

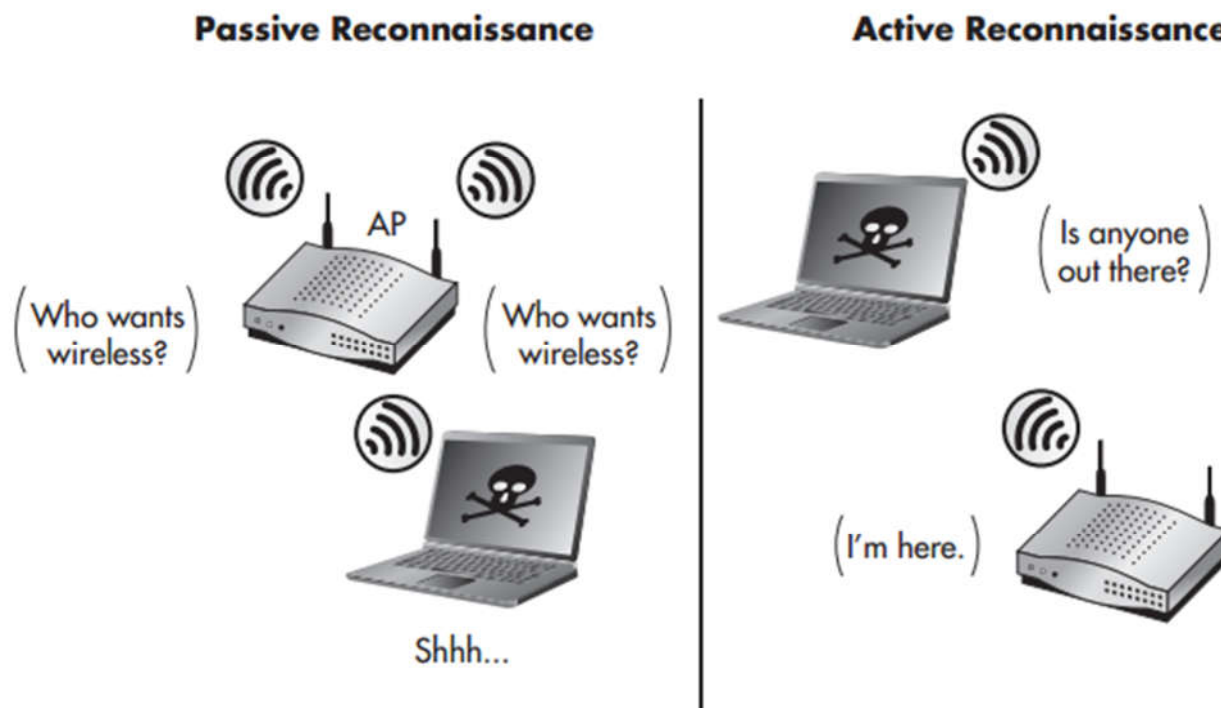
Wireless LAN Security

- Attacks on Wireless Network
 - Wireless reconnaissance
 - SSID Decloaking
 - Passive packet capturing
 - Man in the Middle attack

Wireless reconnaissance

- **Wireless reconnaissance** is the act of identifying available wireless networks, clients, communications, and so on.
- Generally, wireless enumeration can be performed either **passively** or **actively**.
- You can think of passively enumerating access points as just sitting quietly and listening for an access point to shout out “**Who wants wireless?**”

Wireless reconnaissance (Cont...)



- Whereas active enumeration would be you shouting
“I’d like wireless, who’s out there?”

SSID Decloaking

- Many network administrators feel it's enough to not broadcast the existence of their wireless network.
- For most access points, this is referred to as ***SSID cloaking***.
- This, technically, does not disable beacons being sent from your access point; instead, it configures the access point to send beacons with a ***blank SSID field***.

Passive Packet Captures

- In order to capture traffic, an attacker need to be within range of the target communicating station.
- As you're sitting in your favorite coffee shop, the websites you visit could be watched by someone sitting at the next table, a building across the street, or even a few blocks away.

-

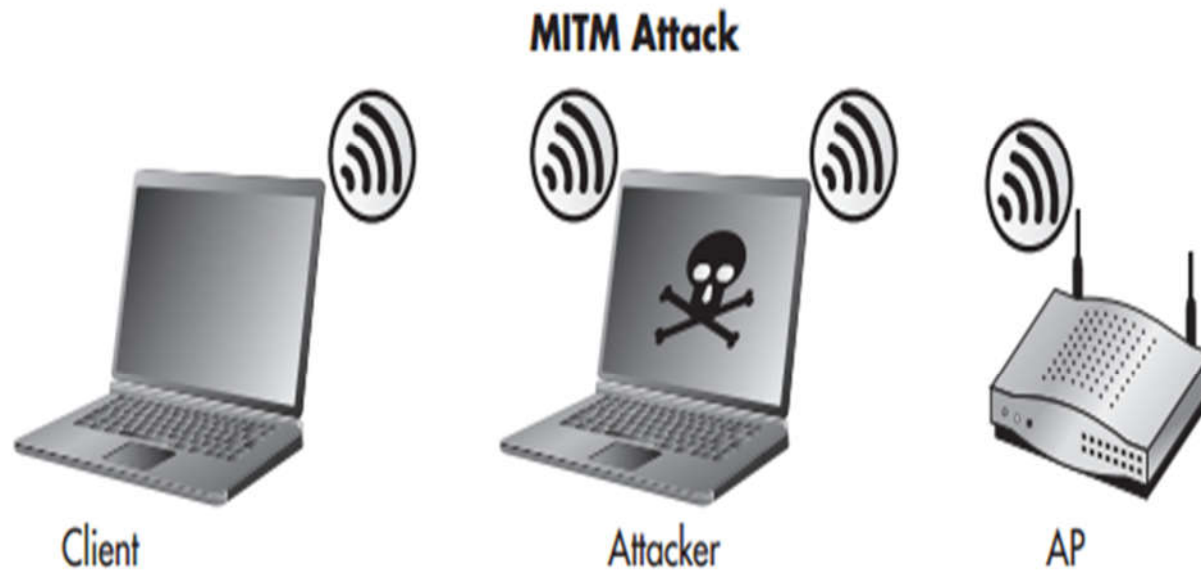
Passive Packet Captures (Cont...)

- Many of the most popular network protocols are still insecure by nature. Protocols that do not natively encrypt their data are known as clear text protocols.

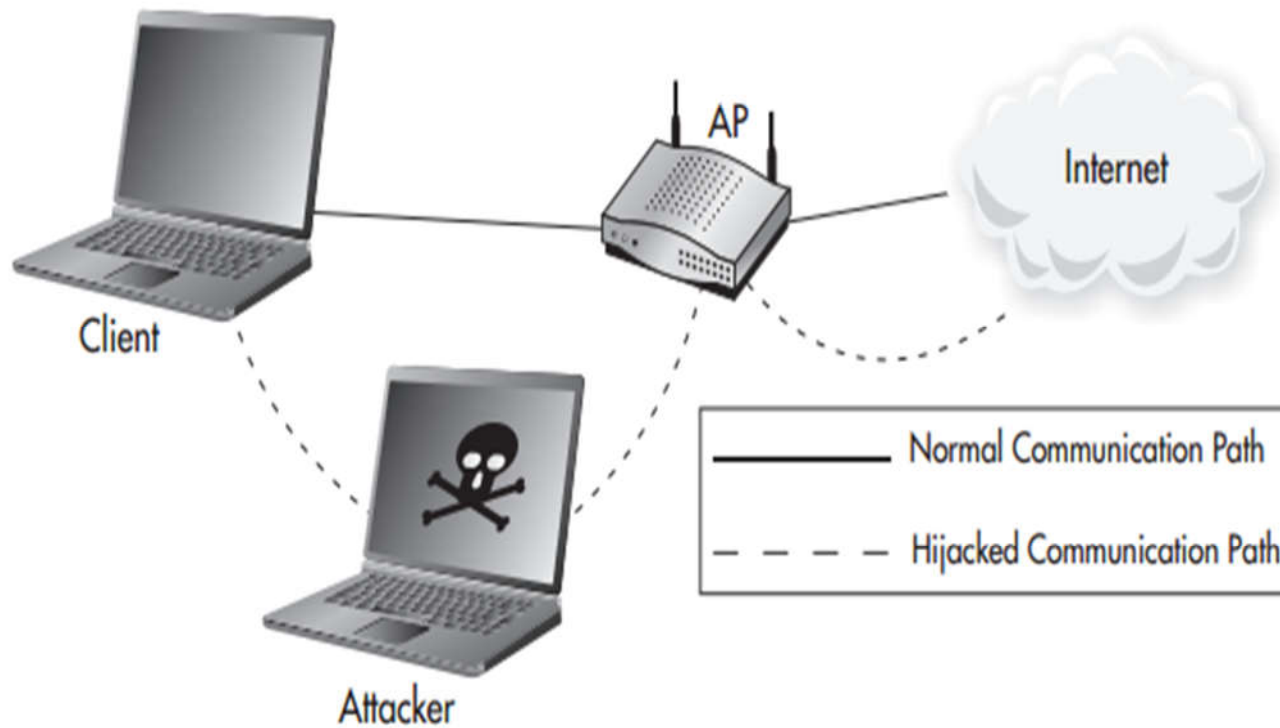
Some common clear text protocols include the following:

- ✓ HTTP (Hypertext Transfer Protocol; websites)
- ✓ SMTP (Simple Mail Transfer Protocol; sending e-mail)
- ✓ FTP (File Transfer Protocol; file transfers)
- ✓ POP3 (Post Office Protocol version 3; receiving e-mail)
- ✓ IMAP (Internet Mail Access Protocol; receiving e-mail)

Man in the Middle attack



Man in the Middle attack (Cont...)

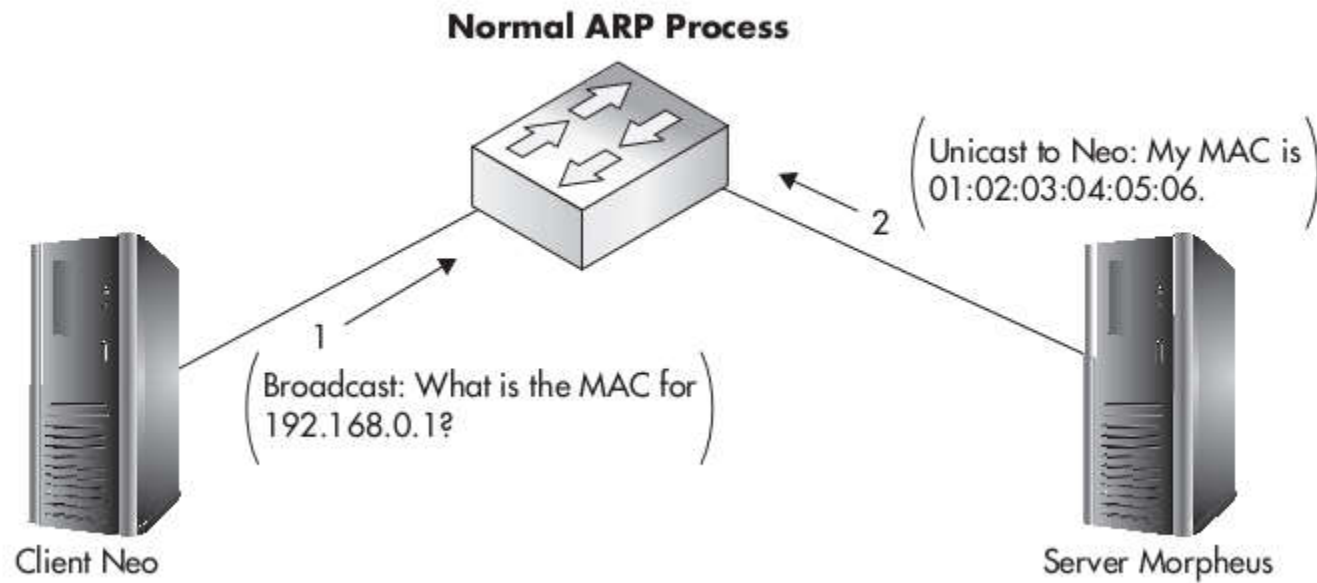


Man in the Middle attack (Cont...)

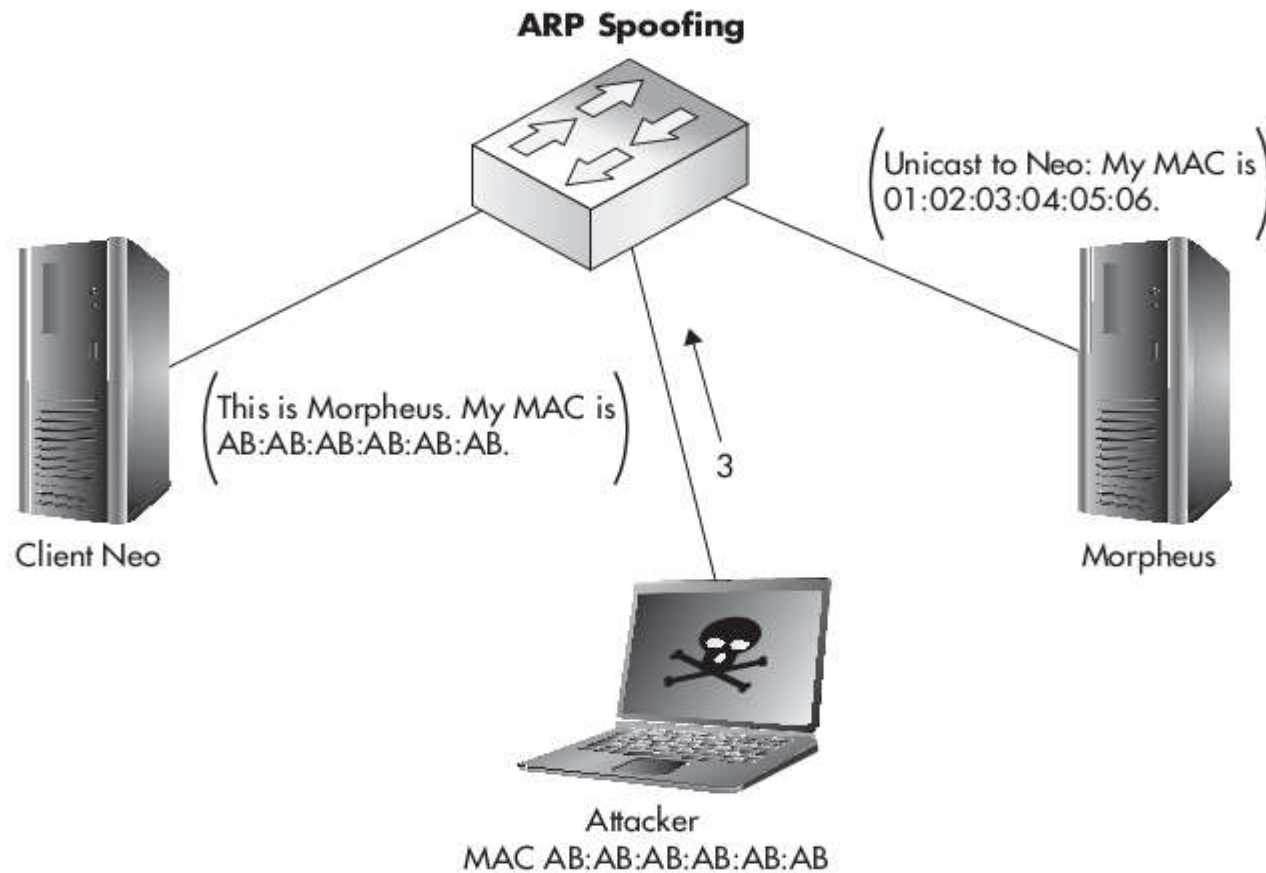
The following are some of the more common techniques for establishing a man-in-the-middle attack:

- ✓ **ARP spoofing or ARP poisoning**
- ✓ **Rogue DHCP server**
- ✓ **ICMP redirects**

