Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14402
Date:	2010-09-07
Replaces:	
Document Type:	National Body Contribution
Document Title:	NB of China's contribution on the Initial Study Report and calling for a Study Period for further enhancement on LAN Security
Document Source:	NB of China
Project Number:	
Document Status:	For consideration at the SC 6/WG 1 London meeting.
Action ID:	FYI
Due Date:	
No. of Pages:	28

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)
Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;
Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

Initial Study Report and calling for a Study Period for further enhancement on LAN Security

SC6 Mirror Committee, China

Date: 2010-08

Notice: This document is prepared for presentation at the ISO/IEC JTC1/SC6/WG1 meeting, September27-October1, 2010. It is the basis for discussion. 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.

Agenda

1 LAN Overview

2 Current Standard Overview

3 TLSec Protocol

4 Summary and Next Step

LAN Overview

➢LAN Application Overview：

- ✓ Due to the high efficiency of network information transmission, Local area networks are more and more popular in enterprises and institutions. Many universities, research institutes, banks and public security departments have established their own local area network.
- ✓ However, in practice, due to the lack of effective LAN security protection, unauthorized network devices or users are likely to access networks automatically through LAN access devices, creating a great security threat. Therefore, the potential of LANs cannot be fully exploited.

LAN Overview

➢LAN Secure Overview

✓ Network security incident:

- **Outside Network**: attacks from outside, such as malicious attacks, remote intrusion, viruses, worms and so on.
- **Inside Network**: attacks from inside, such as sniffing.

✓ Most of network administrators emphasize external protection, but underestimate internal management;

✓ According to the authoritative department statistics, 70% of the network security attacks come from internal.

LAN Overview

➢LAN Secure Overview ：

✓Network security incident in LAN：

- Unauthorized access
- Impersonate legitimate user
- Undermine the integrity of data
- Interfere normal operation of system and the availability of network system
- Viruses and malicious attacks

LAN Overview

➢LAN Secure Overview：

- ✓Local area network has kinds of loopholes in physical, protocols, operations and management, which is the root cause of LAN attacks.
- ✓LAN security needs a multi-level, three-dimensional protection system to set up a sound , effective and secure network.

Current Standard Overview

- ➢ISO/IEC 8802-3:2000(E) **Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications**
- ➢IEEE802.3,2008 Edition **Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications**
  - ✓ No secure access control
  - ✓ No confidentiality
- ➢As long as the hacker accesses to the LAN control device, he can accesses to any equipment or resource in LAN.

IEEE 802.1AE Security Overview

➢IEEE 802.1 Security Task Group

✓ **IEEE 802.1AE-2006：Media Access Control (MAC) Security；**

- The scope of this project is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.
- Key management and the establishment of secure associations is outside the scope but will be referenced by this project.
- Approved on June 8th, 2006.

✓ **IEEE 802.1AF：Authenticated Key Agreement for MACSec；**

- Key management and the establishment of secure associations are specified in 802.1AF.
- This project was subsumed into a revision of IEEE 802.1X-2004 （IEEE 802.1X-2010）

✓ **IEEE 802.1AR：Secure Device Identity；**

- Approved on December 10th, 2009.

✓ **802.1X-2010 - Revision of 802.1X-2004：Port Based Network Access Control；**

- This revision extended IEEE Std 802.1X to support IEEE Std 802.1AE MAC Security.
- IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols
- Approved on February 5th,2010.

IEEE 802.1AE Security Overview

➢IEEE 802.1AE

- ✓ The scope of this project is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients .
- ✓ Key management and the establishment of secure associations is outside the scope .
- ✓ Hop-by-Hop Encryption help secure the network from the inside.

IEEE 802.1AE Security Overview

➢IEEE 802.1AE Analysis

✓Protocol Completeness：

- Key management and the establishment of secure associations is outside the scope of 802.1AE, but is specified by IEEE 802.1X-2010 .
- IEEE 802.1X-2010 doesn’t give a specific authentication mechanism.
- Authentication in 802.1x is just between client and server. The LAN switch doesn’t have an identity and is not authenticated.

