attachment of Next Generation Corporate Network (NGCN) equipment, this includes the capability to "host" functionality relating to an enterprise within the NGN itself.

These hosting arrangements are:

a) virtual leased line, where NGCN sites are interconnected through the NGN;

b) business trunking application, where the NGN hosts transit capabilities between NGCN's, break-in capabilities where the NGN converts public network traffic to private network traffic for delivery at a served NGCN and break-out capabilities where the NGN converts private network traffic from a served NGCN to public network traffic; and

c) hosted enterprise services, where an NGN hosts originating and/or terminating business communication capabilities for business communication users that are directly attached to an NGN.

ETSI TISPAN has requirements that can be met by the introduction of an explicit indication for private network traffic.

The traffic generated or received by a public NGN on behalf of a private network can be either:

- public network traffic: traffic sent to or received from an NGN for processing according to the rules for ordinary subscribers of a public telecommunication network. This type of traffic is known as public network traffic;

- private network traffic: traffic sent to the NGN for processing according to an agreed set of rules specific to an enterprise. This type of traffic is known as private network traffic. Private network traffic is normally exchanged within a single enterprise, but private network traffic can also be exchanged between two or more different enterprises, based on some prior arrangements, if not precluded for regulatory reasons.

1.5. Indication types

A private network indication as proposed by this document indicates to the receiving network element (supporting this specification) that this request is related to a private network traffic as opposed to a public network traffic. This indication does not identify an end user on a private network and is not for delivery to an end user on the private network. It is an indication that special service arrangements apply (if such service is configured based on private network traffic) for an enterprise, and therefore it is an indication of service on behalf of an enterprise, not an indication of service to a private network's end user.

In order to allow NGN IMS nodes to perform different processing, ETSI TISPAN formulated the following requirements on NGN:

1. The NGN shall distinguish public network traffic from private network traffic.

2. The NGN shall distinguish private network traffic belonging to one enterprise from that belonging to another enterprise.

To summarize a few example reasons for a public NGN to make the distinction between the two types of traffic:

- Different regulations apply to two types of traffic, for example an emergency calls may be handled differently depending on the type of traffic.

- Different charging regimes may apply.

- Call recording for business reasons (e.g. quality control, training, non-repudiation) might apply only to a specific type of traffic.

- Different levels of signaling and/or media transparency may apply to the different types of traffic.

There are several reasons why there is a need for an explicit indication in the signaling:

1. Caller and callee addresses can not always be used to determine whether a certain call is to be treated as private or public network traffic.

2. Nodes spanning multiple networks often need to have different behavior depending upon the type of traffic. When this is done using implicit schemes, enterprise specific logic must be distributed across multiple nodes in multiple operator's networks. That is clearly not a manageable architecture and solution.

3. There may be cases where treating the call as a public network call although both participants are from the same enterprise is advantageous to the enterprise.

Based on the background provided, this document formulates requirements for SIP to support an explicit private network indication and defines a P-header, P-Private-Network-Indication, to support those requirements.

2. Conventions

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 BCP 14, RFC 2119 [RFC2119].

3. Definitions

3.1. Traffic

In the context of this document the term traffic is understood as all communication pertaining to and/or controlled by a SIP transaction or dialog.

3.2. Public network traffic

Traffic sent to or received from a public telecommunication network for processing according to the rules for ordinary subscribers of a public telecommunication network.

3.3. Private network traffic

Traffic sent to or received from a public telecommunication network for processing according to an agreed set of rules specific to an enterprise or a community of closely related enterprises.

3.4. Break-in

Act of converting public network traffic to private network traffic. The header defined in this specification will be added to indicate the traffic is a private network traffic after conversion.

3.5. Break-out

Act of converting private network traffic to public network traffic. The header defined in this specification will be removed to indicate the traffic is a public network traffic after conversion

3.6. Trust domain

The term Trust Domain in this document is taken from RFC3324 [RFC3324]. A trust domain applies to the private network indication. The rules for specifying such a trust domain are specified in RFC3324 [RFC3324] which require the Specifying a Spec (T).

