Detailed Comments on IEEE 802.11i (1N7537)

Chinese National Body

Date: 2005.08.29

Notice: This document is prepared for presentation at the ISO/IEC JTC1/SC6 plenary meeting August 28-September 2, 2005. 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.

Foreword

This document contains detailed technical comments as a follow up to comments from Chinese NB on October 15, 2004 during one-month fast-track review, which was 6N12732, regarding 1N7537, which is U.K. NB contribution to JTC1 SC6 based on IEEE 802.11i.

Overview Statement

- IEEE 802.11i contains useful technology.
- There are many issues to be resolved for successful integration of IEEE 802.11i into ISO/IEC 8802-11.

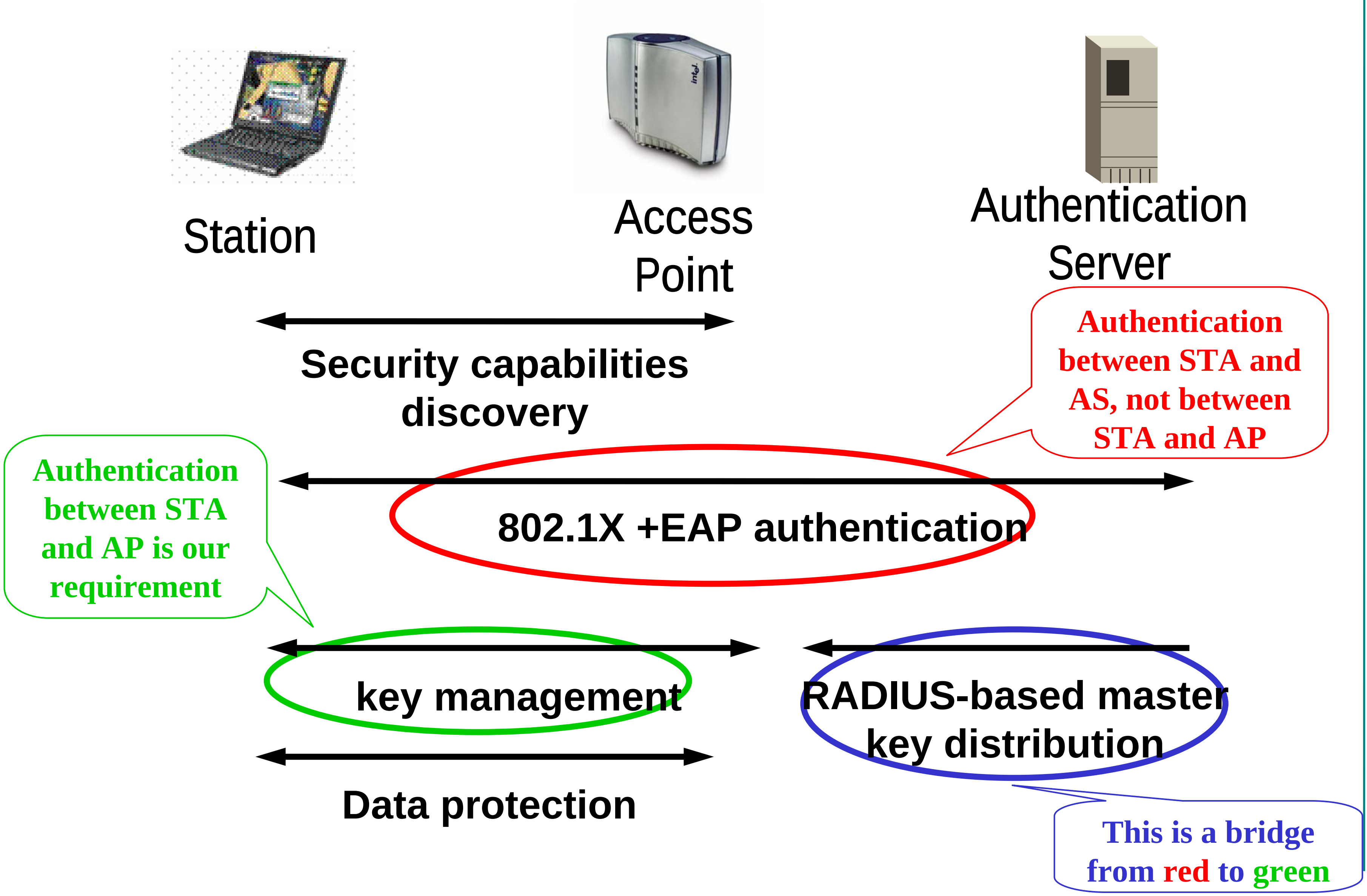
Comments on 1N7537
on 2004-10-15

- No Mutual Authentication Specified
- Difficult to Expand Networks
- Complex Authentication Protocol
- Security of Master Key

Part 1

No Mutual Authentication Specified

In IEEE 802.11i, the mutual authentication between AP and STA is implemented based on authentication process between STA and the authentication server (AS), but it is not the true mutual authentication we need.