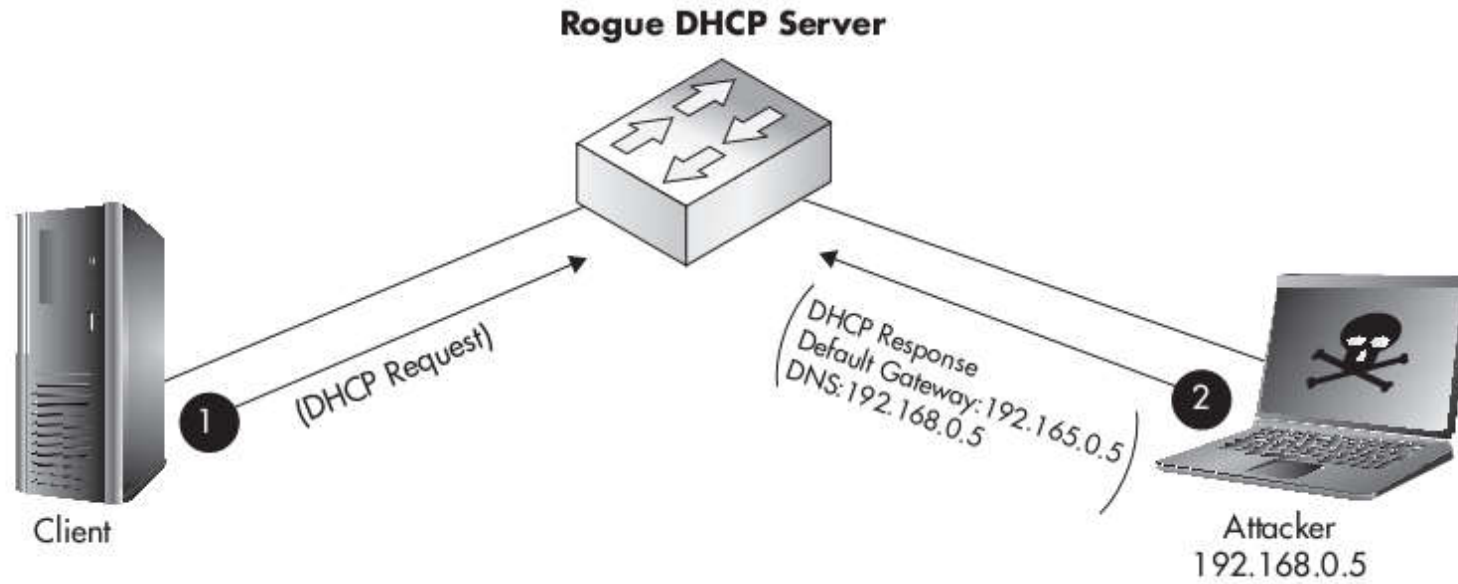
ARP spoofing or ARP poisoning



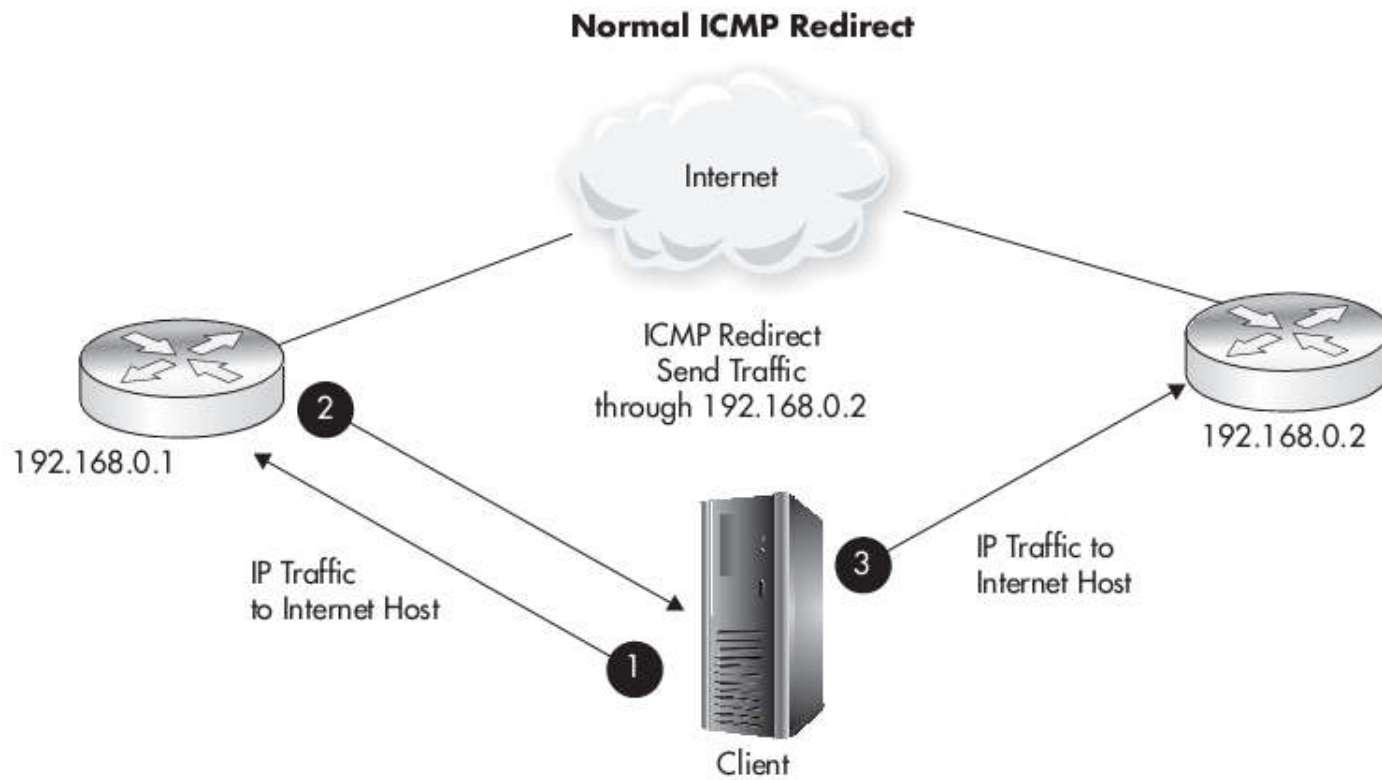
ARP spoofing or ARP poisoning (Cont...)



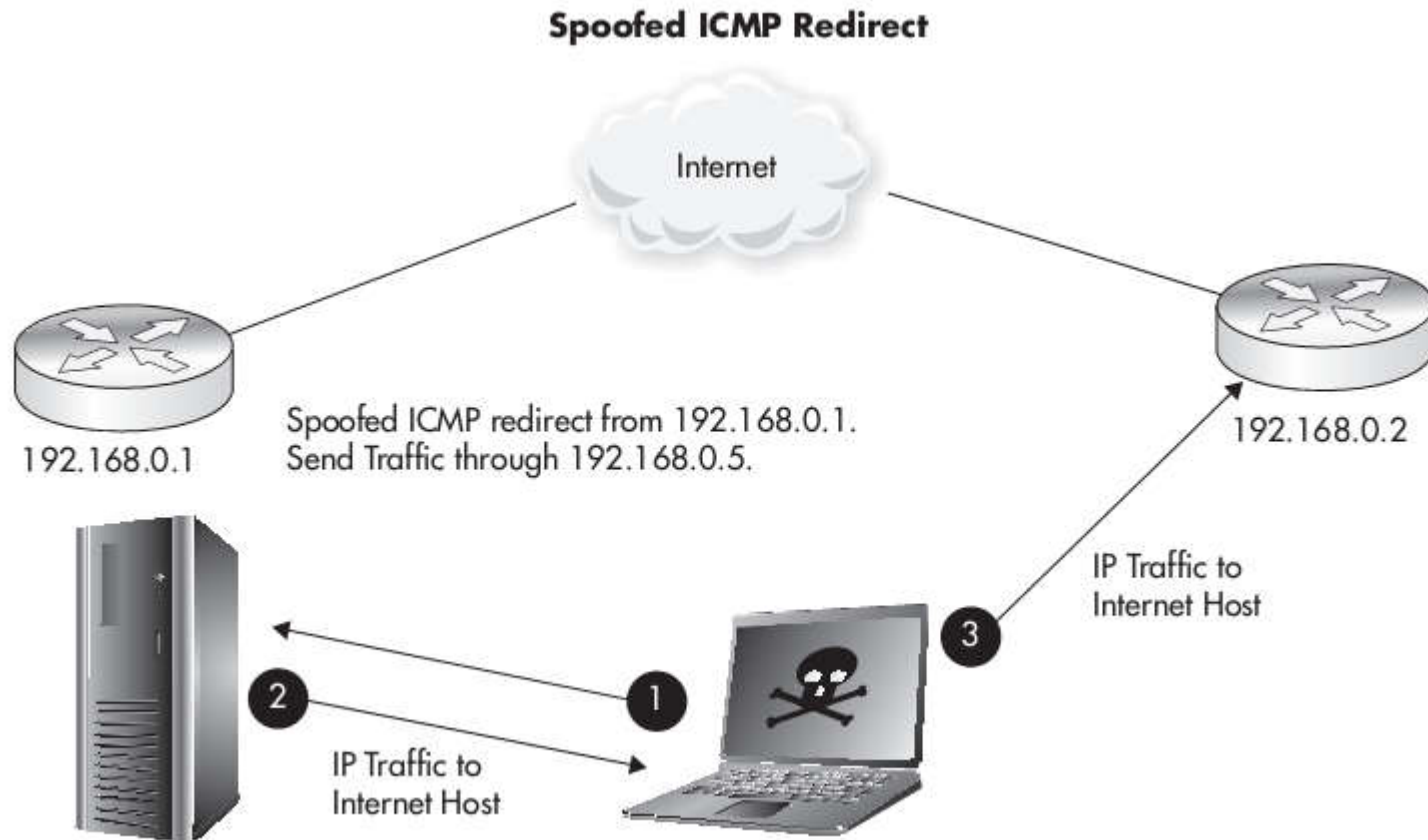
Rogue DHCP



ICMP Redirects



ICMP Redirects (Cont...)



IEEE 802.11 security mechanisms

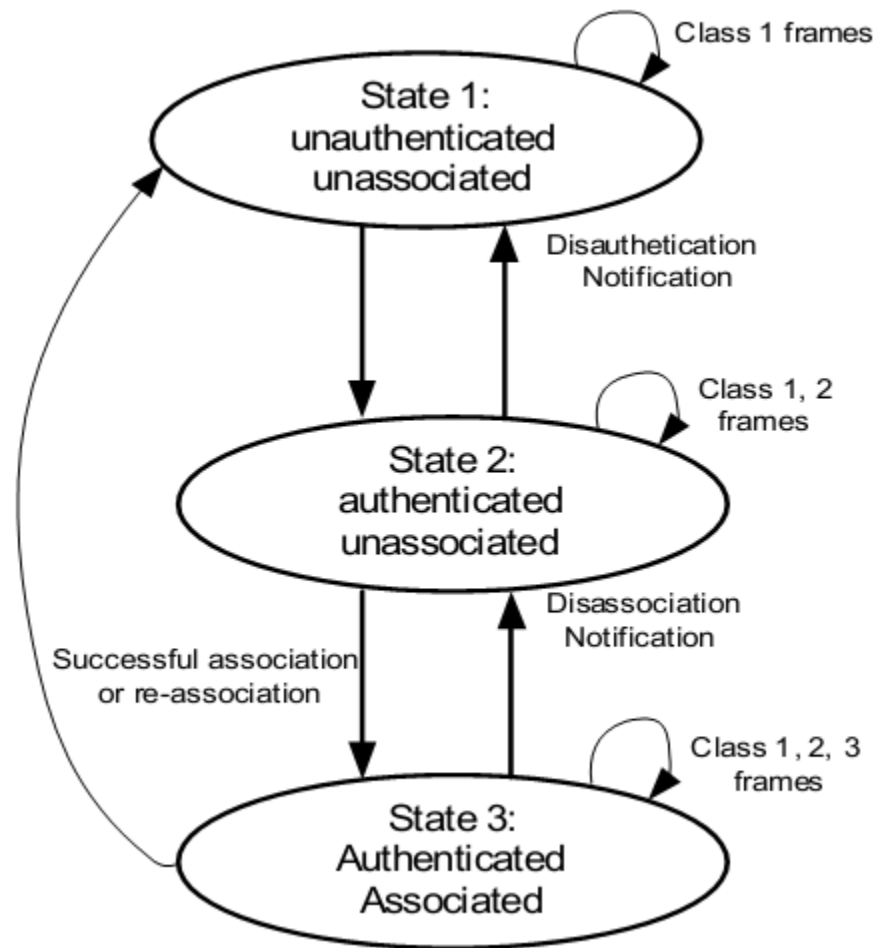
- The access points used in wireless networks broadcast data to all stations in their emission range.
- As a result, a malicious user can enter the area of a network and retrieve information in order to obtain access to the network.
- To overcome this problem, a client must establish a relationship, called an association with an access point.

IEEE 802.11 security mechanisms (Cont....)

A complete association with an access point requires the client to pass through three states:

- 1) Non-authenticated, non-associated;
- 2) Authenticated, non-associated;
- 3) Authenticated, associated.

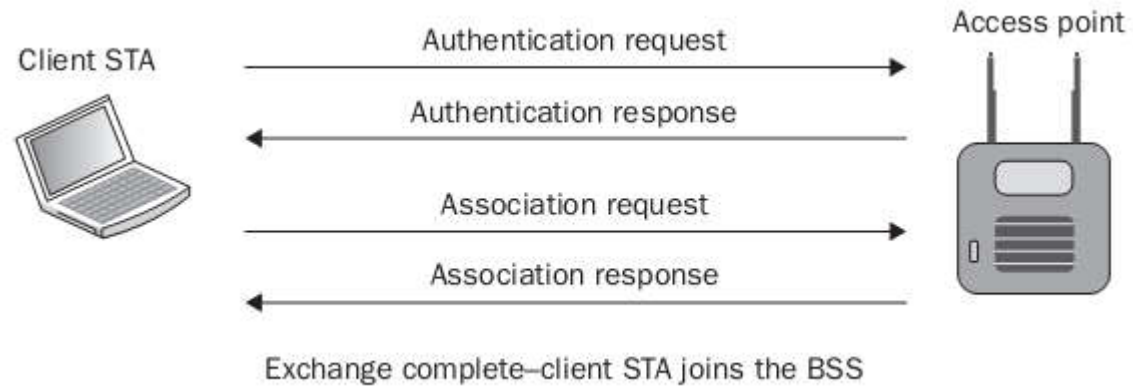
State machine for authentication in an 802.11 network



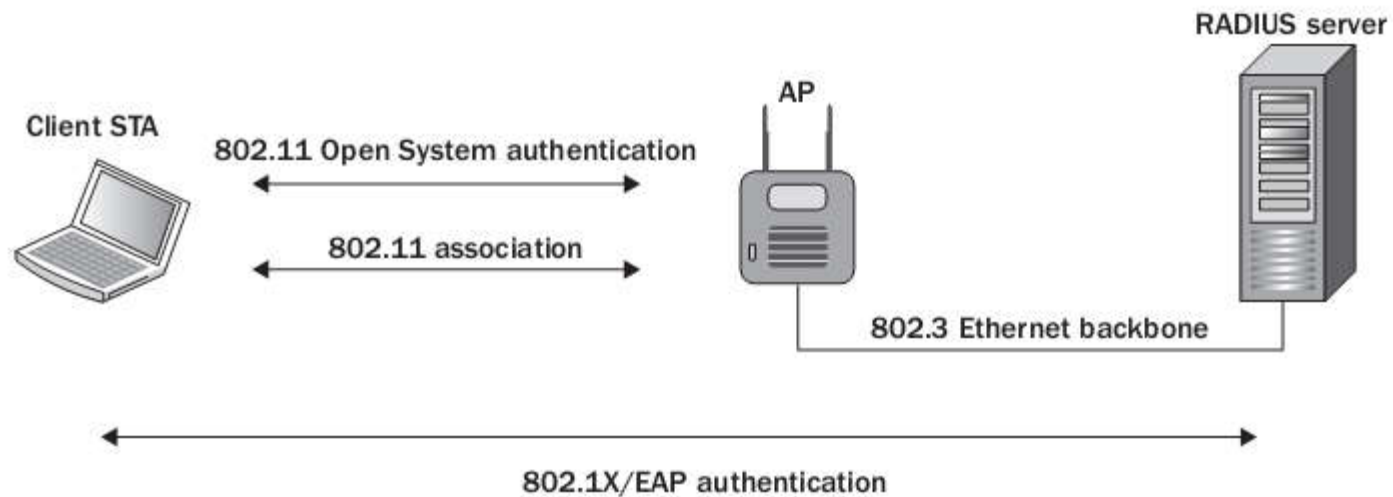
Authentication

- ✓ When an 802.11 device needs to communicate, it must first authenticate with the access point.
- ✓ The 802.11 - 2007 standard specifies two different methods of authentication:
 - Open System authentication
 - Shared Key authentication.

