General Architecture for Inter-network Communication across 802.16 LE Systems

IEEE 802.16 Presentation Submission Template (Rev. 8.3)
Document Number: IEEE S802.16h-05/012
Date Submitted: 2005-05-04
Source:
Chi-Chen Lee, Hung-Lin Chou, Tzu-Ming Lin, Fang-Ching Ren,
Sheng-Fu Tsai, Keng-Ming Huang, Han-Chiang Liu
CCL, ITRI
Bldg. 11, 195 Sec. 4, Chung Hsing Rd. Chutung,
HsinChu, Taiwan 310, R.O.C.
Venue:
Session #37, 2-5 May, 2005
Base Document:
Purpose:
Facilitate co-channel and adjacent channel coexistence for 802.16 LE.
Notice:
This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release:
The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
IEEE 802.16 Patent Policy:
The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.
Outline

• Inter-Network Communication Problem
• IP Security Family
• Solution 1 - 802.16h (CP) System (C80216h-05_012)
• Solution 2 – IPSec enhancement with IKEv2
• Solution 3 – Trusted third party & IKEv2
• Summary
Inter-Network Communication Problem

In 802.16 LE network, how do BSs of different network operators perform inter-communication without a well-defined communication mechanism? BSs belong to different operators may do not have any info. between each other, e.g., IP address, security policy, etc. The same situation happens on the inter-communication between BS and CIS.

On the other hand, a rough BS may fake a valid member of this network to perform actions not permitted. It may cause the network operating not correctly (DoS, etc).

An inter-communication protocol, coexistence protocol (CP) is proposed in previous presentation. And in this presentation, we will mention the security issues.
IP-Security (IP-Sec) Family

We will adopt IPsec protocol into 802.16 LE network to solve the problems. There are two major parts in IPsec. One part defines the encryption and authentication algorithms. The other part defines the key management protocols. The IP Security Protocol provides cryptographically based security for IP. The protection offered by IPsec is achieved by using one or both of the data protection protocols (AH and ESP). ESP has been adopted for 802.11F for message authentication and encryption.

Internet Key Exchange (IKE) defines the negotiation procedure and provides keying material in a protected manner. IKE is the default automated key management protocol selected for use with IPsec. Currently, new version of IKE, named IKE-v2, is available under draft version
When a mobile host moves from one AP to another AP, it must perform re-association procedure. The old AP information (for example, BSSID) will be included in the re-association request message.
Solution 1 - 802.16h (CP) System (C80216h-05_012)

Radius-Server

Radius-accept-request
(BS1 -> BS2 or BS1 -> CIS)

Radius-accept-accept
(Return IP-Sec Parameters)

Including ESP Encryption/Authentication algorithm IDs and key materials

IP-Sec Connection (ESP)

Coexistence Identification Server (CIS)
When BS or CIS startup, they first send RADIUS-Registration-Access-Request to the RADIUS server. It contains the BS’s IP address and BSID, letting RADIUS server be aware of the address mapping information. It also contains the list of supported encryption and authentication algorithms for Encapsulating Security Payload (ESP) protocol.

After RADIUS server authenticate the BS (or CIS) as a valid member of the network, it responds with RADIUS-Registration-Access-Accept to the BS (or CIS). It contains the encryption and authentication algorithm identifier selected by the RADIUS server for later RADIUS message usage.

If a BS wants to communicate with CIS, it first sends RADIUS-Access-Request message to the RADIUS server. The message contains the MAC address of CIS for looking up the CIS’s IP address in the RADIUS server.

In RADIUS-Access-Accept message, two security blocks are included. One is used for the originated BS, and the other is used for the terminating BS.

The security block for the terminating BS will be carried in the first LE_CP-REQ message with type Send-Security-Block. After receiving LE_CP-RSP with type ACK-Security-Block, CP procedure for querying neighbor topology starts.

Coexistence protocol message exchange for DRRM
Solution 1 – Pros & Cons

• Pros
  – Adoption of RADIUS protocol provides the possibility of integration between networks belonging to different operators, and even heterogeneous networks (WLAN/802.11f/802.11i and WMAN/802.16e).