Station

Access Point

Authentication Server

Authentication between STA and AS, not between STA and AP

Security capabilities discovery

Authentication between STA and AP is our requirement

802.1X +EAP authentication

key management

RADIUS-based master key distribution

Data protection

This is a bridge from red to green

Description (1)

- AP has no independent identity. Radius only send a master key (PMK) known by STA to AP.
- The master key (PMK) is the only trusted relation.
- STA never knows the identity of its associated AP.
  - ✓ AP never notifies its authenticated identity to STA
  - ✓ BSSID is the only identifier the AP exposes to the STA
- AP never knows the identity of its associated STA.
  - ✓ STA never notifies its authenticated identity to AP
  - ✓ STA MAC address is the only identifier the STA exposes to the AP
- The STA and AP do not know the peer’s authenticated identity. It is dangerous for the authenticated key agreement protocol.

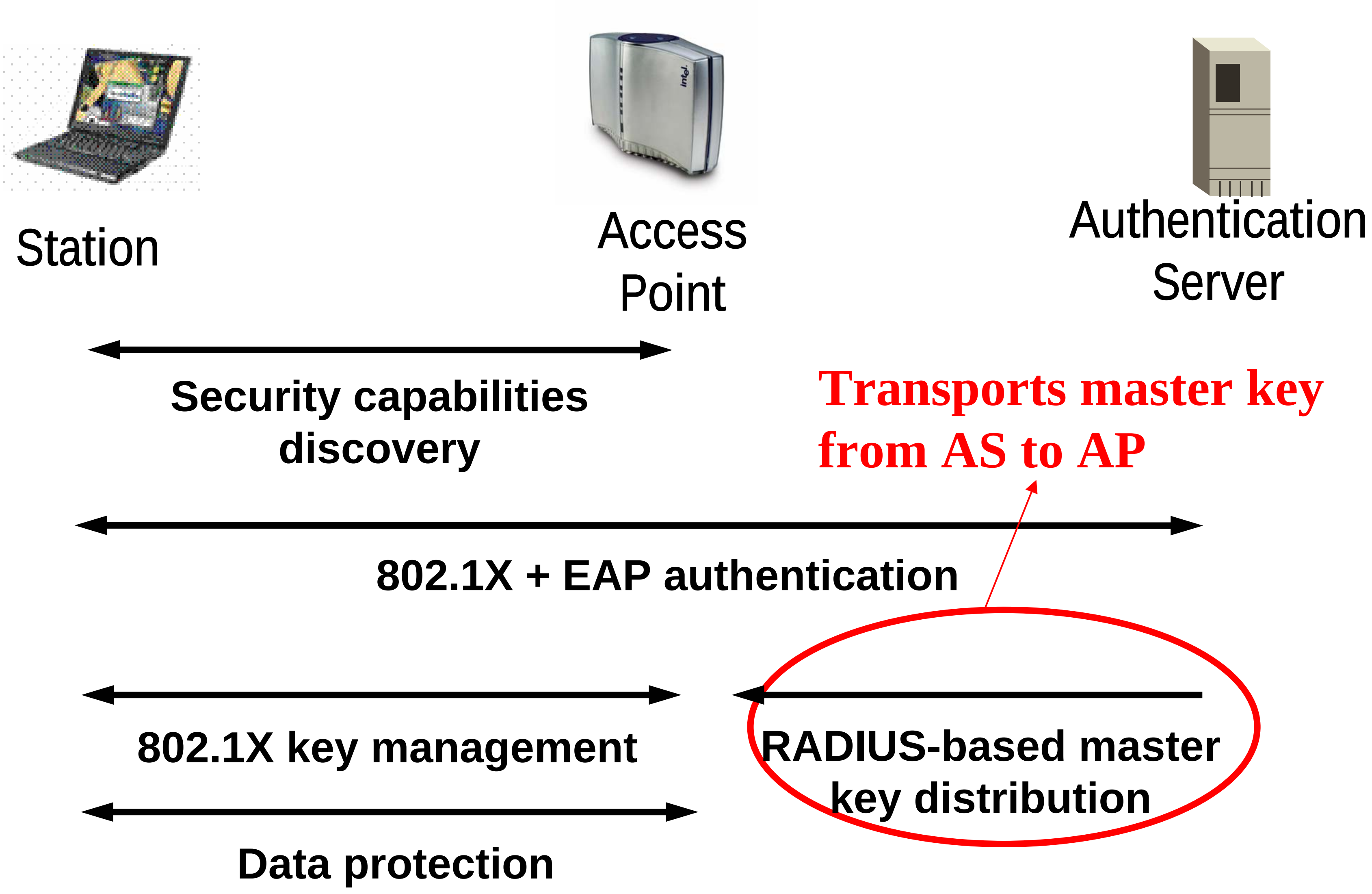
Description (2)