The Spec (T) need not specify the same contents and trust domain

boundaries that are used for other header fields like for example the P-Asserted-Identity.

4. Application of terminology

Figure 1 shows the interconnection of sites belonging to two private networks using the public network. Traffic in the public network relating to the interconnection of the two sites of enterprise 1 are tagged as private network traffic relating to enterprise 1. In certain cases an enterprise can also choose to send traffic from one enterprise site to another enterprise site as public network traffic when this is beneficial to the enterprise. Traffic in the public network relating to the interconnection of the two sites of enterprise 2 are tagged as private network traffic relating to enterprise 2. Enterprise 1 also generates traffic to public phones and this is public network traffic (untagged in the public network). There may be circumstances where traffic between two different enterprises are tagged as private network traffic using a pre-arranged domain name agreed by the two involved enterprises.

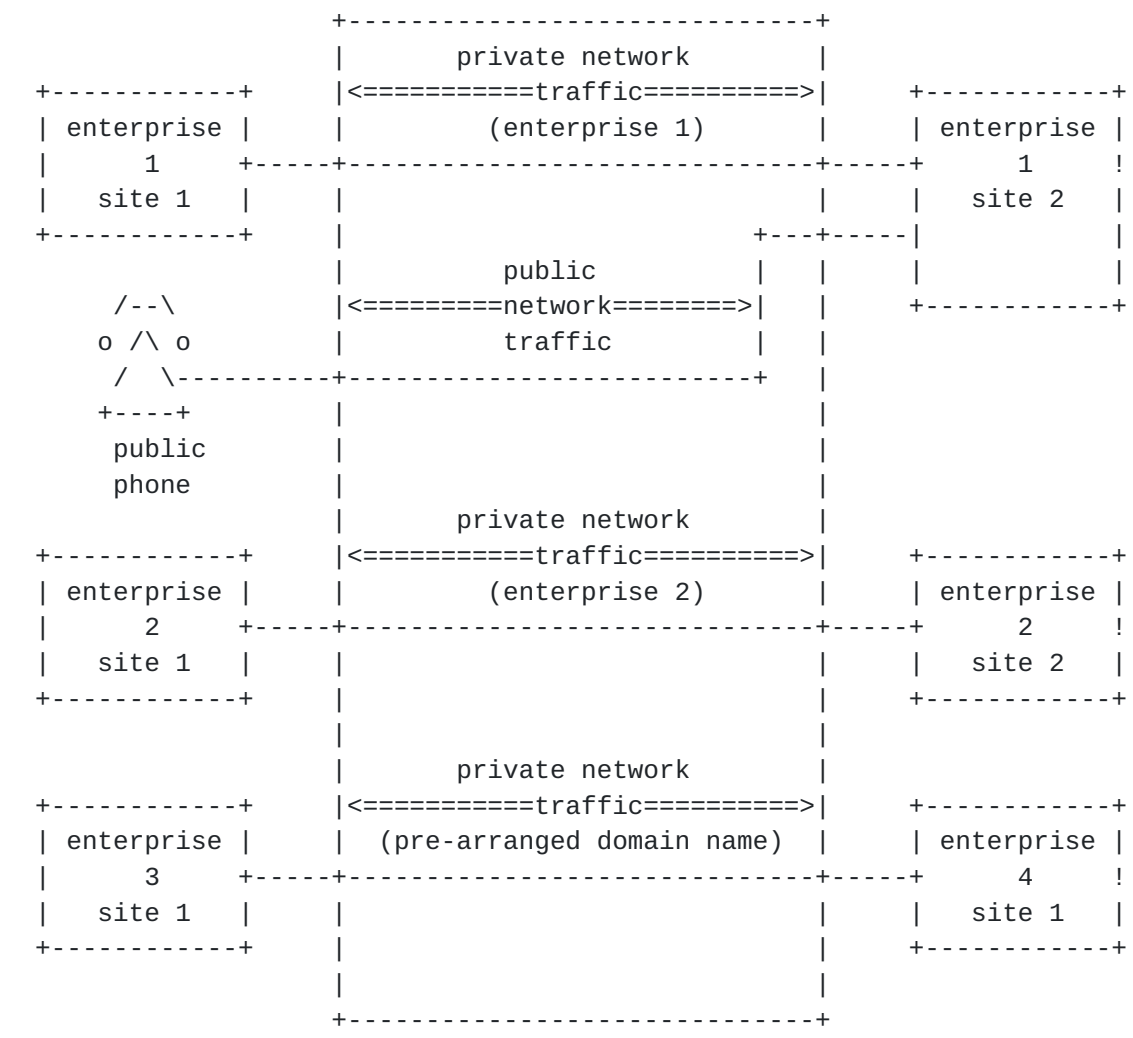

Figure 1 : Two Private Networks

Figure 2 shows the interconnection of sites belonging to a private network using the public network, and supported in the public network by a server providing a business trunking application. The business trunking application provides routing capabilities for the enterprise traffic, and supports the identification of calls to and from public network users, break-in and break-out of that traffic. (Note that the business trunking application may consist of a concatenation of application logic provided to the originating enterprise site and application logic that is provided to the terminating enterprise site.) Traffic in the public network relating to the interconnection of the two sites of enterprise 1 are tagged as private network traffic relating to enterprise 1. The business trunking application also routes traffic to public phones and this is public network traffic (untagged in the public network).