IEEE 802.1AE Security Overview

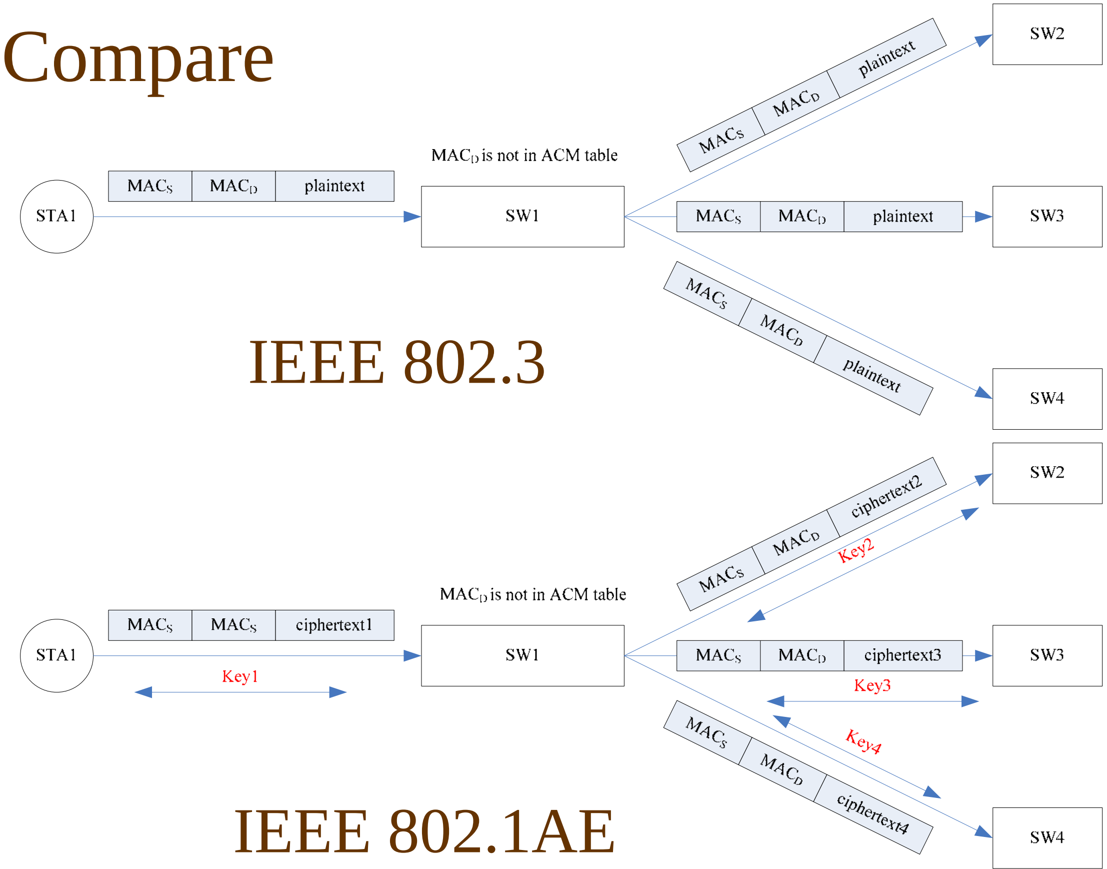
➢IEEE 802.1AE Analysis

✓ Hop-by-Hop Encryption

- It requires LAN switch decrypt each received packet with one key, encrypt it with another key, and then transmit it.
- High Latency, High cost.
- Flood is more terrible.
  - Flood :If the MAC_D of frame is not in the MAC Address table of switch, it will be transmitted to all other ports.
  - If the attacker sends a lot of frames with unknown MAC_D , it can affect the performance of the switch.
  - The MACSec switch needs to decrypt this kind of frame with one key, encrypt it with several different keys and then transmit it to all other ports.

