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 Voice: 886-3-5913274
CCL, ITRI Fax: 886-3-5829733
Bldg. 11, 195 Sec. 4, Chung Hsing Rd. Chutung, E-mail: Lucien@itri.org.tw
HsinChu, Taiwan 310, R.O.C.

Venue:

Session #37, 2-5 May, 2005

Base Document:

Purpose:

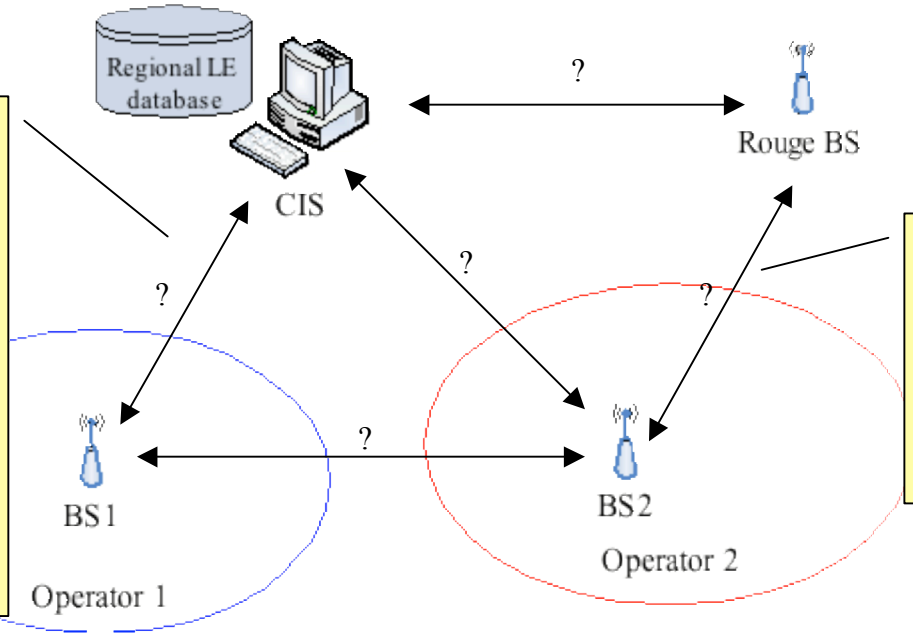
Facilitate co-channel and adjacent channel coexistence for 802.16 LE.

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

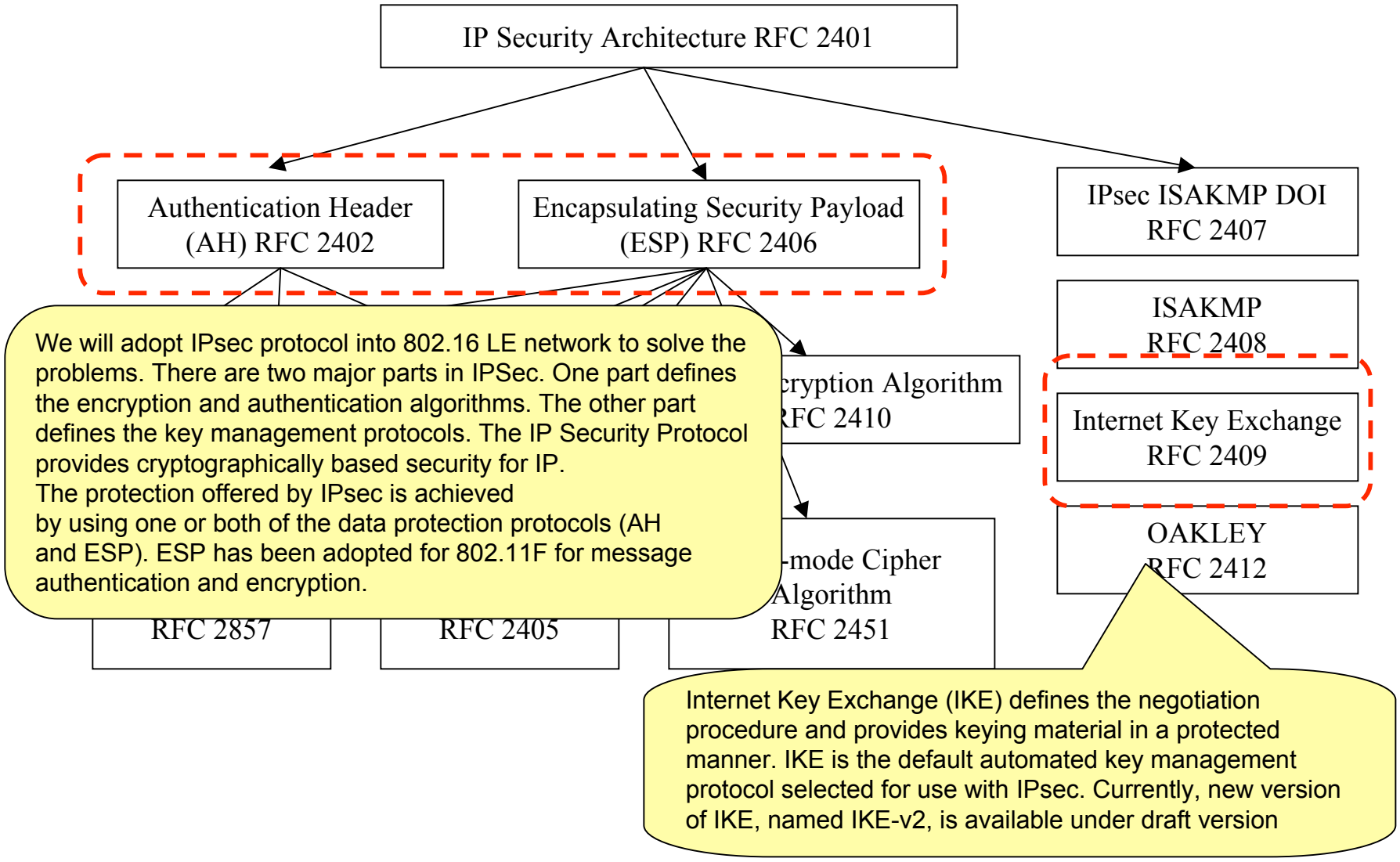
In 802.16 LE network, how do BSs of different network operators perform inter-communication without a well defined communication mechanism? BSs belong to different operators may do not have any info. between each other, e.x. IP address, security policy, etc. The same situation happens on the inter-communication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



