05 - WLAN Encryption and Data Integrity Protocols

WIRELESS LAN SECURITY

Introduction

- 802.11i adds new encryption and data integrity methods.
- includes encryption algorithms to protect the data, cryptographic integrity checks to prevent message modification and replay, and dynamic key management algorithms
- describes the new security association concept associated with 802.11i.

IEEE 802.11i

- enhances 802.11 with several new security mechanisms to ensure message confidentiality and integrity.

- also incorporates the 802.1x port authentication algorithm to provide a framework for strong mutual authentication and key management.

Features

- Two new network types, called Transition Security Network (TSN) and Robust Security Network (RSN)
- New data encryption and data integrity methods: Temporal Key Integrity Protocol (TKIP) and Counter mode/CBC-MAC Protocol (CCMP)
- New authentication mechanisms using the Extensible Authentication Protocol (EAP)
- Key management via security handshake protocols conducted over 802.1x

TKIP

- a cipher suite
- includes a key mixing algorithm and a packet counter to protect cryptographic keys
- includes Michael, a Message Integrity Check (MIC) algorithm that, along with the packet counter, prevents packet replay and modification

CCMP

- based on AES that accomplishes encryption and data integrity
- provides stronger encryption and message integrity than TKIP
- not compatible with the older WEP-oriented hardware

RSN

- RSN allows only machines using TKIP/Michael and CCMP.
- A TSN is one that supports both RSN and pre-RSN (WEP) machines to operate.
- RSN is definitely preferred, and getting all networks to use CCMP exclusively would be ideal.

Encryption Protocols

- Three encryption protocols: WEP, TKIP, and CCMP.
- They primarily are used for confidentiality but also include message integrity.
- TKIP and CCMP also include replay protection.
- WEP does not provide robust message integrity or replay protection.

Wired Equivalent Privacy

Three main design goals:

- To prevent disclosure of packets in transit
- To prevent modification of packets in transit
- To provide access control for use of the network

Preventing Disclosure of Packets

- uses the RC4 algorithm
- RC4 is a stream cipher and is not supposed to be reused with the same key
- Therefore, the designers added the initialization vector (IV), which allows a fresh RC4 key to be used for every packet.
- Failure to prevent repeats of IV means that an attacker can replay packets, or attack on the RC4 keystream.

Preventing Modification of Packets

- uses the integrity check vector (ICV)
- The ICV is a four-octet linear checksum calculated over the packet's plaintext payload and included in the encrypted payload.
- It uses the 32-bit cyclic redundancy check (CRC-32) algorithm.

Achieving Access Control

- chooses a challenge-response mechanism based on knowledge of the WEP key, called shared-key authentication
- The idea was that a station needed to prove its knowledge of the WEP key to gain access to the network.
- This method not only is flawed, but it also compromises bits of the keystream.

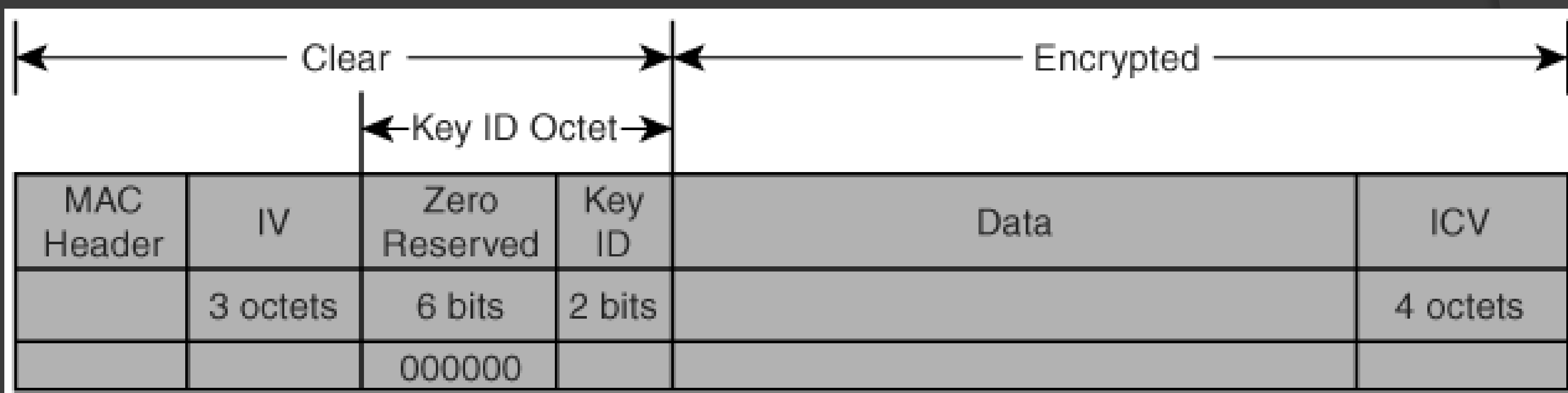
RC4

- RC4 is the basic encryption algorithm that WEP employs.
- RC4 is a symmetric stream cipher, so it produces a keystream of the same length as the data.
- In WEP, this keystream is combined with the data using the exclusive OR (XOR) operation to produce the ciphertext.

