Network Working Group
Request for Comments: 3012
Category: Standards Track

C. Perkins
Nokia Research Center
P. Calhoun
Sun Microsystems Laboratories

November 2000

Mobile IPv4 Challenge/Response Extensions

Status of this Memo

Copyright Notice

Abstract

Mobile IP, as originally specified, defines an authentication extension (the Mobile-Foreign Authentication extension) by which a mobile node can authenticate itself to a foreign agent. Unfortunately, this extension does not provide ironclad replay protection for the foreign agent, and does not allow for the use of existing techniques (such as CHAP) for authenticating portable computer devices. In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow a foreign agent to use a challenge/response mechanism to authenticate the mobile node.

Table of Contents

1. Introduction

Mobile IP, as originally specified, defines an authentication extension (the Mobile-Foreign Authentication extension) by which a mobile node can authenticate itself to a foreign agent.

Unfortunately, this extension does not provide ironclad replay protection, from the point of view of the foreign agent, and does not allow for the use of existing techniques (such as CHAP [12]) for authenticating portable computer devices. In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow a foreign agent to a use challenge/response mechanism to authenticate the mobile node.

All SPI values defined in this document refer to values for the Security Parameter Index, as defined in RFC 2002 [8]. 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 [1].

2. Mobile IP Agent Advertisement Challenge Extension

This section defines a new extension to the Router Discovery Protocol [3] for use by foreign agents that need to issue a challenge for authenticating mobile nodes.

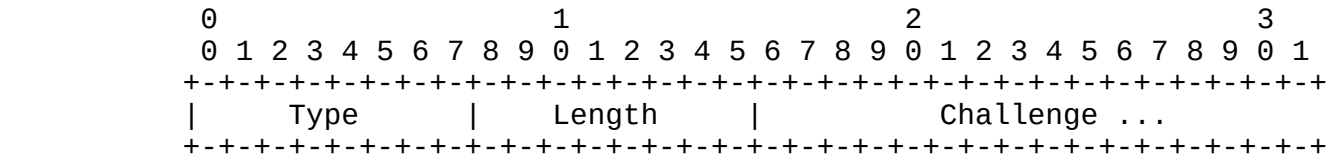

Figure 1: The Challenge Extension

Type 24

Length The length of the Challenge value in bytes; SHOULD be at least 4

Challenge A random value that SHOULD be at least 32 bits.

The Challenge extension, illustrated in figure 1, is inserted in the Agent Advertisements by the Foreign Agent, in order to communicate the latest challenge value that can be used by the mobile node to compute an authentication for its registration request message. The challenge is selected by the foreign agent to provide local assurance that the mobile node is not replaying any earlier registration request. Eastlake, et al. [4] provides more information on generating pseudo-random numbers suitable for use as values for the challenge.

3. Operation

This section describes modifications to the Mobile IP registration process which may occur after the Foreign Agent issues a Mobile IP Agent Advertisement containing the Challenge on its local link.

3.1. Mobile Node Processing for Registration Requests

Whenever the Agent Advertisement contains the Challenge extension, if the mobile node does not have a security association with the Foreign Agent, then it MUST include the Challenge value in a MN-FA Challenge extension to the Registration Request message. If, on the other hand, the mobile node does have a security association with the foreign agent, it SHOULD include the Challenge value in its Registration Request message.

If the Mobile Node has a security association with the Foreign Agent, it MUST include a Mobile-Foreign Authentication extension in its Registration Request message, according to the base Mobile IP specification [8]. When the Registration Request contains the MN-FA Challenge extension specified in section 4, the Mobile-Foreign Authentication MUST follow the Challenge extension in the Registration Request.

If the Mobile Node does not have a security association with the Foreign Agent, the Mobile Node MUST include the MN-AAA Authentication extension as defined in section 6. In addition, the Mobile Node SHOULD include the NAI extension [2], to enable the foreign agent to make use of any available verification infrastructure. The SPI field of the MN-AAA Authentication extension specifies the particular secret and algorithm (shared between the Mobile Node and the verification infrastructure) that must be used to perform the authentication. If the SPI value is chosen as CHAP_SPI (see section 9), then the mobile node specifies CHAP-style authentication [12] using MD5 [11].