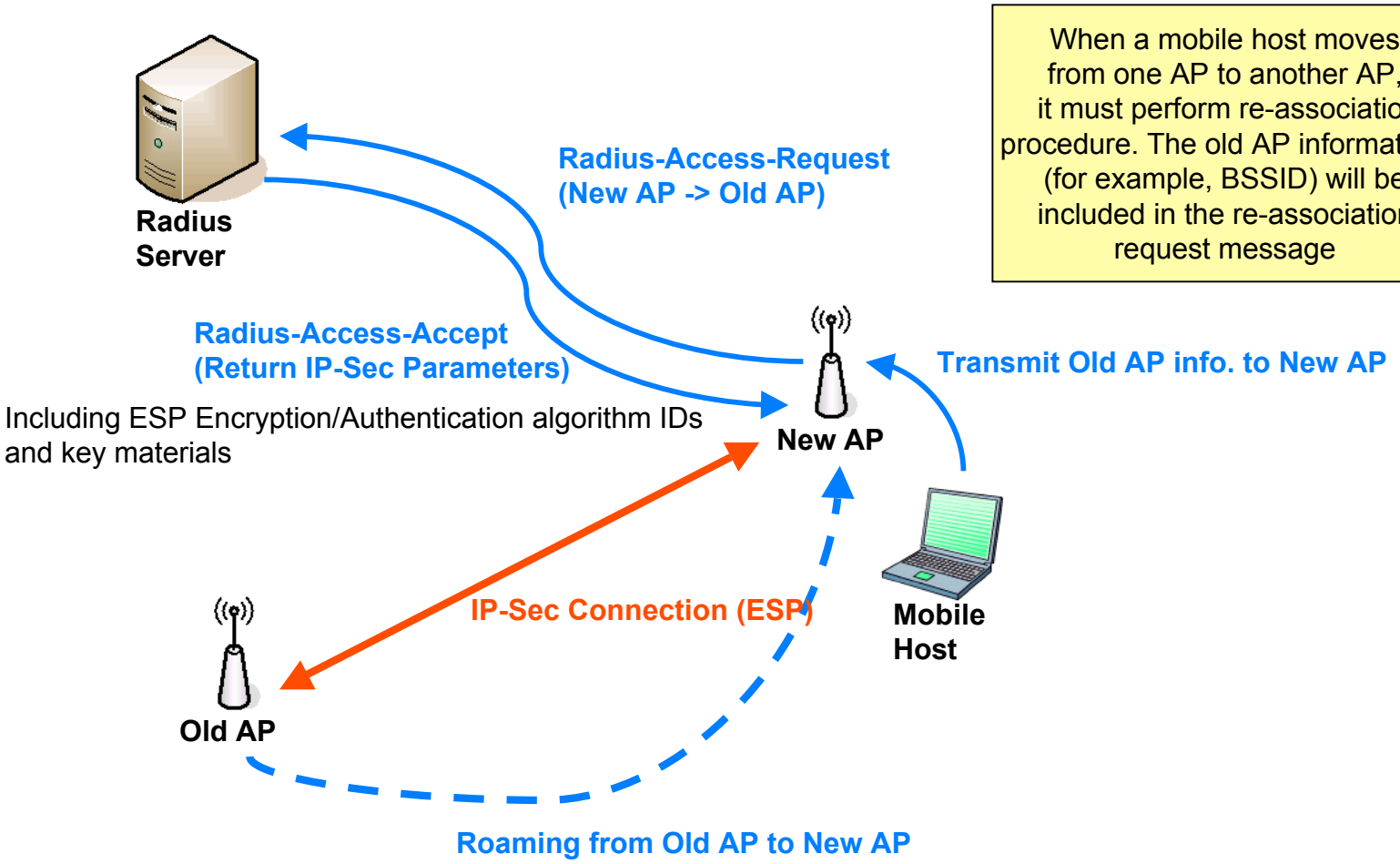
On the other hand, a rough BS may fake a valid member of this network to perform actions not permitted. It may cause the network operating not correctly (DoS, etc)