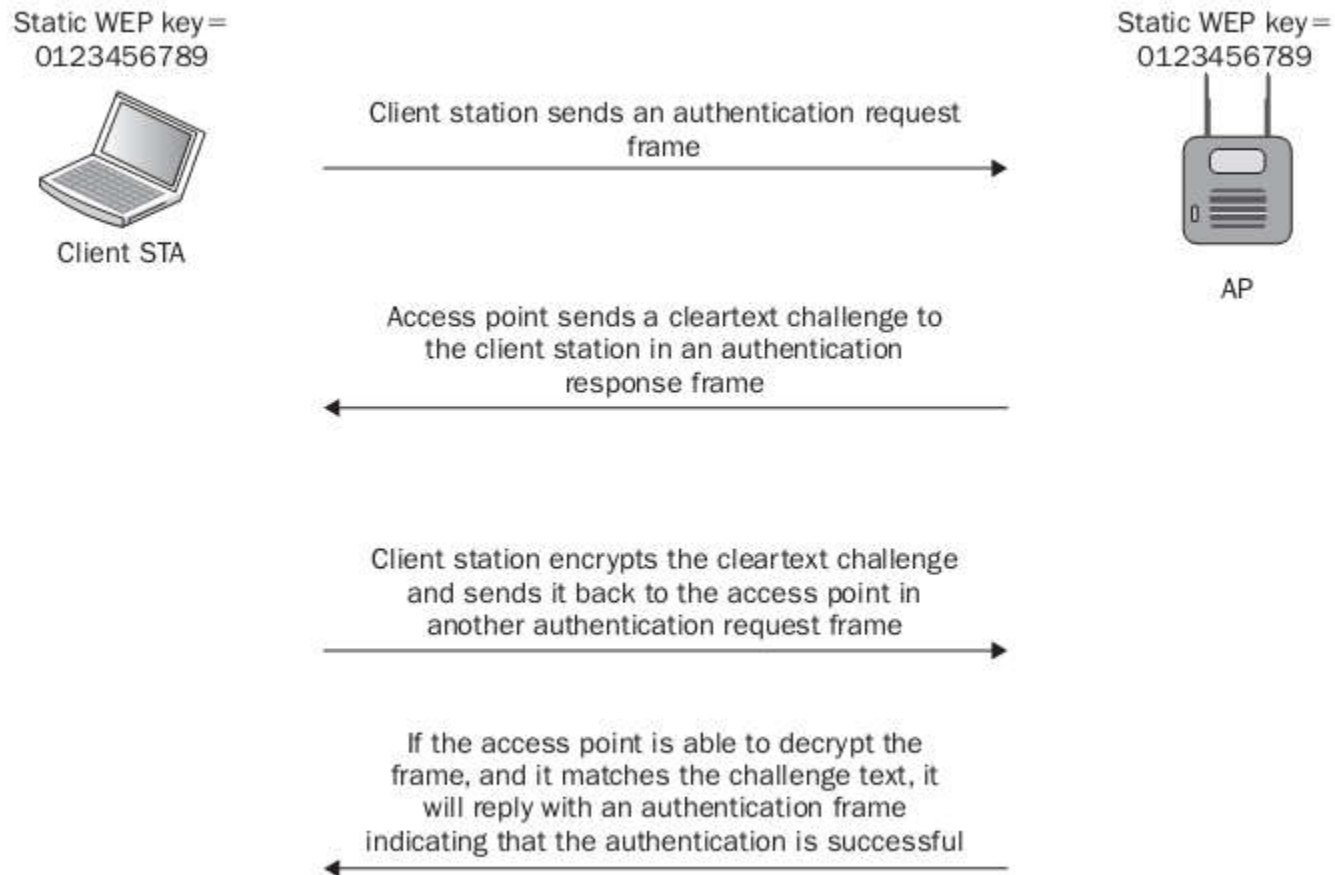
Open System Authentication



Open System and 802.1X/EAP authentication

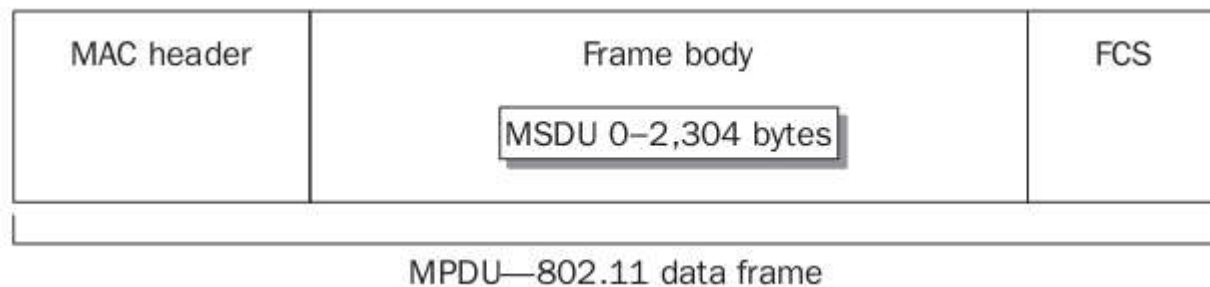


Shared Key Authentication



WLAN Encryption Methods

- ✓ The 802.11 - 2012 standard defines three encryption methods that operate at Layer 2 of the OSI model: **WEP, TKIP, and CCMP**.
- ✓ The upper layers of 3 – 7. Layer 2 encryption methods are used to provide data privacy for 802.11 **data frames**.
- ✓ The technical name for an 802.11 data frame is a **MAC Protocol Data Unit (MPDU)**.



WLAN Encryption Methods (Cont...)

- ✓ WEP, TKIP, and CCMP are encryption methods that all use symmetric algorithms.
- ✓ **WEP and TKIP** use the **RC4** cipher, while **CCMP** uses the **AES cipher**.
- ✓ The current 802.11 - 2012 standard defines WEP as a legacy encryption method for pre - RSNA security.
- ✓ TKIP and CCMP are considered to be compliant robust security network (RSN) encryption protocols.

WEP (Wired Equivalent Privacy)

Since transmissions are broadcast on a radio wave, it is necessary to introduce a mechanism to protect communications from malicious eavesdropping.

WEP is based on a symmetric cipher *RC4 stream* and was created to satisfy *access control*, *privacy*, *authentication* and *integrity*.

The SSID

- ✓ The network identifier or **SSID (Service Set ID)** is the first mechanism of security offered by WEP for network access control.
- ✓ All stations and all access points belonging to the same network must have the SSID

The ACL (Access Control List)

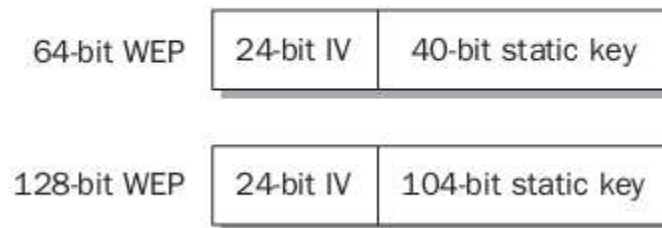
- Some Wi-Fi manufacturers implement the ACL on MAC addresses of the terminals.

Confidentiality

- ✓ Wired Equivalent Privacy (WEP) is a Layer 2 encryption method that uses the ARC4 streaming cipher.
- ✓ Because WEP encryption occurs at Layer 2, the information that is being protected is the upper layers of 3 – 7.
- ✓ The payload of an 802.11 data frame is called the MAC Service Data Unit (MSDU). The MSDU contains data from the LLC and **Layers 3 – 7**.
- ✓ WEP and other Layer 2 encryption methods encrypt the MSDU payload of an 802.11 data frame.

- ✓ The original 802.11 standard defined both 64 - bit WEP and 128 - bits WEP as supported encryption methods.

Static WEP encryption key and initialization vector

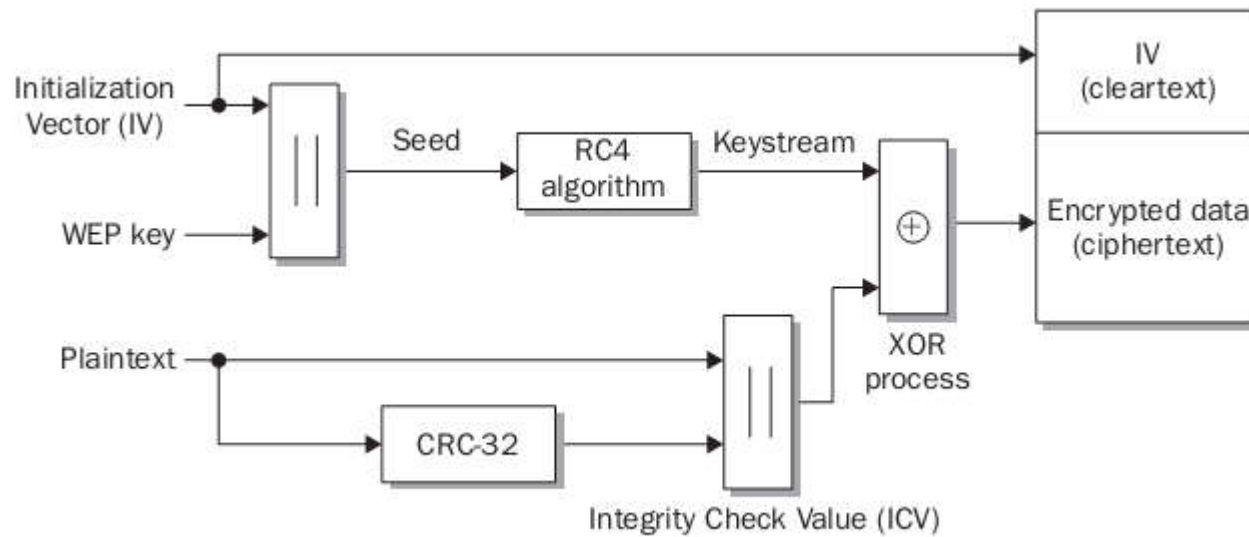


- ✓ Although both 64 - bit and 128 - bit WEP were defined in 1997 in the original IEEE 802.11 standard, the U.S. government initially allowed the export of only 64 - bit technology.

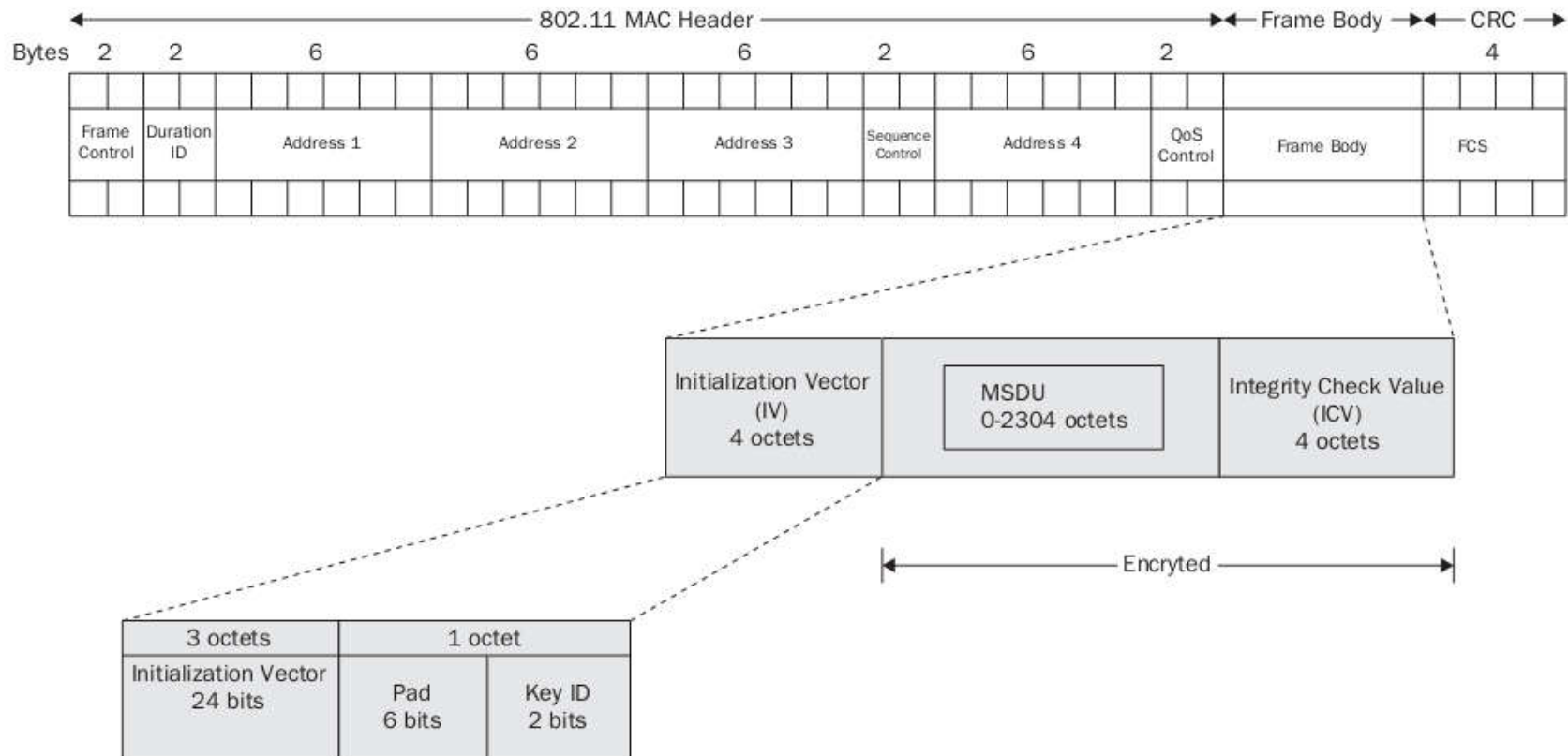
- ✓ The three main intended goals of WEP encryption include **confidentiality**, **access control**, and **data integrity**.
- ✓ The primary goal of confidentiality was to provide data privacy by encrypting the data before transmission.
- ✓ WEP also provides access control, which is basically a crude form of authorization.
- ✓ Client stations that do not have the same matching static WEP key as an access point are refused access to network resources.

- ✓ A data integrity checksum, known as the **Integrity Check Value (ICV)**, is computed on data **before encryption** and used to prevent data from being modified.

WEP encryption process



WEP MPDU Format



WEP encryption adds 8 bytes of overhead to an 802.11 MPDU.

WEP Vulnerability

A unique key

- ✓ The original standard defines a key size of **40 bits**, which is much too short to counter attacks by brute force.
- ✓ Since then, all manufacturers identified a key size of **104 bits**, for what is called **WEP 2**, which is much more resistant to brute force attacks.
- ✓ One secret key is shared by all stations in the network and the access point.

A unique key (Cont....)

- ✓ If all the stations use the same key, it is even easier for an attacker to retrieve the data, hence the role of the IV in the WEP.
- ✓ IV makes it possible to define different encryption flows for the same shared secret key.

IV collisions (From Hakima)

- ✓ The IV is concatenated with this key in order to create different flow encryption.
- ✓ The IV is 24-bit and there may be up to 2^{24} or 16 million different keys.

Weak Key Attack

- ✓ Because of the ARC4 key - scheduling algorithm, weak IV keys are generated. An attacker can recover the secret key much easier by recovering the known weak IV keys.

Reinjection Attack

- ✓ Hacker tools exist that implement a packet reinjection attack to accelerate the collection of weak IVs on a network with little traffic.

Attacking WEP Encrypted Networks (Tylor WRIGHTSON)

Basic attack flow would look like this:

- ✓ Identify target wireless network.
- ✓ Passively monitor encrypted packets sent between the client and the access point using a sniffer.
- ✓ Save around 50,000 encrypted packets to a file on the attacking laptop.
- ✓ Run the **aircrack-ng** program against the saved encrypted packets to determine WEP key.

Packet injection attack or an ARP replay attack

“What if the target wireless network isn’t heavily utilized? It might take us a surprising amount of time to get the necessary amount of packets to crack the WEP key”

“Well, there is a solution—we simply make the wireless network generate more traffic.”

So how does one incite the systems on the wireless network to generate more traffic?

BUT HOW????????????

Answer: ARP

The modified attack flow would look like this

- ✓ Identify the target wireless network
- ✓ Passively monitor encrypted packets sent between the client and the access point using a sniffer.
- ✓ Monitor for an ARP packet.
- ✓ Continuously resend the ARP packet.
- ✓ Every ARP response will have another unique IV.
- ✓ Save around 50,000 encrypted packets to a file on the attacking laptop.
- ✓ Run the **aircrack-ng** program against the saved encrypted packets to determine the WEP key.

Weaknesses of WEP

- ¹ The IV value is too short and not protected from reuse.
- ² The way keys are constructed from the IV makes it susceptible to weak key attacks.
- ³ There is no effective detection of message tampering (message integrity).
- ⁴ It directly uses the master key and has no built-in provision to update the keys.
- ⁵ There is no protection against message replay.

Changes from WEP to TKIP

Purpose	Change	Weakness Addressed
Message Integrity	Add a message integrity protocol to prevent tampering that can be implemented in software on a low-power microprocessor.	(3)
IV selection and use	Change the rules for how IV values are selected and reuse the IV as a replay counter.	(1) (3)
Per-Packet Key Mixing	Change the encryption key for every frame.	(1)(2)(4)
IV Size	Increase the size of the IV to avoid ever reusing the same IV.	(1)(4)
Key Management	Add a mechanism to distribute and change the broadcast keys (see Chapter 10).	(4)

TKIP (Temporal Key Integrity Protocol (TKIP))

- ✓ Temporal Key Integrity Protocol (**TKIP**) is a security protocol that was created to replace WEP.
- ✓ The IEEE **802.11i** security task group first defined TKIP to provide a stronger security solution without requiring users to replace their legacy equipment.
- ✓ Most legacy 802.11 radios could implement TKIP with a firmware upgrade, but not all legacy APs and STAs were upgradeable.

✓ TKIP (Temporal Key Integrity Protocol) (TKIP) (Cont...)

- ✓ The intent of **TKIP** was to provide a better temporary security solution until WLAN vendors could provide hardware that supported **CCMP/AES** encryption.
- ✓ The IEEE **802.11 - 2012** standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP, with TKIP support optional.
- ✓ In April 2003, the Wi - Fi Alliance introduced the Wi - Fi Protected Access (WPA) certification, which requires the use of TKIP encryption.

TKIP (Temporal Key Integrity Protocol (TKIP))

- ✓ Like WEP, TKIP uses the ARC4 algorithm for performing its encryption and decryption processes.

TKIP modifies WEP as follows:

✚Temporal Keys

- ✓ TKIP uses **dynamically created encryption keys** as opposed to the static keys.
- ✓ Static keys are susceptible to social engineering attacks. Dynamic encryption key generation is designed to defeat social engineering attacks.

✚ Sequencing

- ✓ TKIP uses a **per - MPDU TKIP sequence counter** (TSC) to sequence the MPDUs it sends.
 - ✓ An 802.11 station drops all MPDUs that are received out of order.
- Sequencing is designed to **defeat replay and reinjection attacks** that are used against WEP.