In either case, the MN-FA Challenge extension and one of the above specified authentication extensions MUST follow the Mobile-Home Authentication extension, if present.

A successful Registration Reply from the Foreign Agent MAY include a new Challenge value (see section 3.3). The Mobile Node MAY use either the value found in the latest Advertisement, or the one found in the last Registration Reply from the Foreign Agent. This approach enables the Mobile Node to make use of the challenge without having to wait for advertisements.

A Mobile Node might receive an UNKNOWN_CHALLENGE error (see section 9) if it moves to a new Foreign Agent that cannot validate the challenge provided in the Registration Request. In such instances, the Mobile Node MUST use a new Challenge value in any new registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

A Mobile Node that does not include a Challenge when the Mobile-Foreign Authentication extension is present may receive a MISSING_CHALLENGE (see section 10) error. In this case, the foreign agent will not process the request from the mobile node unless the request contains a valid Challenge.

A Mobile Node that receives a BAD_AUTHENTICATION error code (see section 10) SHOULD include the MN-AAA Authentication Extension in the next Registration Request. This will make it possible for the Foreign Agent to use its AAA infrastructure in order to authenticate the Mobile Node.

3.2. Foreign Agent Processing for Registration Requests

Upon receipt of the Registration Request, if the Foreign Agent has issued a Challenge as part of its Agent Advertisements, and it does not have a security association with the mobile node, then the Foreign Agent MUST check that the MN-FA Challenge extension exists, and that it contains a challenge value previously unused by the Mobile Node. This ensures that the mobile node is not attempting to replay a previous advertisement and authentication. If the challenge extension is needed and does not exist, the Foreign Agent MUST send a Registration Reply to the mobile node with the error code MISSING_CHALLENGE.

A foreign agent that sends Agent Advertisements containing a Challenge value MAY send a Registration Reply message with a MISSING_CHALLENGE error if the mobile node sends a Registration Request with a Mobile-Foreign Authentication extension without including a Challenge. In other words, such a foreign agent MAY refuse to process a Registration Request request from the mobile node unless the request contains a valid Challenge.

If a mobile node retransmits a Registration Request with the same Identification field and the same Challenge extension, and the Foreign Agent still has a pending Registration Request record in effect for the mobile node, then the Foreign Agent forwards the Registration Request to the Home Agent again. In all other circumstances, if the Foreign Agent receives a Registration Request with a Challenge extension containing a Challenge value previously used by that mobile node, the Foreign Agent SHOULD send a Registration Reply to the mobile node containing the Code value STALE_CHALLENGE.

The Foreign Agent MUST NOT accept any Challenge in the Registration Request unless it was offered in last successful Registration Reply issued to the Mobile Node, or else advertised as one of the last CHALLENGE_WINDOW (see section 9) Challenge values inserted into the immediately preceding Agent advertisements. If the Challenge is not one of the recently advertised values, the foreign Agent SHOULD send a Registration Reply with Code UNKNOWN_CHALLENGE (see section 10).

Furthermore, the Foreign Agent MUST check that there is either a Mobile-Foreign, or a MN-AAA Authentication extension after the Challenge extension. Any registration message containing the Challenge extension without either of these authentication extensions MUST be silently discarded. If the registration message contains a Mobile-Foreign Authentication extension with an incorrect authenticator that fails verification, the Foreign Agent MAY send a Registration Reply to the mobile node with Code value BAD_AUTHENTICATION (see Section 10).

If the MN-AAA Authentication extension (see Section 6) is present in the message, or if an NAI extension is included indicating that the mobile node belongs to a different administrative domain, the foreign agent may take actions outside the scope of this protocol specification to carry out the authentication of the mobile node. The Foreign Agent MUST NOT remove the MN-AAA Authentication Extension from the Registration Request prior to the completion of the authentication performed by the AAA infrastructure. The appendix provides an example of an action that could be taken by a foreign agent.

