PANA Working Group
Internet Draft
Document: draft-ietf-pana-ipsec-04.txt
Expires: March 2005

M. Parthasarathy
Nokia

September 2004

PANA enabling IPsec based Access Control

Status of this Memo

This Internet-Draft will expire on December 2004.

Copyright Notice

Abstract

The PANA (Protocol for carrying Authentication for Network Access) working group is developing a protocol for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of a successful authentication. This document discusses the details for establishing an IPsec security association using the PANA security association for enabling IPsec based access control.

Table of Contents

1.0 Introduction

The PANA (Protocol for carrying Authentication for Network Access) working group is developing a protocol for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of successful authentication. The PANA authentication agent (PAA) indicates the results of the authentication using the PANA-Bind-Request message wherein it can indicate the access control method enforced by the access network. The PANA protocol [PANA-PROT] does not discuss any details of IPsec [RFC2401] security association (SA) establishment, when IPsec is used for access control. This document discusses the details of establishing an IPsec security association between PANA client and the enforcement point. The IPsec SA is established using IKE, which in turn uses the pre-shared key derived from the PANA SA for authentication. The IPsec SA used to protect the packet provides the assurance that the packet comes from the client that authenticated to the network. Thus, the IPsec can be used for access control and specifically used to prevent the service theft mentioned in [PANA-THREATS]. The term "access control" in this document refers to the per-packet authentication provided by IPsec.

Please refer to [PANAREQ] for terminology and definitions of terms used in this document. The following picture illustrates what is being protected with IPsec. The different scenarios of PANA usage are described in the [PANAREQ]. When IPsec is used, scenario 3 and 5 are supported as shown below. As shown in Figure 1, Enforcement Point (EP), Access Router (AR) and the PANA authentication agent are co-located which is described as scenario 3 in [PANAREQ].

```
                   PaC ----------------------+
                   [D1]                      |
                                             +------EP/AR/PAA
                                             |
                   PaC ----------------------+
                   [D2]
                   |-----------IPsec----------|
```

Figure 1: PAA/EP/AR are co-located

As show in Figure 2, only AR and EP are co-located. PAA is a separate node though located on the same link as AR and EP. All of them are one IP hop away from the PaC. This is the same as scenario 5 described in [PANAREQ].

```
                                     +------PAA
                                     |
                   PaC ----------------------+
                   [D1]                      |
                                             +------EP/AR
                                             |
                   PaC ----------------------+
                   [D2]

                   |-----------IPsec----------|
```

Figure 2: EP and AR are co-located

The IPsec security association protects the traffic between PaC and EP. In IPsec terms, EP is a security gateway (therefore a router) and forwards packets coming from the PaC to other nodes.

First, this document discusses some of the pre-requisites for IPsec SA establishment. Next, it gives details on what should be communicated between PAA and EP. Then, it gives the details of IKE exchange with IPsec packet formats and SPD entries. Finally, it discusses the dual stack operation.

2.0 Keywords

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 [RFC2118].

3.0 Pre-requisites for IPsec SA establisment

This document assumes that the following have already happened before the IKE exchange starts.

1) PANA client (PaC) and PAA mutually authenticate each other using EAP methods that derive AAA-key [EAP-KEY].

2) PaC learns the IP address of the Enforcement point (EP) during the PANA exchange.

3) PaC learns that the network uses IPsec [RFC2401] for securing the link between PaC and EP during the PANA exchange.

4.0 IP Address Configuration

The IP address configuration is explained in [PANA-FRAME]. Some of the details relevant to IPsec are briefly repeated here for clarity. PaC configures an IP address before the PANA protocol exchange begins. This address is called a pre-PANA address (PRPA). After a successful authentication, the client may have to configure a post-PANA address (POPA) for communication with other nodes, if PRPA is a local-use (e.g., link-local or private address) or a temporarily allocated IP address.

The PRPA of the PaC may be a link-local address [IPV4-LINK] or a private address [RFC1918] or a routable address or an IPv6 link-local address [RFC2462]. Please refer to [PANA-FRAME] for more details on how these addresses may be configured. PaC would use the PRPA as the outer address of IPsec tunnel mode SA (IPsec-TOA). PaC also needs to configure an inner address (IPsec-TIA). There are different ways to configure IPsec-TIA.

1) Some IPv4 IPsec implementations are known to work properly when the same address is configured as both the IPsec-TIA and IPsec-TOA. When PRPA is a routable address, PRPA may be used as both IPsec-TIA and IPsec-TOA and POPA may not be configured.