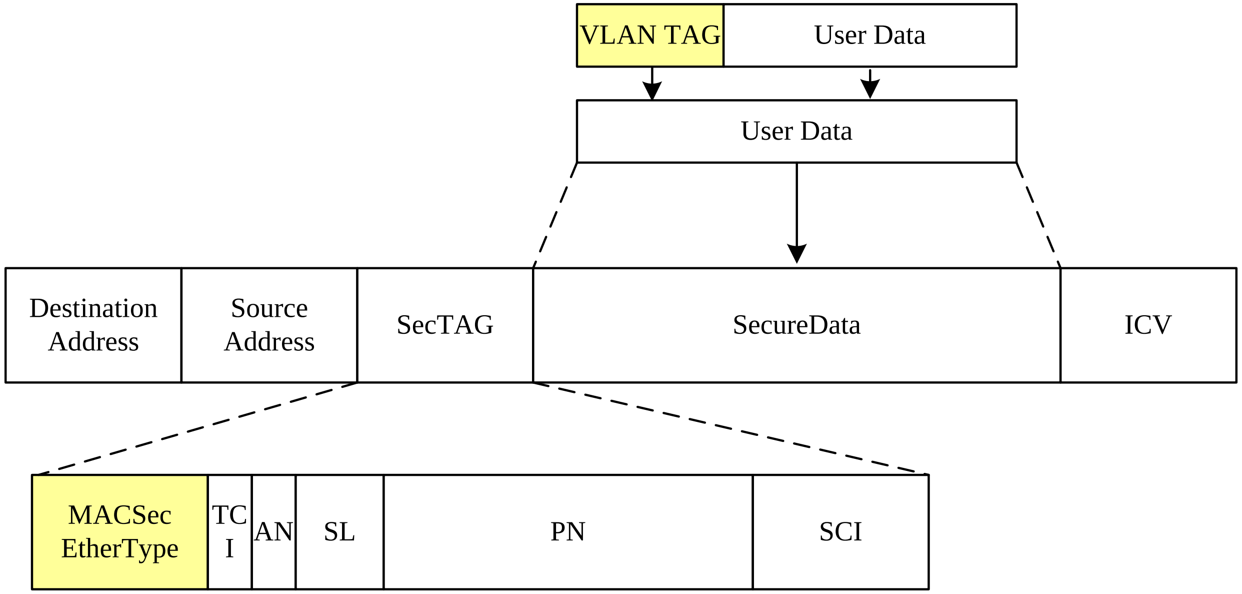
IEEE 802.1AE Security Overview

- Flood Compare


MAC$_D$ is not in ACM table
STA1
MAC_S | MAC_D | plaintext
SW1
MAC_S | MAC_D | plaintext
SW2
MAC_S | MAC_D | plaintext
SW3
MAC_S | MAC_D | plaintext
SW4
IEEE 802.3
MAC$_D$ is not in ACM table
STA1
MAC_S | MAC_S | ciphertext1
Key1
SW1
MAC_S | MAC_D | ciphertext2
Key2
SW2
MAC_S | MAC_D | ciphertext3
Key3
SW3
MAC_S | MAC_D | ciphertext4
Key4
SW4
IEEE 802.1AE

IEEE 802.1AE Security Overview

- IEEE 802.1AE Frame Format



IEEE 802.1AE Security Overview

➢IEEE 802.1AE Analysis

✓Network upgrade cost

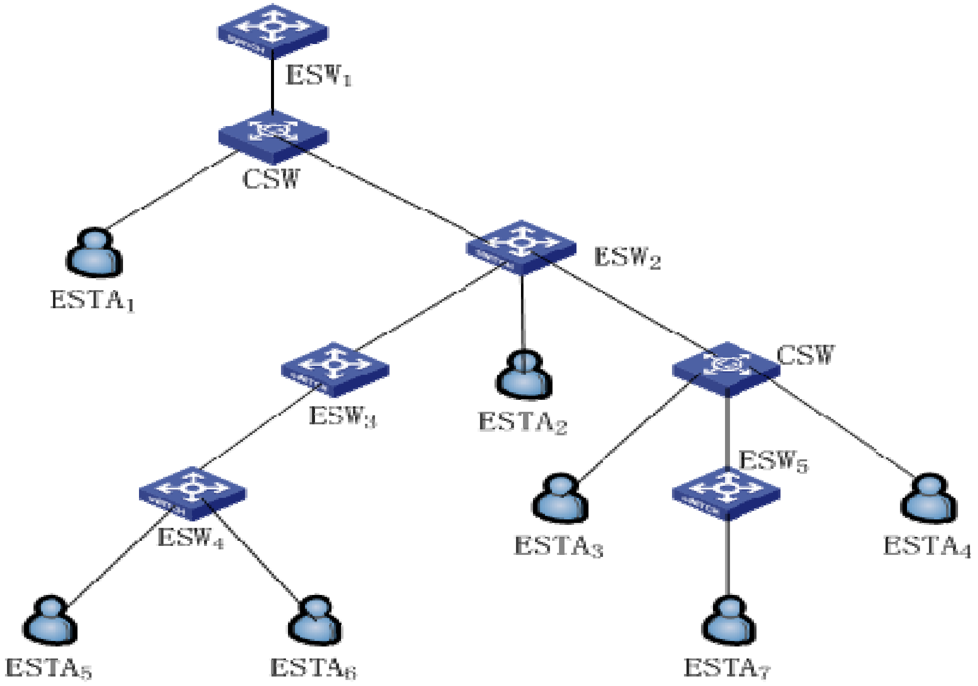
- Hop-by-Hop Encryption in MACSec requires each switch in Secure LAN to support MACSec.
- VLAN TAG in MACSec Frame is put into User Data in ciphertext. Current common switches with no encryption capability cannot distinguish VLAN TAG from MACSec Frames.
- So, MACSec can’t support hybrid network with current common switches and MACSec switches. Network upgrade cost is high。

TLSec Protocol

➢It is designed to resolve layer 2 secure problems

- ✓ Ensure Legitimate nodes access legitimate network；
- ✓ Implement key negotiation and dynamic update management
- ✓ for link layer data protection；
- ✓ Protect data confidentiality, integrity, source identification and anti-replay;
- ✓ Support multiple methods of identification, good scalability ；
- ✓ Support partial update of the network equipment.
- ✓ Provide LAN-integrated security.