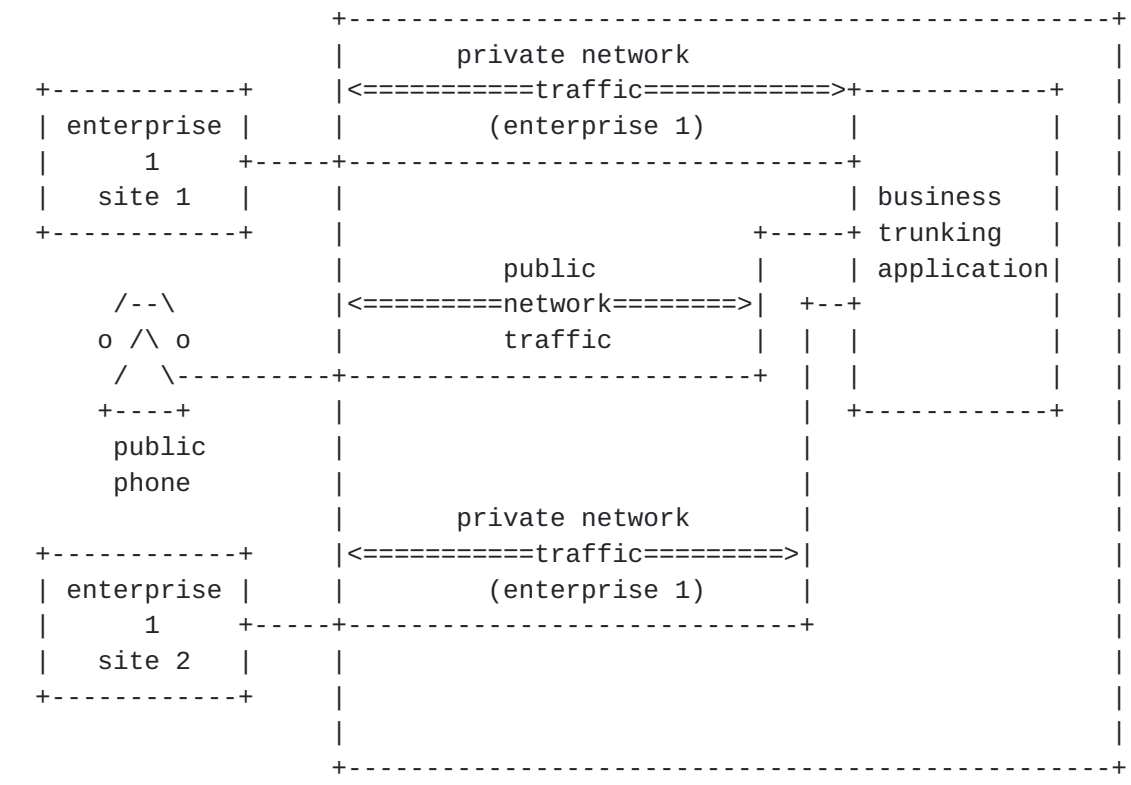

Figure 2 : Private Network and Business Trunking

Figure 3 shows the interconnection of sites belonging to a private network on a server providing a hosted enterprise service application (also known as Centrex). The hosted enterprise service application supports phones belonging to the enterprise and is also able to route traffic to and from public network phones using break-in or break-out functionality. Traffic in the public network relating to the interconnection of the site of enterprise 1 and the hosted enterprise service belonging to enterprise 1 are tagged as private network traffic relating to enterprise 1. The hosted enterprise service application also routes traffic to public phones and this is