Chap. 7 Wireless Network Security

- WiFi Security
- WEP (Wired Equivalent privacy)
- Robust Secure Network (IEEE 802.11i)

Vulnerability in Wireless Communication

- No physical contact to network infrastructure
  - physical connections replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure
- communications by broadcasting
  - radio signal is broadcasted in a transmission range
  - transmissions can be overheard by anyone in the range
  - anyone can generate transmissions, and anyone in the range can receive the messages
  - anyone can interfere with other nearby transmissions and may prevent their correct reception (jamming attack)

Vulnerability in Wireless Communication

Major concerns

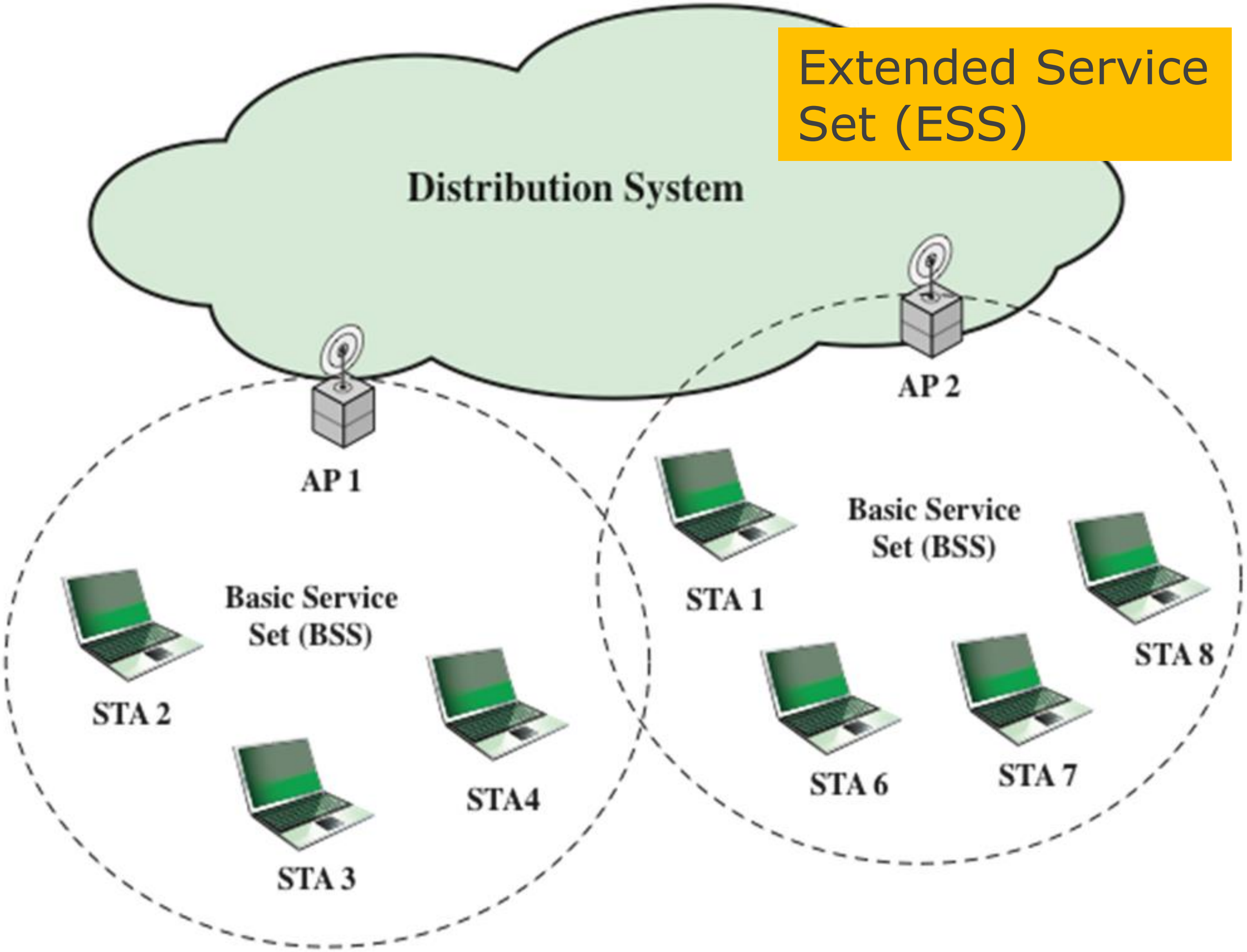
- eavesdropping is easy
- injecting bogus messages into network is easy
- replaying previously recorded messages is easy
- illegitimate access to the network and its services is easy
- denial of service by jamming messages is easy