TLSec Protocol

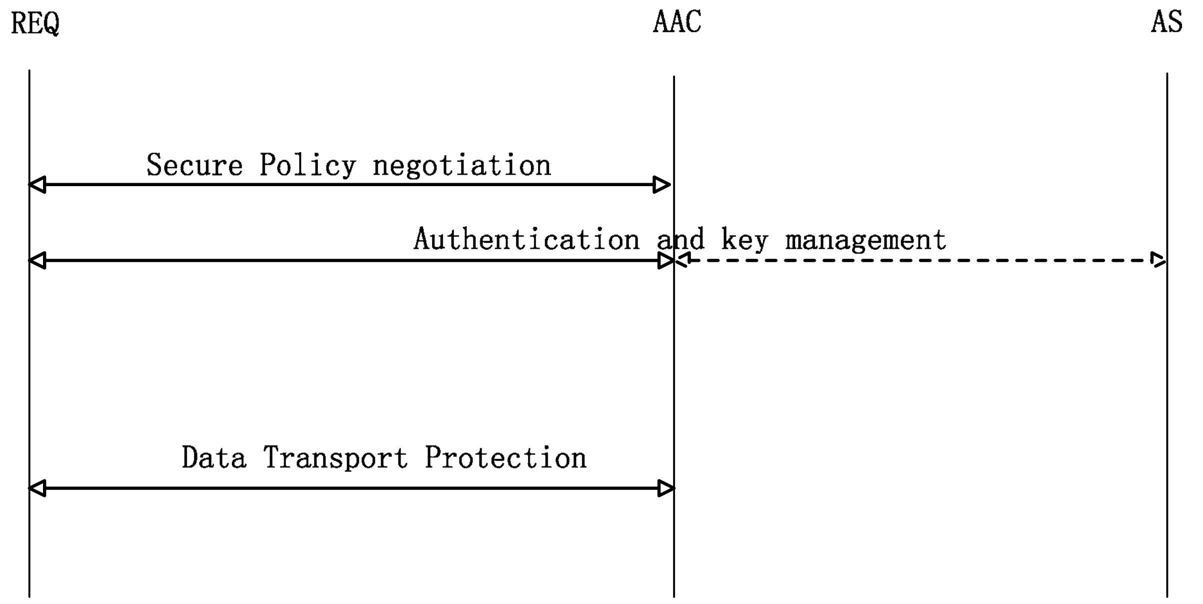


➢**The figure shows：**

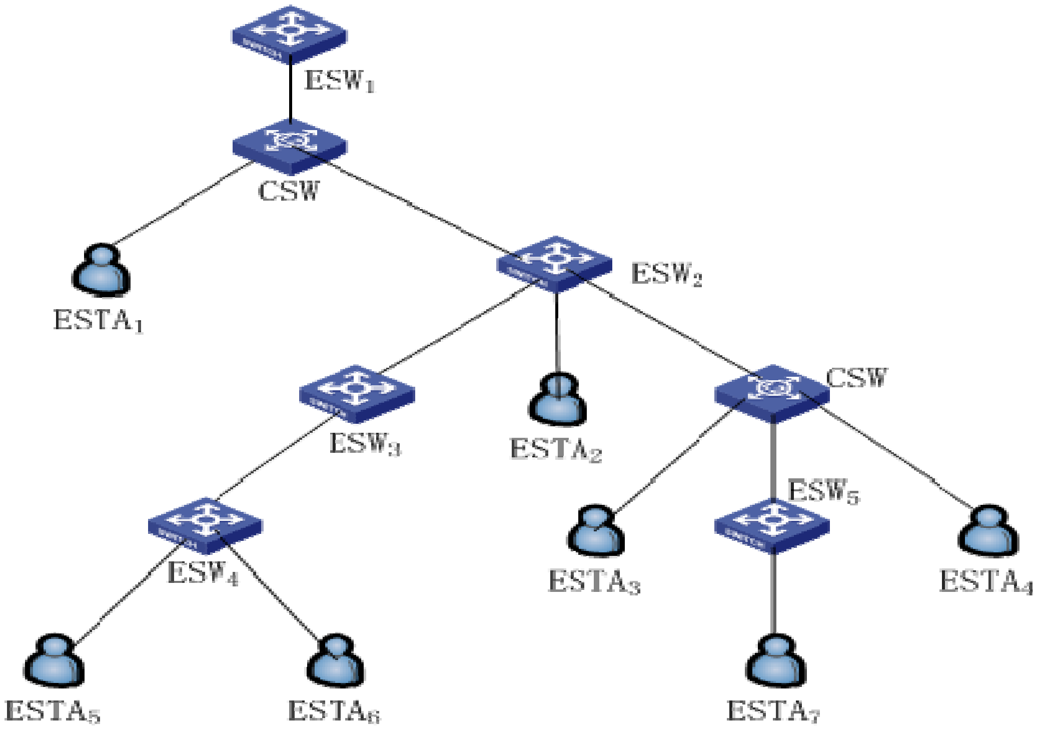
- ✓ 1： Current common switch with no encryption capability can exist in Secure LAN with TLSec switch；
- ✓ 2：Each TLSec equipment in LAN has an identity. STAs can authenticate each other to ensure legitimate nodes accessing legitimate networks；
- ✓ 3：User data in frames between two stations are always transmitted in ciphertext.