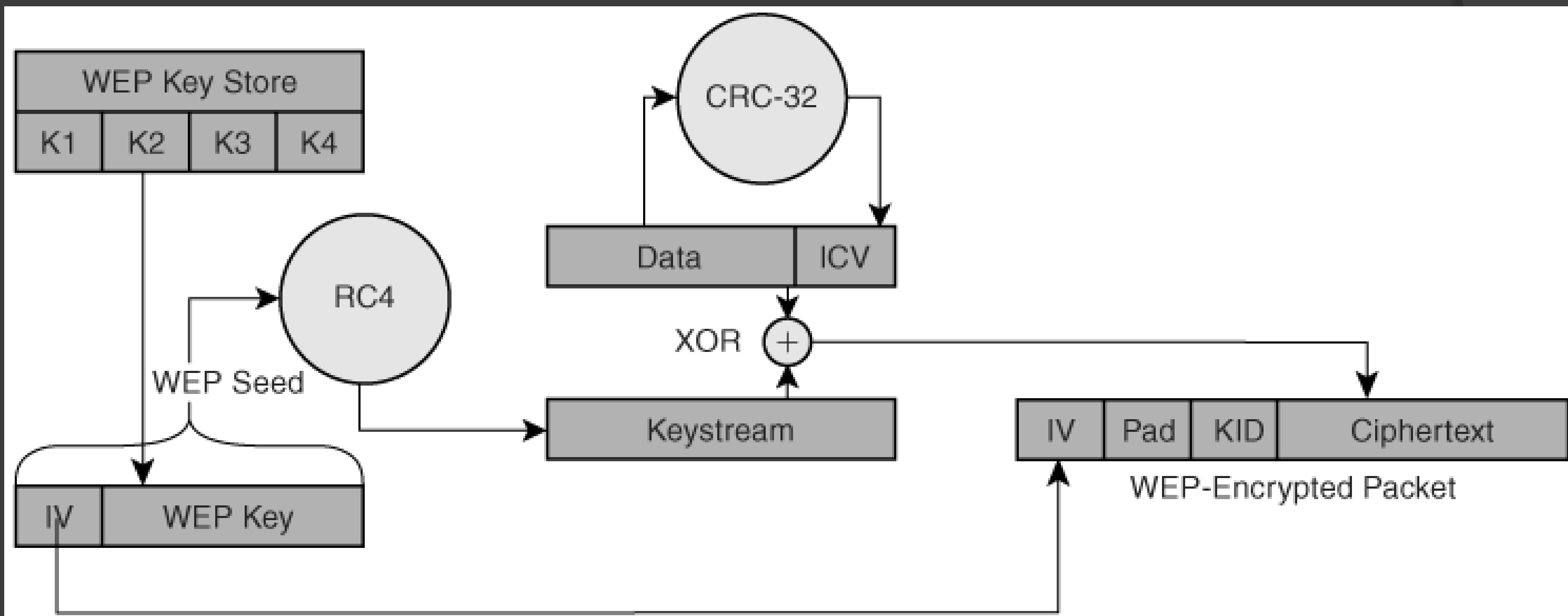
WEP Encapsulation

- involves encryption, integrity check calculation, possible fragmentation, and attachment of headers.
- Decapsulation is the opposite, involving processes such as removing headers, decryption, reassembling packets, and verifying integrity checks.

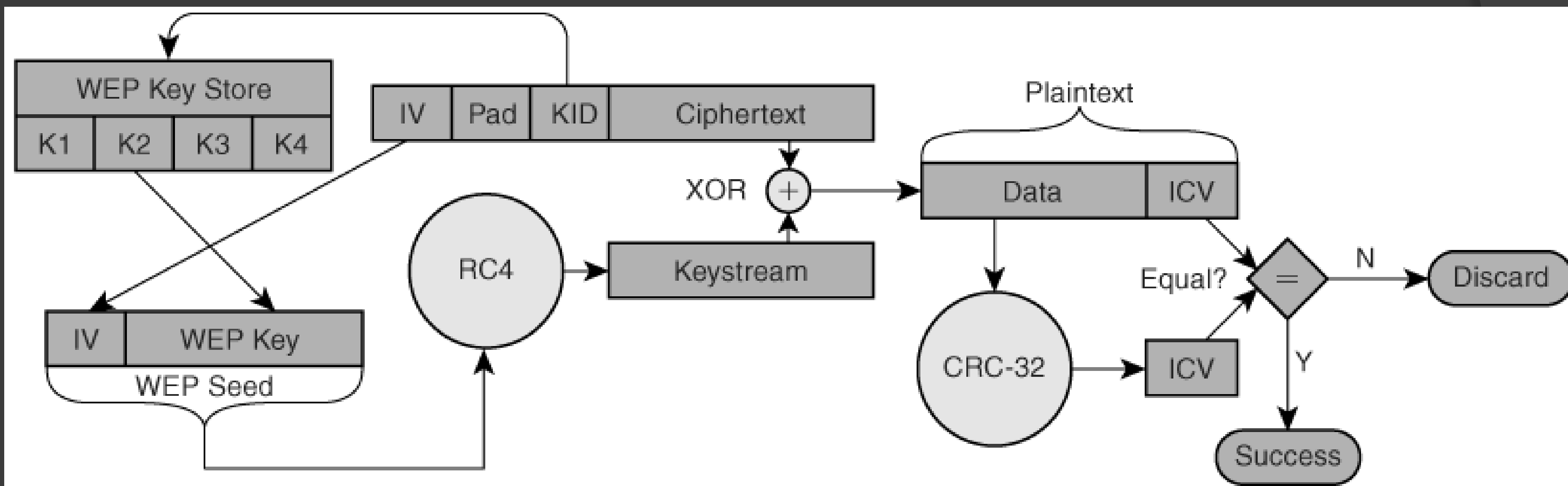
WEP Packet Format



The Process of Encapsulation of the WEP Packet



WEP Decapsulation



TKIP (802.11i/WPA)

- 2 main design goals:
  - to fix the problems with WEP
  - to work with legacy hardware: the initialization vector, RC4 encryption, and integrity check vector

- TKIP consists of three protocols:
  - a cryptographic message integrity algorithm
  - a key mixing algorithm
  - an enhancement to the initialization vector.