In the event that the Challenge extension is authenticated through the Mobile-Foreign Authentication Extension, the Foreign Agent MAY remove the Challenge Extension from the Registration Request without disturbing the authentication value computed by the Mobile Node for use by the AAA or the Home Agent. If the Challenge extension is not removed, it MUST precede the Foreign-Home Authentication extension.

If the Foreign Agent does not remove the Challenge extension, then the Foreign Agent SHOULD store the Challenge value as part of the pending registration request list [8]. Also in this case, the Foreign Agent MUST reject any Registration Reply message coming from the Home Agent that does not also include the Challenge Extension with the same Challenge Value that was included in the Registration Request. The Foreign Agent MUST send the rejected Registration message to the mobile node, and change the status in the Registration Reply to the value MISSING_CHALLENGE (see section 10).

If the Foreign Agent does remove the Challenge extension and applicable authentication from the Registration Request message, then it SHOULD insert the Identification field from the Registration Request message along with its record-keeping information about the particular Mobile Node in order to protect against replays.

3.3. Foreign Agent Processing for Registration Replies

The Foreign Agent MAY include a new Challenge extension in any Registration Reply, successful or not. If the foreign agent includes this extension in a successful Registration Reply, the extension SHOULD precede a MN-FA authentication extension.

Suppose the Registration Reply includes a Challenge extension from the Home Agent, and the foreign agent wishes to include another Challenge extension with the Registration Reply for use by the mobile node. In that case, the foreign agent MUST delete the Challenge extension from the Home Agent from the Registration Reply, along with any FA-HA authentication extension, before appending the new Challenge extension to the Registration Reply.

3.4. Home Agent Processing for the Challenge Extensions

If the Home Agent receives a Registration Request with the MN-FA Challenge extension, and recognizes the extension, the Home Agent MUST include the Challenge extension in the Registration Reply. The Challenge Extension MUST be placed after the Mobile-Home authentication extension, and the extension SHOULD be authenticated by a Foreign-Home Authentication extension.

Since the extension type for the Challenge extension is within the range 128-255, the Home Agent MUST process such a Registration Request even if it does not recognize the Challenge extension [8]. In this case, the Home Agent will send a Registration Reply to the Foreign Agent that does not include the Challenge extension.

4. MN-FA Challenge Extension

This section specifies a new Mobile IP Registration extension that is used to satisfy a Challenge in an Agent Advertisement. The Challenge extension to the Registration Request message is used to indicate the challenge that the mobile node is attempting to satisfy.

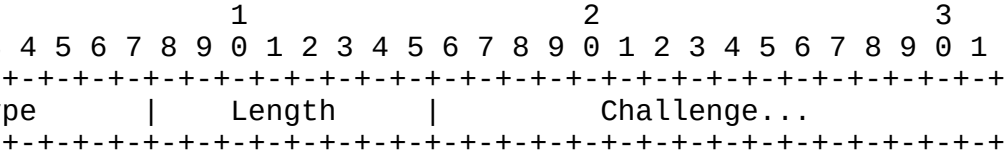

Figure 2: The MN-FA Challenge Extension

Type 132 (skippable) (see [8])

Length Length of the Challenge value

Challenge The Challenge field is copied from the Challenge field found in the Agent Advertisement Challenge extension (see section 2).

5. Generalized Mobile IP Authentication Extension

Several new authentication extensions have been designed for various control messages proposed for extensions to Mobile IP (see, for example, [9]). A new authentication extension is required for a mobile node to present its credentials to any other entity other than the ones already defined; the only entities defined in the base Mobile IP specification [8] are the home agent and the foreign agent. It is the purpose of the generalized authentication extension defined here to collect together data for all such new authentication applications into a single extension type with subtypes.

