Network Working Group   R. Housley
Request for Comments: 4705   Vigil Security
Category: Informational   A. Corry
                                                               GigaBeam
                                                           October 2006

                  GigaBeam High-Speed Radio Link Encryption

Status of This Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

Abstract

   This document describes the encryption and key management used by
   GigaBeam as part of the WiFiber(tm) family of radio link products.
   The security solution is documented in the hope that other wireless
   product development efforts will include comparable capabilities.

1. Introduction

   The GigaBeam WiFiber(tm) product family provides a high-speed point-
   to-point radio link. Data rates exceed 1 gigabit/second at a
   distance of about a mile. The transmission beam width is less than
   one degree, which means that attempts to intercept the signal are
   most successful when the attacker is either between the transmitter
   and receiver or the attacker is directly behind the receiver. Since
   interception is possible, some customers require confidentiality and
   integrity protection for the data on the radio link. This document
   describes the security solution designed and deployed by GigaBeam to
   provide these security services.

   The GigaBeam security solution employs:

      o AES-GCM [GCM] with a custom security protocol specified in this
         document to provide confidentiality and integrity protection of
         subscriber traffic on the radio link;

      o AES-CBC [CBC] and HMAC-SHA-1 [HMAC] with IPsec ESP [ESP] to
         provide confidentiality and integrity protection of management
         traffic between the radio control modules;

      o AES-CBC [CBC] and HMAC-SHA-1 [HMAC] with the IKE protocol [IKE]
         to provide confidentiality and integrity protection of key
         management traffic between the radio control modules; and

      o OAKLEY key agreement [OAKLEY] and RSA digital signatures
         [PKCS1] are used with IKE to establish keying material and to
         provide authentication.

   AES-GCM is used with the custom security protocol in a manner that is
   very similar to its use in ESP [ESP-GCM].

2. GigaBeam High-Speed Radio Link Overview

   The GigaBeam high-speed radio link appears to be a fiber interface
   between two network devices. Figure 1 illustrates the connection of
   two devices that normally communicate using Gigabit Ethernet over a
   fiber optic cable.

```
    +---------+     +----------+         +----------+     +---------+
    |         |     |          |  +----/  |          |     |         |
    | Network |     | GigaBeam |  /       | GigaBeam |     | Network |
    | Device  +=====+  Radio   | /---- +  Radio    +=====+ Device  |
    |         |     |          |         |          |     |         |
    +---------+  ^  +----------+  ^      +----------+  ^  +---------+
              |                |                    |
              |                |                    |
        Gigabit Ethernet       |          Gigabit Ethernet
                        GigaBeam Radio Link
```
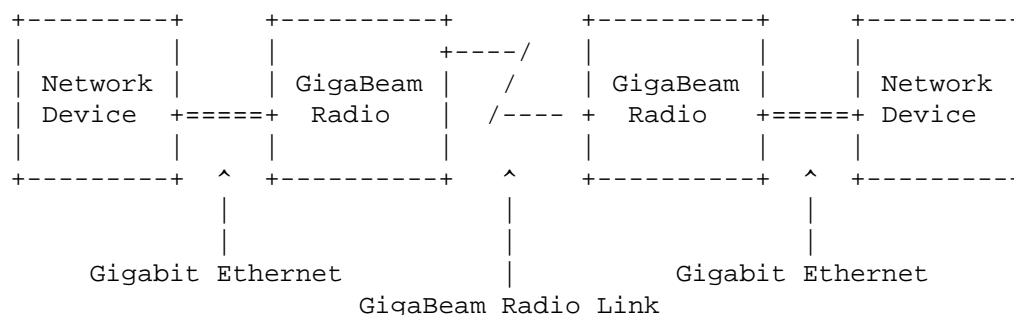
                  Figure 1. GigaBeam Radio Link Example.