TLSec Protocol

➢Protocol Architecture


REQ
AAC
AS
Secure Policy negotiation
Authentication and key management
Data Transport Protection

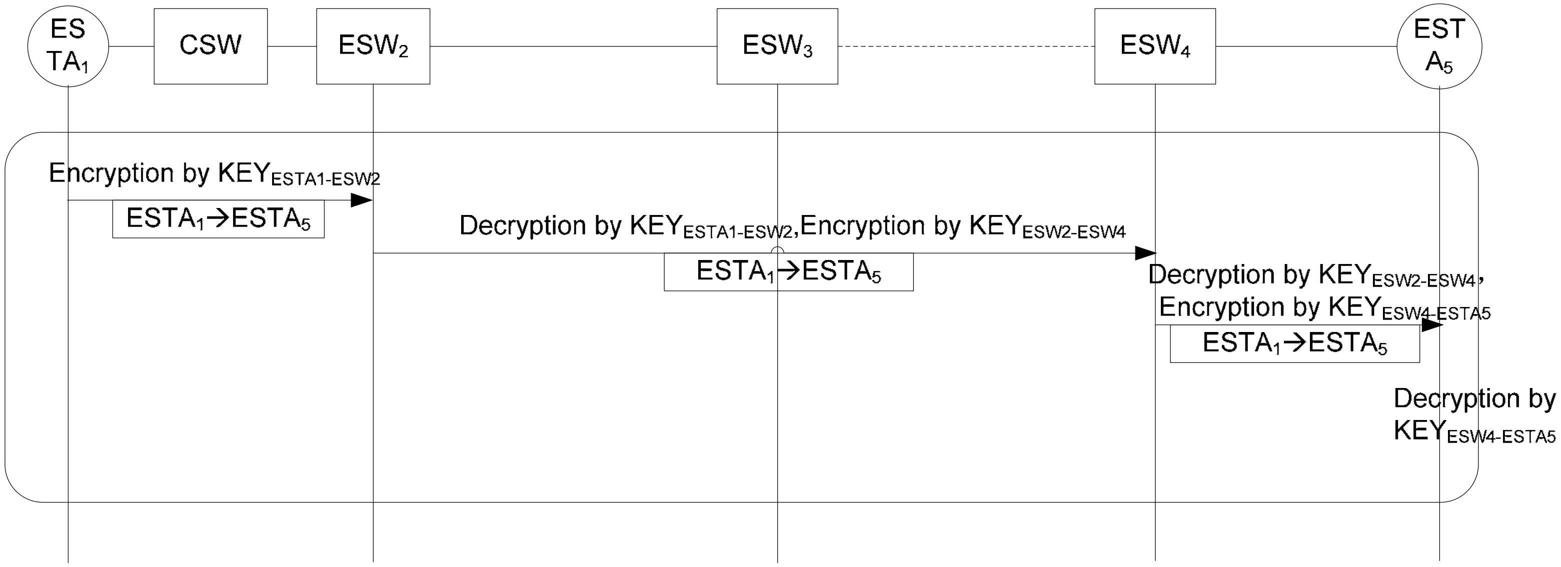
TLSec Protocol



➢Support hybrid network with current common switches and TLSec switches.