public network traffic (untagged in the public network). Traffic from the enterprise phones would not normally be tagged, but it can be tagged as private network traffic. (Note that the hosted enterprise service logic may precede or succeed a business trunking application that offers services on behalf of an enterprise site.)

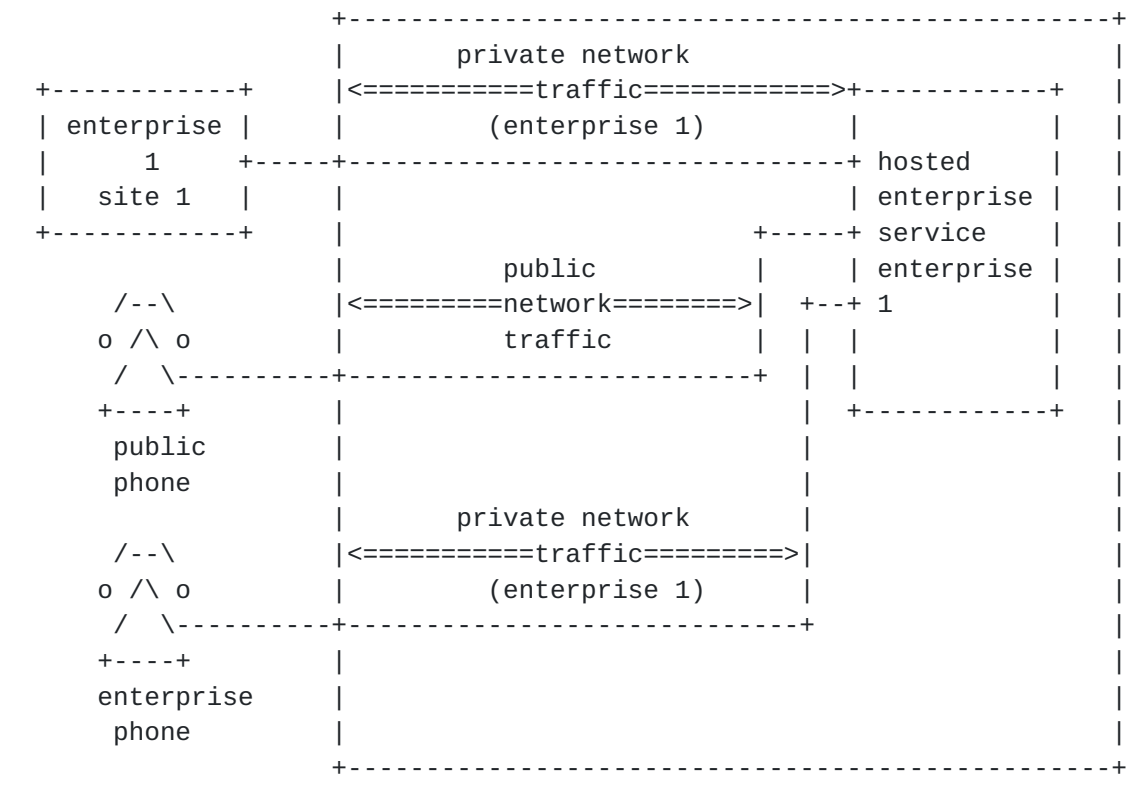

Figure 3 : Hosted Service and Private Network

5. Requirements

This section lists the requirements on SIP derived from the considerations in Section 1:

R1: It is REQUIRED that an indication can be sent in SIP initial requests for a dialog or SIP standalone requests to indicate that the request or associated session is to be treated according to the rules of private network traffic.