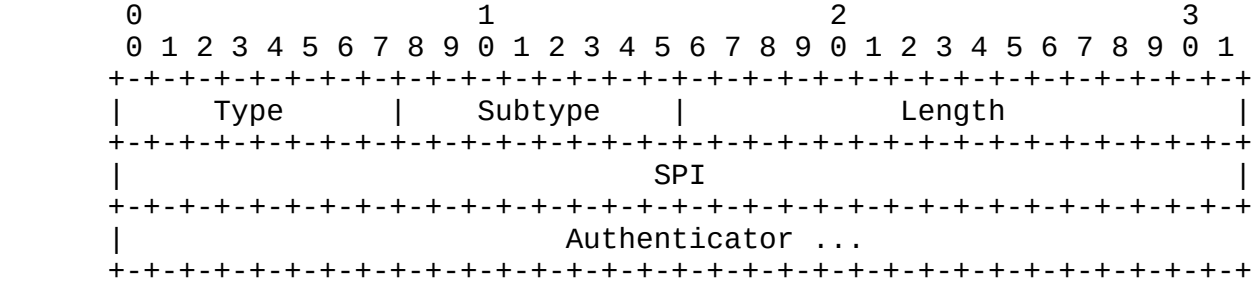

Figure 3: The Generalized Mobile IP Authentication Extension

Type 36 (not skippable) (see [8])

Subtype a number assigned to identify the kind of endpoints or characteristics of the particular authentication strategy

Length 4 plus the number of bytes in the Authenticator; MUST be at least 20.

SPI Security Parameters Index

Authenticator The variable length Authenticator field

In this document, only one subtype is defined:

1 MN-AAA Authentication subtype (see section 6)

6. MN-AAA Authentication subtype

The Generalized Authentication extension with subtype 1 will be referred to as a MN-AAA Authentication extension. If the mobile node does not include a Mobile-Foreign Authentication [8] extension, then it MUST include the MN-AAA Authentication extension whenever the Challenge extension is present. If the MN-AAA Authentication extension is present, then the Registration Message sent by the mobile node MUST contain the Mobile-HA Authentication extension [8] if it shares a security association with the Home Agent. If present, the Mobile-HA Authentication Extension MUST appear prior to the MN-AAA Authentication extension. The mobile node MAY include a MN-AAA Authentication extension in any Registration Request. The corresponding response MUST include the MN-HA Authentication Extension, and MUST NOT include the MN-AAA Authentication Extension.

The default algorithm for computation of the authenticator is HMAC-MD5 [5] computed on the following data, in the order shown:

```
Preceding Mobile IP data || Type, Subtype, Length, SPI
```

where the Type, Length, Subtype, and SPI are as shown in section 5. The resulting function call, as described in [5], would be:

```
hmac_md5(data, datalen, Key, KeyLength, authenticator);
```

Each mobile node MUST support the ability to produce the authenticator by using HMAC-MD5 as shown. Just as with Mobile IP, this default algorithm MUST be able to be configured for selection at any arbitrary 32-bit SPI outside of the SPIs in the reserved range 0-255.

7. Reserved SPIs for Mobile IP

Mobile IP defines several authentication extensions for use in Registration Requests and Replies. Each authentication extension carries a Security Parameters Index (SPI) which should be used to index a table of security associations. Values in the range 0 - 255 are reserved for special use. A list of reserved SPI numbers is to be maintained by IANA at the following URL:

```
http://www.iana.org/numbers.html
```

8. SPI For RADIUS AAA Servers

Some AAA servers only admit a single security association, and thus do not use the SPI numbers for Mobile IP authentication extensions for use when determining the security association that would be necessary for verifying the authentication information included with the Authentication extension.

SPI number CHAP_SPI (see section 9) is reserved (see section 7) for indicating the following procedure for computing authentication data (called the "authenticator"), which is used by many RADIUS servers [10] today.

To compute the authenticator, apply MD5 [11] computed on the following data, in the order shown:

```
High-order byte from Challenge || Key ||
MD5(Preceding Mobile IP data ||
Type, Subtype (if present), Length, SPI) ||
Least-order 237 bytes from Challenge
```

where the Type, Length, SPI, and possibly Subtype, are the fields of the authentication extension in use. For instance, all four of these fields would be in use when SPI == CHAP_SPI is used with the Generalized Authentication extension. Since the RADIUS protocol cannot carry attributes greater than 253 in size, the preceding Mobile IP data, type, subtype (if present), length and SPI are hashed using MD5. Finally, the least significant 237 bytes of the challenge are concatenated.

9. Configurable Parameters

Every Mobile IP agent supporting the extensions defined in this document SHOULD be able to configure each parameter in the following table. Each table entry contains the name of the parameter, the default value, and the section of the document in which the parameter first appears.