2) In IPv4, an IPsec-TIA can be obtained via the configuration method available using DHCP over IPsec tunnels [RFC3456]. The minor difference from the original usage of [RFC3456] is that the IPsec-TOA does not need to be a routable address when [RFC3456] is used between PaC and EP.

3) When IKEv2 [IKEV2] is used for security association negotiation, the address configuration method available in [IKEV2] can be used for configuring the IPsec-TIA for both IPv4 and IPv6.

There are other address configuration methods possible. They have some implementation issues, which are described in the Appendix A.

5.0 IKE Pre-shared key derivation

If the network chooses IPsec to secure the link between PaC and EP, PAA should communicate the IKE pre-shared key, Key-Id, PRPA of the PaC, and the session-Id to EP before the IKE exchange begins. Whenever the IKE pre-shared key changes due to re-authentication as described below, the new value is computed by the PAA and communicated to the EP with all the other parameters.

The IKE exchange between PaC and PAA is equivalent to the 4-way handshake in [IEEE80211i] following the EAP exchange. The IKE exchange establishes the IPsec SA similar to the pair-wise transient keys (PTK) established in [IEEE80211i]. The IKE exchange provides both key confirmation and protected cipher-suite negotiation.

IKE pre-shared key is derived as follows.

```
IKE Pre-shared Key = HMAC-SHA-1 (AAA-key, "IKE-preshared key" |
                        Session ID | Key-ID | EP-address)
```

The values have the following meaning:

AAA-key: A key derived by the peer and EAP server and transported to the authenticator [EAP-KEY].

Session ID: The value as defined in the PANA protocol [PANA-PROT], identifies a particular session of a client.

Key-ID: This identifies the AAA-key within a given session [PANA-PROT]. During the lifetime of the PANA session, there could be multiple EAP re-authentications. As EAP re-authentication changes the AAA-key, key-ID is used to identify the right AAA-key. This is contained in the Key-Id AVP [PANA-PROT].

EP-address: This is the address of the enforcement point with which the IKE exchange is being performed. When PAA is controlling multiple EPs, this provides a different pre-shared key for each of the EPs.

The character "|" denotes concatenation as defined in [RFC2409].

During EAP re-authentication, the AAA-key changes. Whenever the AAA-key changes, a new value of Key-ID is established between the PaC and

PAA/EP as defined in [PANA-PROT]. If there is already an IKE SA or IPsec SA established, it MUST continue to be used till it expires. A change in the value of AAA-key MUST NOT result in re-negotiating a new IKE SA or IPsec SA immediately. But any new negotiation of IKE SA or IPsec SA MUST use the new pre-shared key derived from the latest AAA-key and is indicated by the Key-ID in the above equation. In case where two EAP authentications are performed during a single PANA authentication phase, AAA-key is derived from both authentications as specified in the [PANA-PROT].

6.0 IKE and IPsec details

IKE [RFC2409] MUST be used for establishing the IPsec SA. The details specified in this document works with IKE as well as IKEv2 [IKEV2] also. Any difference between them would be explicitly noted. PANA authenticates the client and derives the keys to protect the traffic. Hence, manual keying cannot be used. Aggressive mode with pre-shared key MUST be supported. PaC and EP SHOULD use the following value in the payload of the ID_KEY_ID to identify the pre-shared key.

```
        ID_KEY_ID data = (Session-Id | Key-Id)
```

The Session-Id and Key-Id are the values contained in the data portion of the Session-Id and Key-Id AVP respectively [PANA-PROT]. They are concatenated to form the content of ID_KEY_ID data. IP addresses cannot be used as identifier as the PaC may be re-authenticated multiple times and hence may not uniquely identify the pre-shared key. For the same reason, main mode of IKE cannot be used, as it requires addresses to be used as identifiers.

After Phase I SA is established, quick mode exchange is performed to establish an ESP tunnel mode IPsec SA for protecting the traffic between PaC and EP. The identities used during Phase II are explained in the next section. As mentioned in section 4.0, an address (POPA) may also have to be configured. The address configuration method to be used by the PaC is indicated in the PANA-Bind-Request message at the end of the successful PANA authentication. The PaC chooses the appropriate method and replies back in PANA-Bind-Answer message.

7.0 Packet Formats

Following acronyms are used throughout this document.

PAC-TIA denotes the IPsec-TIA used by the PaC. PAC-TIA may be set to a PRPA when the same PRPA is used as IPsec-TIA and IPsec-TOA on the PaC. Otherwise, PAC-TIA is set to POPA.