R2: The indication from R1 can be inserted by a SIP proxy belonging to an administrative domain for onward routing and for the traffic within that administrative domain, that needs to be so distinguished. The indication is not needed where the traffic is assumed to be all public, or where the traffic is assumed to be all private (contained within the closed network, not crossing any public network).

R3: The indication from R1 can be removed by a SIP proxy belonging to an administrative domain for onward routing where the traffic no longer needs to be so distinguished. An example exists where the traffic reaches an NGCN site where the traffic is assumed to be all private network traffic. Another example is on the final hop to the UA.

R4: It is REQUIRED that the indication from R1 allows entities to determine the set of rules that are applicable, these rules may be enterprise specific.

R5: It is REQUIRED that the indication from R1 allows entities receiving it to distinguish private network traffic from different enterprises.

R6: The identifier to distinguish private network traffic belonging to one enterprise from that belonging to another enterprise MUST be globally unique. Business communication arrangements for any particular enterprise can be expected to span multiple NGN operators potentially in multiple countries.

Note: The indication from R1 relates primarily to the SIP signaling. Applying the same concept to media may be possible, but is not necessarily meaningful where media is routed differently from signaling.

6. Overview of solution

The mechanism proposed in this document relies on a new header field called 'P-Private-Network-Indication' that contains a private network identifier expressed as a domain name, for example:

P-Private-Network-Indication: example.com

A proxy server which handles a message MAY insert such a P-Private-Network-Indication header field into the message based on authentication of the source of a message, configuration or local policy. A proxy server MAY forward the message to other proxies in the same administrative domain or proxies in a trusted domain to be handled as private network traffic. A proxy that forwards a message to a proxy server or UA that it does not trust MUST remove the P-Private-Network-Indication header field before forwarding the message.

The private network identifier expressed as a domain name allows it to be a globally unique identifier, associated with the originating

and/or terminating enterprise(s). Domain name is used, as it allows reuse of a company owned internet domain name, without requiring an additional private network identifier registry. When the enterprise needs more than one identifier it can freely add subdomains under its own control.

The formal syntax for the P-Private-Network-Indication header is presented in Section 8.

7. Behavior

7.1. Proxy behavior

7.1.1. P-Private-Network-Indication generation

Proxies that are responsible for determining certain traffic to be treated as private network traffic or contain a break-in function that converts incoming public network traffic to private network traffic MUST insert a P-Private-Network-Indication header field into incoming or outgoing requests for a dialog or for a standalone transaction. The value MUST be set to the private network identifier corresponding to the enterprise(s) to which the traffic belongs.

7.1.2. Private-Network-Indication consumption

Proxies that are responsible for applying different processing behaviors to specific private network traffic MUST support this extension. The P-Private-Network-Indication header field MUST NOT be used by a proxy in case it is received in a request from an entity that it does not trust, in such a case it MUST be removed before the request is forwarded.

7.1.3. P-Private-Network-Indication removal

Proxies that are at the edge of the trust domain or contain a break-out function that converts incoming private network traffic to public network traffic MUST remove the P-Private-Network-Indication header field before forwarding a request that contains such a header field.

7.1.4. P-Private-Network-Indication verification

When proxies supporting this specification receive a P-Private-Network-Indication header field in a SIP request from a trusted node, proxies MUST check whether the received domain name in the request is the same as the domain name associated with the provisioned domain name. If the received domain name does not match, proxies MUST remove the P-Private-Network-Indication header field.

8. P-Private-Network-Indication header field definition

This document defines the SIP P-Private-Network-Indication header field. This header field can be added by a proxy to initial requests for a dialog or standalone requests. The presence of the P-Private-Network-Indication header field signifies to proxies that understand the header field that the request is to be treated as private network traffic. The P-Private-Network-Indication header field contains a domain name value, that allows the private network traffic to be associated with an enterprise, to which it belongs and that allows proxies that understand this header field to process the request according to the local policy configured for a specific enterprise(s).