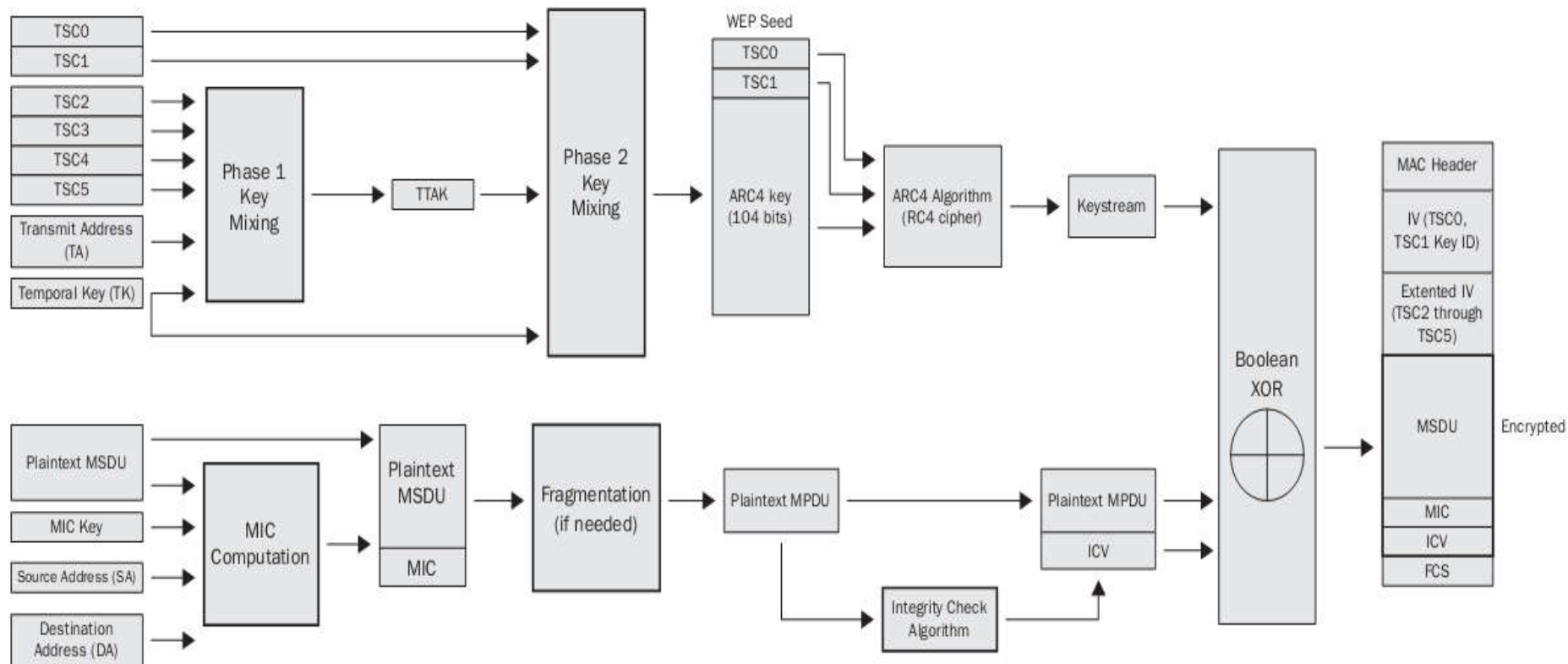
✚ Key Mixing

- ✓ TKIP uses a complex **two - phase cryptographic mixing process** to create stronger seeding material for the RC4 cipher.
- ✓ The key mixing process is designed to defeat the **known IV collisions** and **weak - key attacks** used against WEP.

Enhanced Data Integrity

- ✓ TKIP uses a stronger data integrity check known as the **Message Integrity Code (MIC)**.
- ✓ The MIC is designed to **defeat bit-flipping and forgery attacks** that are used against WEP.

TKIP Encryption and Data Integrity Process



TKIP Protocol steps

- ✓ TKIP starts with a 128 - bit temporal key.
- ✓ 128 - Bit temporal key is a dynamically generated key that comes from a 4 - Way Handshake creation process.
- ✓ 128 - Bit temporal key can either be a pairwise transient key (PTK) used to encrypt unicast traffic or a group temporal key (GTK) used to encrypt broadcast and multicast traffic.
- ✓ After the appropriate 128 - bit temporal key (pairwise or group) is created, the two - phase key - mixing process begins.

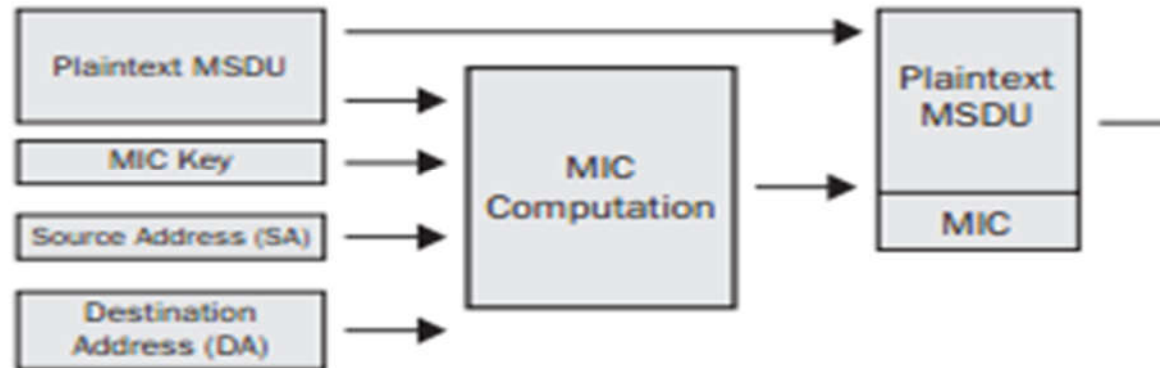
- ✓ A 48 - bit TKIP sequence counter (TSC) is generated and broken into 6 octets labeled TSC0 (least significant octet) through TSC5 (most significant octet).
- ✓ The two-phase key - mixing process can be summarized as follows:

TTAK = Phase 1 (TK, TA, TSC)

WEP seed = Phase 2 (TTAK, TK, TSC)

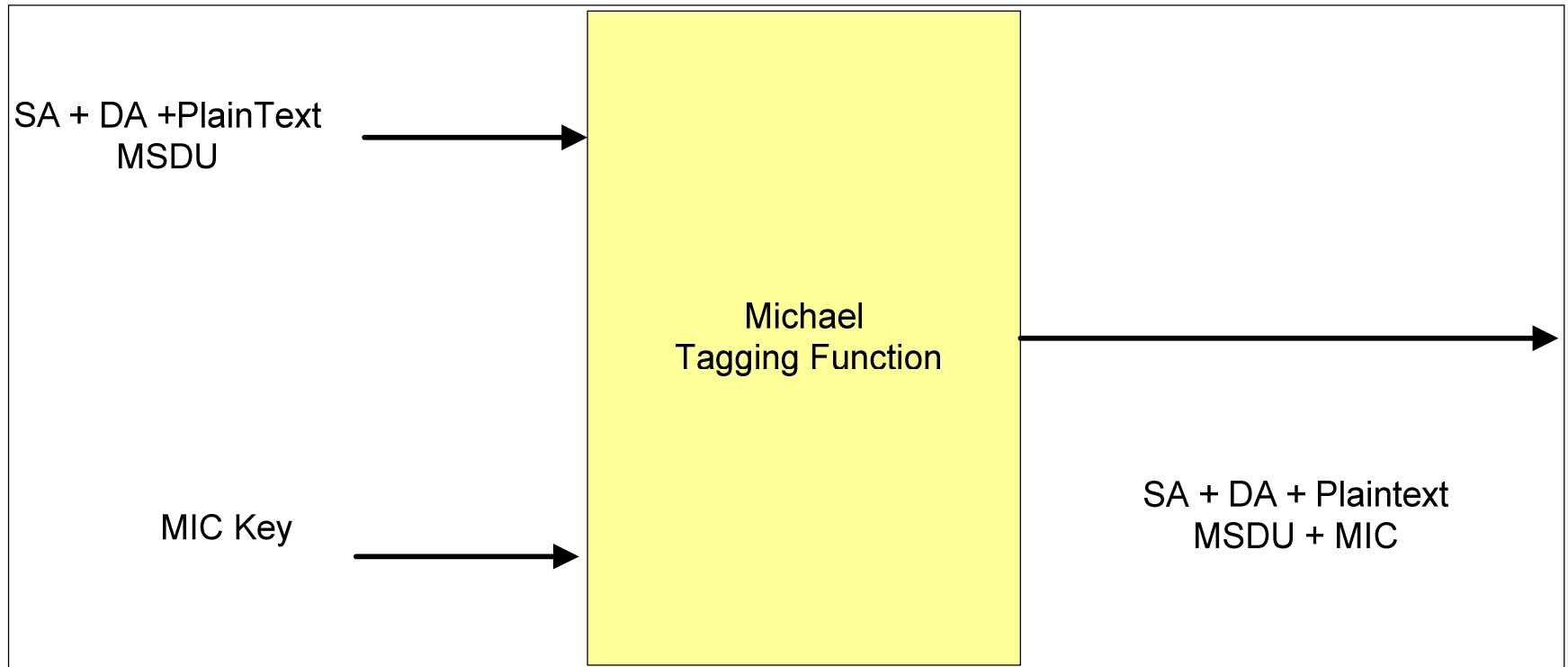
- ✓ TKIP uses a stronger data integrity check known as the Message Integrity Code (MIC) to mitigate known forgery attacks against WEP.

HOW MIC IS GENERATED?

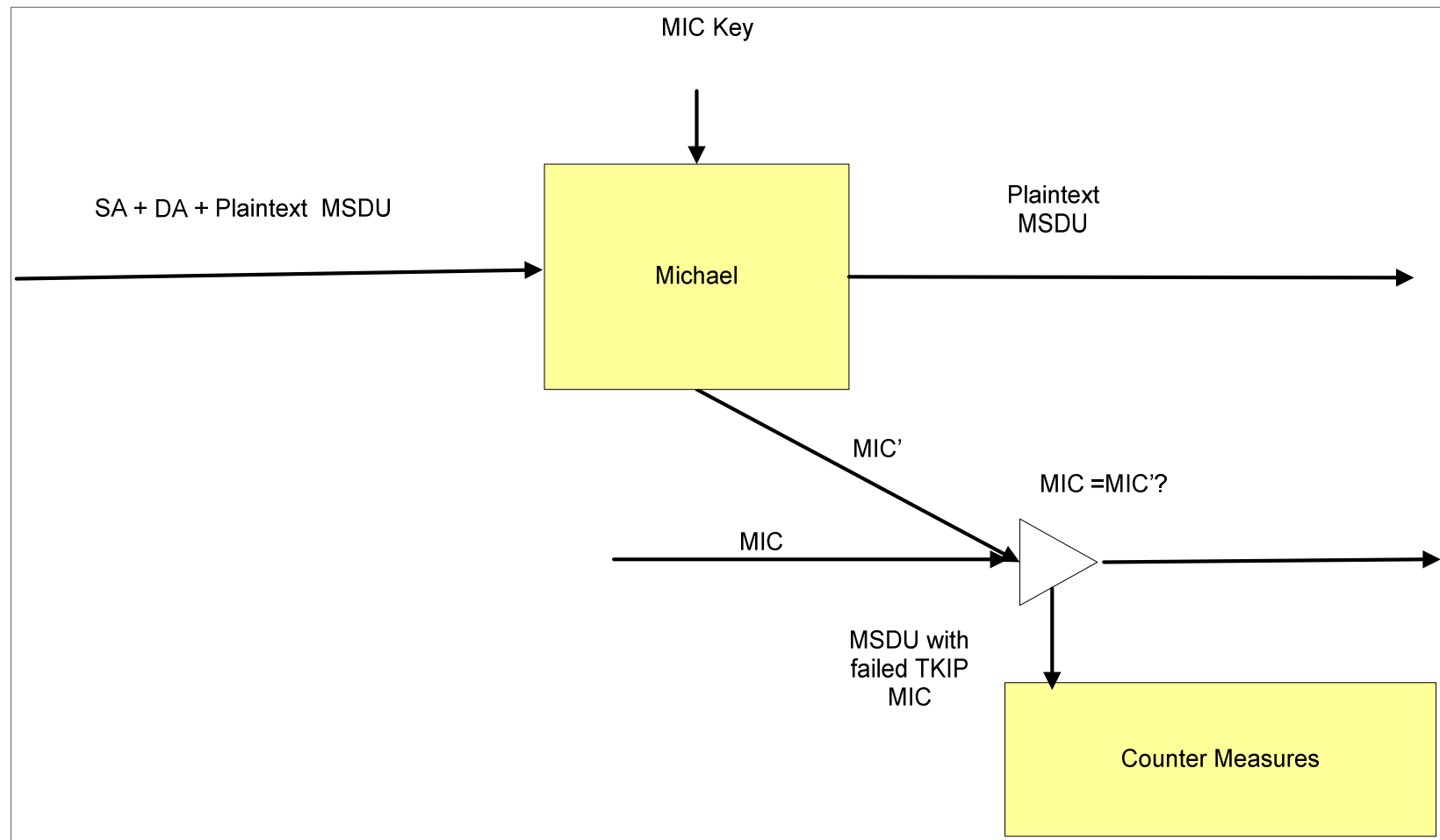


- ✓ The MIC is computed using the **destination address (DA)**, **source address (SA)**, **MIC Key**, and the entire unencrypted **MSDU** plaintext data.
- ✓ The MIC is **8 octets** in size and is labeled individually as M0 through M7.
- ✓ MIC contains only **20 bits** of effective security strength, making it somewhat vulnerable to brute - force attacks.

Michael: Tagging Function



Michael: Verification Predicate



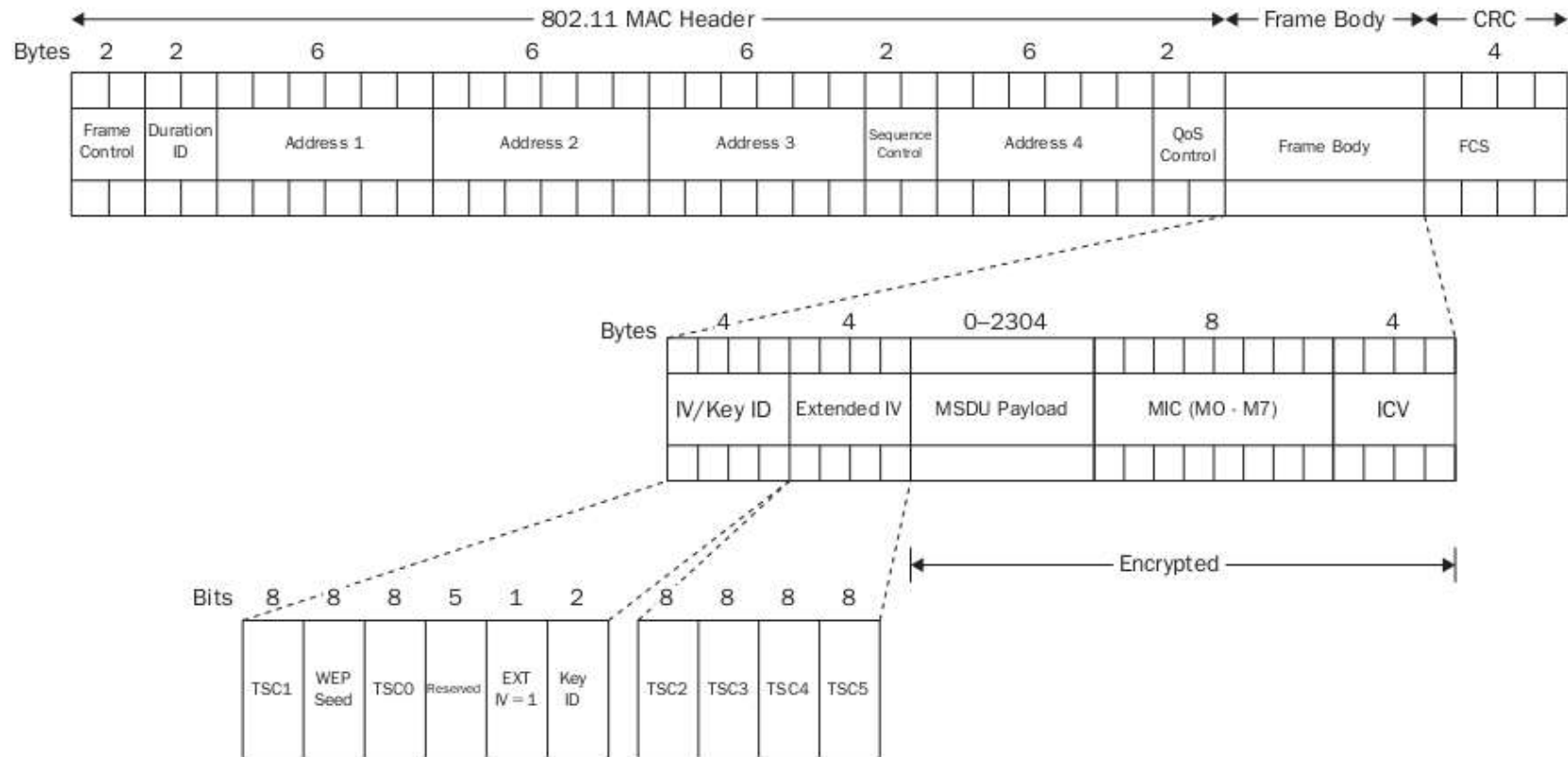
TKIP countermeasures

Logging: MIC failure would indicate an active attack that should be logged. MIC failure events can then be followed up by a system administrator.