• Cons
  – The RADIUS server needs to manage all SAs used by all communication pairs and increasing its overload
  – Pre-set shared key makes it harder to prevent from artificial stealing and causes the problem of key distribution
  – More steps for re-key procedure
  – The security policy is assigned by RADIUS server, loosing the flexibility

Note: In this case, IP addresses of BSs are located in the RADIUS server.
Solution 2 – IPSec enhancement with IKEv2

IKEv2 Phase 1
Create ISAKMP SA

IKEv2 Phase 2
(encrypted by ISAKMP SA)
Create IPSec SA

IPSec Connection
Encrypted by IPSec SA

IPSec Key lifetime
IKEv2 Rekeying

Update IPSec SA

Dynamic generate IPSec SA
(Encryption/Authentication algorithm IDs and key materials)

When implementing IKEv2, the RADIUS server is not needed. IKEv2 contains two phase procedures to create the Security Association (SA).
IKEv2 phase 1 is used to create ISAKMP SA by using Diffie-Hellman (DH) algorithm.
IKEv2 phase 2 is used to create IPsec SA, which is encrypted by ISAKMP SA. Then the IPSec Connection is established. The created SA can be valid in a time period, IPSec Key Lifetime. After the lifetime is expired, the Re-key procedure is executed. New version of IPSec SA is created again.
Solution 2 – Pros & Cons

• Pros
  – It is a distributed key management system and therefore does not need the RADIUS server
  – Pre-set shared key is not necessary. Dynamic creation of the used shared key by DH algorithm is more secure than the pre-set ones
  – Re-key procedure is simpler
  – The security policy is negotiated between the peer entity of communication, not assigned by RADIUS server. It increases the flexibility

• Cons
  – Lack of third party such as RADIUS server which is trusted by all network components makes detection of rouge BS harder

Note: In this case, IP addresses of BSs are located in the CIS.
Therefore, we propose a modified security architecture, which combines the advantages of solution 1 and 2. In solution 3, RADIUS server is reserved for the authentication purpose and the SA creation and management relies on the IKEv2 protocol. Detailed procedure will be described in the next slide.
Solution 3 – Trusted third party & IKEv2

RADIUS-Access-Request with **zero** Sequence Number triggers the RADIUS server to send 32-bytes MPPE-Send-Key, 32-bytes MPPE-Recv-Key and a unique nonzero Key Sequence Number x, which is for later authentication usage. IPSec Policies of BS-1 and BS-2, also the BS-2 IP address is sent, letting the BS-1 could perform IKEv2 with BS-2.

Before any info. negotiation procedure is started using coexistence protocol, the authentication procedure shall be executed first or LE_CP-RSP may define several message types for Trust-Request, Trust-Response, Trust-Accept, and even Trust-Reject.

Then BS-1 will send Trust-Request message to BS-2. The message contains an authentication code generated by 16-bytes truncating the output of HMAC-SHA-1 algorithm. The input of the HMAC-SHA-1 algorithm contains the first 16 bytes of MPPE-Recv-Key, BS-2 ID, and MPPE-Send-Key. Also the Key Sequence Number is included.

Secure IP connection is established.

The Key Sequence Number got from Trust-Request is used to let RADIUS server uniquely identify the MPPE-Send-Key and MPPE-Recv-Key pair. Different Key Sequence Number will get different key pair. Then BS-2 could check BS-1's authentication code to make sure that whether BS-1 is a valid member. Trust-Response is transmitted same as Trust-Request, except the difference of the input parameter for HMAC-SHA-1.
Solution 3 – Pros & Cons

• Pros
  – It is a distributed key management system, reducing the loading of RADIUS server
  – Pre-set shared key is not necessary. Dynamic creation of the used shared key by DH algorithm is more secure than the pre-set ones
  – Re-key procedure is simpler
  – RADIUS server is not involved in the negotiation of this security policy, increasing the flexibility
  – Authentication relies on the third party (RADIUS server in this case)

• Cons
  – RADIUS needs slightly modification for BS authentication

Note: In this case, IP addresses of BSs are located in the RADIUS server
Summary

• A secure inter-network communication is needed while coexistence protocol (CP) is based on the secure connection

• Three solutions are presented and a simple analysis is also made
  – Solution 3 has the advantages of solution 1 & 2
    • IKEv2 supports the distributed key management
    • Adoption of RADIUS server supports centralized authentication mechanism
    • Both the features make the inter-communication more safely
References