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

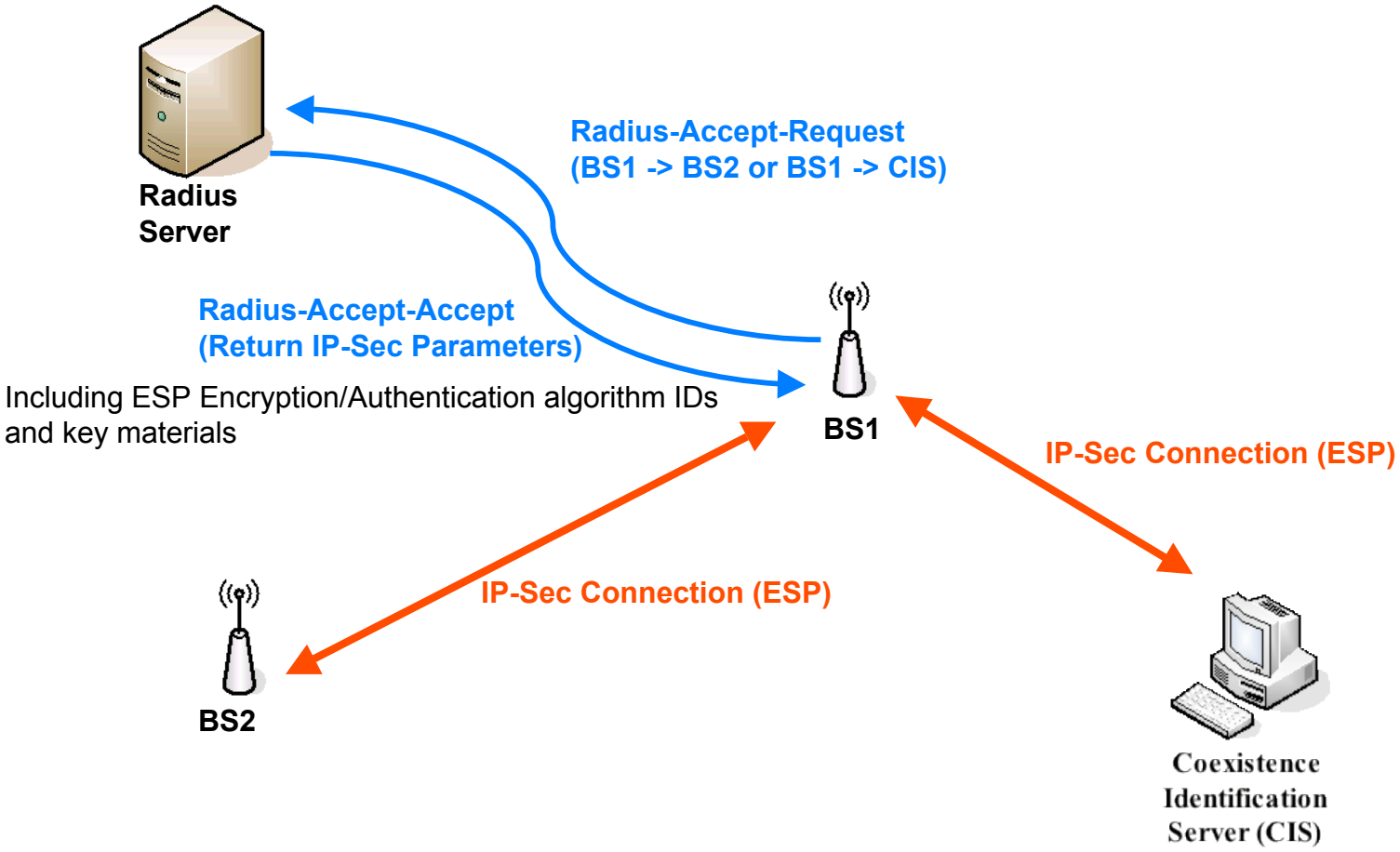
IP-Security (IP-Sec) Family

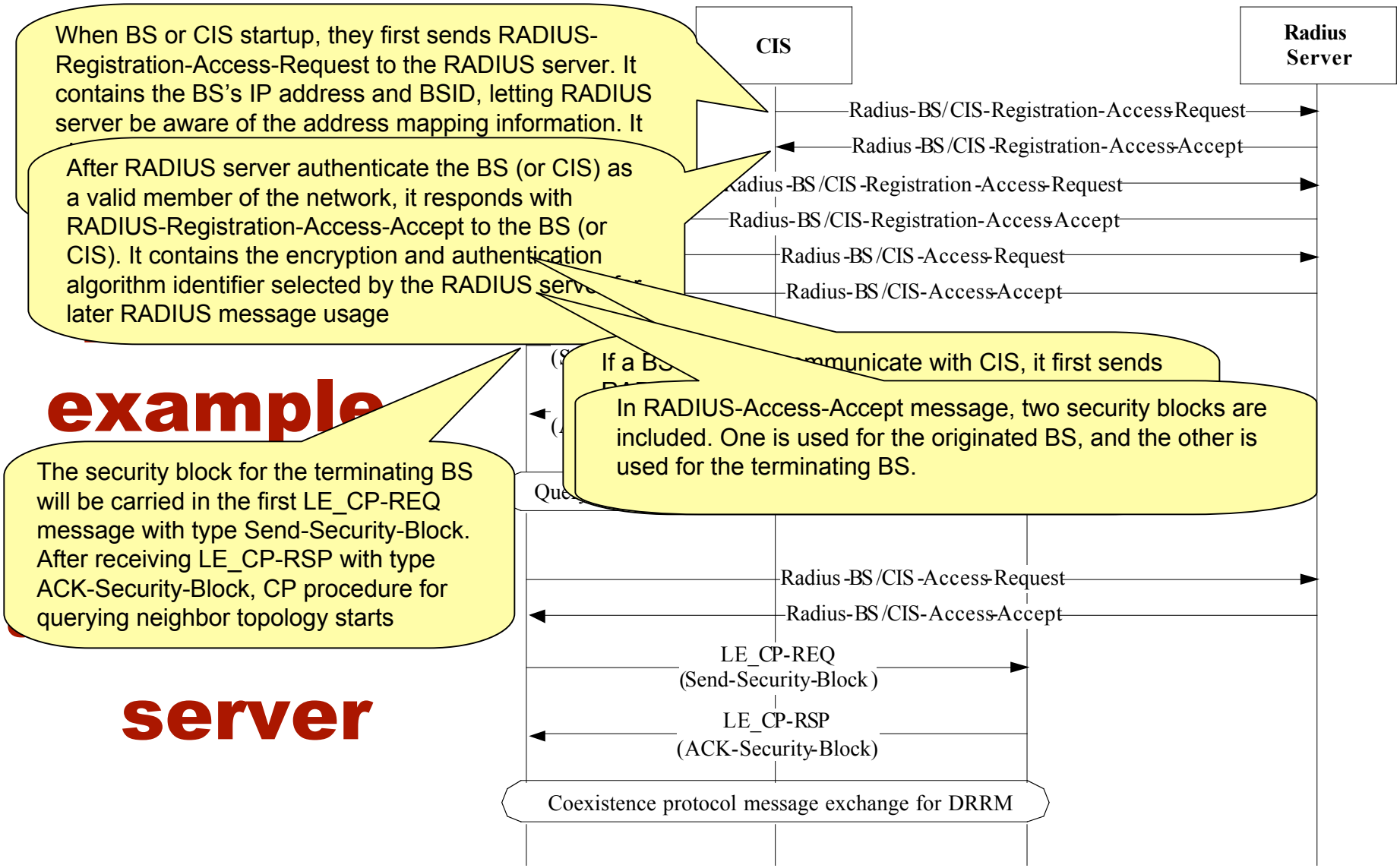


802.11F (IAPP) System



Solution 1 - 802.16h (CP) System (C80216h-05_012)