60 Second Shutdown:

- ✓ If two MIC failures occur within 60 seconds of each other, the STA or AP must disable all reception of TKIP frames for 60 seconds.
- ✓ This shutdown method theoretically provides a risk of a denial - of - service (DoS) attack.

TKIP MPDU



Because of the extra overhead from the IV (4 bytes), Extended IV (4 bytes), MIC (8 bytes), and ICV (4 bytes), a total of 20 bytes of overhead is added to the frame body of a TKIP encrypted 802.11 data frame.

CCMP

“Counter Mode with Cipher - Block Chaining Message Authentication Code Protocol”

- ✓ (CCMP) is the security protocol that was created as part of the 802.11i security amendment and was designed to replace TKIP and WEP.
- ✓ CCMP uses the AES block cipher
- ✓ CCMP is mandatory for **robust security network (RSN)** compliance.
- ✓ In **September 2004**, the Wi - Fi Alliance introduced version 2 of the Wi - Fi Protected Access certification, called **WPA2**, which requires the use of CCMP/AES encryption.

CCMP (Cont...)

- ✓ CounterMode is often represented as CTR. The CTR is used to provide **data confidentiality**.
- ✓ The CBC - MAC is used for **authentication** and **integrity**.
- ✓ The integrity check is used to provide data integrity for both the **MSDU data** and **portions of the MAC header of the MPDU**.
- ✓ The inputs used by the CCMP encryption/data integrity process include:
 - **Temporal Keys (128 bits)**
 - **Packet Number (48 bits)**
 - **Nonce**
 - **Data Frame (MPDU)**
 - **Additional authentication data (AAD)**

CCMP (Cont...)

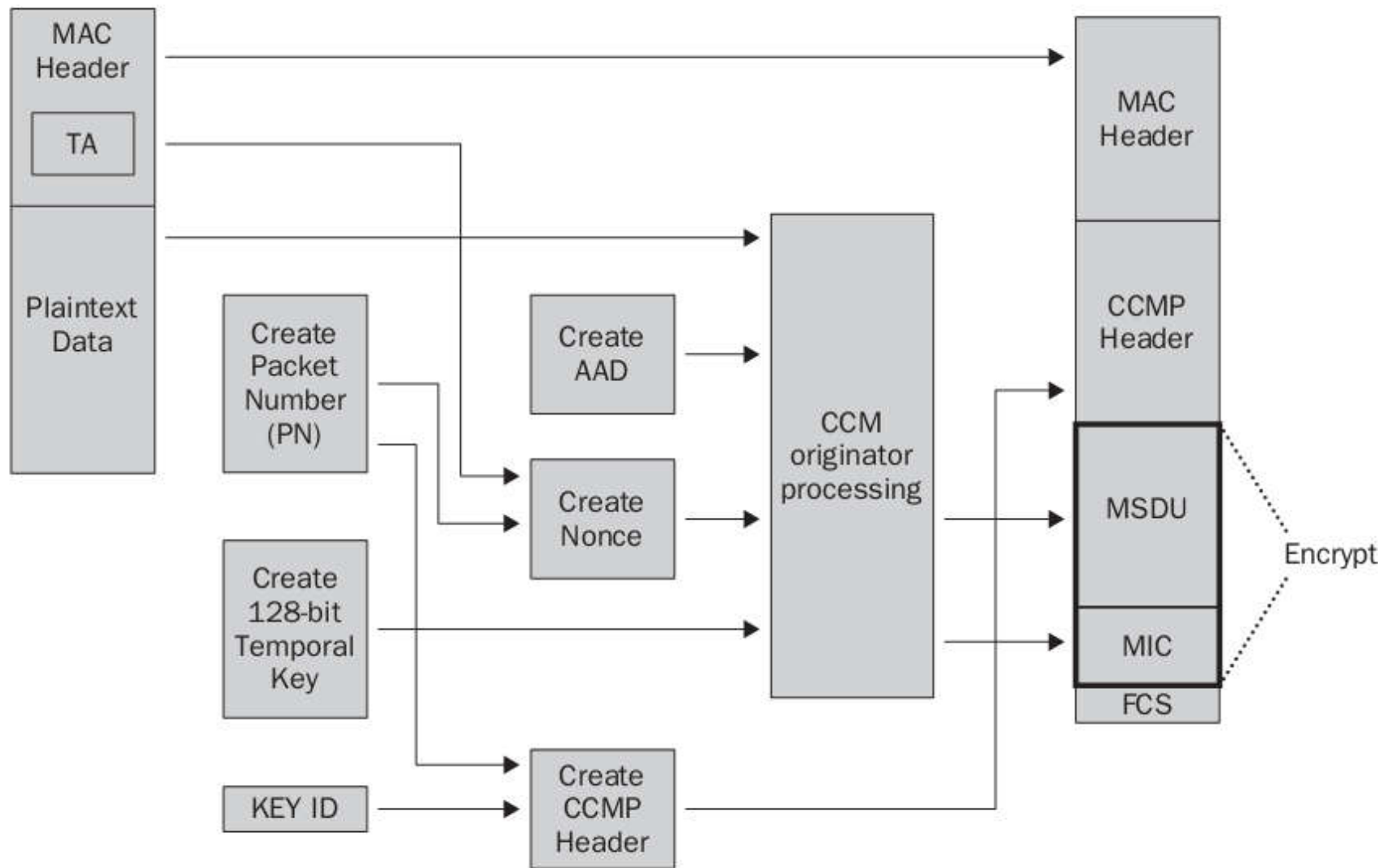
- ✓ CCMP starts with a 128 - bit **temporal key**.
- ✓ The **48 - bit packet number (PN)** is much like a TKIP sequence number.
- ✓ The **PN** uniquely identifies the frame and is incremented with each frame transmission. This protects CCMP from **replay** and **injection attacks**.
- ✓ A 104 - bit unique nonce is constructed from the **packet number (PN)**, **priority data** used in **QoS**, and the **transmitter address (TA)**.

CCMP (Cont...)

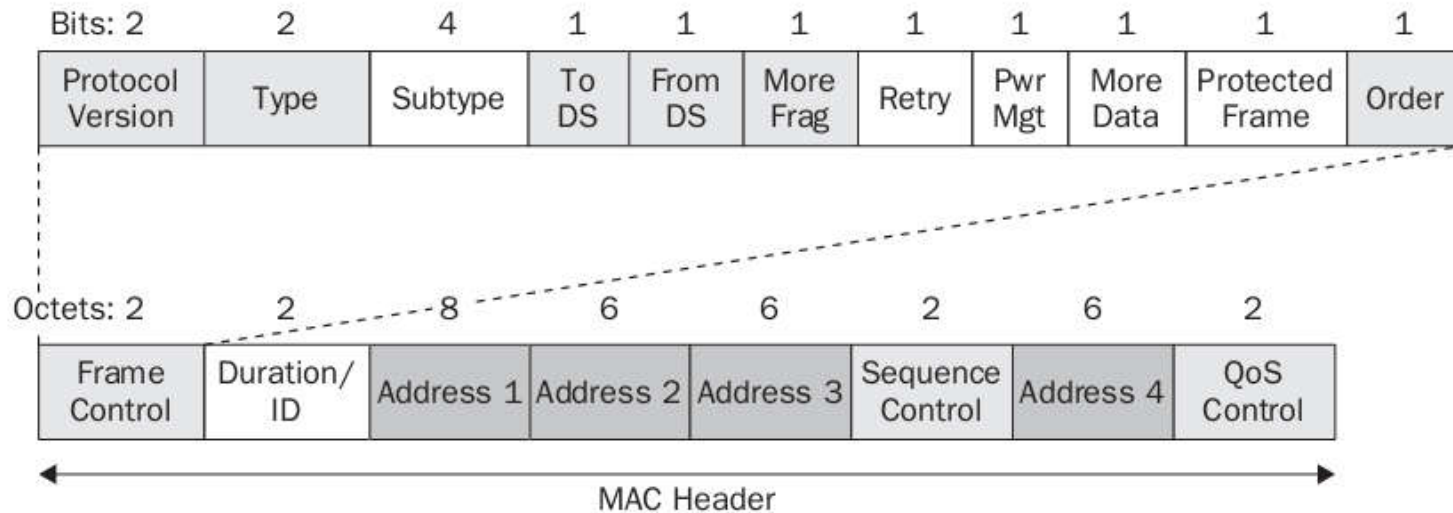
- ✓ The frame body encapsulates the **MSDU upper - layer payload** that will be encrypted and protected by a Message Integrity Code (MIC).
- ✓ The MPDU header, also known as the MAC header, will not be encrypted but is partially protected by the MIC.




Additional authentication data (AAD) is constructed from portions of the MPDU header. This information is used for data integrity of portions of the MAC header.

CCMP encryption and data integrity process

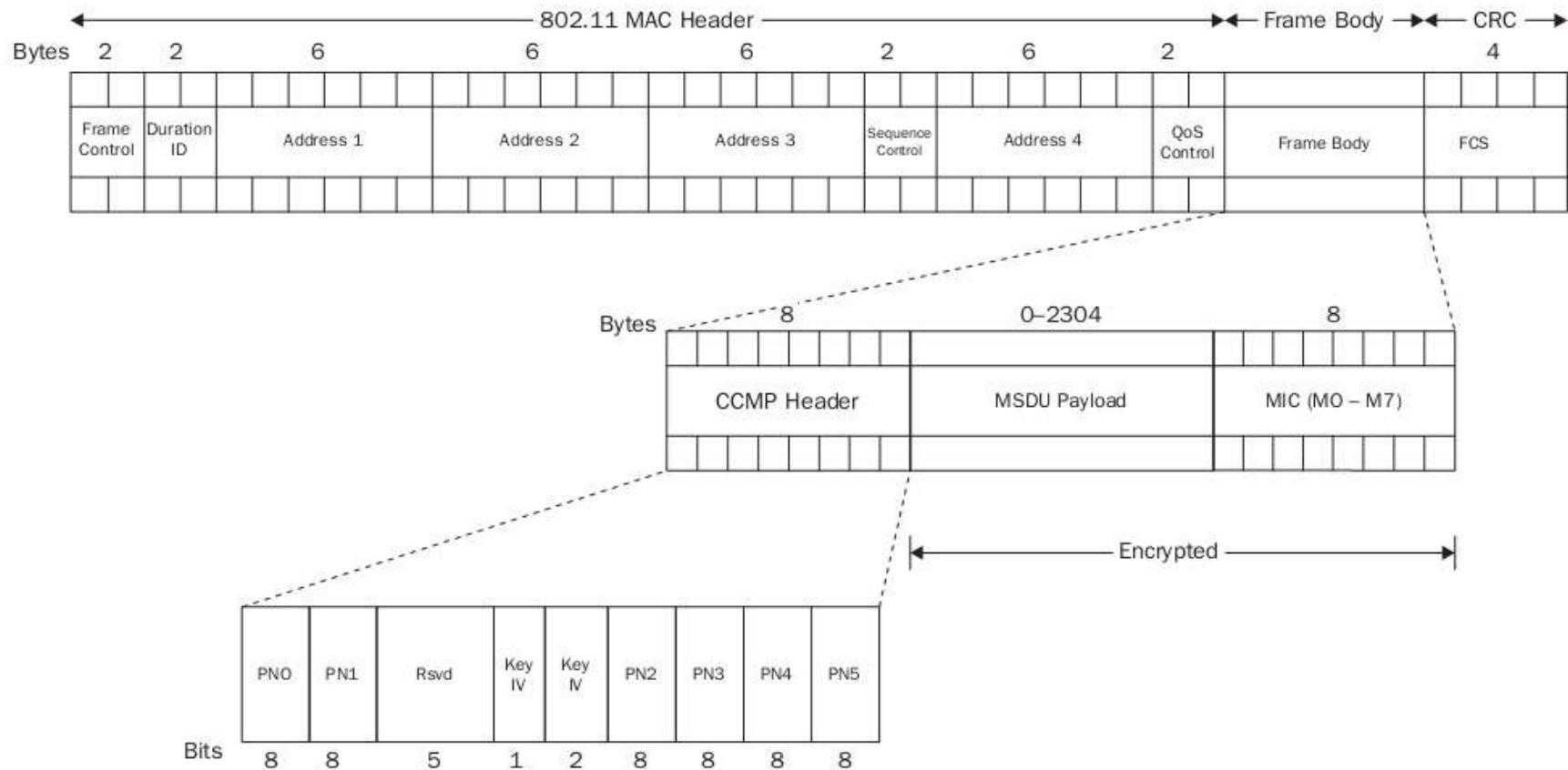


Additional authentication data (AAD)



-  Used to construct AAD and protected by CCM integrity
-  Some fields used to construct AAD and protected by CCM integrity
Some subfields masked to 0 and not protected by CCM integrity
-  Not used to construct AAD and not protected by CCM integrity

CCMP MPDU



The overhead that results from CCMP encryption includes CCMP header (8 bytes) and the MIC (8 bytes)

Security in 802.1x

Problem

Wireline or wireless local area networks are often deployed in environments that allow unauthorized equipment to be attached or unauthorized users to access the network using attached equipment.

Solution

- ✓ IEEE **802.1x authentication protocol**, or **Port Based Network Access Control**, makes it possible to block the flow of data from an unauthenticated user.

802.1x architecture

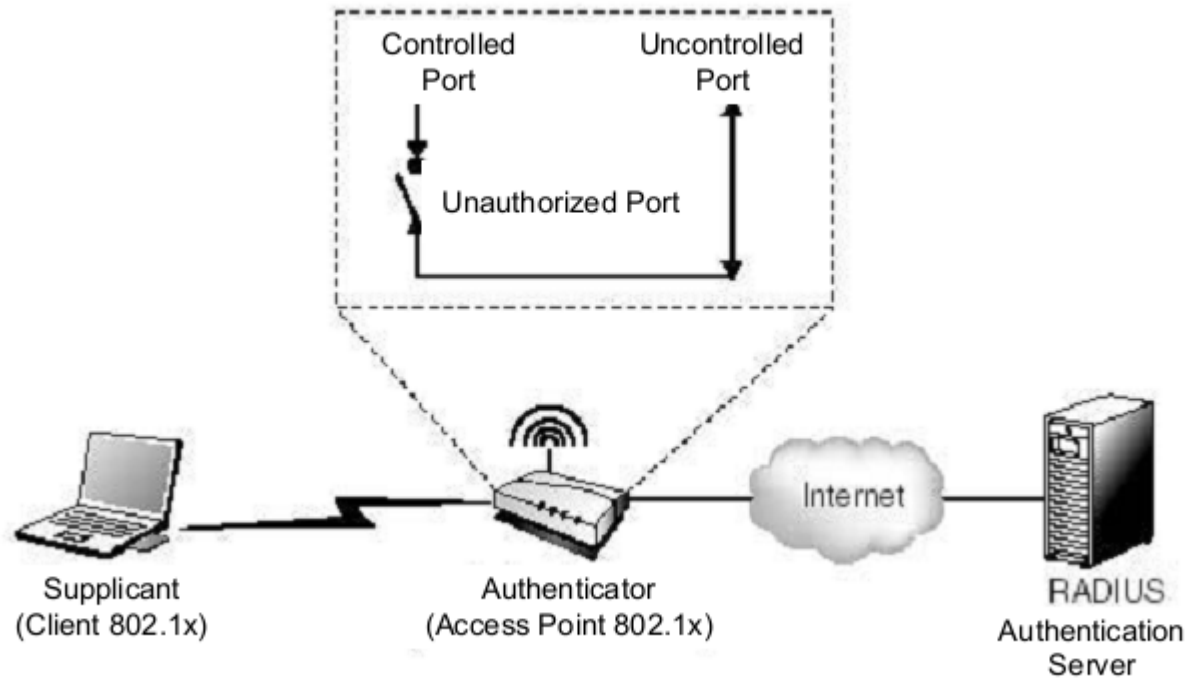
The 802.1x architecture relies on the three functional entities

- ✓ The supplicant or client **802.1x**. This is a terminal wishing to use the resources offered by a communications network.
- ✓ **The authenticator or controller.** This system controls a port for network access. It may be a switch in a wired network or access point in a wireless network.
- ✓ The authentication server, typically **RADIUS**

The flow of **802.1x** client data is divided into two classes of frame:

- ✓ The frames used by the EAP (**Extensible Authentication Protocol**).
- ✓ Other frames that are blocked when the port is in the “**not authorized**” state