Michael MIC (802.11i/WPA)

- The ICV can be recalculated even in an encrypted stream
- prevents message modification
- uses a cryptographic hash
- calculated over the length of the packet
- based on shift operations and XOR additions, which are quick to calculate.
- uses a key called the Michael key

Michael Algorithm

- calculated over something called the padded MSDU, which is never transmitted
- The padded MSDU is the real MSDU plus some extra fields: the source and destination MAC addresses, some reserved octets, and a priority octet.
- The reason for adding these fields is that it protects them against modification when the MIC is checked on the other end.

Michael Padded MSDU

Source Address	Destination Address	Reserved	Priority	MSDU	Stop Octet	Padding
6 octets	6 octets	3 octets	1 octet		1 octet	4 to 7 octets
		0x000000	0x00		0x5A	0x00 values

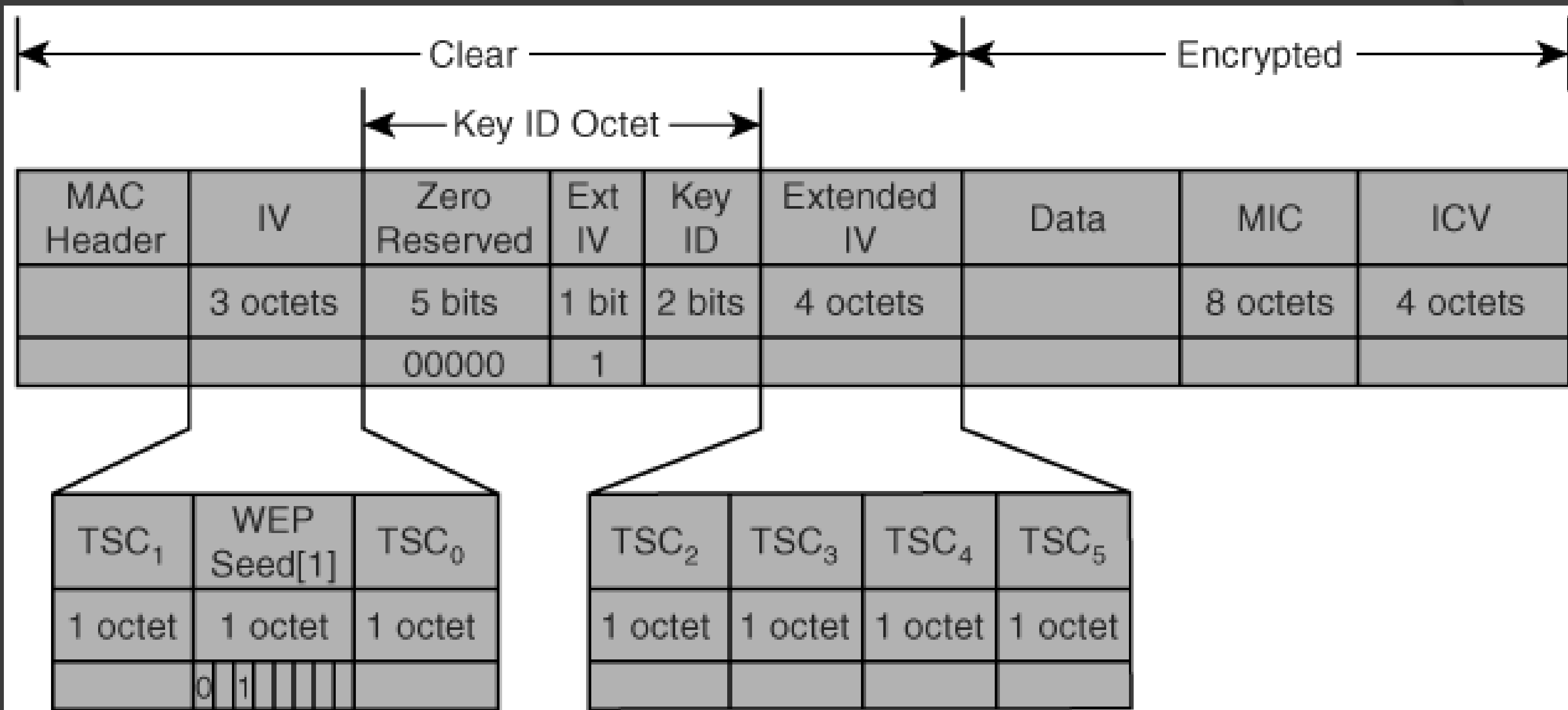
Preventing Replay Attacks

- The WEP specification fails to require that implementers use unique IVs, so it is easy for an attacker to replay packets.
- The TSC is a 48-bit counter that starts at 0 and increases by 1 for each packet. TSCs must be remembered because they must never repeat for a given key.
- If the receiver receives a packet that has a TSC value lower than or equal to one it has already received, it assumes it is a rebroadcast and drops it.

Preventing Replay Attacks (cont.)

- The ICV and MIC prevent an attacker from changing the TSC and using it to rebroadcast a packet.
- An attacker could attempt a DoS attack, in which he sends or modifies packets so that they have a future value of the TSC.
- The specification prevents this threat by specifying that the receiver not update his incoming TSC counter until he successfully verifies the MIC for each packet.