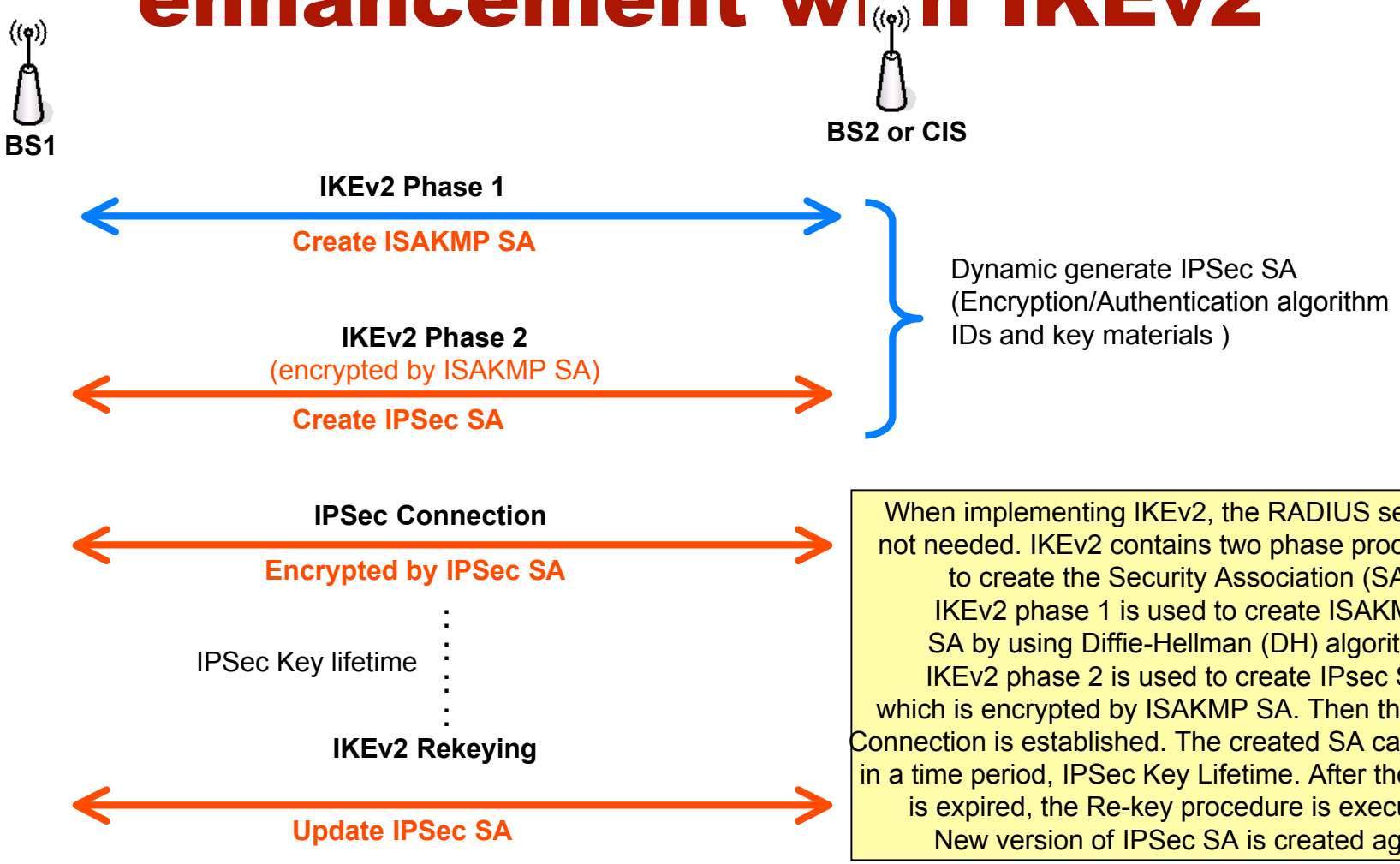

When BS or CIS startup, they first sends RADIUS-Registration-Access-Request to the RADIUS server. It contains the BS's IP address and BSID, letting RADIUS server be aware of the address mapping information. It
After RADIUS server authenticate the BS (or CIS) as a valid member of the network, it responds with RADIUS-Registration-Access-Accept to the BS (or CIS). It contains the encryption and authentication algorithm identifier selected by the RADIUS serv
later RADIUS message usage
example
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
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.
CIS
Radius Server
Radius-BS/CIS-Registration-Access-Request
Radius-BS/CIS-Registration-Access-Accept
Radius-BS/CIS-Registration-Access-Request
Radius-BS/CIS-Registration-Access-Accept
Radius-BS/CIS-Access-Request
Radius-BS/CIS-Access-Accept
Radius-BS/CIS-Access-Request
Radius-BS/CIS-Access-Accept
LE_CP-REQ
(Send-Security-Block)
LE_CP-RSP
(ACK-Security-Block)
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