- At present, Radius can not provide a secure channel for key delivery.
  - ✓ Who can ensure the security of the delivery of PMK?
  - ✓ If the PMK is attacked successfully, the security will lost.
- Then the bridge from red part to green part is in risk.
- So, the mutual authentication between AP and STA is not true.

Part 2

Difficult to Expand Networks

In IEEE802.11i, a shared channel must be set up for each AP and the authentication server (AS) manually, which leads to the bad expansibility. In a large-scale network, it is very difficult to manage the network.



Station

Access Point

Authentication Server

Security capabilities discovery

Transports master key from AS to AP

802.1X + EAP authentication

802.1X key management

RADIUS-based master key distribution

Data protection

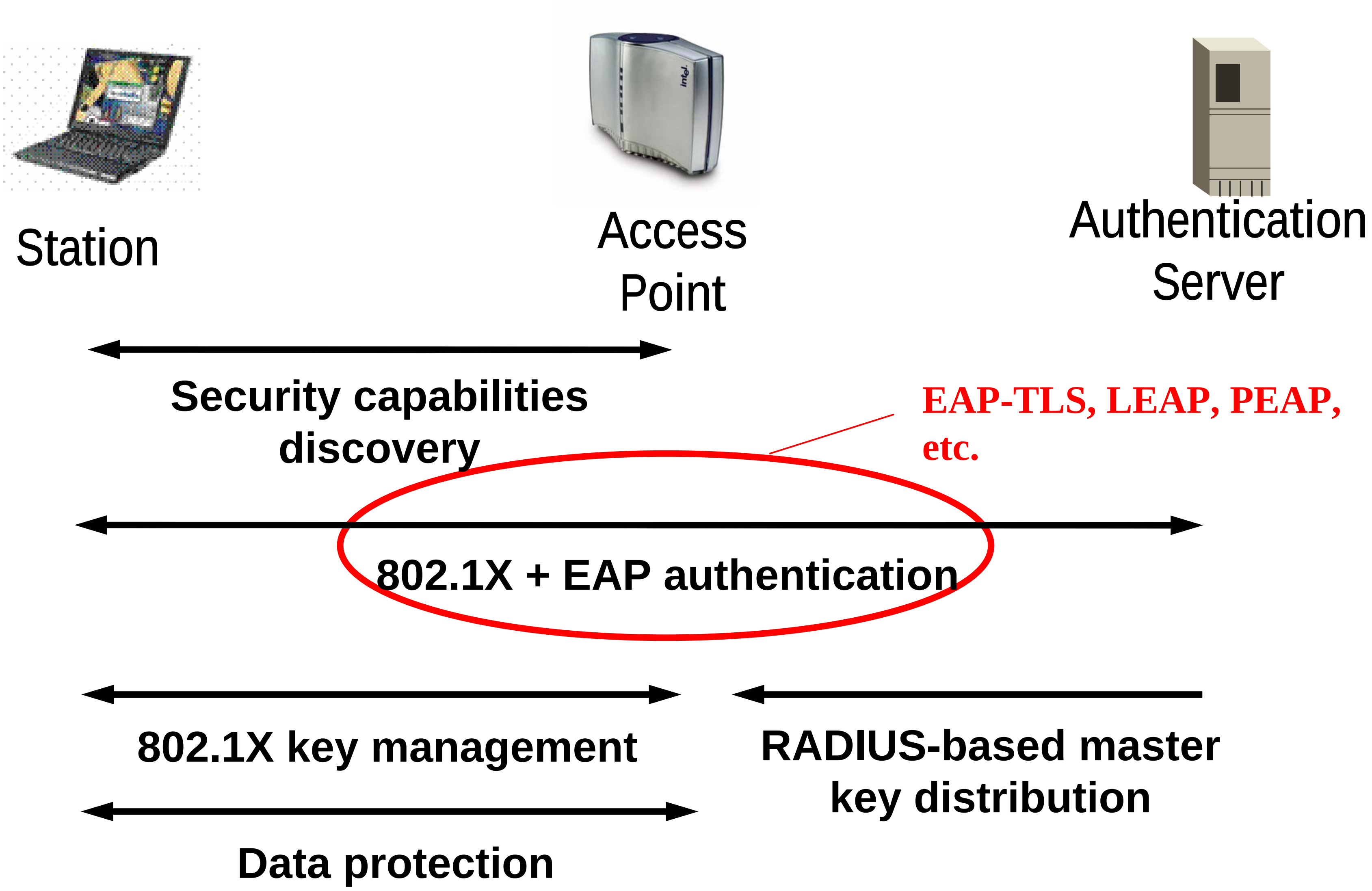
Description

- When IEEE802.11i network is deployed, AS and AP may pre-configure a secure channel (IPsec or TLS or others).
  - ✓ In a large-scale network, maintaining the secure channel is costly.
- In practice, AS and all APs may be set up a shared key.
  - ✓ When a new AP is added in existing network, it must be manually configured.
  - ✓ When the shared key requires to be changed, all APs must be manually reconfigured.
  - ✓ In a large-scale network, changing the shared key is very troublesome.

Part 3

Complex Authentication Protocol

In IEEE 802.11i, the authentication protocol is complex.



Station

Access Point

Authentication Server

Security capabilities discovery

EAP-TLS, LEAP, PEAP, etc.

802.1X + EAP authentication

802.1X key management

RADIUS-based master key distribution

Data protection

Description (1)

- IEEE802.1x only provides an authentication framework.
- When IEEE802.11i network is practically deployed, EAP-TLS, LEAP, PEAP etc. should be implemented.
- Most of EAP-TLS, LEAP, PEAP etc. are just IETF draft documents, so interoperability and conformance between different products are difficult to assure.

Description (2)

- **The fact that many kinds of authentication protocols must be supported makes the implementation of the products complex.**
- **The fact that many kinds of authentication protocols must be supported makes the management and maintenance of the products complex.**

Part 4

Security of Master Key

In IEEE802.11i, the master key (PMK) is produced by the negotiation between the mobile endpoint (STA) and the authentication server (AS), and transmitted in the channel between the AP and AS. Therefore, it will introduce new attack points.

Description (1)

- PMK is negotiated between STA and AS.
- PMK is not directly negotiated between STA and AP.
- PMK must be transported by AS to AP.
- IEEE802.11i is agnostic to the key delivery mechanism, as the delivery mechanism is outside the scope of IEEE802.11i. The risk to disclose the PMK is not avoided.

Description (2)

- **IEEE802.1x don’t bind authenticated identities of STA and AP to the PMK. PMK is possible to be reused across different APs.**
  - ✓ **Compromise of one AP could compromise STA’s traffic at another AP.**
  - ✓ **Only mechanism STA has to detect conformance is the AP’s BSSID.**

Part 5

Other Issues

TKIP description

- WEP provides 0 bits of security.
- TKIP use Message Integrity Code (MIC) called Michael to detect forgery attempts.
- On average 2^{29} messages are required to succeed in an attack
- However, IEEE802.11i assumes only 2^{20} message are required to succeed in an attack.
- So IEEE802.11i adds the countermeasures which mean that if two invalid messages are detected within one minute (i.e. evidence of active attack) then the network is shut down for one minute.