   Gigabit Ethernet traffic is encoded in 8B/10B format. The GigaBeam
   Radio Control Module (RCM) removes this coding to recover the 8-bit
   characters plus an indication of whether the character is a control
   code. The radio link frame is constructed from 224 10-bit input
   words, and a 4-way interleaved (56,50,10) Reed-Solomon Forward Error
   Correction (FEC) block is employed. Conversion of the Gigabit
   Ethernet data from 8B/10B format creates 224 bits of additional
   capacity in each frame, and another 196 bits is gained by recoding
   the 9-bit data using 64B/65B block codes. This additional 420 bits
   of capacity is used for the framing overhead required for FEC and
   link control.

2.1. GigaBeam Radio Link Frame Format

   The GigaBeam radio link frame fields are summarized in Figure 2,
   which also provides the length of each field in bits.

```
       Field    Length    Description
       -----    ------    -----------
       SYNC        11     Frame Synchronization Pattern ('10110111000'b)
       KEYSEL       1     Indicates which AES key was used for this frame
       PN          40     AES-GCM Packet Number
       FLAGS       28     Control bits, one bit for each 64B/65B data block
       DCC          8     Data Communications Channel
       DATA      1792     Data (28 encrypted 64B/65B code blocks)
       TAG         96     Authentication Tag
       SPARE       24     Reserved for alternative FEC algorithms
       CHECK      240     Reed-Solomon Check Words for 4 10-bit
                          symbol (56,50) code
```

              Figure 2. GigaBeam Radio Link Frame Structure.

   Each of the fields in the GigaBeam 2240-bit radio link frame is
   described below.

       SYNC   Synchronization field, an 11-bit Barker code. Always set
                 to '10110111000'b.

       KEYSEL   Key Selector -- select the appropriate key register for
                 this frame. Two key registers are maintained to allow
                 seamless rollover between encryption keys.

       PN   Packet Number -- needed by AES-GCM; it carries the unique
                 counter value for this frame. The value is incremented
                 for each frame.

       FLAGS   Control bits, one for each 64B/65B data block carried in
                 the DATA field. If the bit is set, then the
                 corresponding 64B/65B block in the DATA field contains a
                 control code. This field is integrity protected by AES-
                 GCM.

       DCC   Data Communications Channel -- each frame carries one
                 octet of the point-to-point data communications channel
                 between the two radio control modules. See Section 2.2
                 for more information on the DCC.

       DATA   Subscriber data carried as 28 64B/65B code blocks. This
                 field is encrypted and integrity protected by AES-GCM.

        TAG   The authentication tag generated by AES-GCM, truncated to
                  96 bits.

        SPARE   24 bits, set to zero.

        CHECK   Forward error correction check value -- 24 check symbols
                  are generated by a 4-way interleaved Reed-Solomon
                  (56,50,10) algorithm. FEC is always active, but
                  correction can be selectively enabled. For each frame,
                  FEC processing also returns the number of bit errors, the
                  number of symbols in error, and whether the FEC
                  processing failed for the frame. This information allows
                  an estimation of the bit error rate for the link.

2.2. Data Communications Channel

   The Data Communications Channel (DCC) field reserves eight bits in
   each 2240-bit radio link frame for use in constructing a dedicated
   point-to-point link between the two RCMs. The DCC content is
   connected to a Universal Asynchronous Receiver/Transmitter (UART)
   controller that processes the DCC bit stream to provide an
   asynchronous serial channel that is visible to the RCM operating
   system. The Point-to-Point Protocol (PPP) [PPP] is used on the
   serial channel to create a simple two-node Internet Protocol (IP)
   network. Each IP datagram is spread over a large number of radio
   link frames. This two-node IP network carries management protocols
   between the GigaBeam RCMs.

   IKE [IKE] runs on this two-node IP network to manage all
   cryptographic keying material. IPsec ESP [ESP] is used in the usual
   fashion to protect all non-IKE traffic on the data control channel.
   IPsec ESP employs AES-CBC as described in [ESP-CBC] and HMAC-SHA-1 as
   described in [ESP-HMAC].