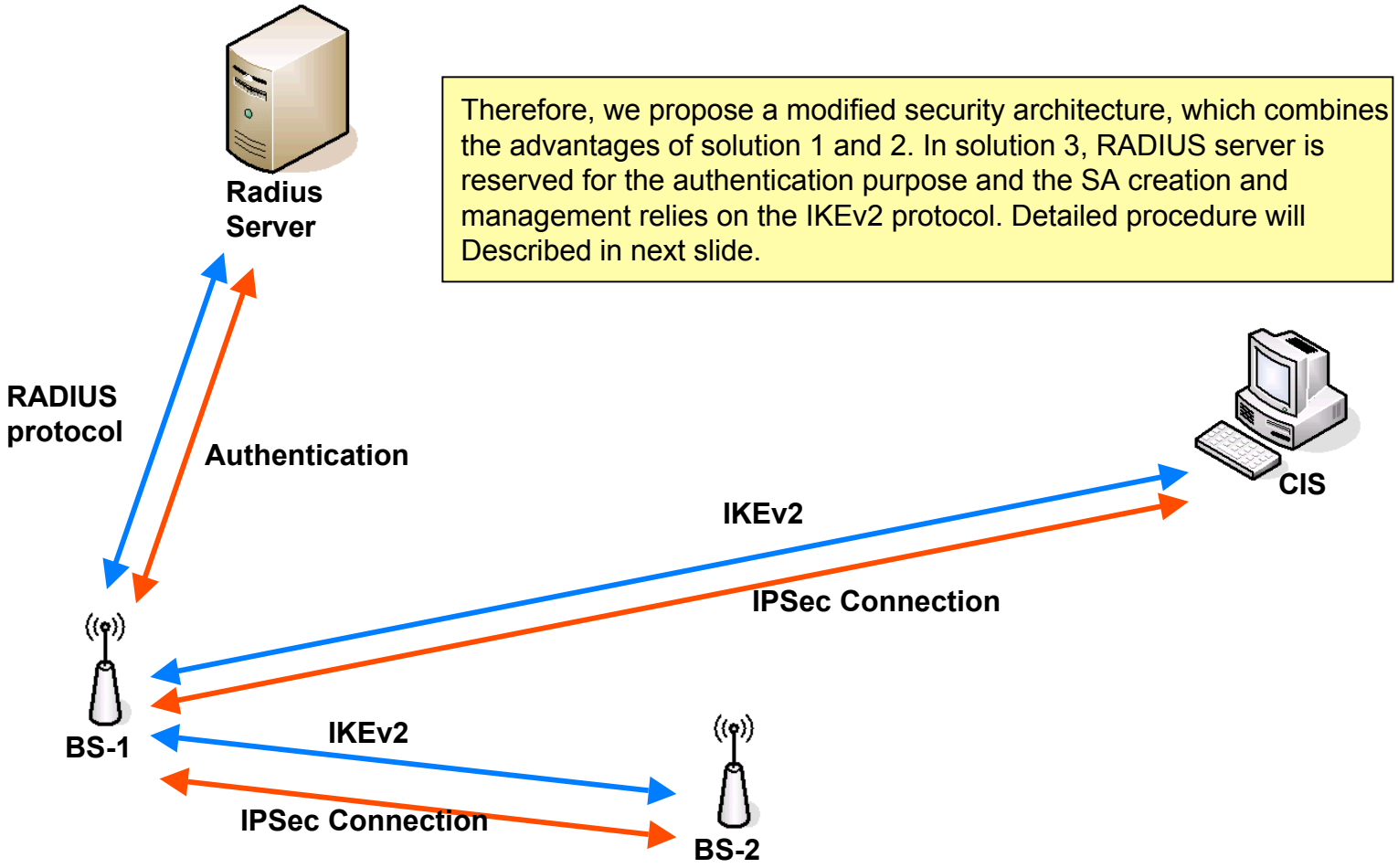
When implementing IKEv2, the RADIUS server is not needed. IKEv2 contains two phase procedures to create the Security Association (SA). IKEv2 phase 1 is used to create ISAKMP SA by using Diffie-Hellman (DH) algorithm. IKEv2 phase 2 is used to create IPsec SA, which is encrypted by ISAKMP SA. Then the 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

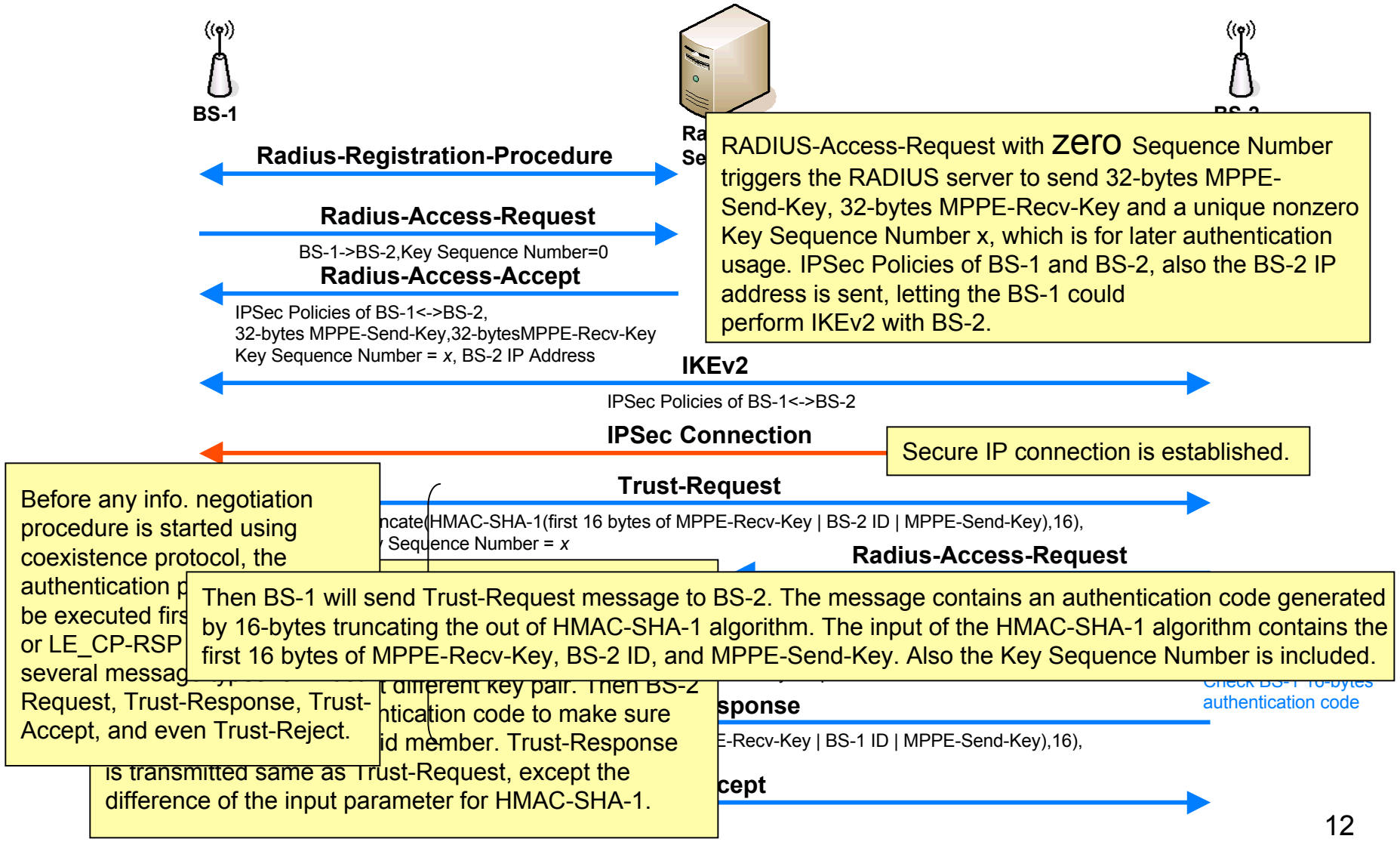
Note: In this case, IP addresses of BSs are located in the CIS.

Solution 3 – Trusted third party & IKEv2



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 Described in next slide.