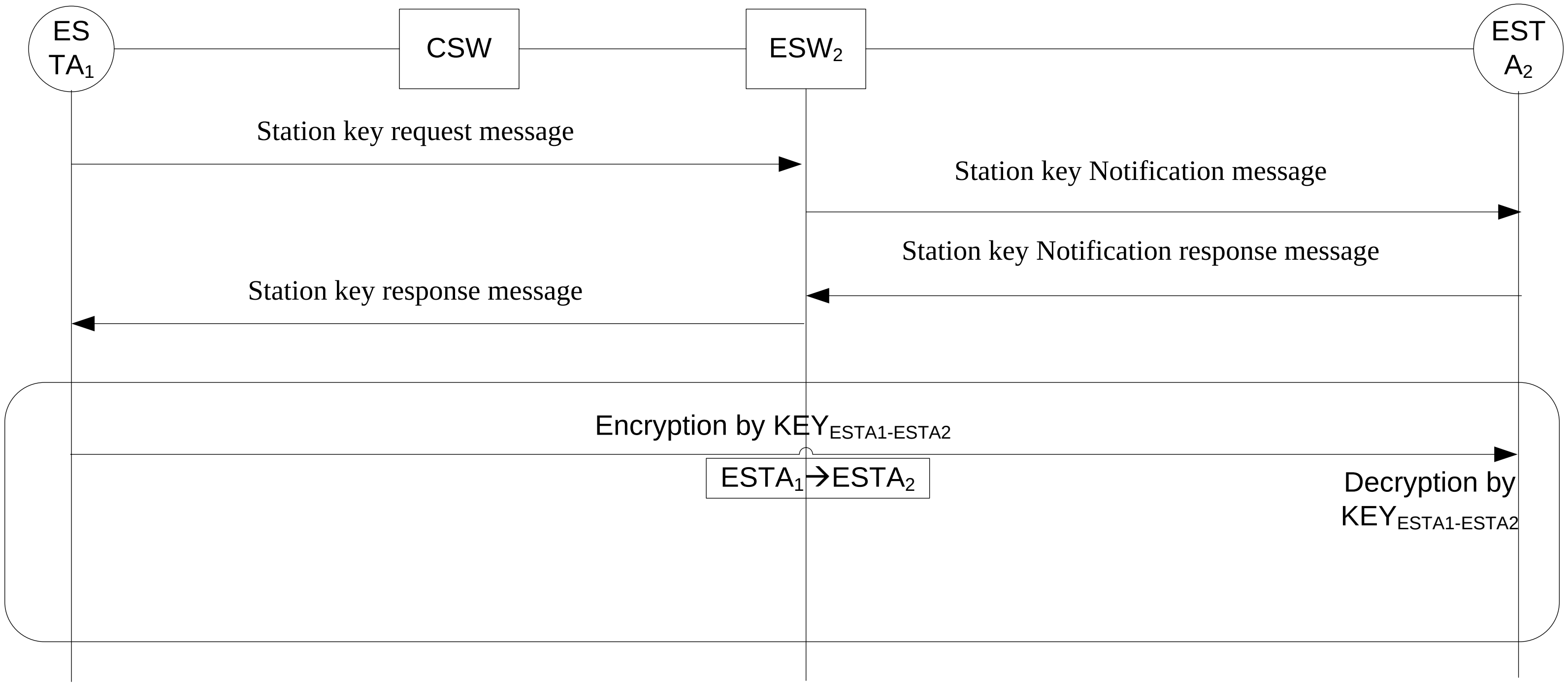
- ✓ 1：eg：ESTA1 to ESTA5/67，more than one TLSec switches: Three-stop encryption ;
- ✓ 2：eg： ESTA1 to ESTA2/3/4，just one TLSec switch: Encryption with station key ;
- ✓ 3：eg： ESTA3 to ESTA4，no TLSec switch: Encryption with station key ;

Data Transport Protection （1）


ESTA1
CSW
ESW2
ESW3
ESW4
ESTA5
Encryption by KEYESTA1-ESW2
ESTA1→ESTA5
Decryption by KEYESTA1-ESW2,Encryption by KEYESW2-ESW4
ESTA1→ESTA5
Decryption by KEYESW2-ESW4，
Encryption by KEYESW4-ESTA5
ESTA1→ESTA5
Decryption by KEYESW4-ESTA5