802.1x architecture



Authentication by port

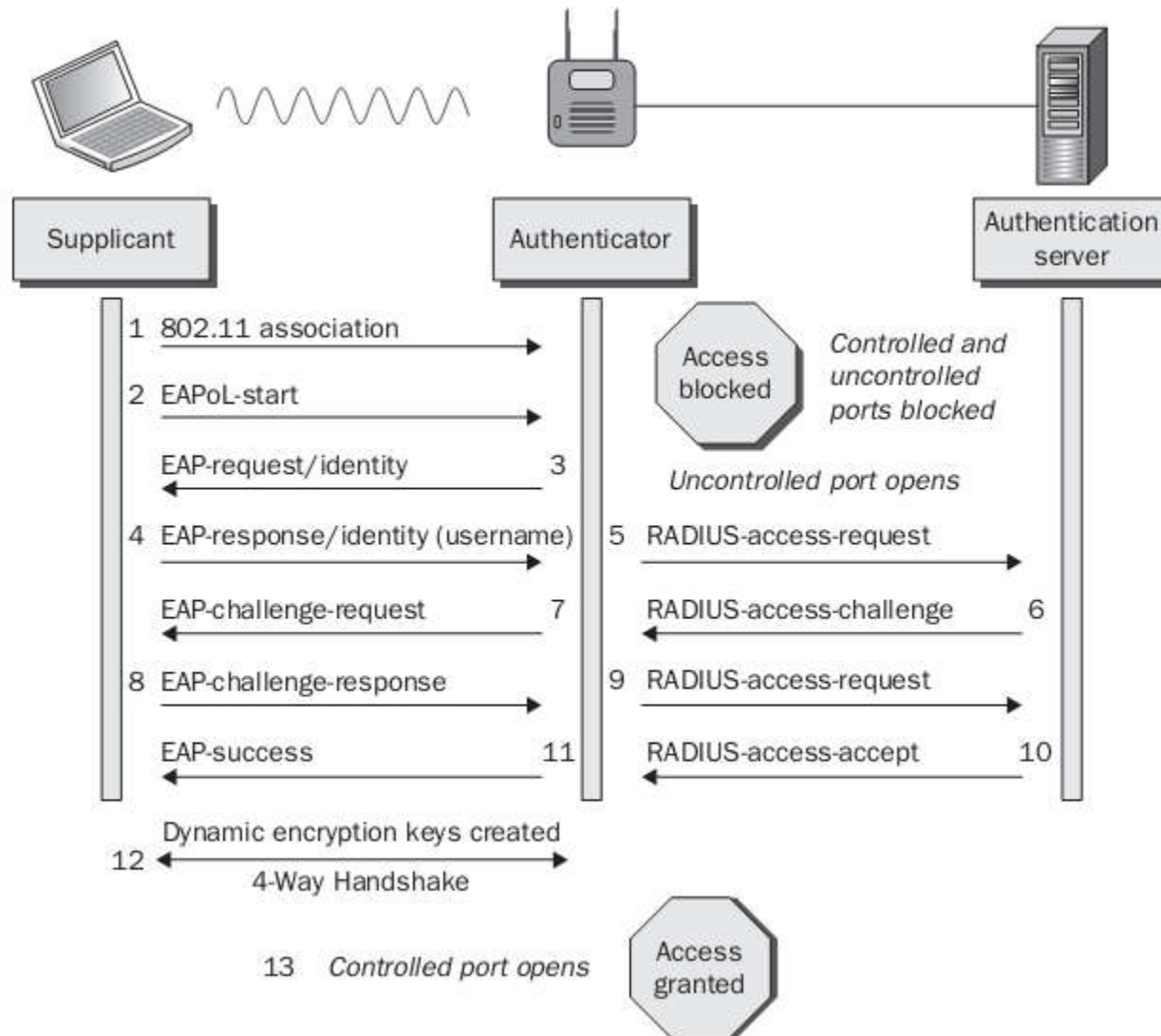
“The 802.1x standard defines a control network access based on ports. Its function is to authenticate and authorize equipment attached to the port of a local network.”

- ✓ In IEEE 802.11 wireless networks, a port is an association between a station and an access point.
- ✓ The controlled port behaves like a switch with two states. In the unauthorized state, only the frames dedicated to EAP authentication are not blocked.
- ✓ In the authorized state, the flow of information passes freely.

Authentication by port (Cont...)

- ✓ The 802.1x standard defines encapsulation techniques used to carry EAP packets between the client **802.1x port** and **access point port** or switch.
- ✓ These ports are called PAE (Port Access Entity). The encapsulation is known as EAPoL (EAP over LAN).
- ✓ **EAPoL** indicates the beginning and the end (optional) of an authentication session with the notification messages **EAPOL-START** and **EAPOL-LOGOFF**.
- ✓ In the authorized state, the port controls the duration of the session, meaning the time that we consider the client remains authenticated.

Authentication procedure



Authentication procedure (Cont...)

1. The **802.11 client (supplicant)** associates with the AP and joins the BSS. Both the controlled and uncontrolled ports are blocked on the authenticator.
2. The supplicant initiates the EAP authentication process by sending an **802.11 EAPOL - Start frame** to the authenticator. This is an optional frame and may or may not be used by different types of EAP.
3. The authenticator sends an **802.11 EAP - Request frame** requesting the identity of the supplicant. **The EAP - Request Identity frame** is always a required frame.

4. The supplicant sends an **EAP response frame** with the supplicant's identity in clear text. The username is always in clear text in the **EAP - Response Identity frame**. At this point, the uncontrolled port opens to allow EAP traffic through. All other traffic remains blocked by the controlled port.
5. The authenticator encapsulates the EAP response frame in a RADIUS packet and forwards it to the authentication server.
6. The AS looks at the supplicant's name and checks the database of users and passwords. The AS will then send a password challenge to the supplicant encapsulated in a RADIUS packet.

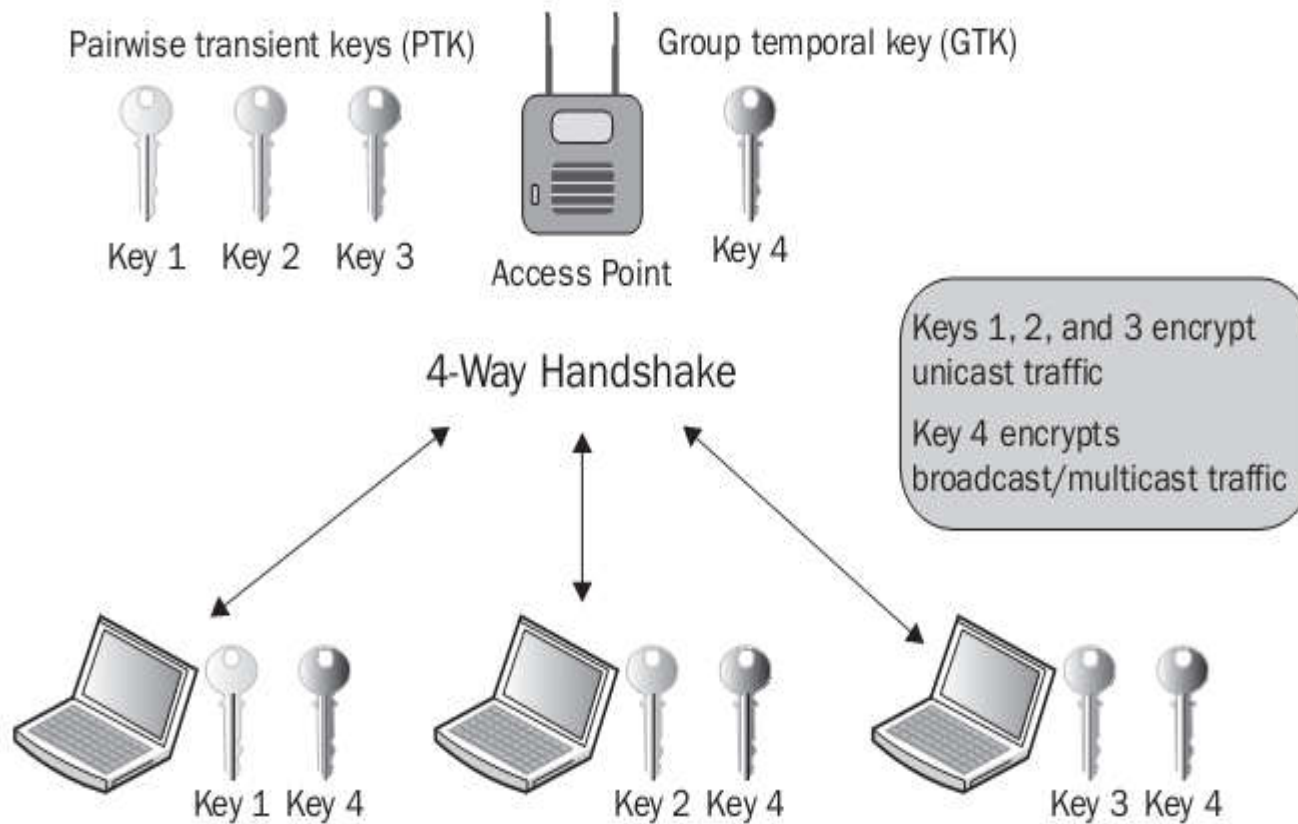
7. The authenticator forwards the password challenge to the supplicant in an 802.11 EAP frame.
8. The supplicant takes the password and hashes it with a hash algorithm such as MD - 5 or MS - CHAPv2. The supplicant then sends the hash response in an EAP from back to the AS.
9. The authenticator forwards the challenge response in a RADIUS packet to the AS.
10. The AS runs an identical hash and checks to see if the response is correct. The AS will then send either a success or failure message back to the supplicant.

11. The authenticator forwards the AS message to the supplicant in an EAP - Success frame. The supplicant has now been authenticated.
12. The final step is the **4-Way Handshake negotiation** between the authenticator and the supplicant. This is a complex process used to **generate dynamic encryption keys.**
13. Once the supplicant has completed Layer 2 EAP authentication and **created dynamic encryption keys**, the **controlled port is unblocked.** The supplicant is then authorized to use network resources.

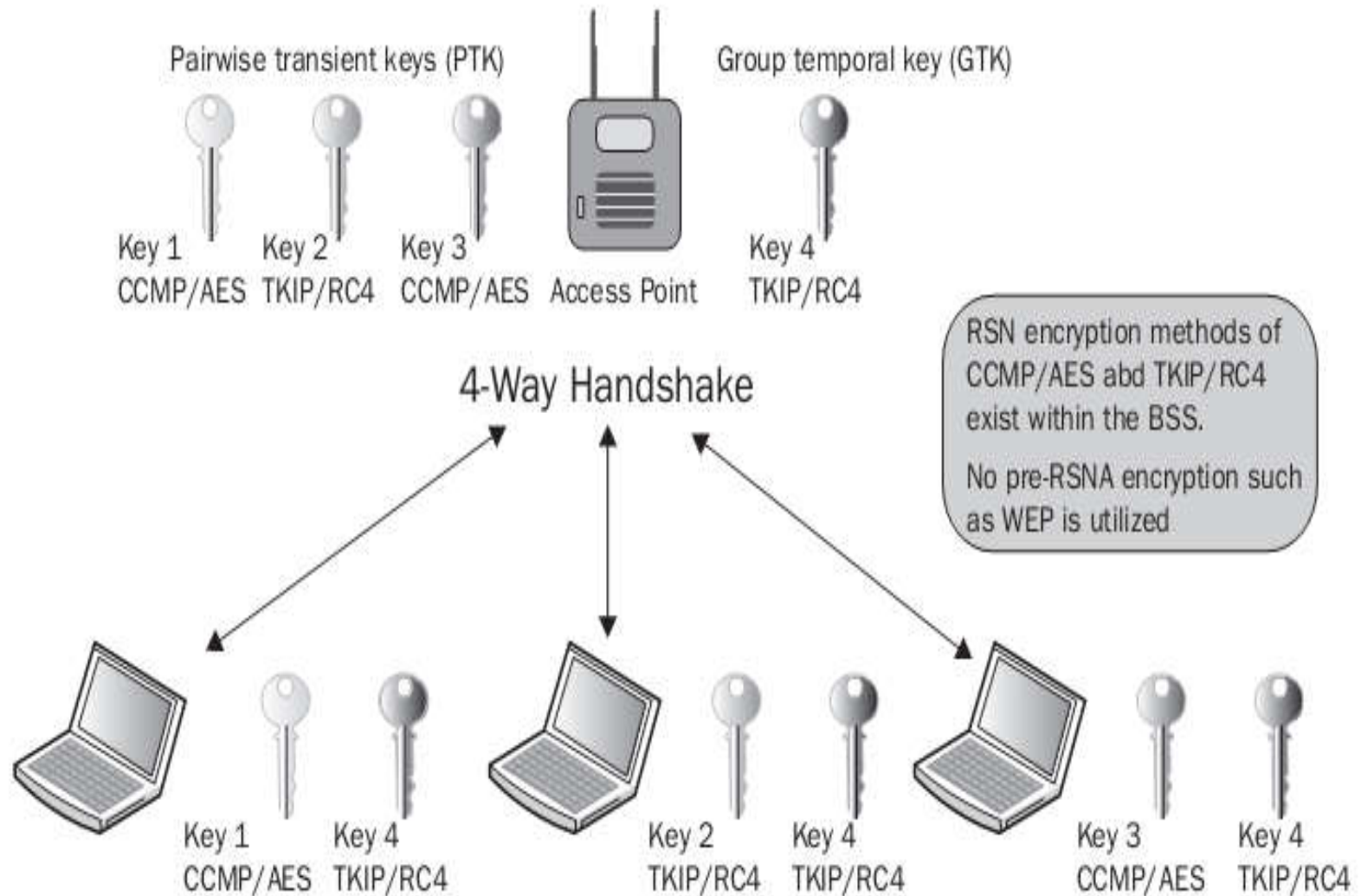
Robust Security Network

- ✓ A security association is a set of policies and keys used to protect information.
- ✓ A **robust security network association (RSNA)** requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the **4 - Way Handshake**.
- ✓ When RSN security associations are used within a BSS, all of the client station radios have unique encryption keys that are shared with the radio of the access point.

RSNA within a BSS



Robust security network



RSN Information Element

- ✓ Within a BSS, how can client stations and an access point notify each other about their RSN capabilities?
- ✓ RSN security can be identified by a field found in certain 802.11 management frames.
- ✓ The RSN information element can identify the encryption capabilities of each station.
- ✓ The RSN information element will also indicate whether **802.1X/EAP authentication** or **preshared key (PSK)** authentication is being used.

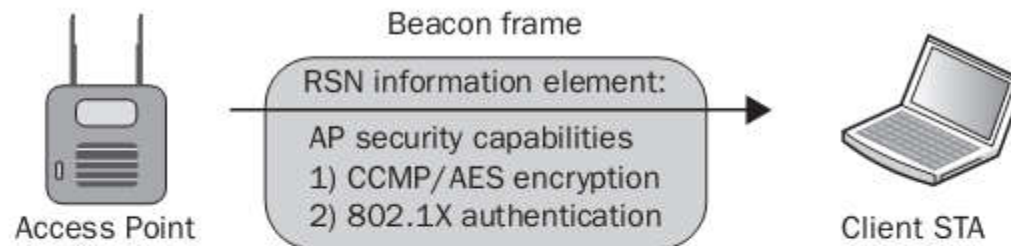
✓ The RSN information element field is found in four different **802.11 management frames:**

- beacon management frames
- probe response frames
- association request frames
- reassociation request frames

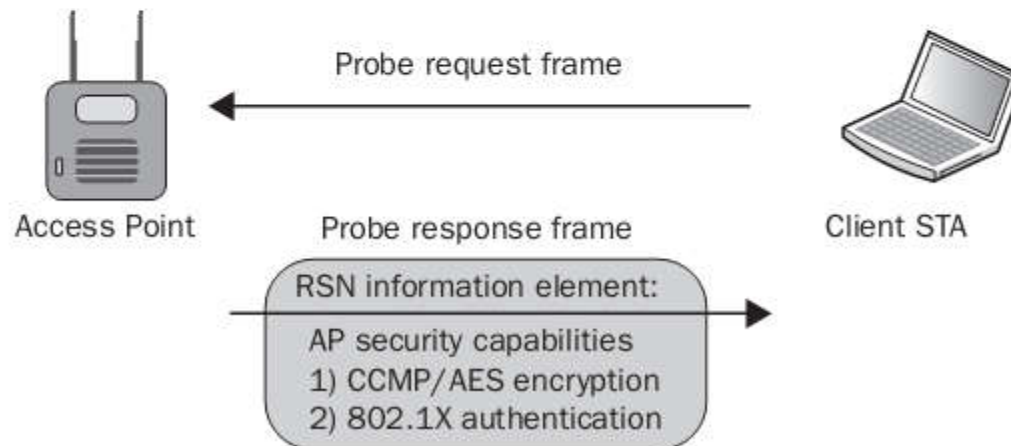
✓ Within a basic service set, an access point and client stations use the **RSN information element** within these four management frames to communicate with each other about their security capabilities prior to establishing association.