- **Will it bring any new security risk?**

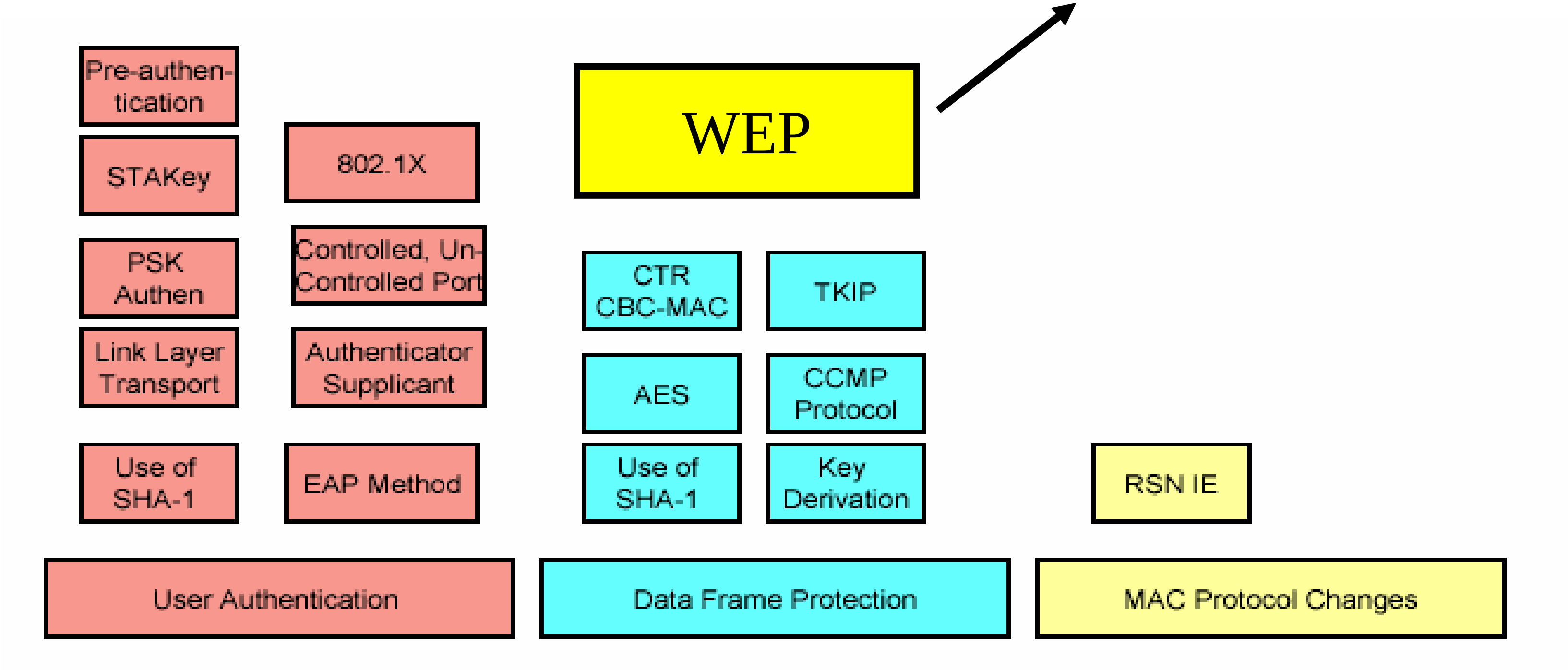
DoS attack

- TKIP convert active attacks into denial of service attacks.
- Is there any methods to lessen the threat?
  - ✓ It is better to shutdown the affected stations rather than the whole network.
  - ✓ It is better to rekey the session key than to shut down the network.

Security Risk (1)

IEEE802.11i Technical Components are illustrated as follows:

All Known WEP Disaster

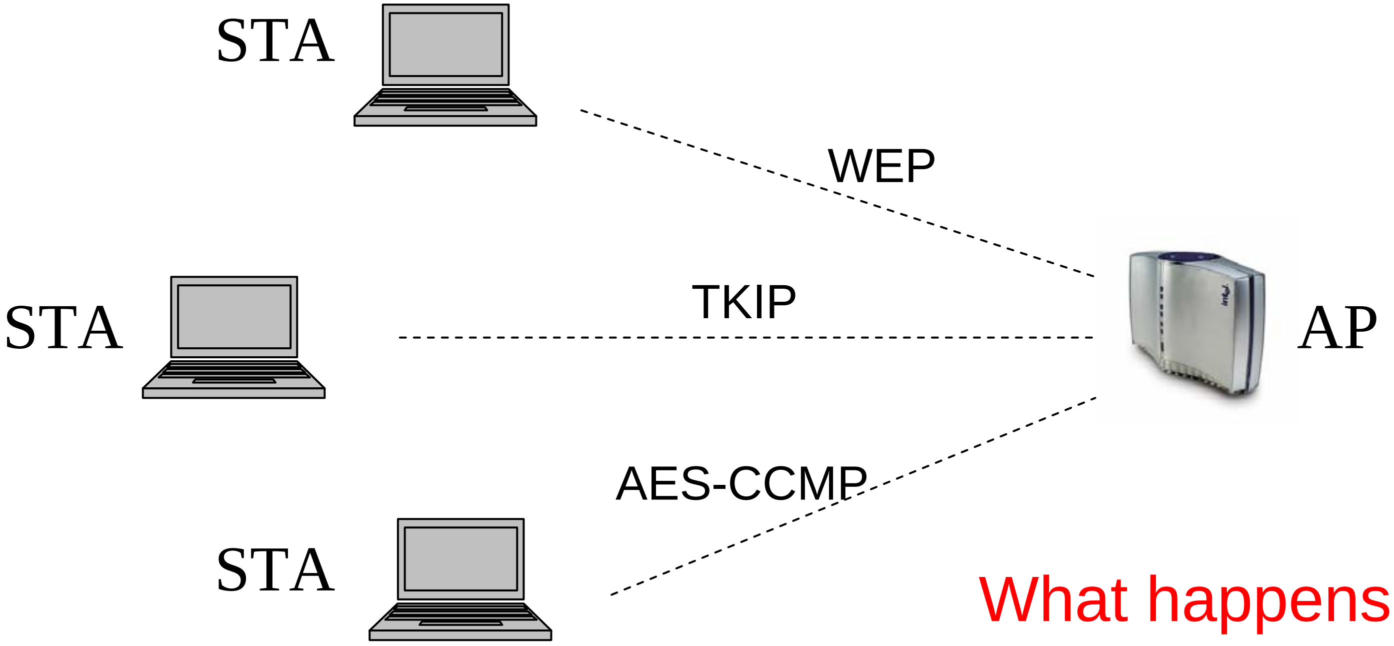


Security risk (2) --Compatibility

- ✓ Three security methods are defined in 802.11i
  - ◆ WEP: for compatibility
  - ◆ TKIP+802.1x/EAP: for compatibility with weak security
  - ◆ AES-CCMP+802.1x/EAP: for high security
- ✓ The mobile station usually implements the three security methods in order to use in all kinds of environment.