Parameter Name	Default Value	Section(s) of Document
CHALLENGE_WINDOW	2	3.2
CHAP_SPI	2	8

10. Error Values

Each entry in the following table contains the name of Code [8] to be returned in a Registration Reply, the value for the Code, and the section in which the error is first mentioned in this specification.

Error Name	Value	Section of Document
UNKNOWN_CHALLENGE	104	3.2
BAD_AUTHENTICATION	67	3.2 - also see [8]
MISSING_CHALLENGE	105	3.1,3.2
STALE_CHALLENGE	106	3.2

11. IANA Considerations

The Generalized Mobile IP Authentication extension defined in Section 5 is a Mobile IP registration extension as defined in RFC 2002 [8] and extended in RFC 2356 [7]. IANA should assign a value of 36 for this extension.

A new number space is to be created for enumerating subtypes of the Generalized Authentication extension (see section 5). New subtypes of the Generalized Authentication extension, other than the number (1) for the MN-AAA authentication extension specified in section 6, must be specified and approved by a designated expert.

The MN-FA Challenge Extension defined in Section 4 is a router advertisement extension as defined in RFC 1256 [3] and extended in RFC 2002 [8]. IANA should assign a value of 132 for this purpose.

The Code values defined in Section 10 are error codes as defined in RFC 2002 [8] and extended in RFC 2344 [6] and RFC 2356 [7]. They correspond to error values conventionally associated with rejection by the foreign agent (i.e., values from the range 64-127). The Code value 67 is a pre-existing value which is to be used in some cases with the extension defined in this specification. IANA should record the values as defined in Section 10.

A new section for enumerating algorithms identified by specific SPIs within the range 0-255 is to be added to

http://www.isi.edu/in-notes/iana/assignments/mobileip-numbers.

The CHAP_SPI number (2) discussed in section 8 is to be assigned from this range of reserved SPI numbers. New assignments from this reserved range must be specified and approved by the Mobile IP working group. SPI number 1 should not be assigned unless in the future the Mobile IP working group decides that SKIP is not important for enumeration in the list of reserved numbers. SPI number 0 should not be assigned.

12. Security Considerations

In the event that a malicious mobile node attempts to replay the authenticator for an old MN-FA Challenge, the Foreign Agent would detect it since the agent always checks whether it has recently advertised the Challenge (see section 3.2). Allowing mobile nodes with different IP addresses or NAIs to use the same Challenge value does not represent a security vulnerability, because the authentication data provided by the mobile node will be computed over data that is different (at least by the bytes of the mobile nodes' IP addresses).

Whenever a Foreign Agent updates a field of the Registration Reply (as suggested in section 3.2), it invalidates the authentication data supplied by the Home Agent in the MN-HA Authentication extension to the Registration Reply. Thus, this opens up a security exposure whereby a node might try to supply a bogus Registration Reply to a mobile node that causes the mobile node to act as if its Registration Reply were rejected. This might happen when, in fact, a Registration Reply showing acceptance of the registration might soon be received by the mobile node.

If the foreign agent chooses a Challenge value (see section 2) with fewer than 4 bytes, the foreign agent SHOULD maintain records that also the Identification field for the mobile node. The foreign agent can then find assurance that the Registration messages using the short Challenge value are in fact unique, and thus assuredly not replayed from any earlier registration.

Section 8 (SPI For RADIUS AAA Servers) defines a method of computing the Generalized Mobile IP Authentication Extension's authenticator field using MD5 in a manner that is consistent with RADIUS [10]. The use of MD5 in the method described in Section 8 is less secure than HMAC-MD5 [5], and should be avoided whenever possible.

13. Acknowledgements

The authors would like to thank Tom Hiller, Mark Munson, the TIA TR45-6 WG, Gabriel Montenegro, Vipul Gupta, and Pete McCann for their useful discussions. A recent draft by Mohamed Khalil, Raja Narayanan, Emad Qaddoura, and Haseeb Akhtar has also suggested the definition of a generalized authentication extension similar to the specification contained in section 5.