Solution 3 – Trusted third party & IKEv2



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

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

TBD: To Be Defined

Table 2 RADIUS-BS/CIS-Registration-Access-Accept

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

Table 3 RADIUS-BS/CIS-Access-Request

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

Table 4 RADIUS-BS/CIS-Access-Accept

Attribute number	Attribute name	Value
1	User-Name	Regional CIS's WM address or neighbor BS's BSID.
8	Framed-IP-Address	IP Address of Regional CIS or neighbor BS.
26	Vendor-Specific-Attribute (VSA)	
26-TBD	Originated-BS-Security-Block	Security Block encrypted using original BS's RADIUS BSID secret, to be decrypted and used by the original BS
26-TBD	Terminated-BS/CIS-Security-Block	Security Block encrypted using neighbor BS's RADIUS BSID secret (or CIS's), to be decrypted and used by the neighbor BS (or CIS)
80	Message-Authenticator	The RADIUS message's authenticator

Table 5 Information elements in the Originated-BS-Security-Block

Element ID	Length	Information
2	8	Security lifetime in seconds.
3	32	ACK nonce.
4	1	ESP transform number.
5	1	ESP authentication number.
6	4	SPI used to identify ESP SA to the regional CIS or neighbor BS
7	Variable	Key used by ESP Transform for ESP packets to the regional CIS or neighbor BS
8	Variable	Key used by ESP Authentication for ESP packets to the regional CIS or neighbor BS
9	4	SPI used to identify ESP SA from the regional CIS or neighbor BS
10	Variable	Key used by ESP Transform for ESP packets from the regional CIS or neighbor BS
11	Variable	Key used by ESP Authentication for ESP packets from the regional CIS or neighbor BS

Table 6 ESP Transform identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
ESP_DES_IV64	1	[RFC2407]
ESP_DES	2	[RFC2407]
ESP_3DES	3	[RFC2407]
ESP_RC5	4	[RFC2407]
ESP_IDEA	5	[RFC2407]
ESP_CAST	6	[RFC2407]
ESP_BLOWFISH	7	[RFC2407]
ESP_3IDEA	8	[RFC2407]
ESP_DES_IV32	9	[RFC2407]
ESP_RC4	10	[RFC2407]
ESP_NULL	11	[RFC2407]
ESP_AES	12	[Leech]
Reserved for private use	249-255	[RFC2407]

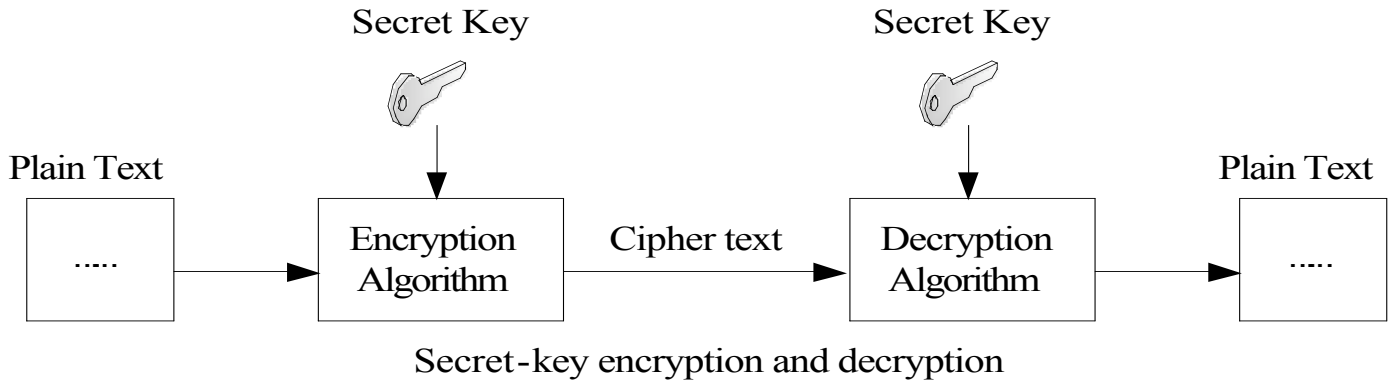
Table 7 ESP Authentication algorithm identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
HMAC-MD5	1	[RFC2407]
HMAC-SHA	2	[RFC2407]
DES-MAC	3	[RFC2407]
KPDK	4	[RFC2407]
HMAC-SHA2-256	5	[Leech]
HMAC-SHA2-384	6	[Leech]
HMAC-SHA2-512	7	[Leech]
HMAC-RIPEMD	8	[RFC2857]
RESERVED	9-61439	
Reserved for private use	61440-65535	

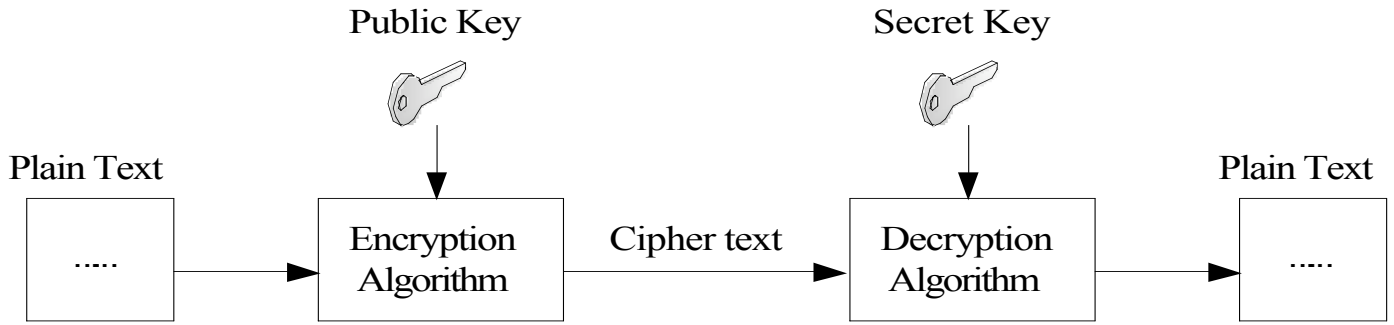
Encryption (1)

- 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



Public -key encryption and decryption

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)