- IEEE C802.16h-05/011, “Storage of identification information and Coexistence Protocol”
- Internet Key Exchange (IKEv2) Protocol see http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt
- IEEE C802.16h-05/009, “Elements of a Coexistence Protocol”
### Table 1 RADIUS-BS/CIS-Registration-Access-Request

<table>
<thead>
<tr>
<th>Attribute number</th>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>BSID. The BSID should be represented in ASCII format, with octet values separated by a “-“. Example: “00-10-A4-23-19-C0”</td>
</tr>
<tr>
<td>2</td>
<td>User-Password</td>
<td>RADIUS BSID Secret.</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
<td>BS’s IP Address</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>CRN-Register (value = TBD, ex. IAPP-Register, value = 15)</td>
</tr>
<tr>
<td>26</td>
<td>Vendor-Specific-Attribute (VSA)</td>
<td></td>
</tr>
<tr>
<td>26-TBD</td>
<td>Supported-ESP-Authentication-Algorithms</td>
<td>The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this BS (See Table 7)</td>
</tr>
<tr>
<td>26-TBD</td>
<td>Supported-ESP-Transforms</td>
<td>The list of ESP Transform IDs corresponding to the ESP transforms supported by this BS (See Table 6)</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
<td>BS’s NAS Identifier</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>The RADIUS message’s authenticator</td>
</tr>
</tbody>
</table>

TBD: To Be Defined
<table>
<thead>
<tr>
<th>Attribute number</th>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>BSID.</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>CRN-Register (value = TBD, ex. IAPP-Register, value = 15)</td>
</tr>
<tr>
<td>26-TBD</td>
<td>Vendor-Specific-Attribute (VSA)</td>
<td>ESP Transform ID of the algorithm to use when encrypting/deciphering the Security Block in the next RADIUS messages</td>
</tr>
<tr>
<td>26-TBD</td>
<td>RADIUS-ESP-Transform-ID</td>
<td>ESP Authentication ID of the algorithm to use when encrypting/deciphering the Security Block in the next RADIUS messages</td>
</tr>
<tr>
<td>26-TBD</td>
<td>RADIUS-ESP-Authentication-ID</td>
<td>SPI used to identify ESP SA (between the BS and RADIUS server)</td>
</tr>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>Number of seconds until the BS should re-issue the registration Access-Request to the RADIUS server to obtain new key information.</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>The RADIUS message’s authenticator</td>
</tr>
</tbody>
</table>
Table 3 RADIUS-BS/CIS-Access-Request

<table>
<thead>
<tr>
<th>Attribute number</th>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>Regional CIS’s WM address or neighbor BS’s BSID.</td>
</tr>
<tr>
<td>2</td>
<td>User-Password</td>
<td>NULL.</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
<td>Original BS’s IP Address (the BS sending this request message)</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>BS/CIS-Check (value = TBD, ex. IAPP-AP-Check, value = 16)</td>
</tr>
<tr>
<td>61</td>
<td>NAS-Port-Type</td>
<td>Wireless – Other (value = 18)</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>The RADIUS message’s authenticator</td>
</tr>
</tbody>
</table>
### Table 4 RADIUS-BS/CIS-Access-Accept

<table>
<thead>
<tr>
<th>Attribute number</th>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>Regional CIS’s WM address or neighbor BS’s BSID.</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
<td>IP Address of Regional CIS or neighbor BS.</td>
</tr>
<tr>
<td>26</td>
<td>Vendor-Specific-Attribute (VSA)</td>
<td></td>
</tr>
<tr>
<td>26-TBD</td>
<td>Originated-BS-Security-Block</td>
<td>Security Block encrypted using original BS’s RADIUS BSID secret, to be decrypted and used by the original BS</td>
</tr>
<tr>
<td>26-TBD</td>
<td>Terminated-BS/CIS-Security-Block</td>
<td>Security Block encrypted using neighbor BS’s RADIUS BSID secret (or CIS’s), to be decrypted and used by the neighbor BS (or CIS)</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>The RADIUS message’s authenticator</td>
</tr>
</tbody>
</table>
Table 5 Information elements in the Originated-BS-Security-Block