PAC-TOA denotes the IPsec-TOA used by the PaC.

EP-ADDR denotes the address of the EP.

The node with which the PaC is communicating is denoted by END-ADDR.

Following is the IPv4 packet format on the wire for packets sent from PaC to EP:

```
      IPv4 header      (source = PAC-TOA,
                        destination = EP-ADDR)
      ESP  header
      IPv4 header      (source = PAC-TIA,
                        destination = END-ADDR)
```

Following is the IPv6 packet format on the wire for packets sent from PaC to EP:

```
      IPv6 header      (source = PAC-TOA,
                        destination = EP-ADDR)
      ESP  header
      IPv6 header      (source = PAC-TIA,
                        destination = END-ADDR)
```

Following is the IPv4 packet format on the wire for packets sent from EP to PaC:

```
      IPv4 header      (source = EP-ADDR,
                        destination = PAC-TOA)
      ESP  header
      IPv4 header      (source = END-ADDR,
                        destination = PAC-TIA)
```

Following is the IPv6 packet format on the wire for packets sent from EP to PaC:

```
      IPv6 header      (source = EP-ADDR,
                        destination = PAC-TOA)
      ESP  header
      IPv6 header      (source = END-ADDR,
                        destination = PAC-TIA)
```

8.0 IPsec SPD entries

The SPD entries for IPv4 and IPv6 are specified separately as they are different. All the SPD entries are dynamically created. When the same address is used as IPsec-TIA and IPsec-TOA, EP can add the entry to the SPD before the IKE exchange starts, as it knows the address a priori. When IKEv2 [IKEV2] or [RFC3456] is used for address configuration, the SPD entry cannot be created until the IPsec SA is

successfully negotiated as the address is not known a priori. This is very similar to the road warrior case described in [IPSEC-BIS]. In this case, an SPD entry with a name selector is used to start with and later changed with the appropriate addresses. The name used here could be the contents of ID_KEY_ID payload. The entries shown below are the entries that are added after the successful IPsec SA negotiation.

The SPD entries shown here affect the flow of data traffic, which includes neighbor discovery messages for IPv6. When PAA and EP are not co-located, any traffic destined to PAA is forwarded to PAA after decrementing the TTL in the IP header. PAA would drop the packet if the TTL is not 255. PaC also would drop the packets coming from PAA if the TTL is not 255. Hence, we need the following explicit SPD entry on PaC and EP for bypassing IPsec protection for PANA traffic.

```
   If source_port = PANA_PORT OR dest_port = PANA_PORT
       THEN BYPASS
```

PANA_PORT is the IANA assigned (TBD) PANA protocol number [PANA-PROT]. There may be other protocols that expect the TTL to be 255 whose SPD entries are not shown here. Also, when the PaC is using IPsec for remote access, there may be additional SPD entries and IPsec security associations, which are not discussed in this document.

8.1 IPv4 SPD entries

PaC's SPD OUT:

```
          IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

          IF source = PAC-TIA & destination = any
           THEN USE ESP TUNNEL MODE SA:
           outer source = PAC-TOA
           outer destination = EP-ADDR
```

PaC's SPD IN:

```
         IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

         IF source = any & destination = PAC-TIA
          THEN USE ESP TUNNEL MODE SA:
          outer source = EP-ADDR
          outer destination = PAC-TOA
```

EP's SPD OUT:

```
         IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

         IF source = any & destination = PAC-TIA
          THEN USE ESP TUNEL MODE SA:
          outer source = EP-ADDR
          outer destination = PAC-TOA
```

EP's SPD IN:

```
         IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

         IF source = PAC-TIA & destination = any
          THEN USE ESP TUNNEL MODE SA:
           outer source = PAC-TOA
           outer destination = EP-ADDR
```

During the IPsec SA setup, PaC uses PAC-TIA as its phase 2 identity (IDci) and EP uses ID_IPV4_ADDR_RANGE or ID_IPV4_ADDR_SUBNET as its phase 2 identity. The starting address is zero IP address and the end address is all ones for ID_IPV4_ADDR_RANGE. The starting address is zero IP address and the end address is all zeroes for ID_IPV4_ADDR_SUBNET.

8.2 IPv6 SPD entries

The IPv6 SPD entries are slightly different from IPv4 to prevent the neighbor and router discovery [RFC2461] packets from being protected with IPsec. The first three entries of the following SPD entries bypass IPsec protection for neighbor and router discovery packets. The latest version of the IPsec [IPSEC-BIS] document allows traffic selectors to be based on ICMPv6 type and code values. In that case, the first three entries can be based on ICMPv6 type and code values.