The augmented Backus-Naur Form (BNF) (RFC5234 [RFC5234]) syntax of the P-Private-Network-Indication header field is described below:

```
P-Private-Network-Indication =
                      "P-Private-Network-Indication" HCOLON PNI-value
                                                    *(SEMI PNI-param)
PNI-param                = generic-param
PNI-value                = hostname
```

EQUAL, HCOLON, SEMI, hostname and generic-param are defined in RFC3261 [RFC3261].

The following is an example of a P-Private-Network-Indication header field:

```
P-Private-Network-Indication: example.com
```

9. Security considerations

The private network indication defined in this document MUST only be used in an environment where elements are trusted and where attackers do not have access to the protocol messages between those elements. Traffic protection between network elements can be achieved by using IPsec and sometimes by physical protection of the network. In any case, the environment where the private network indication will be used ensures the integrity and the confidentiality of the contents of this header field.

A private network indication received from an untrusted node MUST NOT be used and the information MUST be removed from a request or response before it is forwarded to entities in the trust domain.

There is a security risk if a private network indication is allowed to propagate out of the trust domain where it was generated. In that case sensitive information would be revealed by such a breach. To prevent such a breach from happening, proxies MUST NOT insert the information when forwarding requests to a next hop located outside the trust domain. When forwarding the request to a trusted node, proxies MUST NOT insert the header field unless they have sufficient knowledge that the route set includes another proxy in the trust domain that understands this header field. There is no automatic mechanism to learn the support for this specification. Proxies MUST remove the information when forwarding requests to untrusted nodes or when the proxy does not have knowledge of any other proxy in the route set that is able to understand this header field.

10. IANA considerations

This document defines a new SIP header field: P-Private-Network-Indication. This header field needs to be registered by the IANA in the SIP Parameters registry under the Header Fields subregistry.

11. Acknowledgments

The authors thank Bruno Chatras, John Elwell and Salvatore Loreto for providing comments on an early version of this draft. Further we thank John Elwell for performing the expert review.

12. References

12.1. Normative references

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2002.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

12.2. Informative references

[ETSI.181.019]
ETSI, "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements", ETSI TS 181 019 V2, July 2007.

[3GPP.23.228]
3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 V8, July 2007.

[3GPP.24.229]
3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 V8, July 2007.

[RFC3427] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J., and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", RFC 3427, December 2002.

[RFC3455] Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

[RFC3841] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)", RFC 3841, August 2004.

[RFC5727] Peterson, J., Jennings, C., and R. Sparks, "Change Process for the Session Initiation Protocol (SIP) and the Real-time Applications and Infrastructure Area", BCP 67, RFC 5727, March 2010.

[RFC6050] Drage, K., "A Session Initiation Protocol (SIP) Extension for the Identification of Services", RFC 6050, November 2010.

Appendix A. Alternative solutions discussed

Note: The RFC Editor will remove these Appendixes.

A.1. General

It would be technical possible, but extremely complex to perform this function without an explicit indication. For example, a logical distinction of proxies to handle private network traffic relating to enterprise 1, enterprise 2 and the public network traffic could be made by assigning different SIP URIs to these logical entities. This is not regarded as a viable solution.

Several solutions have been raised and whether or not they are suitable and fulfill the requirements need to be discussed:

- Attribute on existing header?
- Token on some existing header?
- Resource-Priority header?
- P-Asserted-Service header?
- Request-Disposition header?
- P-Access-Network-Information header?
- URI parameter?
- New P-header?
- New header?

A.2. Attribute on existing header field

A.3. Token value on existing header field

A.4. Resource-Priority header field

Some of the distinctive functions are already provided for in this header field. A potential mechanism would be to define a namespace for private network traffic. It would however be impossible to define a namespace for each enterprise, and therefore some additional parameter would need to be defined to carry the unique identifier of the particular enterprise to which the private network traffic relates. Successful usage may also require a tightening of the procedures for use of the Resource-Priority header field (much at the moment is left to the particular application of this header field).