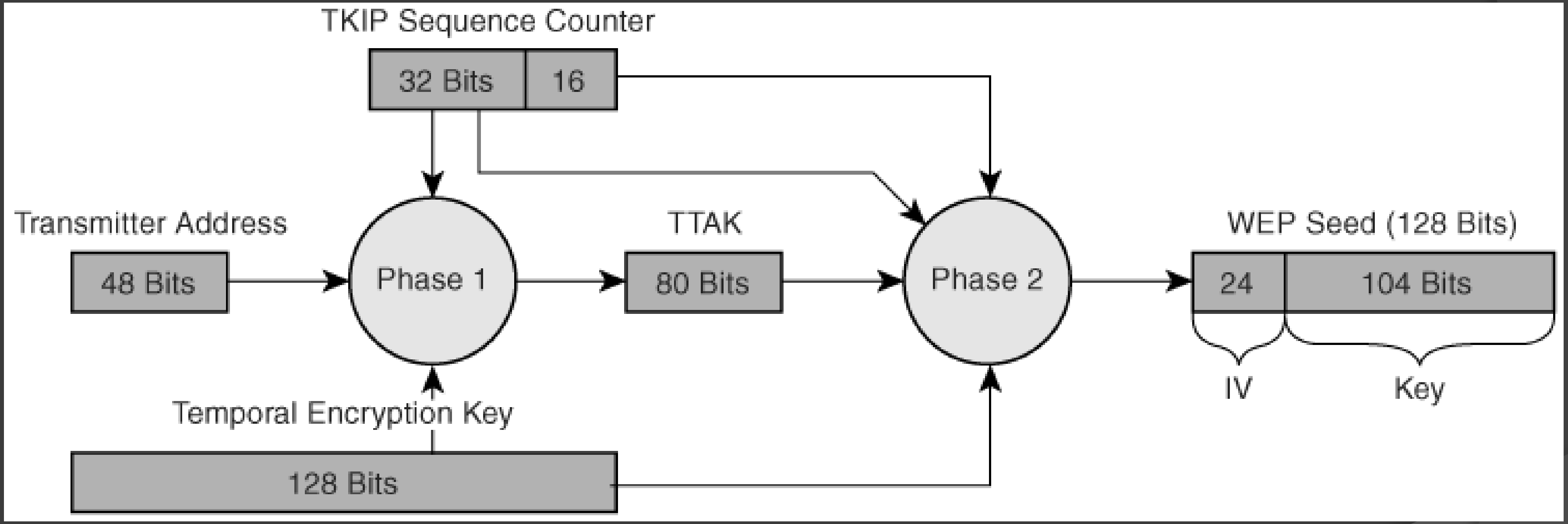
TKIP Packet Format



Key Mixing Algorithm

- to protect the Temporal Encryption Key (TEK), the base key for creating unique per-packet keys.
- starts with the TEK, combines this TEK with the TSC and the Transmitter Address (TA) to create a unique per-packet, 128-bit WEP seed.