Pac's SPD OUT:

```
          IF source = ::/128  & destination = any
           THEN BYPASS

          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
           THEN BYPASS

          IF source_port = PANA_PORT OR dest_port = PANA_PORT
```

```
           THEN BYPASS

          IF source = PAC-TIA & destination = any
           THEN USE ESP TUNNEL MODE SA:
              outer source = PAC-TOA
              outer destination = EP-ADDR

PaC's SPD IN:

          IF source = ::/128 & destination = any
           THEN BYPASS

          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
           THEN BYPASS

          IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

          IF source = any & destination = PAC-TIA
              THEN USE ESP TUNNEL MODE SA:
                 outer source = EP-ADDR
                 outer destination = PAC-TOA

EP's SPD OUT:

          IF source = ::/128 & destination = any
           THEN BYPASS

          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
           THEN BYPASS

           IF source_port = PANA_PORT OR dest_port = PANA_PORT
            THEN BYPASS

          IF source = any & destination = PAC-TIA
              THEN USE ESP TUNNEL MODE SA:
                 outer source = EP-ADDR
                 outer destination = PAC-TOA

EP's SPD IN:

          IF source = ::/128 & destination = any
           THEN BYPASS
```

```
          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
           THEN BYPASS

          IF source_port = PANA_PORT OR dest_port = PANA_PORT
           THEN BYPASS

          IF source = PAC-TIA & destination = any
           THEN USE ESP TUNNEL MODE SA:
              outer source = PAC-TOA
              outer destination = EP-ADDR
```

During the IPsec SA setup, PaC uses PAC-TIA as its phase 2 identity (IDci) and EP uses ID_IPV6_ADDR_RANGE or ID_IPV6_ADDR_SUBNET as its phase 2 identity. The starting address is zero IP address and the end address is all ones for ID_IPV6_ADDR_RANGE. The starting address is zero IP address and the end address is all zeroes for ID_IPV6_ADDR_SUBNET.

9.0 Dual Stack Operation

IKEv2 [IKEV2] can enable configuration of IPsec-TIA for both IPv4 and IPv6 TIAs by sending both IPv4 and IPv6 configuration attributes in the configuration request (CFG-REQUEST). This enables use of single IPsec tunnel mode SA for sending both IPv4 and IPv6 traffic. Therefore, IKEv2 is recommended for handling dual-stack PaCs where single execution of IKE is desired.

10.0 Security considerations

This document discusses the use of IPsec for access control when PANA is used for authenticating the clients to the access network.

If the EP does not verify whether PaC is authorized to use an IP address, it is possible for the PaC to steal the traffic destined to some other PaC. When IKEv2 [IKEV2] and [RFC3456] are used for address configuration, the address is assigned by the EP and hence this attack is not present in such cases. When the same address is used as both IPsec-TIA and IPsec-TOA, EP creates the SPD entry with the appropriate address for the PaC and hence the address is verified implicitly by the virtue of successful IPsec SA negotiation.

When IPv6 is used, the SPD entries bypass all link-local traffic without applying IPsec. This should not be a limitation as the link-local address is used only by link-local services e.g. neighbor and

router discovery, which could use [SEND] to protect their traffic. Moreover, this limitation may not be there in the future if IPsec extends the SPD selectors to specify ICMP types.

11.0 Normative References

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

[RFC2401] S. Kent et al., "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[PANA-PROT] D. Fosberg et al., "Protocol for Carrying Authentication for Network Access", draft-ietf-pana-05.txt

[PANA-THREATS] M. Parthasarathy, "PANA Threat analysis and security requirements", draft-ietf-pana-threats-eval-04.txt

12.0 Informative References

[PANAREQ] A. Yegin et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", draft-ietf-pana-requirements-09.txt

[PANA-FRAME] P. Jayaraman et al., "PANA Framework", draft-ietf-pana-framework-01.txt

[RFC2119] S. Bradner, "Key words for use in RFCS to indicate requirement levels", RFC 2119, March 1997

[RFC2409] D. Harkins et al., "Internet Key Exchange", RFC 2409, November 1998

[IKEV2] C. Kauffman et al., "Internet Key Exchange(IKEv2) Protocol", draft-ietf-ipsec-ikev2-15.txt

[IPSEC-BIS] S. Kent, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-00.txt

[RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[RFC3456] B. Patel et al., "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode", RFC 3456, January 2003

[RFC3315] R. Droms et. al, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, July 2003