<table>
<thead>
<tr>
<th>Element ID</th>
<th>Length</th>
<th>Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>Security lifetime in seconds</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>32</td>
<td>ACK nonce.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>ESP transform number</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>ESP authentication number</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>SPI used to identify ESP SA to the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Variable</td>
<td>Key used by ESP Transform for ESP packets to the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Variable</td>
<td>Key used by ESP Authentication for ESP packets to the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>SPI used to identify ESP SA from the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Variable</td>
<td>Key used by ESP Transform for ESP packets from the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Variable</td>
<td>Key used by ESP Authentication for ESP packets from the regional CIS or neighbor BS</td>
<td></td>
</tr>
<tr>
<td>Transform identifier</td>
<td>Value</td>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>RESERVED</td>
<td>0</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_DES_IV64</td>
<td>1</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_DES</td>
<td>2</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_3DES</td>
<td>3</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_RC5</td>
<td>4</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_IDEA</td>
<td>5</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_CAST</td>
<td>6</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_BLOWFISH</td>
<td>7</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_3IDEA</td>
<td>8</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_DES_IV32</td>
<td>9</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_RC4</td>
<td>10</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_NULL</td>
<td>11</td>
<td>[RFC2407]</td>
<td></td>
</tr>
<tr>
<td>ESP_AES</td>
<td>12</td>
<td>[Leech]</td>
<td></td>
</tr>
<tr>
<td>Reserved for private use</td>
<td>249-255</td>
<td>[RFC2407]</td>
<td></td>
</tr>
</tbody>
</table>
Table 7 ESP Authentication algorithm identifiers

<table>
<thead>
<tr>
<th>Transform identifier</th>
<th>Value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED</td>
<td>0</td>
<td>[RFC2407]</td>
</tr>
<tr>
<td>HMAC-MD5</td>
<td>1</td>
<td>[RFC2407]</td>
</tr>
<tr>
<td>HMAC-SHA</td>
<td>2</td>
<td>[RFC2407]</td>
</tr>
<tr>
<td>DES-MAC</td>
<td>3</td>
<td>[RFC2407]</td>
</tr>
<tr>
<td>KPDK</td>
<td>4</td>
<td>[RFC2407]</td>
</tr>
<tr>
<td>HMAC-SHA2-256</td>
<td>5</td>
<td>[Leech]</td>
</tr>
<tr>
<td>HMAC-SHA2-384</td>
<td>6</td>
<td>[Leech]</td>
</tr>
<tr>
<td>HMAC-SHA2-512</td>
<td>7</td>
<td>[Leech]</td>
</tr>
<tr>
<td>HMAC-RIPEMD</td>
<td>8</td>
<td>[RFC2857]</td>
</tr>
<tr>
<td>RESERVED</td>
<td>9-61439</td>
<td></td>
</tr>
<tr>
<td>Reserved for private use</td>
<td>61440-65535</td>
<td></td>
</tr>
</tbody>
</table>
Encryption (1)

- There are two specific applications in cryptography techniques
  - First: Encryption
    - Secret-Key Algorithm: Sender and Receiver share the same secret key
    - Public-Key Algorithm: Sender will encrypt the message by public key and receiver will decrypt it by secret key
      - Secret key will never be transmitted onto network
      - Once encrypted, only those with secret key are able to decrypt the ciphertext
Encryption (2)

Secret-key encryption and decryption:
- Plain Text
- Encryption Algorithm
- Cipher text
- Decryption Algorithm
- Plain Text

Public-key encryption and decryption:
- Plain Text
- Encryption Algorithm
- Cipher text
- Decryption Algorithm
- Plain Text
Encryption (3)

• A fundamental concern with secret-key algorithms is how to distribute the secret keys in a secure manner

• But it basically is secure unless artificial divulging the secret key
Message Authentication (1)

• There are two specific applications in cryptography techniques (continue)
  – Second: Message Authentication
    • Uses a secret key and the original message as inputs to generate a Message Authentication Code (MAC)
    • A variation of MAC is one-way hash function: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1), both are un-keyed hash functions
Message Authentication (2)

– A one-way hash function takes an arbitrarily long input message and produces a fixed-length, pseudo-random output called a hash
– Knowing a hash, it is computationally difficult to find the message that produced the hash
– It is almost impossible to find different messages that will generate the same hash
Message Authentication (3)