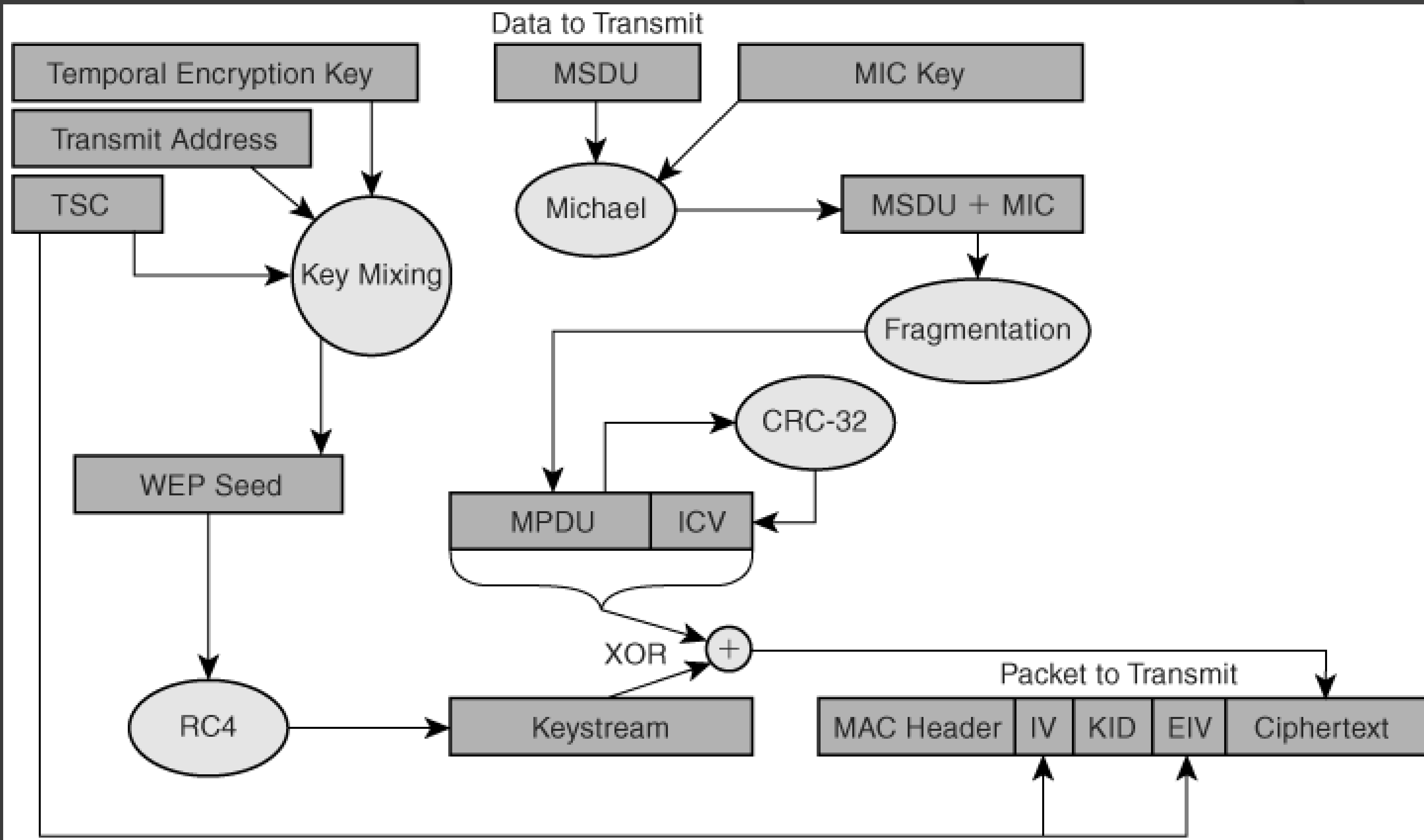
TKIP Key Mixing Algorithm



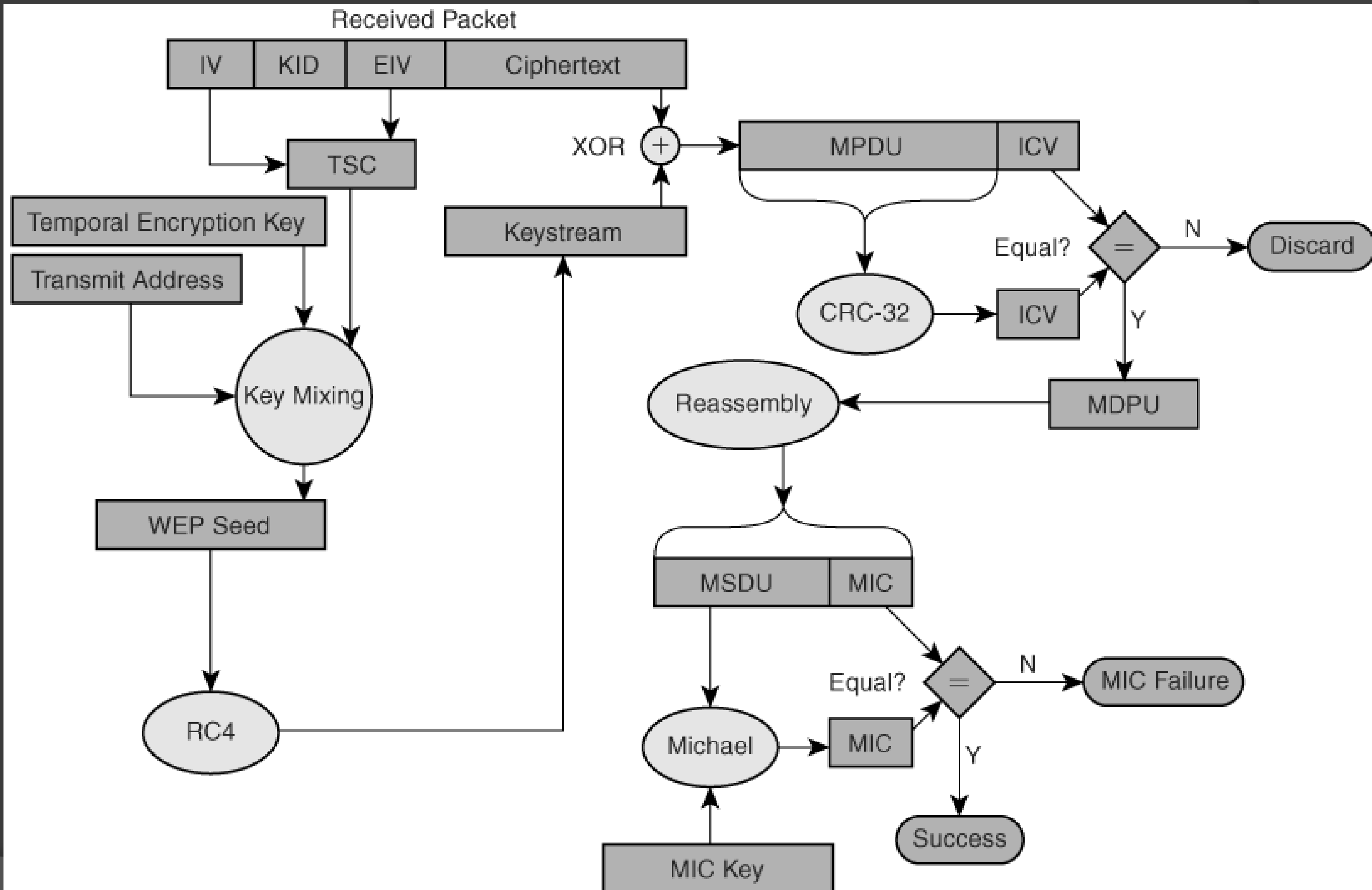
TKIP Packet Construction

- TKIP adds three fields to the standard WEP packet format: the MIC, the Extended IV field, and the Extended IV bit in the KeyID octet.
- TSC_0 and TSC_1 are swapped to avoid known weak keys noted in the Fluhrer-Mantin-Shamir paper.
- The entire TSC is transmitted in plaintext so that the recipient can use it for decryption