References

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

[2] Calhoun, P. and C. Perkins. "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, January 2000.

[3] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[4] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[5] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[6] Montenegro, G., "Reverse Tunneling for Mobile IP", RFC 2344, May 1998.

[7] Montenegro, G. and V. Gupta, "Sun’s SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998.

[8] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[9] Perkins, C. and D. Johnson, "Route Optimization in Mobile IP", Work in Progress.

[10] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[11] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[12] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

A. Verification Infrastructure

The Challenge extensions in this protocol specification are expected to be useful to help the Foreign Agent manage connectivity for visiting mobile nodes, even in situations where the foreign agent does not have any security association with the mobile node or the mobile node's home agent. In order to carry out the necessary authentication, it is expected that the foreign agent will need the assistance of external administrative systems, which have come to be called AAA systems. For the purposes of this document, we call the external administrative support the "verification infrastructure". The verification infrastructure is described to motivate the design of the protocol elements defined in this document, and is not strictly needed for the protocol to work. The foreign agent is free to use any means at its disposal to verify the credentials of the mobile node. This could, for instance, rely on a separate protocol between the foreign agent and the Mobile IP home agent, and still be completely invisible to the mobile node.

In order to verify the credentials of the mobile node, we imagine that the foreign agent has access to a verification infrastructure that can return a secure notification to the foreign agent that the authentication has been performed, along with the results of that authentication. This infrastructure may be visualized as shown in figure 4.

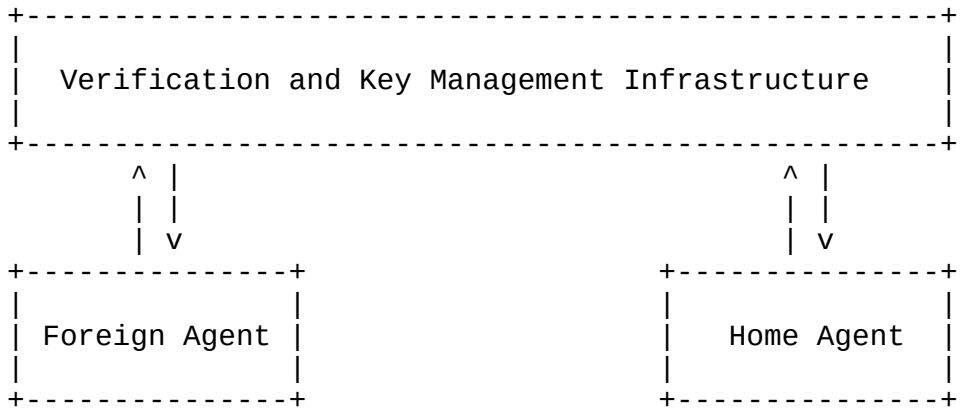

Figure 4: The Verification Infrastructure

After the foreign agent gets the Challenge authentication, it MAY pass the authentication to the (here unspecified) infrastructure, and await a Registration Reply. If the Reply has a positive status (indicating that the registration was accepted), the foreign agent

accepts the registration. If the Reply contains the Code value BAD_AUTHENTICATION (see Section 10), the foreign agent takes actions indicated for rejected registrations.

Implicit in this picture, is the important observation that the Foreign Agent and the Home Agent have to be equipped to make use of whatever protocol is made available to them by the challenge verification and key management infrastructure shown in the figure.

The protocol messages for handling the authentication within the verification infrastructure, and identity of the agent performing the verification of the Foreign Agent challenge, are not specified in this document, because those operations do not have to be performed by any Mobile IP entity.

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
M/S M8-540
Irving, Texas 75039
USA

Phone: +1 972-894-6709
Fax : +1 972-894-5349
EMail: Basavaraj.Patil@nokia.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA

Phone:+1 847-632-3148
EMail: QA3445@email.mot.com

Questions about this memo can also be directed to the authors:

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA

Phone: +1-650 625-2986
Fax: +1 650 625-2502
EMail: charliep@iprg.nokia.com

Pat R. Calhoun
Network & Security Center
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650-786-7733
Fax: +1 650-786-6445
EMail: pcalhoun@eng.sun.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.