- ✓ The AP usually implements and runs the three security methods at the same time for serving all kinds of mobile station.

Security risk (2) --Deploy

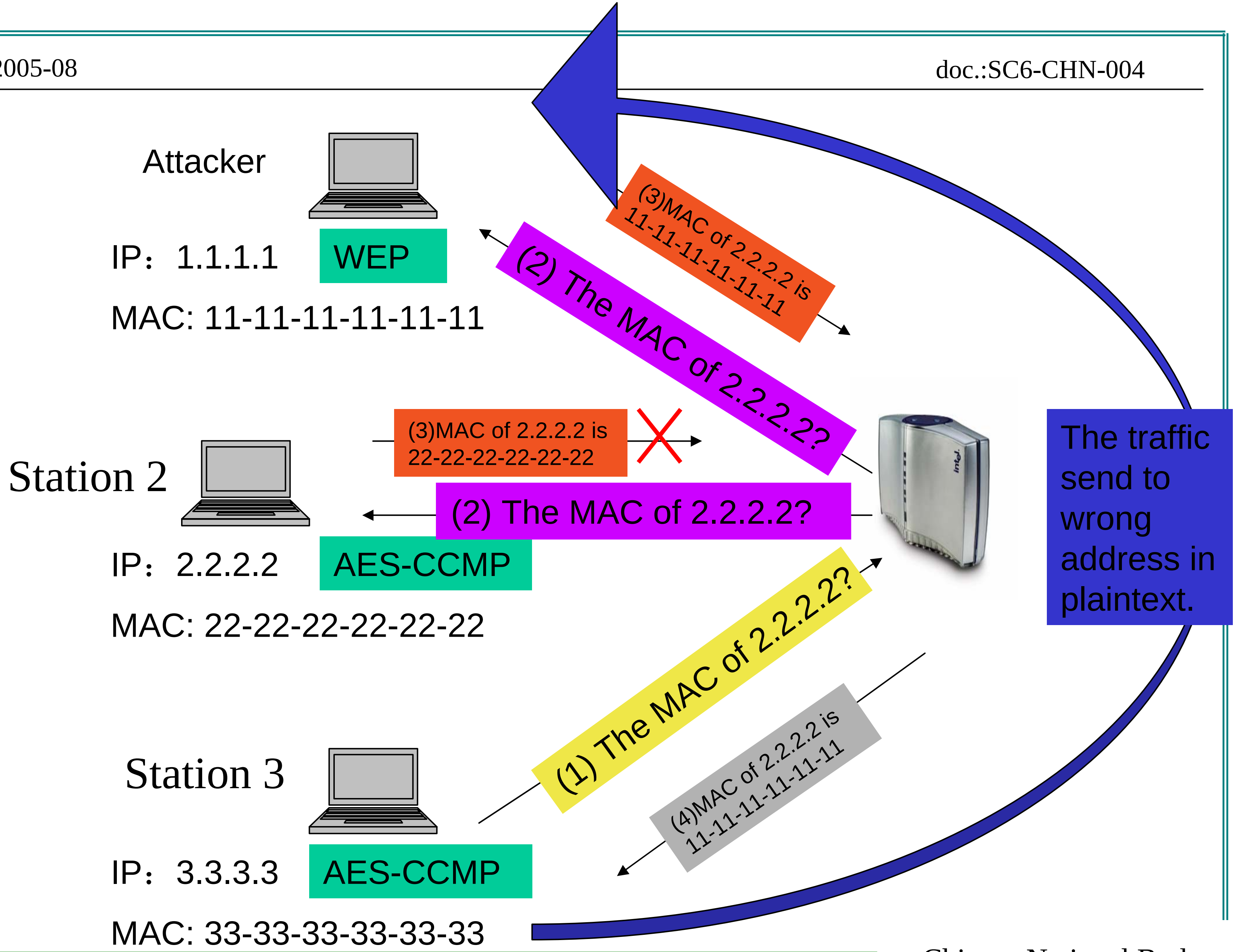
- ✓ It appears that each mobile station accesses the network in its mode.
- ✓ But one case is as follows:



What happens?

Security risk (2) -- Problems

- ✓ The multicast and broadcast traffic send from AP to station by WEP in pre-shared key.
    - ◆ For stations with AES-CCMP or TKIP, the traffic is not as secure as expected.
- ✓ The Unicast traffic is protected by separate security method. It seems that the traffic is as secure as expected.
- ✓ But the attacker can break the unicast traffic by simple manner.



Attacker

IP：1.1.1.1 WEP

MAC: 11-11-11-11-11-11

(2) The MAC of 2.2.2.2?

(3)MAC of 2.2.2.2 is 11-11-11-11-11-11

Station 2

(3)MAC of 2.2.2.2 is 22-22-22-22-22-22

(2) The MAC of 2.2.2.2?

IP：2.2.2.2 AES-CCMP

MAC: 22-22-22-22-22-22

The traffic send to wrong address in plaintext.

(1) The MAC of 2.2.2.2?

(4)MAC of 2.2.2.2 is 11-11-11-11-11-11

Station 3

IP：3.3.3.3 AES-CCMP

MAC: 33-33-33-33-33-33

Security risk (2) -- Discuss

- ✓ In the mixed environment
  - ◆ The multicast and broadcast traffic is not secure.
  - ◆ The unicast traffic is not secure even for stations with AES-CCMP. The stations are cheated.
  - ◆ it downgrades the system security.
- ✓ For compatibility, the mixed environment is common.
- ✓ For some applications, the weak security is not acceptable.

Protocol Incomplete (1)

- ***4-way handshake protocol***

In 4-way handshake, after Supplicant receives Msg.3 and sends Msg.4, the controlled port of Supplicant is unblocked, but the controlled port of Authenticator is still blocked. If Msg. 4 is lost, the state machines of Authenticator and Supplicant are not synchronized. So key management procedure fails.

Note, in wireless network, the loss probability of data frame is larger than that in wired network.

Protocol Incomplete (2)

- ***STAKey protocol***

When STAKey is established between two STAs in BSS, if AP doesn’t successfully notify STAKey to the initiator STA, how to notify the peer STA to delete the STAKey newly installed is not defined.

Summary

- Can not provide true mutual authentication
- Is difficult to expand Networks
- Complex authentication protocol
- Risk of PMK
- Other security issues and incomplete protocol
  - ✓ **TKIP --- weak security introduces DoS attack.**
  - ✓ **Mixed environment – serious security downgrade.**
  - ✓ **4 way handshake – state not synchronized.**
  - ✓ **STAKey protocol – how to revoke a fail stakey.**