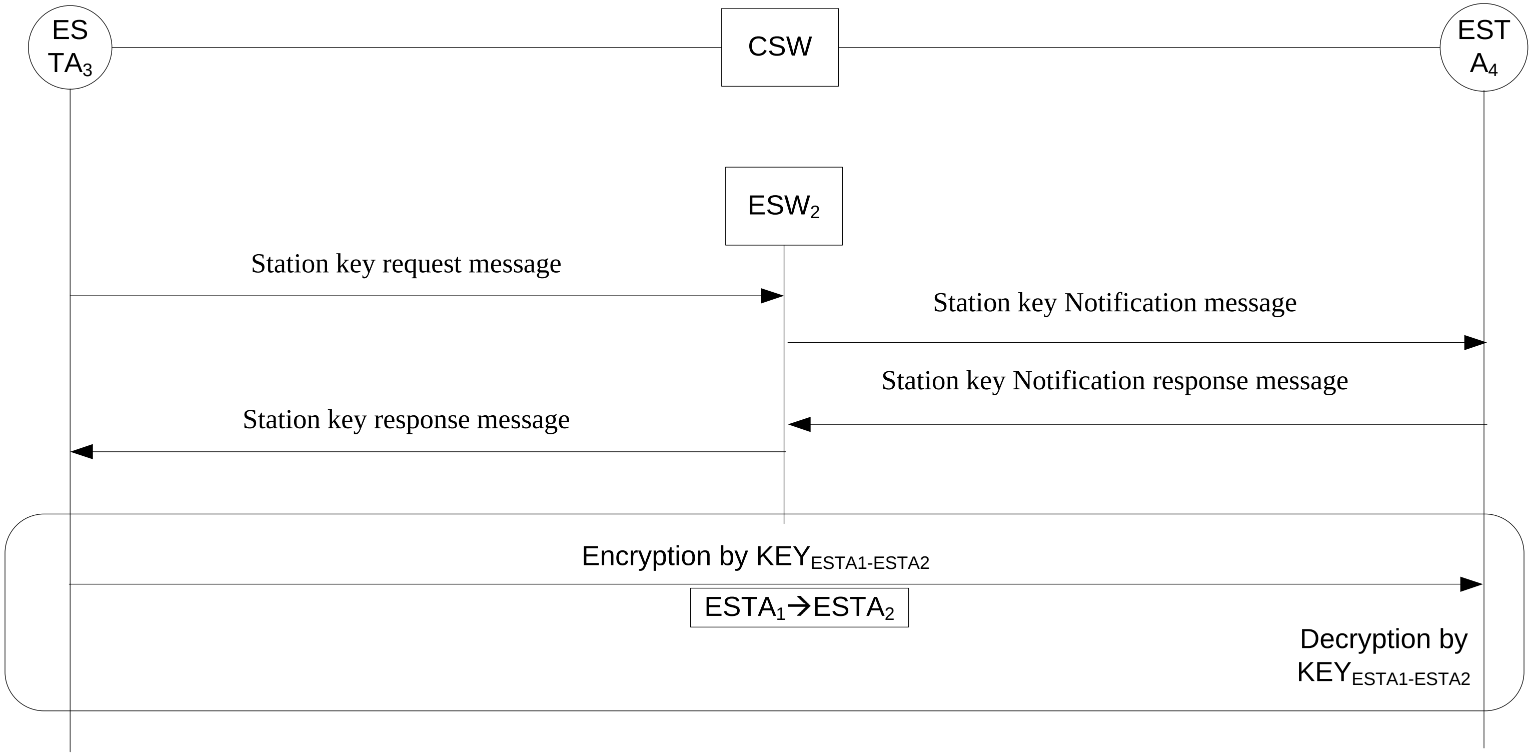
Three-stop encryption

Data Transport Protection （2）


ES TA$_1$
CSW
ESW$_2$
EST A$_2$
Station key request message
Station key Notification message
Station key Notification response message
Station key response message
Encryption by KEY$_{ESTA1-ESTA2}$
ESTA$_1$→ESTA$_2$
Decryption by KEY$_{ESTA1-ESTA2}$