TKIP Encapsulation



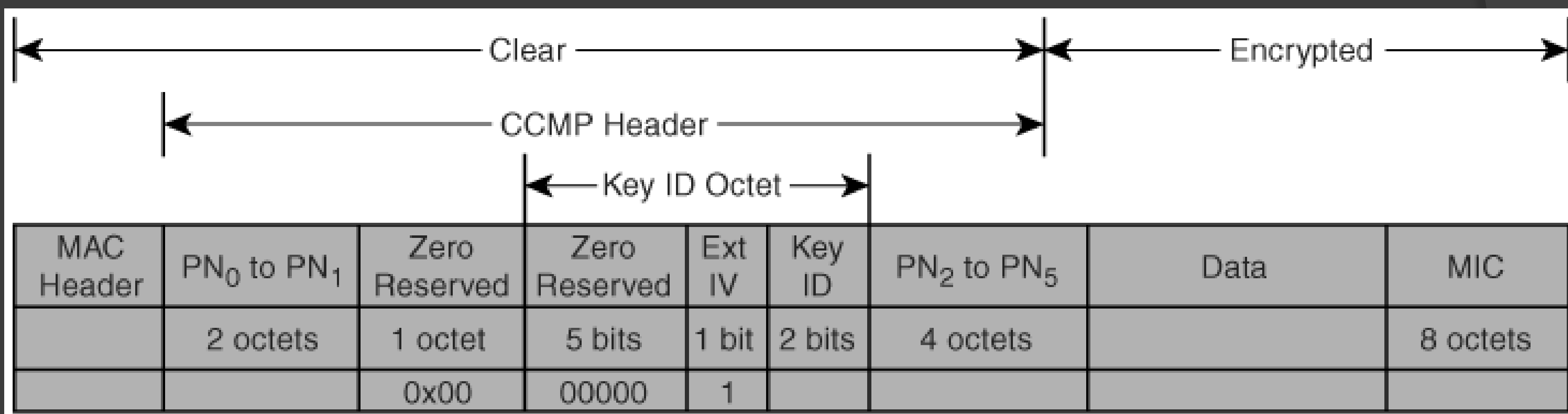
TKIP Decapsulation



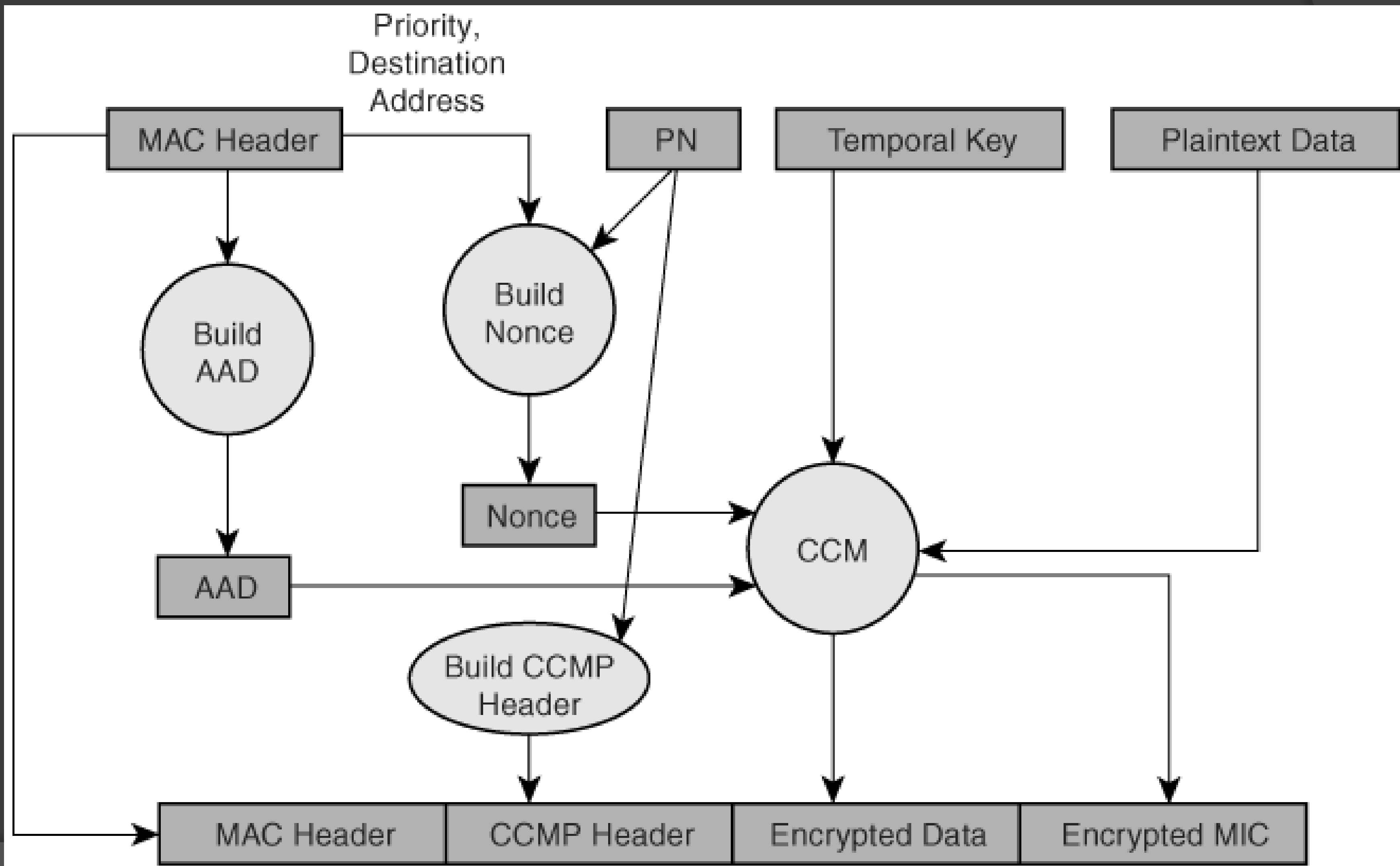
Counter Mode/CBC-MAC Protocol (CCMP)

- based on the Advanced Encryption Standard (AES)
- a stronger set of algorithms than TKIP and also provides confidentiality, integrity, and replay protection
- AES has several modes. CCMP uses the Counter mode for confidentiality and the CBC-MAC mode for integrity.