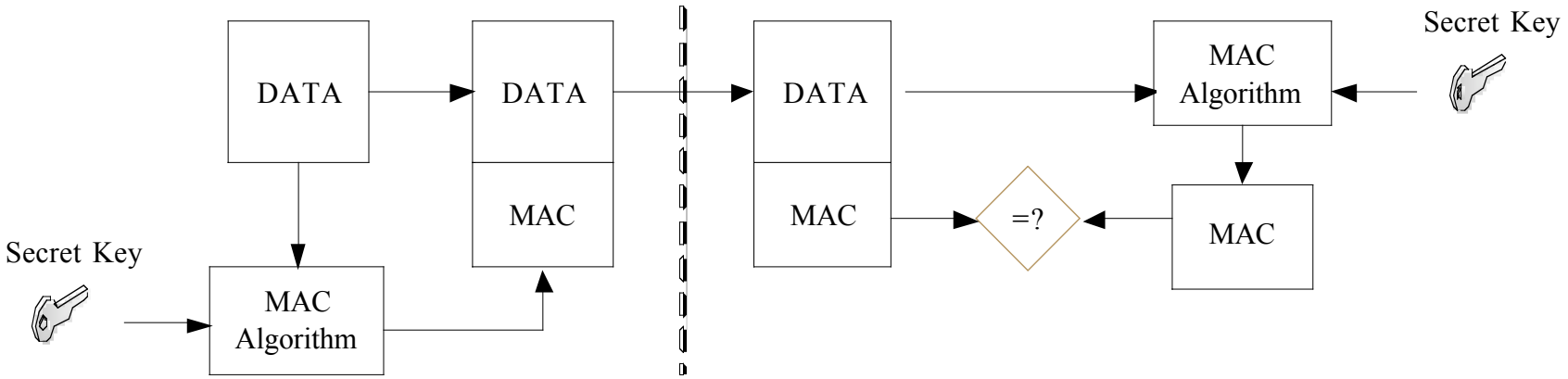
- There are two specific applications in cryptography techniques (continue)
  - Second: Message Authentication
    - Uses a secret key and the original message as inputs to generate a Message Authentication Code (MAC)
    - A variation of MAC is one-way hash function: Message Digest 5 (MD5) and Secure 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

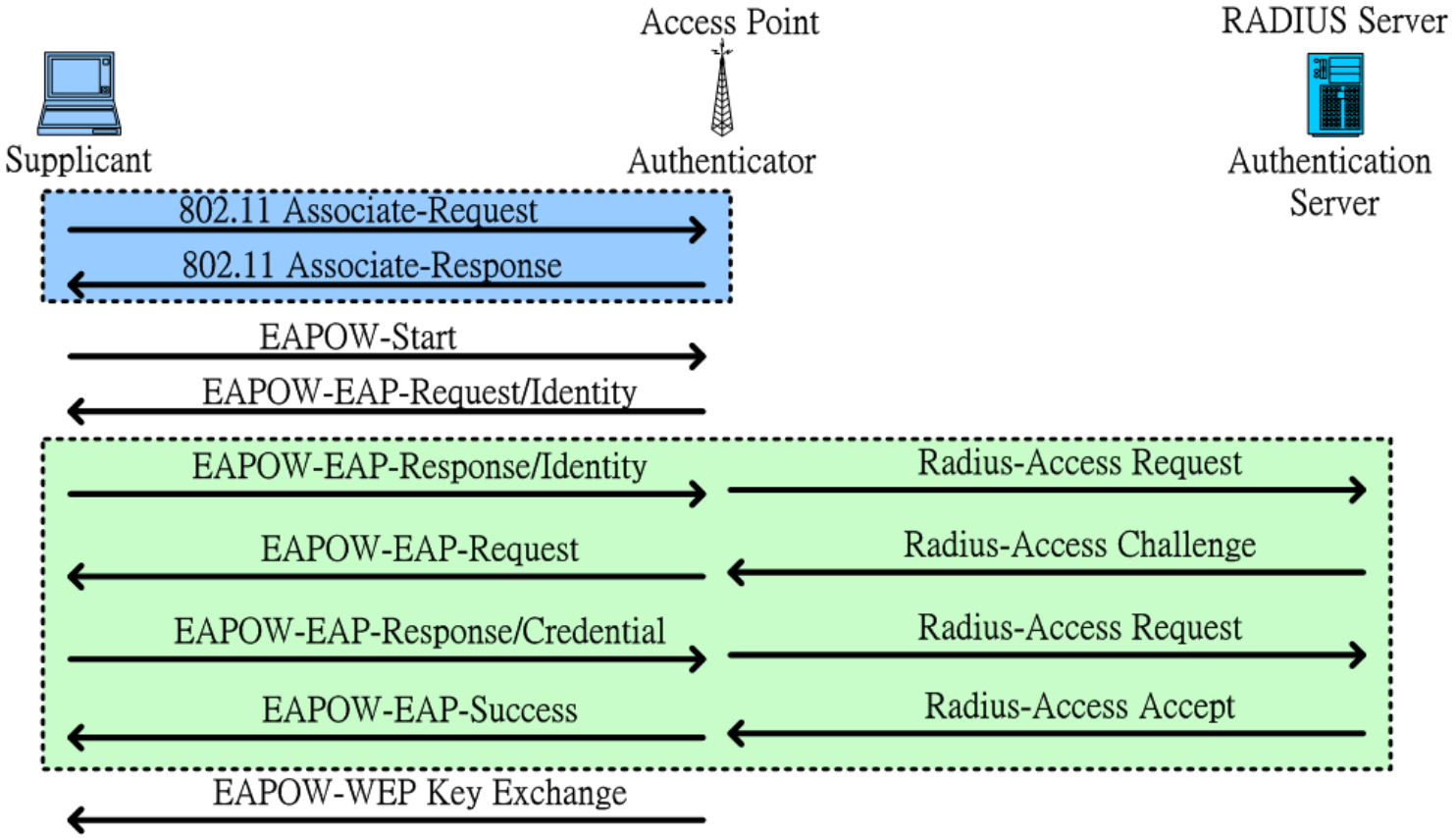


RADIUS Protocol (1)