3. Radio Link Processing

   The fiber interface constantly provides a stream of data encoded in
   8B/10B format. A radio link frame is constructed from 224 10-bit
   input words. Conversion of the data from 8B/10B format creates 224
   bits of additional capacity in each frame, and then recoding using
   64B/65B block codes creates another 196 bits of additional capacity.
   After encryption, the 64B/65B blocks are carried in the DATA field,
   and the control code indicator bits are carried in the FLAGS field.
   The additional capacity is used for the framing overhead.

Processing proceeds as follows:

o encryption and integrity protection as described in Section 3.1;

o forward error correction (FEC) processing as described in Section
   3.2;

o scrambling as described in Section 3.3; and

o differential encoding as described in Section 3.4.

3.1. Encryption and Integrity Protection

The GigaBeam RCM contains two key registers. The single-bit KEYSEL
field indicates which of the two registers was used for the frame.

AES-GCM [GCM] employs counter mode for encryption. Therefore, a
unique value for each frame is needed to construct the counter. The
counter includes a 32-bit salt value provided by IKE and a 40-bit
packet number from the PN field in the radio link frame. The same
counter value must not be used for more than one frame encrypted with
the same key. The 128-bit counter block is constructed as shown in
Figure 3. The first 96 bits of the AES counter block are called the
Nonce in the AES-GCM algorithm description. Note that AES-GCM uses
BLOCK values of zero and one for its own use. The values beginning
with two are used for encrypting the radio link frame payload.

```
    Field    Length   Description
    -----    ------   -----------
    SALT       32     Salt value generated during the IKE exchange
    MBZ1       24     These bits must be zero
    PN         40     AES-GCM Packet Number carried in PN field
    MBZ2       28     These bits must be zero
    BLOCK       4     Block counter used in AES-GCM
```

                Figure 3. AES Counter Block Construction.

AES-GCM is used to protect the FLAGS and DATA fields. The FLAGS
field is treated as authenticated header data, and it is integrity
protected, but it is not encrypted. The DATA field is encrypted and
authenticated. The TAG field contains the authentication tag
generated by AES-GCM, truncated to 96 bits.

Reception processing performs decryption and integrity checking. If
the integrity checks fail, to maintain a continuous stream of
traffic, the frame is replaced with K30.7 control characters. These

control characters are normally used to mark errors in the data
stream. Without encryption and integrity checking, these control
characters usually indicate 8B/10B running disparity or code errors.

3.2. Forward Error Correction (FEC)

The 224 10-bit data symbols that make up each radio link frame are
grouped into 4 subframes each consisting of 56 symbols. The
subframes are formed by symbol interleaving. A Reed-Solomon Code,
RS(56,50), designed for 10-bit symbols is applied to each subframe.

This Reed Solomon Code detects 6 errors and corrects 3 errors within
each subframe. The FEC function is always active; however, it is
possible to disable correction of the received data to support
debugging.

3.3. Scrambler

The scrambler ensures that long series of one bits and long series of
zero bits do not occur. When encryption is enabled, long series of
common bit values is very unlikely; however, during the initial IKE
exchange, the radio link frame payload is all zero bits.

The scrambling polynomial is $(1 + x^{14} + x^{15})$. All words of a frame
except the SYNC pattern are scrambled prior to transmission using
this linear feedback shift register (LFSR). The LFSR is initialized
to all ones at the start of each frame, prior to the first processed
bit. Each processed input bit is added modulo 2 (i.e., an XOR) to
the output of the x15 tap to form the output bit.

On reception, an identical process is performed after frame
synchronization and prior to subsequent processing to recover the
original bit pattern.

3.4. Differential Encoding

The data stream is differentially encoded to avoid symbol ambiguity
at the receiver. Since the demodulator could produce true or
inverted data depending on the details of the radio frequency (RF)
and intermediate frequency (IF) processing chains, differential
encoding is used to ensure proper reception of the intended bit
value. A zero bit is encoded as no change from the previous output
bit, and a one bit is encoded as a change from the previous output
bit. Thus, an output bit is the result of XORing the unencoded bit
with the previously transmitted encoded bit.