- The combination of one-way hash function with the secret key method, Keyed-Hashing for Message Authentication (HMAC) is also used.
RADIUS Protocol (1)

• Remote Authentication Dial-in User Service (RADIUS) protocol
  – Commonly adopted for end-user authentication and key distribution
  – The Access Point is called RADIUS client
RADIUS Protocol (2)

Example of the RADIUS protocol usage

Originally made by Chou Hung-Lin, M100, CCL/ITRI
IAPP Protocol (1)

- IEEE 802.11F (Inter-Access Point Protocol, IAPP)
  - The IAPP is a communication protocol, used by the management entity of an AP to communicate with other APs
    - Facilitate the creation and maintenance of the Extended Service Set (ESS)
    - Support the mobility of STAs
    - Enable APs to enforce the requirement of a single association for each STA at a given time
IAPP Protocol (2)

- RADIUS protocol is adopted between RADIUS client and the RADIUS server, not between end-user and the RADIUS server
- RADIUS is also used to obtain the security information to secure the communication between IAPP entities
- IPSec - Encapsulating Security Payload (ESP), adopted for secure inter-communication between APs, mainly provides message confidentiality (encryption) and authentication for IAPP packets
IAPP Protocol (3)

– RADIUS Registration Access Request (AP ∀ RADIUS server) is used by RADIUS server to
  • Register the AP as a valid member of the ESS
  • Establish a secure channel for broadcast communications to all other APs in the ESS

– The ESP related security parameters for the broadcast communications, contained in RADIUS Registration Access Accept, are encrypted by MPPE(Microsoft Point-to-Point Encryption)-Send-Key
IAPP Protocol (4)

– RADIUS Access Request (AP ∀ RADIUS server) is used by RADIUS server to
  • Verify that the Old AP is a valid member of the ESS New AP belongs to
  • Establish a secure channel for communications with the Old AP

– The ESP related security parameters for the communications with old AP, contained in RADIUS Access Accept, are authenticated and decrypted by ESP obtained above, and with RADIUS BSSID Secret cooperated with HMAC-SHA1 method
IAPP Protocol (5)

- RADIUS Registration Access Request
- RADIUS Registration Access Accept
- RADIUS Access Request
- RADIUS Access Accept
Exchange Security Policies in IKEv2

Radius-Registration-Procedure

BS-1 -> BS-2, Key Sequence Number=0

Radius-Access-Request

BS-1 -> BS-2, Key Sequence Number=0

Radius-Access-Accept

IPSec Policies of BS-1<->BS-2,
32-bytes MPPE-Send-Key, 32-bytes MPPE-Recv-Key
Key Sequence Number, BS-2 IP Address

IKEv2

HDR, SAi1, KEi, Ni

IKEv2

HDR, SAR1, KEr, Nr, {CERTREQ}

IKEv2

HDR, SK {IDi, {CERT}, {CERTREQ}, {IDr} AUTH, SAi2, TSi, TSr}
IPSec - Encapsulating Security Payload (ESP) example

IPv4 – Before applying ESP

<table>
<thead>
<tr>
<th>Original IP hdr</th>
<th>TCP</th>
<th>Data</th>
</tr>
</thead>
</table>

IPv4 – After applying ESP

<table>
<thead>
<tr>
<th>Original IP hdr</th>
<th>ESP header</th>
<th>TCP</th>
<th>Data</th>
<th>ESP trailer</th>
<th>ESP auth</th>
</tr>
</thead>
</table>

After applying ESP:ESP header, ESP trailer, and ESP authenticator

- **Encrypted**: The payload data is encrypted except for mutable fields.
- **Authenticated**: The authentication algorithm is applied from the ESP header to the ESP trailer, and produces an authenticator field, ESP authenticator.

- **ESP header** contains a Security Parameter Index and a Sequence Number. Security Parameter Index identifies a unique Security Association (SA). Sequence Number is used to prevent replay attacks.
- **ESP trailer** consists of Padding and Pad Length to make the plaintext a multiple of some number of bytes, ensuring it is appropriate for the encryption algorithm.

---

IPv4

- Before applying ESP
- After applying ESP

---

The authentication algorithm is applied from the ESP header to the ESP trailer, and produces a field, ESP authenticator.