[RFC2461] T. Narten et al., "Neighbor Discovery for IP version 6 (IPv6) ", RFC 2461, December 1998

[RFC2462] S. Thomson et. al, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998

[RFC3041] T. Narten et al., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001

[EAP-KEY] D. Simon et al., "EAP Key Management Framework", draft-ietf-eap-keying-02.txt

[SEND] J. Arkko et al., "Secure Neighbor Discovery", draft-ietf-send-ndopt-06.txt

[IPV4-LINK] B. Aboba et al., "Dynamic configuration of Link-local IPv4 addresses", draft-ietf-zeroconf-ipv4-linklocal-12.txt

[RFC1918] Y. Rekhter et al., "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996

[IEEE80211i] IEEE Draft 802.11I/D5.0, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange between Systems û LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer specifications: Specification for Enhanced Security", August 2003.

13.0 Acknowledgments

The author would like to thank Francis Dupont, Pasi Eronen, Yoshihiro Ohba, Jari Arkko, Hannes Tschofenig, Alper Yegin, Erik Nordmark and other PANA WG members for their valuable comments and discussions.

14.0 Revision log

Changes between revision 03 and 04

-Comments from Erik Nordmark (mostly editorial)

Changes between revision 02 and 03

-Clarified the use of key-Id in ID_KEY_ID payload
-Clarified the address configuration issues.
-Added an Appendix to clarify implementation issues.

Changes between revision 01 and 02

-Updated the draft with the fixes for all open issues
-Added the IP configuration section

-Modified the IKE pre-shared key derivation to handle PAA controlling multiple EPs
-Clarification regarding DHCP usage and RFC3456 usage.
-Only aggressive mode to be supported. Main mode not needed anymore.

Changes between revision 00 and 01

-Specified the use of ESP tunnel mode SA instead of IP-IP transport mode SA after working group discussion.
-Specified the IKE pre-shared key derivation.

15.0 Appendix A

This section describes the alternate address configuration methods for Post-PANA address (POPA) and the issues associated with it. As mentioned in section 4, there are multiple ways by which the PaC may configure the POPA address. Only [IKEV2] and [RFC3456] address configuration methods were described in section 4. Other possibilities and the issues are as follows.

1) Some IKEv1 implementations support IKEv1 MODECFG for configuring IP address. There is no RFC describing MODECFG feature of IKEv1. Also, there is not much information on its widespread support among the implementations. Hence, this document does not recommend it.

2) The address may also be obtained using DHCP [RFC2131] [RFC3315] before the IKE exchange starts. Normally the implementations associate the address and other configuration information (e.g. default router) with the interface on which the DHCP is performed. This can cause problems with implementations if they attempt to use an IP address that is configured via [RFC2131] [RFC3315] on the physical interface and use it as IPsec-TIA on the IPsec tunnel interface. This may work without problems when IPsec-TIA and IPsec-TOA are same as the IPv4 PRPA that was obtained using DHCP, as the source address selection has to deal with just one address. But using an IPv4 IPsec-TOA different than IPsec-TIA on a single interface may cause source address selection problem, as there is more than one address to be dealt with. Similarly, an IPv6 address obtained and maintained through a physical link but used on a tunnel interface requires additional implementation considerations. Therefore, this document does not handle the case where DHCP is used to acquire an address for IPsec-TIA that is different from IPsec-TOA. Note that this case is different from the address configuration using [RFC3456], which also uses DHCP. When [RFC3456] is used, DHCP is run over the IPsec tunnel and the address (IPsec-TIA) is assigned to the IPsec tunnel interface. The link-local address (IPsec-TOA) is assigned to the physical interface. As there is

only one address on each interface, there are no address selection issues.

3) The address may also be obtained using auto-configuration [RFC2461] including the temporary addresses described in [RFC3041]. The problem described above for DHCP applies to this also. The implementations would associate the auto-configured addresses and the default router with the interface on which the router advertisement was received. As we configure the SPD to bypass IPsec for router discovery and neighbor discovery messages, the address would be associated with the physical interface and not with the IPsec interface. There is also an additional issue, as the address configured by the PaC is not known to the EP. It needs to trust whatever PaC provides in its traffic selector during the IPsec SA negotiation. This leads to DoS attack where the PaC can steal some other PaC's address, which cannot be prevented unless [SEND] is deployed.

16.0 Author's Addresses

Mohan Parthasarathy
313 Fairchild Drive
Mountain View CA-94043

Phone: 408-734-8820
Email: mohanp@sbcglobal.net

Intellectual Property Statement

this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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