On reception, a complementary operation will be performed to produce
the decoded datastream. The bitstream is formed by XORing the
received encoded bit and the previously received encoded bit.

4. Key Management

The Internet Key Exchange (IKE) is used for key management [IKE].
IKE has two phases. In Phase 1, two Internet Security Association
and Key Management Protocol (ISAKMP) peers establish a secure,
authenticated channel with which to communicate. This is called the
ISAKMP Security Association (SA). In the GigaBeam environment, the
Phase 1 exchange is IKE Aggressive Mode with signatures and
certificates. The RSA signature algorithm is used.

Phase 2 negotiates the Security Associations for the GigaBeam custom
security protocol that protects subscriber traffic and IPsec ESP that
protects management traffic between the GigaBeam RCMs. In the
GigaBeam environment, the Phase 2 exchange is IKE Quick Mode, without
perfect forward secrecy (PFS). The information exchanged along with
Quick Mode is protected by the ISAKMP SA. That is, all payloads
except the ISAKMP header are encrypted. A detailed description of
Quick Mode can be found in Section 5.5 of [IKE].

When the Security Association is no longer needed, the ISAKMP Delete
Payload is used to tell the peer GigaBeam device that it is being
discarded.

4.1. Certificates

Each GigaBeam device generates its own public/private key pair. This
generation is performed at the factory, and the public key is
certified by a Certification Authority (CA) in the factory. The
certificate includes a name of the following format:

C=US O=GigaBeam Corporation OU=GigaBeam WiFiber(tm)
SerialNumber=<device-model-identifier>/<device-serial-number>

The ISAKMP Certificate Payload is used to transport certificates, and
in the GigaBeam environment, the "X.509 Certificate - Signature"
certificate encoding type (indicated by a value of 4) is always used.

GigaBeam devices are always installed in pairs. At installation
time, each one is configured with the device model identifier and
device serial number of its peer. The device model identifier and
device serial number of a backup device can also be provided. An
access control check is performed when certificates are exchanged.
The certificate subject name must match one of these configured

   values, and the certification path must validate to a configured
   trust anchor, such as the GigaBeam Root CA, using the validation
   rules in [PKIX1].

4.2. Oakley Groups

   With IKE, several possible Diffie-Hellman groups are supported.
   These groups originated with the Oakley protocol and are therefore
   called "Oakley Groups".

   GigaBeam devices use group 14, which is described in Section 3 of
   [MODP].

4.3. Security Protocol Identifier

   The ISAKMP proposal syntax was specifically designed to allow for the
   simultaneous negotiation of multiple Phase 2 security protocol
   suites. The identifiers for the IPsec Domain of Interpretation (DOI)
   are given in [IPDOI].

   The GigaBeam custom security protocol has been assigned the
   PROTO_GIGABEAM_RADIO protocol identifier, with a value of 5.

   The PROTO_GIGABEAM_RADIO specifies the use of the GigaBeam radio link
   frame structure, which uses a single algorithm for both
   confidentiality and authentication. The following table indicates
   the algorithm values that are currently defined.

       Transform ID   Value
       ------------   -----
       RESERVED   0
       GIGABEAM_AES128_GCM   1

4.4. Keying Material

   GIGABEAM_AES128_GCM requires 20 octets of keying material (called
   KEYMAT in [IKE]). The first 16 octets are the 128-bit AES key, and
   the remaining four octets are used as the salt value in the AES
   counter block.

   Presently, AES with a 128-bit key is the only encryption algorithm
   that is supported. Other encryption algorithms could be registered
   in the future.

4.5. Identification Type Values

   The following table lists the assigned values for the Identification
   Type field found in the ISAKMP Identification Payload.