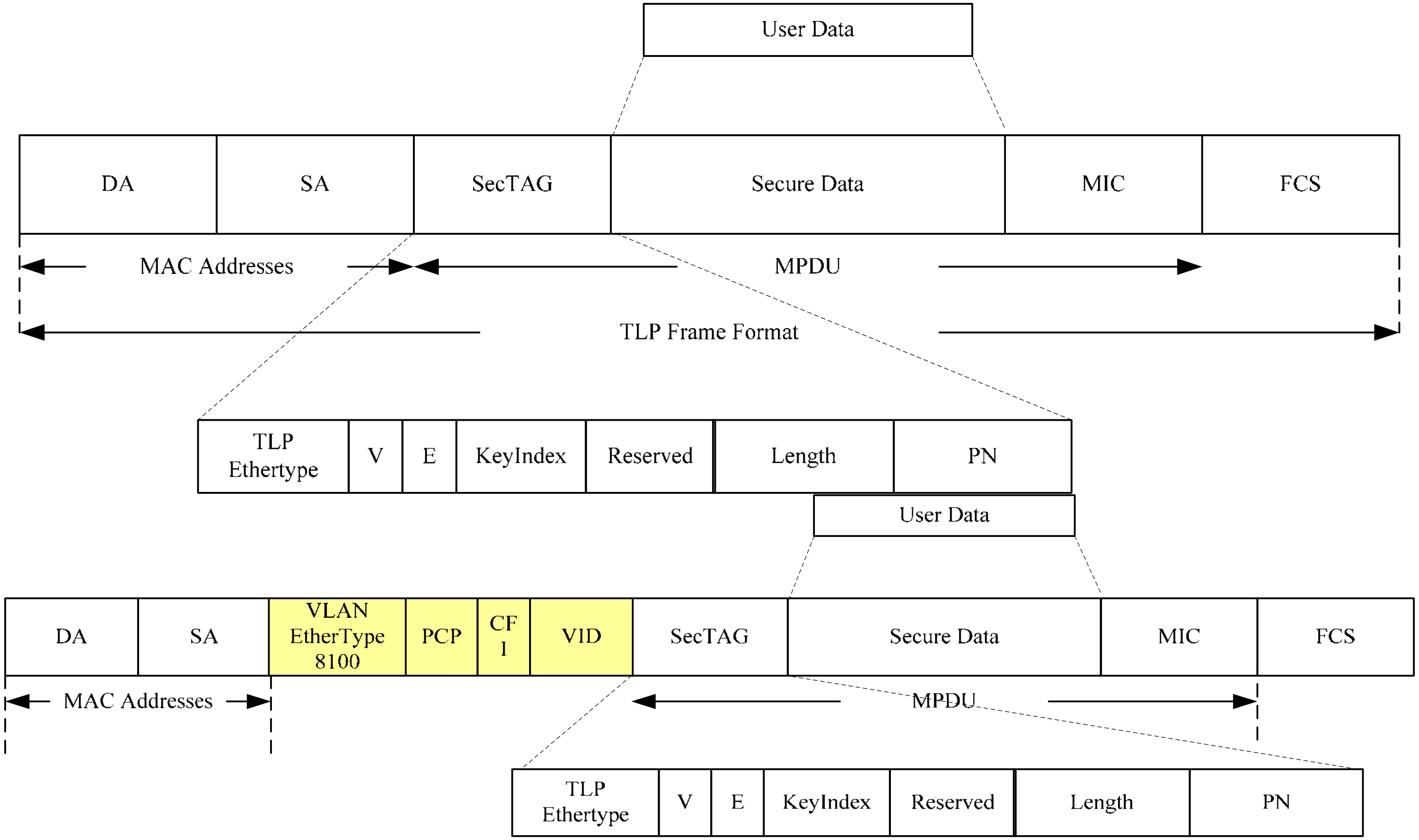
Encryption with station key

Data Transport Protection （3）


ES TA$_3$
CSW
EST A$_4$
ESW$_2$
Station key request message
Station key Notification message
Station key Notification response message
Station key response message
Encryption by KEY$_{ESTA1-ESTA2}$
ESTA$_1$→ESTA$_2$
Decryption by KEY$_{ESTA1-ESTA2}$

Encryption with station key

Secure Frame Format



TLSec Protocol

➢TLSec Protocol

- ✓ Two alternative authentication mechanisms: Certificate Based Authentication and pre-Shared key Based Authentication. Authentication mechanisms in TLSec are expanded easily.
- ✓ Three-stop encryption and encryption with station key provide flexible encryption between clients.
- ✓ Current common switches with no encryption capability can co-exist in Secure LAN with TLSec switches.
- ✓ No need to decrypt all the received packets, part of the data frame can be directly transmitted, reducing the computational burden and the transmission delay;
- ✓ Lower latency, Lower cost, Lower Network upgrade cost.

Summary and Next Step

➢Need

- ✓ ISO/IEC8802-3:2000
  - No secure access control. No confidentiality
- ✓ 802.1AE-2006：
  - High latency, High cost, High Network upgrade cost；
  - Flood is terrible for switch.
- ✓ It is necessary to do more research on LAN security
  - Secure access control.
  - Confidentiality.
  - Lower latency. Lower cost.
  - Lower Network upgrade cost.

Summary and Next Step

➢TLSec status

- ✓ One of the basis mechanism of TLSec which named TePA is approved on June 1th, 2010 in ISO/IEC JTC 1/SC 27；
  - ISO/IEC 9798-3:1998/FDAM 1 -- Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques – Amendment 1
- ✓ TLSec is under development as a national standards.
- ✓ TLSec chip and system product are under development by cooperating with several prominent firm. The product will be released in the end of this year.

Summary and Next Step

- ➢**Next Step：**
  - ✓We propose to establish a study period for the enhancement on LAN Security in ISO/IEC JTC1/SC6.

Thanks!