CCMP Packet (MPDU) Format



CCMP Encapsulation



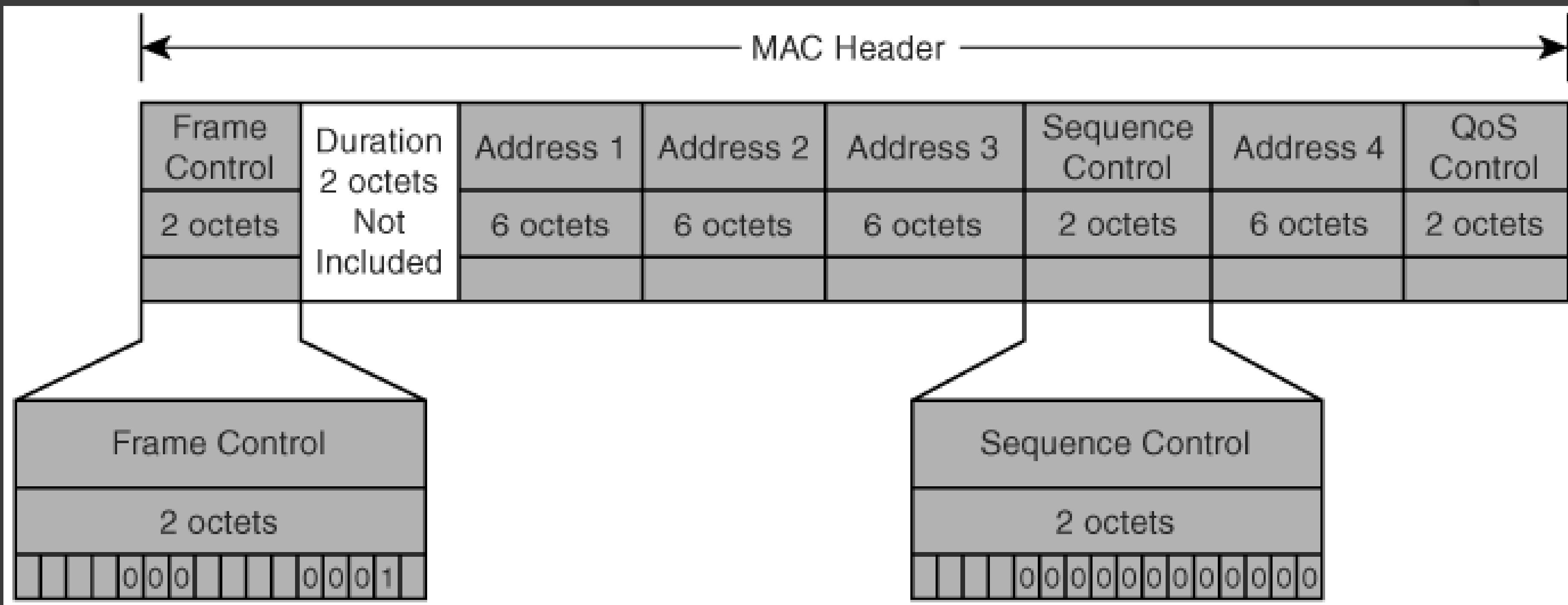
Confidentiality

- CCM encryption ensures the confidentiality of data.
- The block cipher encryption process prevents anyone without the key from reading the message that is in transit.
- The strength of the AES CTR mode and the protection of the key are the guarantees of this confidentiality.

Integrity

- CCM encryption includes the calculation of a Message Integrity Check (MIC) that ensures the integrity of data and includes protection from replay attacks.
- CCMP uses a different algorithm than TKIP does: the AES CBC-MAC mode.
- The MIC is calculated over the data plus some portions of the MAC header, called the Additional Authentication Data (AAD).

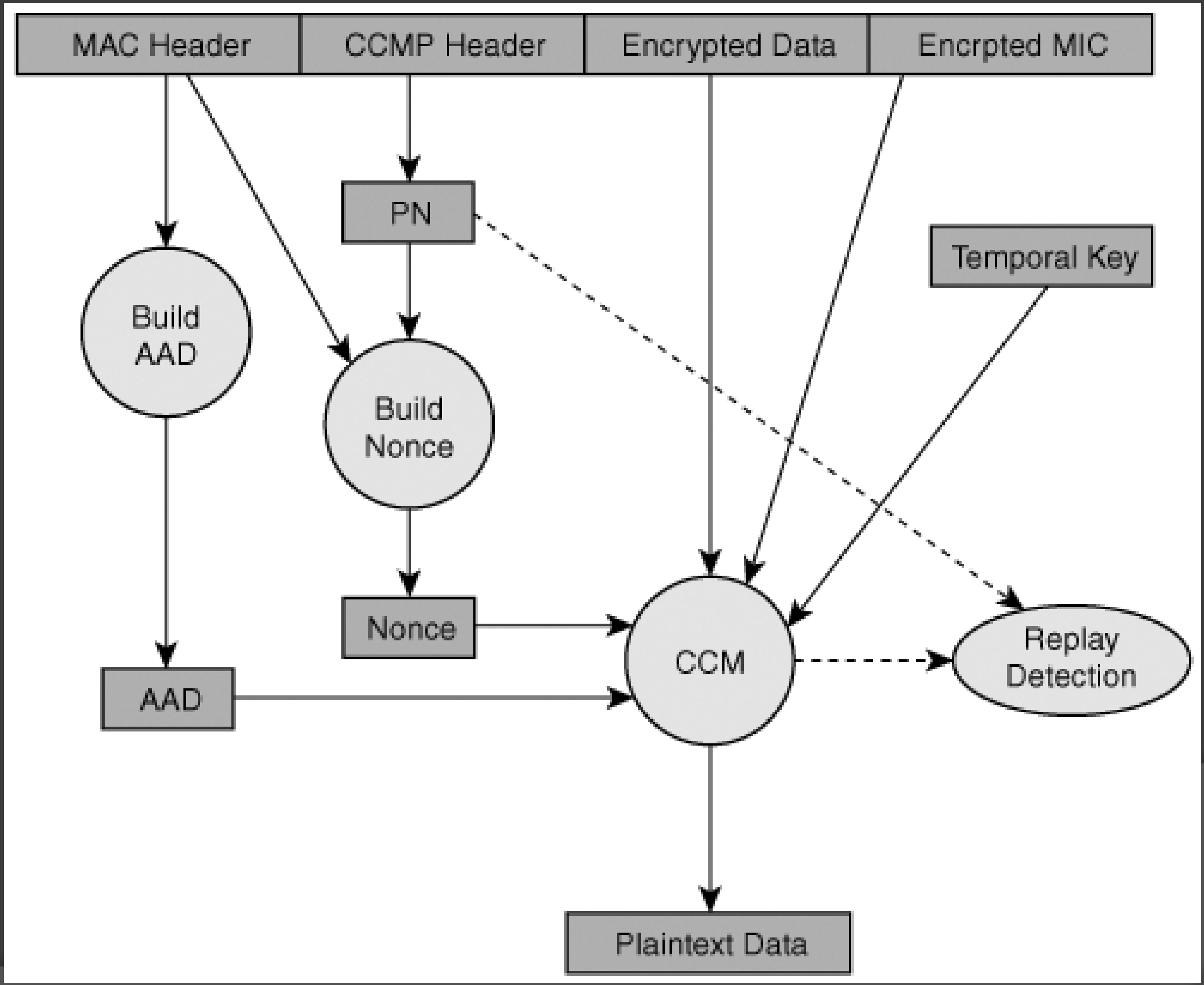
CCMP Additional Authentication Data Construction