        ID Type   Value
        -------   -----
        RESERVED   0
        ID_IPV4_ADDR   1
        ID_FQDN   2
        ID_USER_FQDN   3
        ID_IPV4_ADDR_SUBNET   4
        ID_IPV6_ADDR   5
        ID_IPV6_ADDR_SUBNET   6
        ID_IPV4_ADDR_RANGE   7
        ID_IPV6_ADDR_RANGE   8
        ID_DER_ASN1_DN   9
        ID_DER_ASN1_GN   10
        ID_KEY_ID   11

   The ID_DER_ASN1_DN will be used when negotiating security
   associations for use with the GigaBeam custom security protocol. The
   provided distinguished name must match the peer's subject name
   provided in the X.509 certificate.

4.6. Security Parameter Index

   The least significant bit of the Security Parameter Index (SPI) is
   used in the GigaBeam custom security protocol. When two GigaBeam
   custom security protocol security associations are active at the same
   time for communications in the same direction, the least significant
   bit of the SPI must be different to ensure that these active security
   associations can be distinguished by the single bit in the GigaBeam
   custom security protocol.

4.7. Key Management Latency

   The IKE exchange over the DCC must complete before subscriber data
   can be exchanged in the GigaBeam radio link frame payload. Since
   each radio link frame carries a small portion of an IP datagram, many
   radio link frames carrying all zero bits must be sent and received to
   complete the IKE exchange.

   Once the initial keying material is in place, the IKE exchanges to
   establish subsequent keying material can be performed concurrent with
   the transfer of subscriber data in the radio link frame payload. The
   KEYSEL field in the radio link frame is used to indicate which keying
   material is being used.

The PN field in radio link frame provides a continuous indication of
the number of frames that have been encrypted with a particular key.
Once a threshold is exceeded, the IKE exchanges begin to establish
the replacement keying material. Currently, the exchanges begin when
half of the packet numbers have been used, but any threshold can be
employed, as long as the replacement keying material is available
before the packet counters are exhausted.

5. Security Considerations

The security considerations in [IKE], [OAKLEY], [PKCS1], and [ESP]
apply to the security system defined in this document.

Confidentiality and integrity are provided by the use of negotiated
algorithms. AES-GCM [GCM] is used with the GigaBeam custom security
protocol to provide confidentiality and integrity protection of
subscriber traffic on the radio link. AES-CBC [CBC] and HMAC-SHA-1
[HMAC] are used with IPsec ESP [ESP] to provide confidentiality and
integrity protection of management traffic between the radio control
modules.

AES-GCM makes use of AES Counter mode to provide confidentiality.
Unfortunately, it is very easy to misuse counter mode. If counter
block values are ever used for more than one frame with the same key,
then the same key stream will be used to encrypt both frames, and the
confidentiality guarantees are voided. Using AES Counter mode with
the same counter values to encrypt two plaintexts under the same key
leaks the plaintext. The automated key management described here is
intended to prevent this from ever happening.

Since AES has a 128-bit block size, regardless of the mode employed,
the ciphertext generated by AES encryption becomes distinguishable
from random values after 2^{64} blocks are encrypted with a single key.
Since the GigaBeam radio link frame allows for up to 2^{40} fixed-
length frames in a single security association, there is no
possibility for more than 2^{64} blocks to be encrypted with one key.

The lifetime of a particular AES key can be shorter than 2^{40} frames.
A smaller threshold can be used as a trigger to transition to the
next key. This capability allows straightforward implementation of
policies that require the key to be changed after a particular volume
of traffic or a particular amount of time.

There are fairly generic precomputation attacks against all block
cipher modes that allow a meet-in-the-middle attack against the key.
These attacks require the creation and searching of huge tables of
ciphertext associated with known plaintext and known keys. Assuming
that the memory and processor resources are available for a

precomputation attack, then the theoretical strength of AES Counter
mode (and any other block cipher mode) is limited to $2^{(n/2)}$ bits,
where n is the number of bits in the key. The use of long keys is
the best countermeasure to precomputation attacks. The unpredictable
nonce value in the counter block significantly increases the size of
the table that the attacker must compute to mount a successful
precomputation attack.