Access point RSN security capabilities

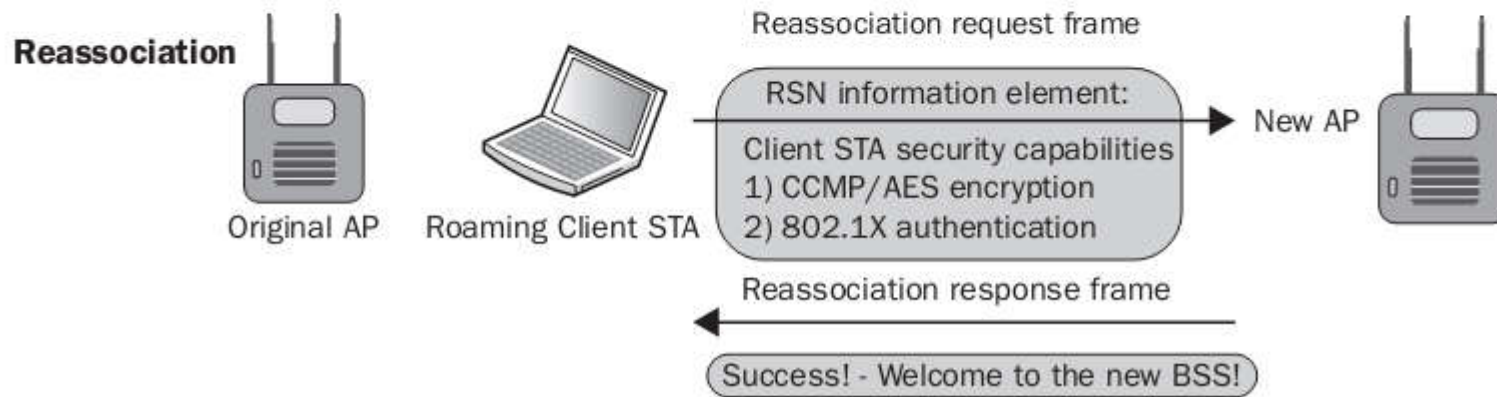
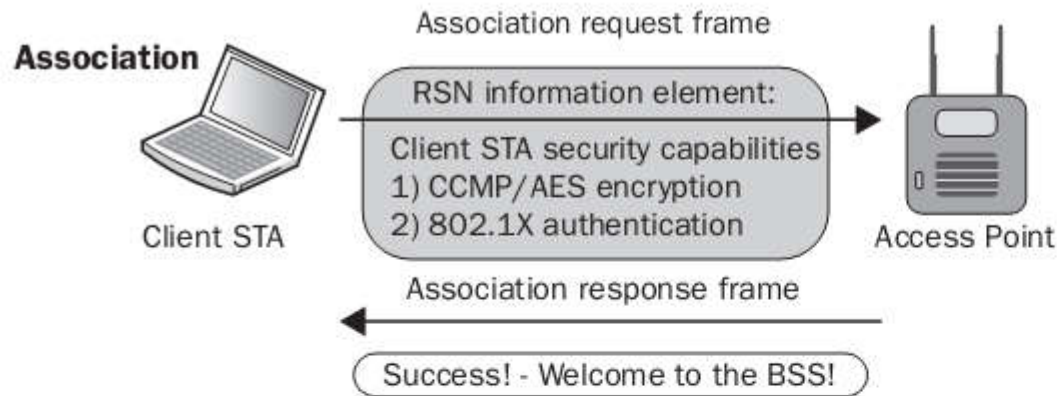
Passive scanning



Active scanning



Client station RSN security capabilities

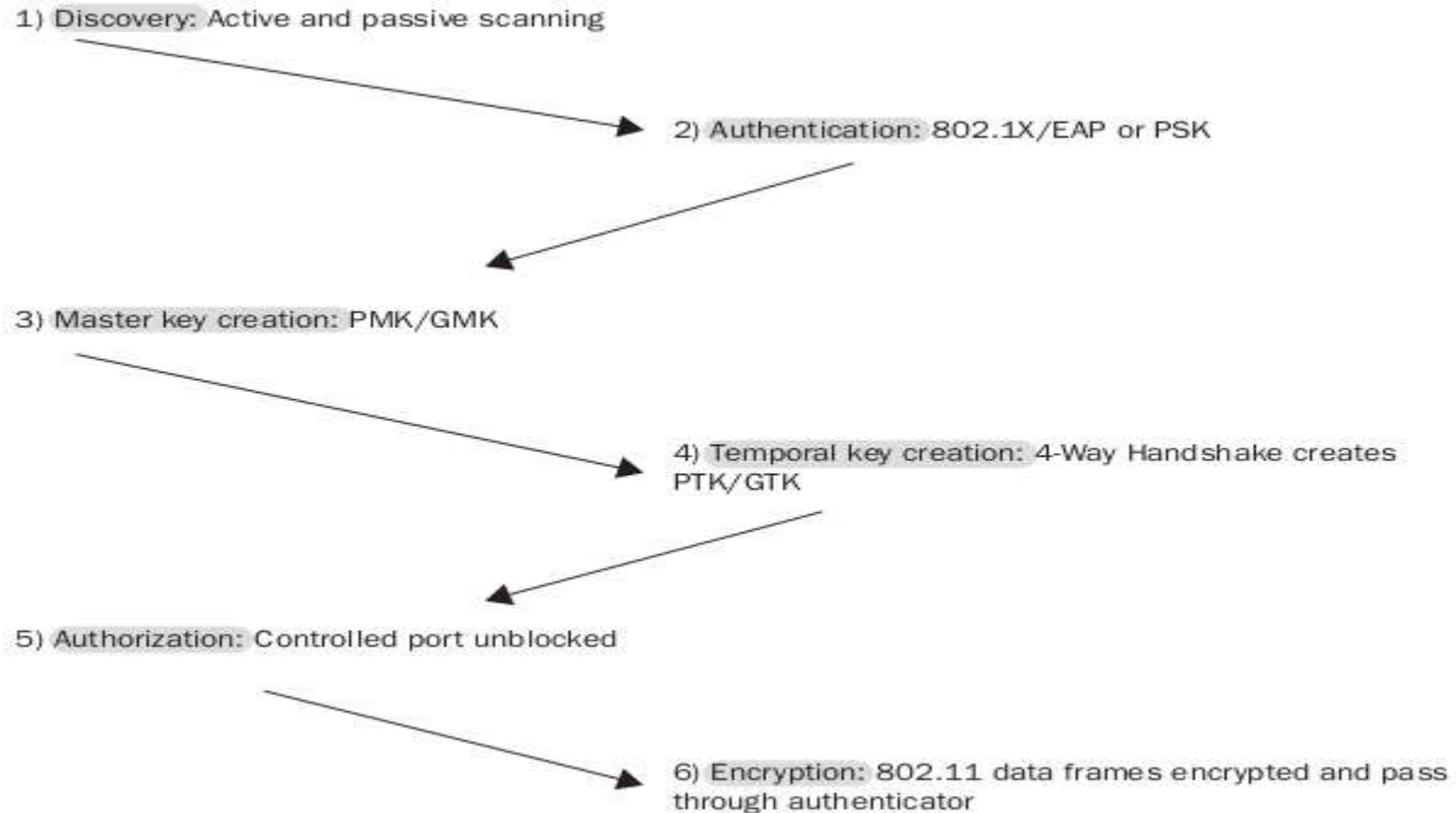


Authentication and Key Management (AKM)

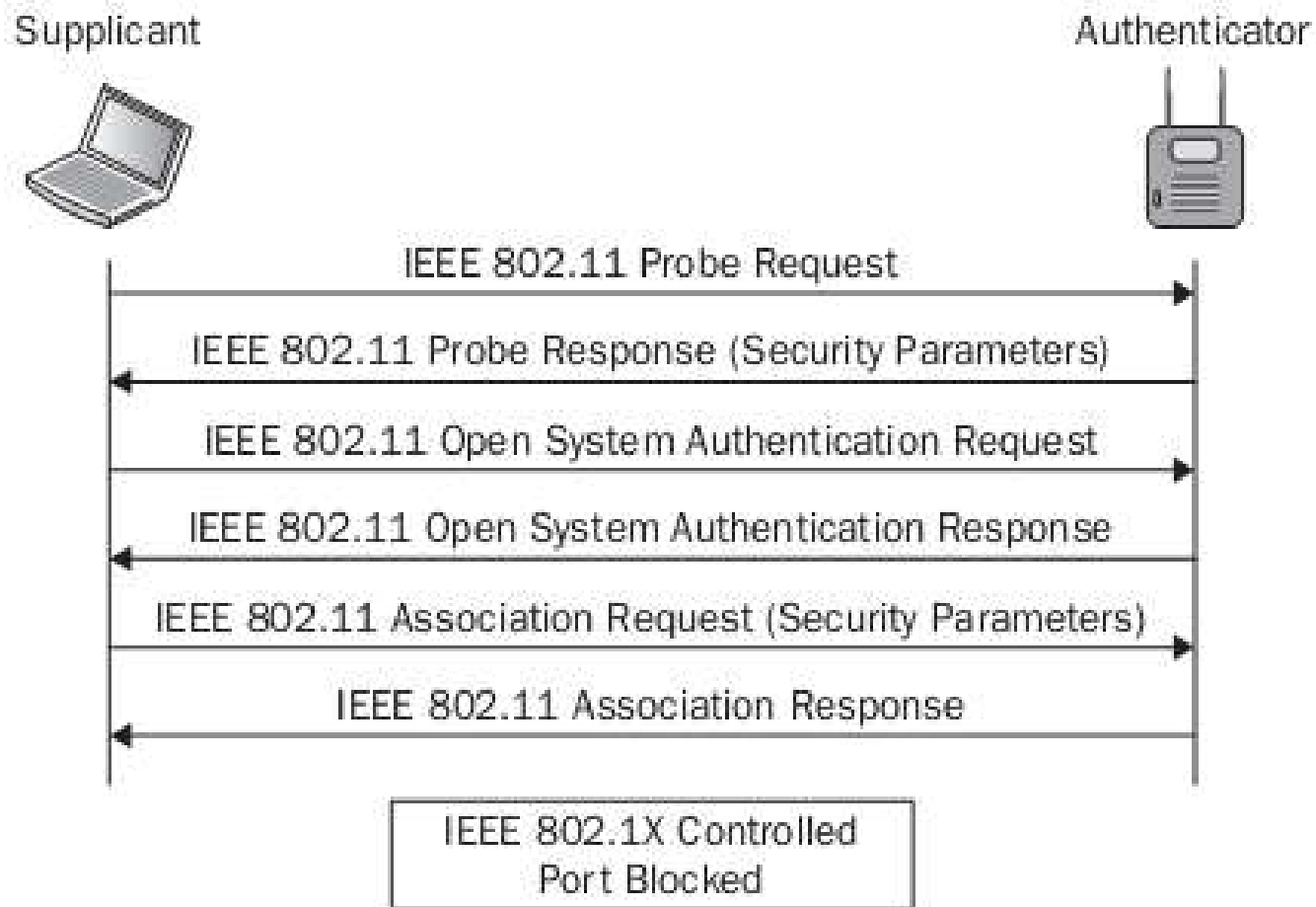
- ✓ **Authentication and key management (AKM)** services. The AKM services consist of a set of one or more algorithms designed to provide authentication and key management
- ✓ **An authentication and key management protocol (AKMP)** can be either a preshared key (PSK) or an EAP protocol used during 802.1X authentication.
- ✓ The main goal of 802.1X/EAP is twofold:
 - Authentication
 - Authorization

- ✓ **AKM** services require both **authentication processes** and the **generation and management of encryption keys**.
- ✓ The **802.1X/EAP** and **PSK authentication processes** generate the seeding material needed to create dynamic encryption keys.
- ✓ Furthermore, until dynamic encryption keys are created, the controlled port of an 802.1X authenticator will not open.

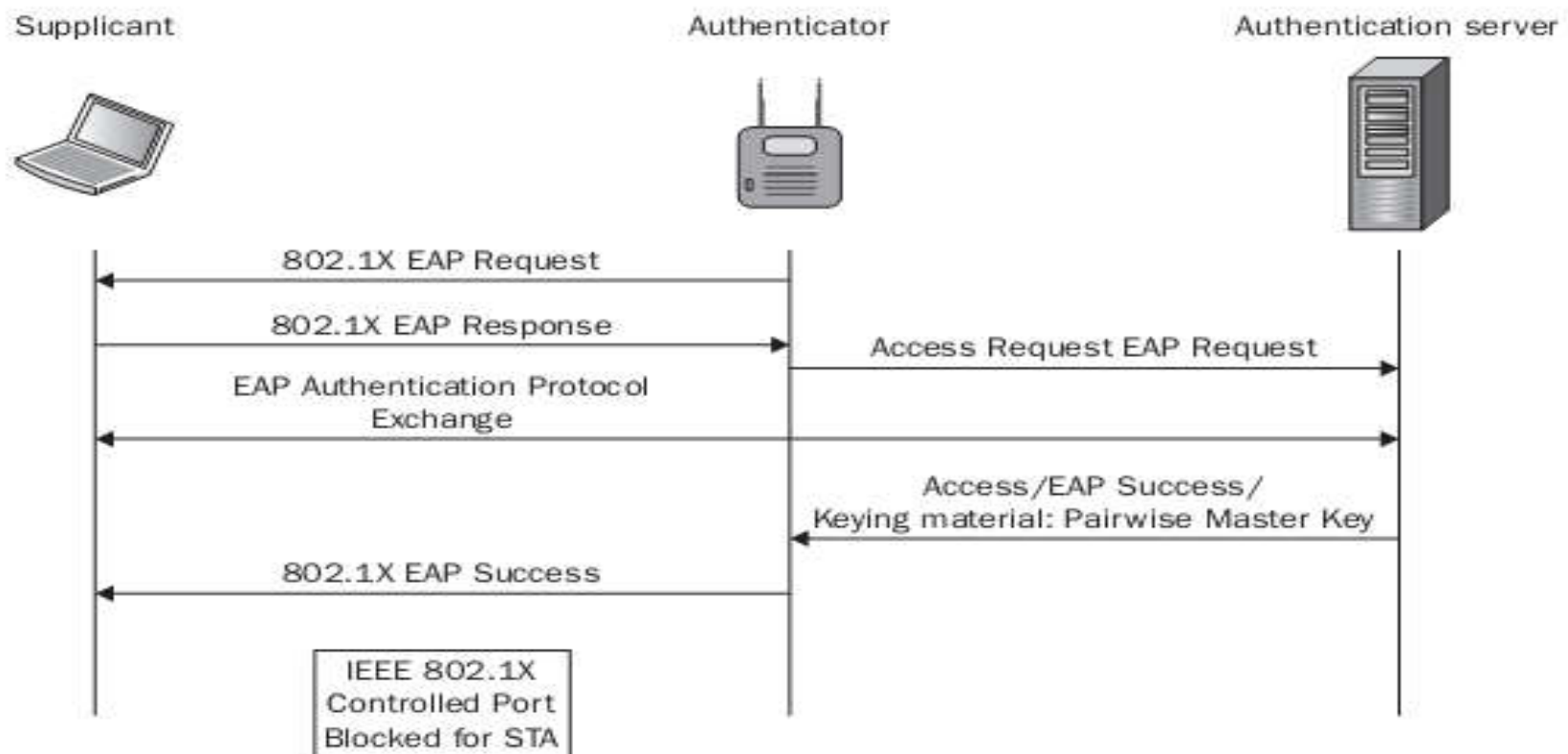
Authentication and key management (AKM)—overview



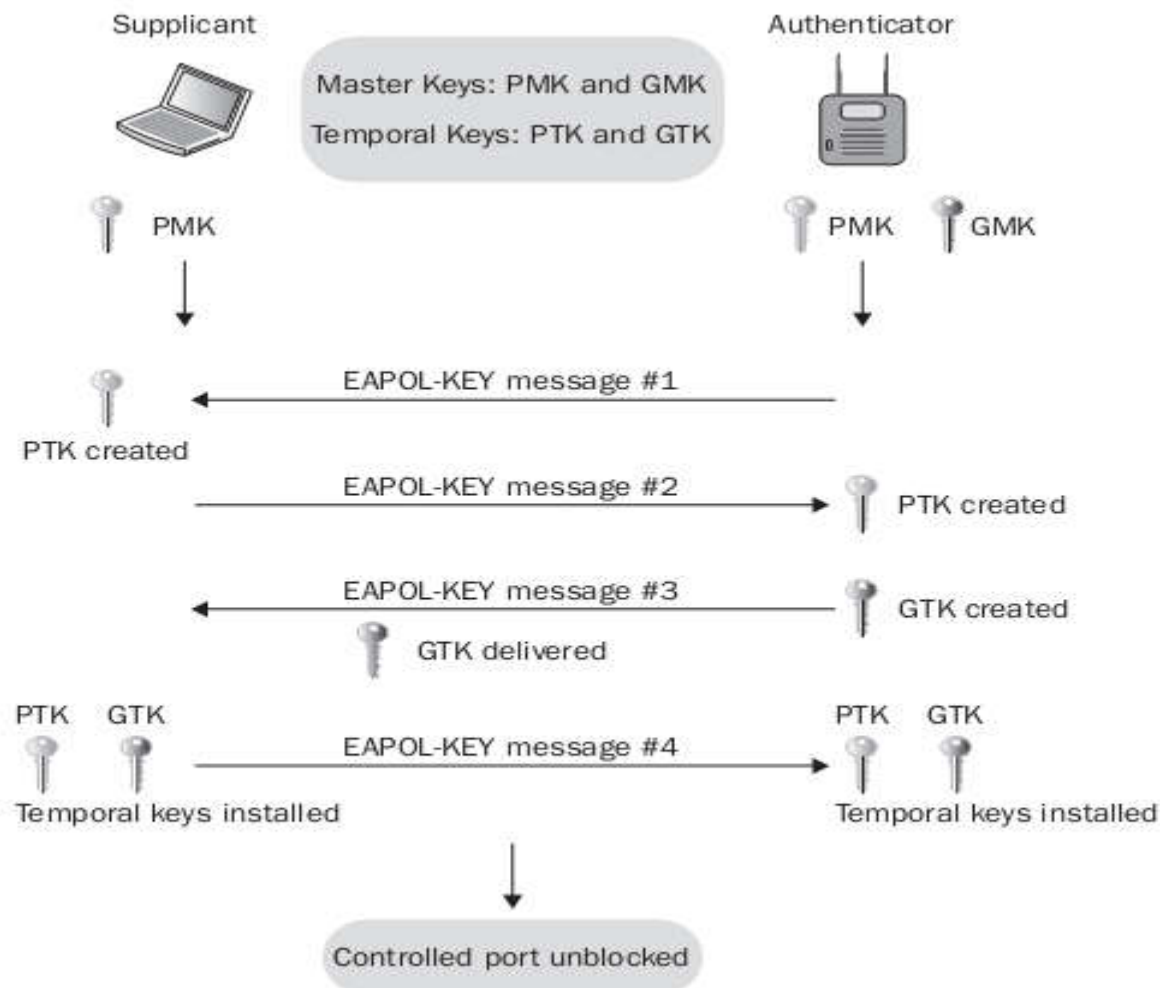
Authentication and key management (AKM)—discovery component