- 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

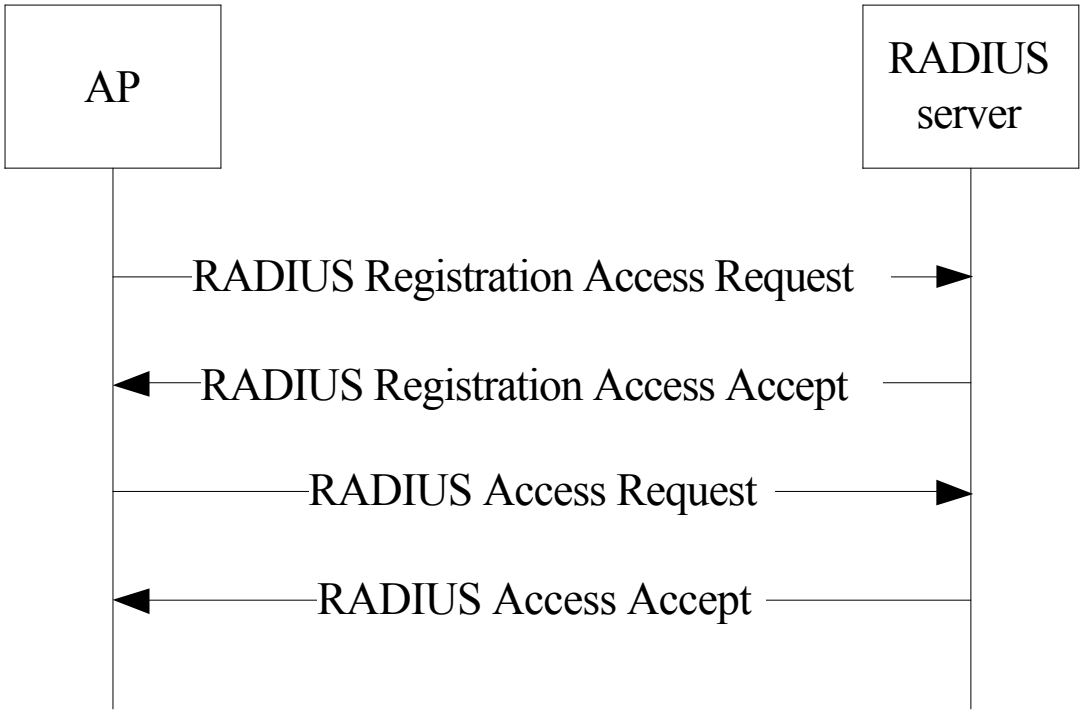
IAPP Protocol (3)

- 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

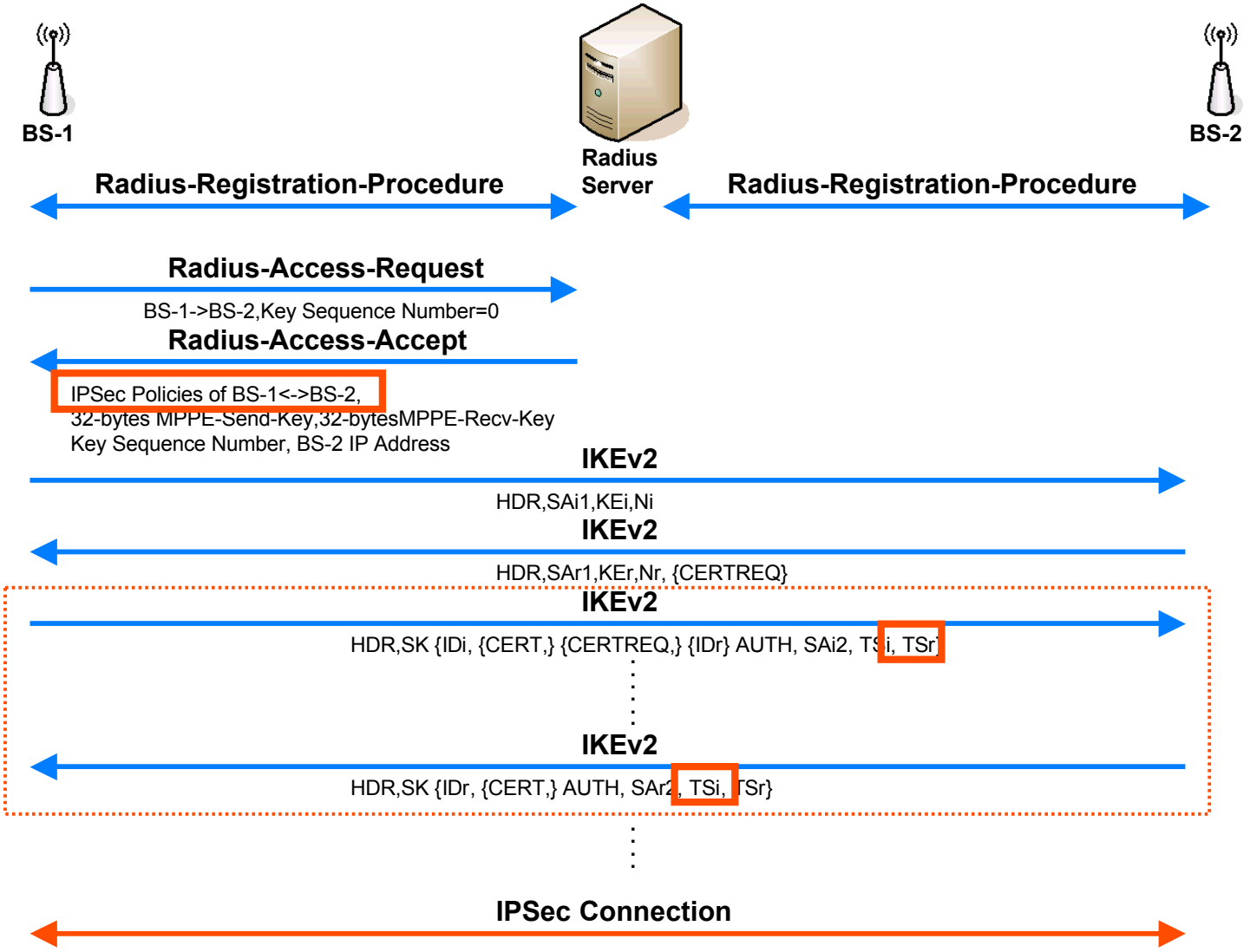
IAPP Protocol (4)

- 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)



Exchange Security Policies in IKEv2



IPSec - Encapsulating Security Payload (ESP) example

IPv4 – Before applying ESP

IPv4 – After applying ESP