Rekeying with Quick Mode results in new keys to protect GigaBeam
radio link frames; however, these keys are generated from the same
Diffie-Hellman shared secret. In order to limit the amount of data
that would be exposed by the disclosure of this Diffie-Hellman shared
secret or the associated Diffie-Hellman private key, implementations
should periodically rekey using a new Phase 1 exchange.

Diffie-Hellman exponents used in IKE Phase 1 should be erased from
memory immediately after use. Likewise, AES and HMAC-SHA-1 keying
material should be erased from memory when it is no longer needed.

This security solution makes use of IKEv1 [IKE]. IKEv1 was selected
over IKEv2 [IKEv2] primarily due to the availability of an
implementation for the processing environment. The use of IKEv2
would provide some useful capabilities, such as Diffie-Hellman group
negotiation. These additional capabilities would not significantly
improve the security of the overall key management solution that runs
on the two-node IP network.

6. IANA Considerations

IANA has assigned one IPsec Security Protocol Identifier in
http://www.iana.org/assignments/isakmp-registry for
PROTO_GIGABEAM_RADIO. It was assigned the value 5.

7. Informative References

   [CBC]   Dworkin, M., "Recommendation for Block Cipher Modes of
               Operation: Methods and Techniques," NIST Special
               Publication 800-38A, December 2001.

   [ESP]   Kent, S., "IP Encapsulating Security Payload (ESP)", RFC
               4303, December 2005.

   [ESP-CBC]   Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher
               Algorithm and Its Use with IPsec", RFC 3602, September
               2003.

   [ESP-GCM]   Viega, J. and D. McGrew, "The Use of Galois/Counter Mode
               (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC
               4106, June 2005.

   [ESP-HMAC] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within
               ESP and AH", RFC 2404, November 1998.

   [GCM]   McGrew, D. and J. Viega, "The Galois/Counter Mode of
               Operation (GCM)", Submission to NIST.
               http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/
               gcm/gcm-spec.pdf, January 2004. [Soon: NIST SP 800-38D.]

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

   [IKE]   Harkins, D. and D. Carrel, "The Internet Key Exchange
               (IKE)", RFC 2409, November 1998.

   [IKEv2]   Kaufman, C., "The Internet Key Exchange (IKEv2) Protocol",
               RFC 2306, December 2005.

   [IPDOI]   Piper, D., "The Internet IP Security Domain of
               Interpretation for ISAKMP", RFC 2407, November 1998.

   [MODP]   Kivinen, T. and M. Kojo. "More Modular Exponential (MODP)
               Diffie-Hellman groups for Internet Key Exchange (IKE)",
               RFC 3526, May 2003.

   [OAKLEY]   Orman, H., "The Oakley Key Determination Protocol", RFC
               2412, November 1998.

   [PKCS1]   Kaliski, B., "PKCS #1: RSA Encryption Version 1.5", RFC
               2313, March 1998.

   [PKIX1]   Housley, R., Polk, W., Ford, W., and D. Solo, "Internet
               X.509 Public Key Infrastructure Certificate and
               Certificate Revocation List (CRL) Profile", RFC 3280,
               April 2002.

   [PPP]   Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51,
               RFC 1661, July 1994.

8. Acknowledgements

Authors' Addresses

   Russell Housley
   Vigil Security, LLC
   918 Spring Knoll Drive
   Herndon, VA 20170
   USA

   EMail: housley@vigilsec.com

   Alan Corry
   GigaBeam Corporation
   470 Springpark Place, Suite 900
   Herndon, VA 20170
   USA

   EMail: publications@gigabeam.com

Full Copyright Statement

   Copyright (C) The Internet Society (2006).

   This document is subject to the rights, licenses and restrictions
   contained in BCP 78, and except as set forth therein, the authors
   retain all their rights.

   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.

Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the procedures with respect to rights in RFC documents can be
   found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use of
   such proprietary rights by implementers or users of this
   specification can be obtained from the IETF on-line IPR repository at
   http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at
   ietf-ipr@ietf.org.

Acknowledgement

   Funding for the RFC Editor function is provided by the IETF
   Administrative Support Activity (IASA).