Replay Prevention

- employs an incrementing packet counter (PN)
- Along with the destination address and the Priority field, the PN is part of a nonce.
- This nonce is included in the CCM encryption algorithm, and it helps ensure that the inputs to CCM are different with every packet.

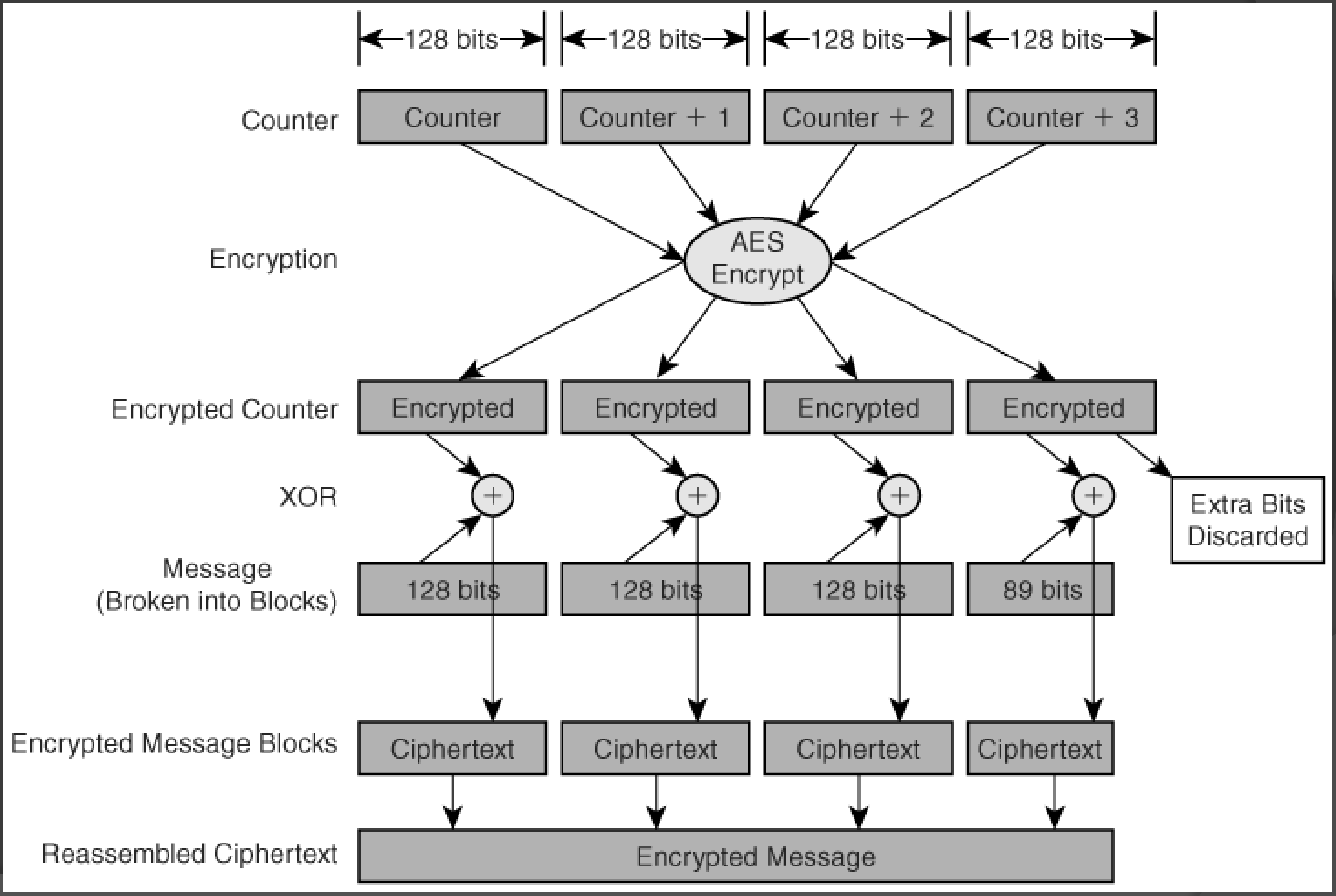
CCMP Decapsulation



CCM Algorithm

- AES is a block cipher.
- In CCM, AES takes a 128-bit chunk of data and returns a 128-bit chunk of encrypted data, when provided with a 128-bit key.
- CCM uses two AES modes of operation: Counter mode (CTR) for encryption and Cipher Block Chaining (CBC-MAC) to create the MIC.

AES Counter Mode



AES CBC-MAC Mode