Private network traffic may, but is not necessarily handled with a different priority then public network traffic. Use of the Resource-

Priority header field however seems to imply that the main focus of the indication is on prioritizing private network traffic. This may render use of the Resource-Priority header field as less appropriate for our particular purpose.

A.5. P-Asserted-Service header field

The services envisaged by the P-Asserted-Service header field (RFC6050 [RFC6050]) are those applied to the end user. The end user in these cases is the end user of the enterprise or NGCN, not the enterprise itself. Therefore this header field is not considered suitable for this problem.

A.6. Request-Disposition header field

The Request-Disposition header field (RFC3841 [RFC3841]) specifies caller preferences for how a server should process a request. The caller in these cases is the end user of the enterprise or NGCN, not the enterprise itself. Therefore this header field is not considered suitable for this problem. Further RFC3841 explicitly states that the set of request disposition directives is not extensible.

A.7. P-Access-Network-Information

The P-Access-Network-Info header field (RFC3455 [RFC3455]) contains information about the access network that a UA uses to get IP connectivity. However the access that one uses does not define the private network that a call that one sets up is to be part of.

Particular examples that illustrate this:

- A Hosted Enterprise Services user (i.e. Centrex) uses the access of the operator while still being able to setup calls that will turn out to be private network traffic.

- A corporate network UE that attaches to an operator network, but receives services from its home corporate network.

A.8. URI parameter

A marking on the entities within the Via header field that are treating this as private network traffic. Potential marking on the route header field of entities that are expected to treat it as private network traffic.

A.9. New header field

A.9.1. General

If none of the existing header fields is appropriate a logical step is to define a new header field for the private network indication.

A.9.2. Full SIP header field

A full SIP header field is appropriate when the usage of this information element is more general then closed networks like ETSI TISPAN NGN or 3GPP IMS.

A.9.3. New P-header field

In case no general usage is foreseen other then usage in closed networks like those specified by ETSI TISPAN NGN or 3GPP IMS a P-header field seems the appropriate choice.

Appendix B. Revision Information

B.1. version 00, SIPPING

1. 2008-02-18, Initial version

B.2. version 01, SIPPING

1. 2008-02-23, Added a solution based on a new header field. Added Overview, Behavior and Header Definition sections. Updated the trust domain definition. Improved some of the existing text based on comments from John Elwell.

B.3. version 02, SIPPING

1. 2008-07-11, Changed to a P-header field. Changed title. Added Terminology application and Applicability sections. Moved the Potential solutions section to appendix Alternative solutions discussed.

B.4. version 03, SIPPING

1. 2009-02-19, Updated boilerplate.

B.5. version 00, DISPATCH

1. 2009-07-06, Updates as result of Expert review. Moved to DISPATCH.

B.6. version 01, DISPATCH

1. 2010-06-15, Resubmission. Authors address changed. No content changes. Moved reference to RFC3427 to informative section as it is deprecated by RFC5727 [RFC5727].

B.7. version 02, DISPATCH

1. 2013-07-12, Updates according to the comments after Expert review. Some changes for the consistency with other RFCs that specify P-headers. Some editorial changes.

B.8. version 03, DISPATCH

1. 2013-09-12, Updates according to the discussion in DISPATCH list.

Authors' Addresses

Hans Erik van Elburg
Detecon International Gmbh
Oberkasselerstrasse 2
Bonn 53227
Germany

Email: ietf.hanserik@gmail.com

Keith Drage
Alcatel-Lucent
The Quadrant, Stonehill Green, Westlea
Swindon SN5 7DJ
UK

Email: drage@alcatel-lucent.com

Mayumi Ohsugi
NTT Corporation

Phone: +81 422 36 7502
Email: mayumi.ohsugi@ntt-at.co.jp

Shida Schubert
NTT Corporation

Phone: +1 415 323 9942
Email: shida@ntt-at.com

Kenjiro Arai
NTT Corporation
9-11, Midori-cho 3-Chome
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 3518
Email: arai.kenjiro@lab.ntt.co.jp
URI: http://www.ntt.co.jp