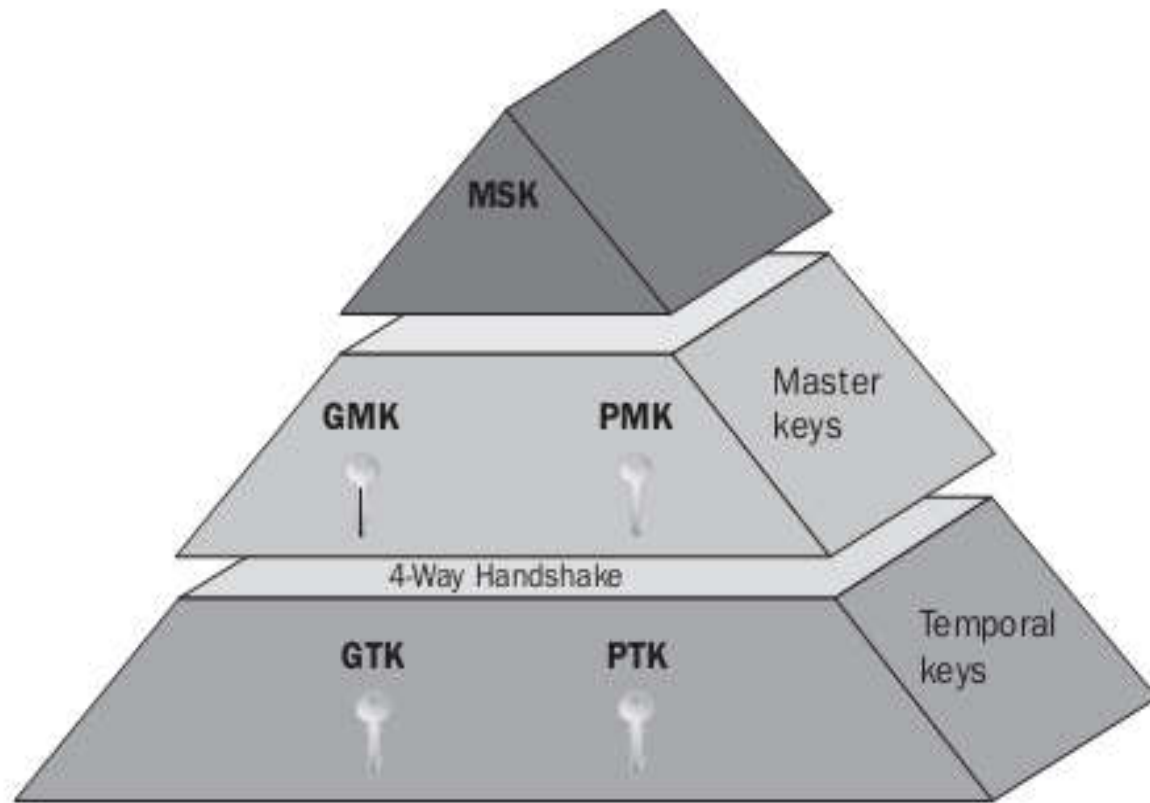
Authentication and key management (AKM)—authentication and master key generation component



Authentication and key management (AKM)—temporal key generation and authorization



RSNA Key Hierarchy



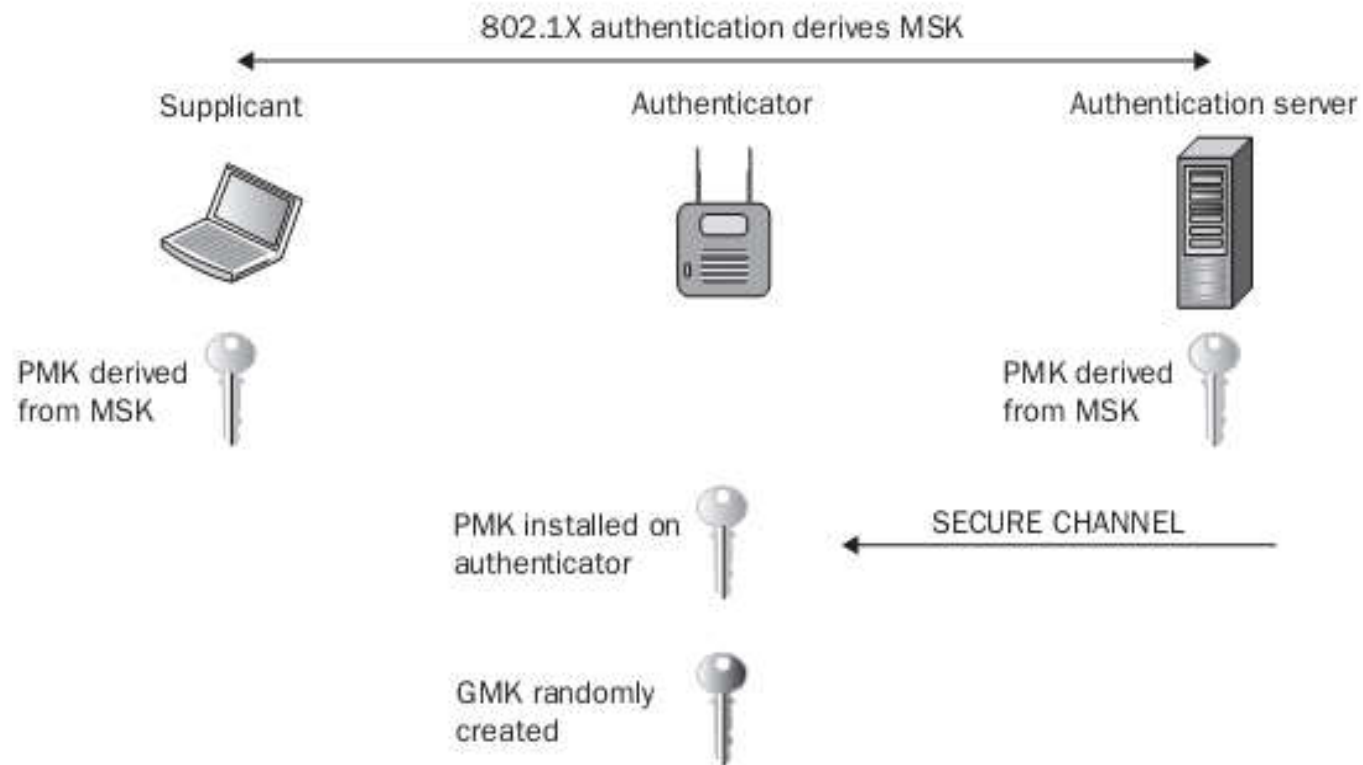
Master Session Key (MSK)

- ✓ At the top of the RSNA key hierarchy is the master session key (MSK)
- ✓ The MSK is generated either from an 802.1X/EAP process or is derived from PSK authentication.

Master Keys

- ✓ After the creation of the MSK as a result of 802.1X/EAP, two master keys are created.
- ✓ The MSK seeding material is then used to create a master key called the pairwise master key (PMK).

- ✓ The PMK is simply computed as the first 256 bits (bits 0 – 255) of the MSK.
- ✓ PMK is then sent from the authentication server over a secure channel to the authenticator.



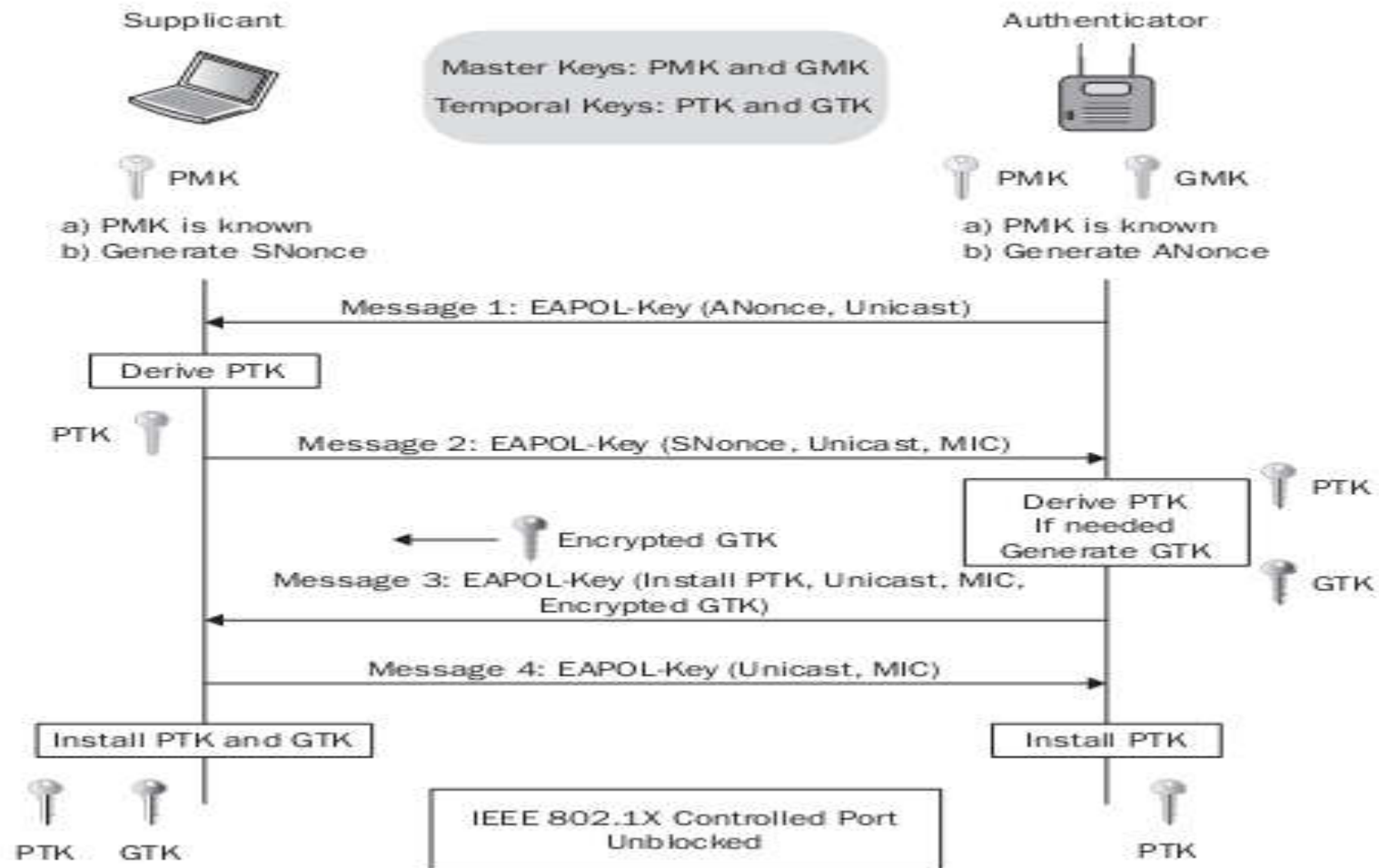
- ✓ Another master key, called the group master key (GMK), is randomly created on the access point/authenticator.
- ✓ The master keys are now the seeding material for the 4 - Way Handshake process.
- ✓ The **4 - Way Handshake** process is used to create the keys that are used to encrypt and decrypt data.
- ✓ The keys generated from the **4 - Way Handshake** are called the **pairwise transient key (PTK)** and the **group temporal key (GTK)**.

4 - Way Handshake

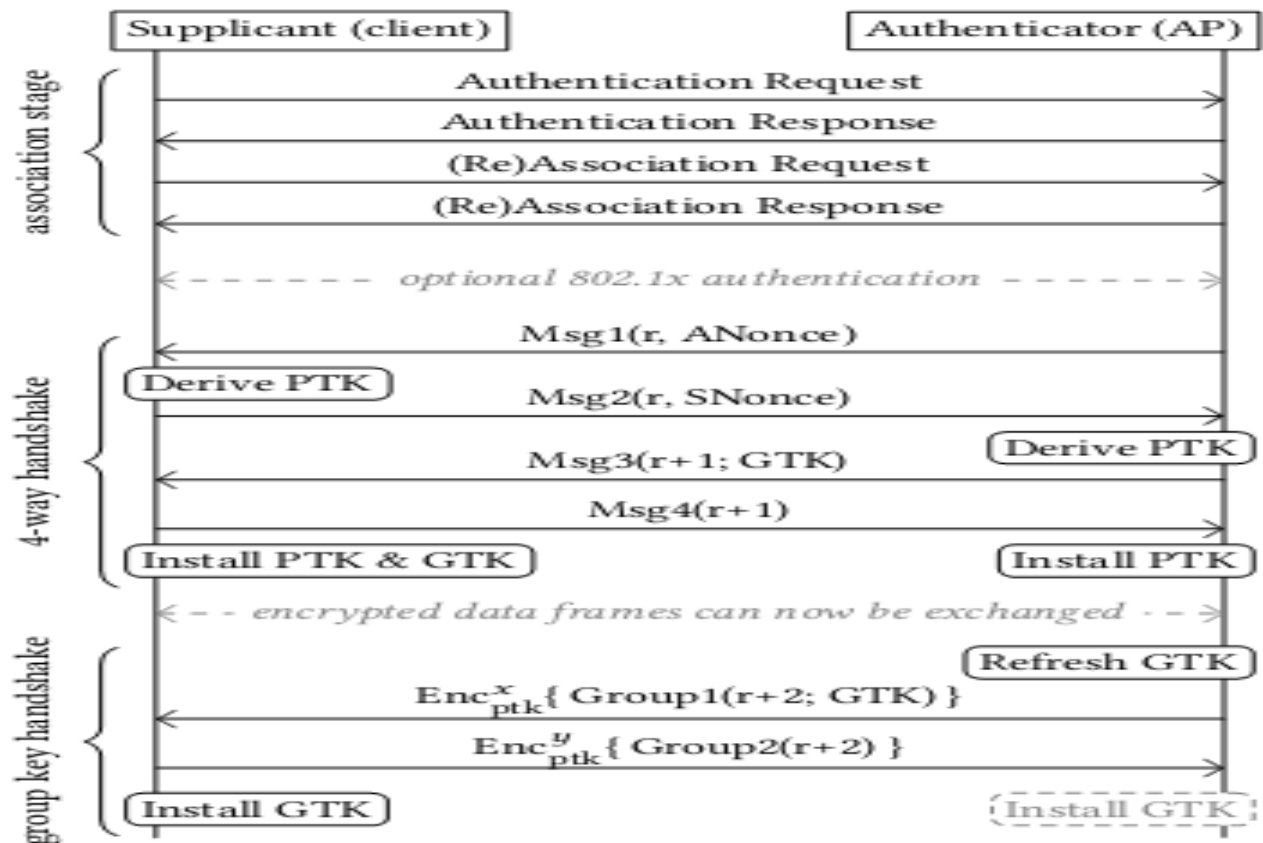
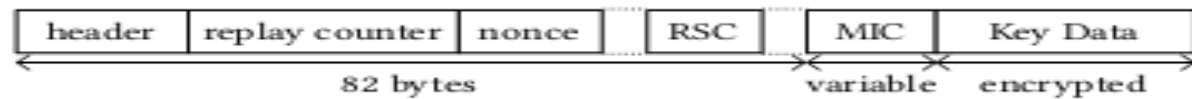
To create the pairwise transient key, the 4 - Way Handshake uses a pseudo - random function that combines the pairwise master key, a numerical **authenticator nonce**, a **supplicant nonce**, the **authenticator ' s MAC address (AA)**, and **the supplicant ' s MAC address (SPA)**.

$$PTK = PRF (PMK + ANonce + SNonce + AA + SPA)$$

4 - Way Handshake



EAPOL Frame



Passphrase to PSK mapping

- ✓ The PSK authentication used during RSNA is often known by the more common name of WPA - Personal or WPA2 - Personal.
- ✓ A WPA/WPA2 preshared key is a **static** key that is configured on the access point and all the clients.
- ✓ The same static PSK is used by all members of the basic service set (BSS).
- ✓ The RSNA PSK is **256 bits** in length or 64 characters when expressed in hex.

- ✓ The PSK is generated using a **password-based key generation function (PBKDF)**.

Here is the formula to convert a passphrase to a PSK:

$$\text{PSK} = \text{PBKDF2}(\text{PassPhrase}, \text{ssid}, \text{ssidLength}, 4096, 256)$$

- ✓ **4096 is the number of times the passphrase is hashed.**
- ✓ **256 is the number of bits output by the passphrase mapping**