Security Requirements in Wireless Networks

- Confidentiality: messages must be encrypted
- Authenticity: origin of messages must be verified
- Integrity: integrity of messages must be verified
- Protection from replay attacks: integrity of messages must be verified
- Access control: access to the network services should be provided only to legitimate entities
- Protection against jamming

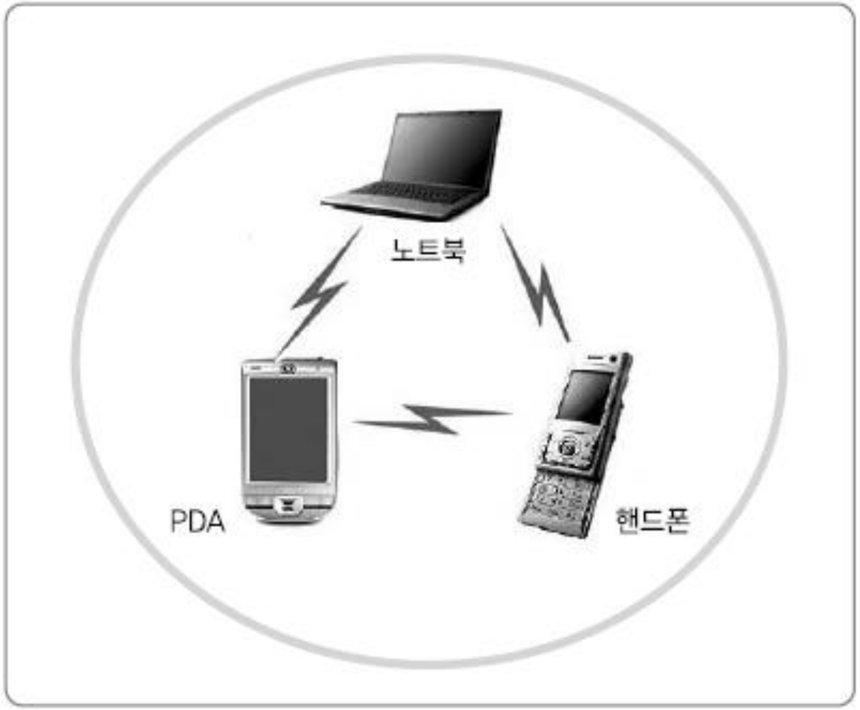
WLAN Components

- WLAN – infra-structured mode



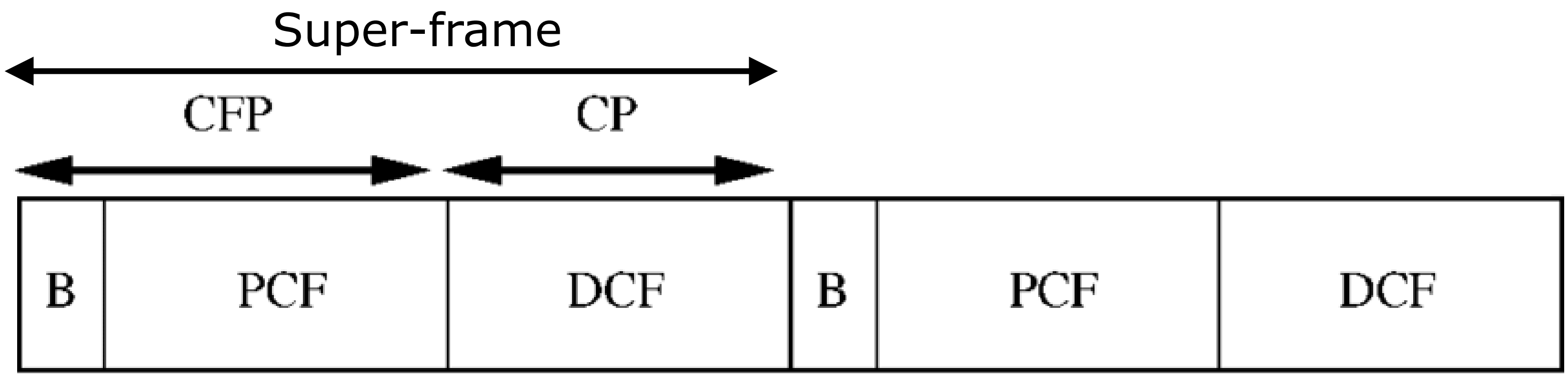
WLAN 구성요소

- WLAN 구조 – ad hoc mode



IEEE 802.11 Wireless MAC

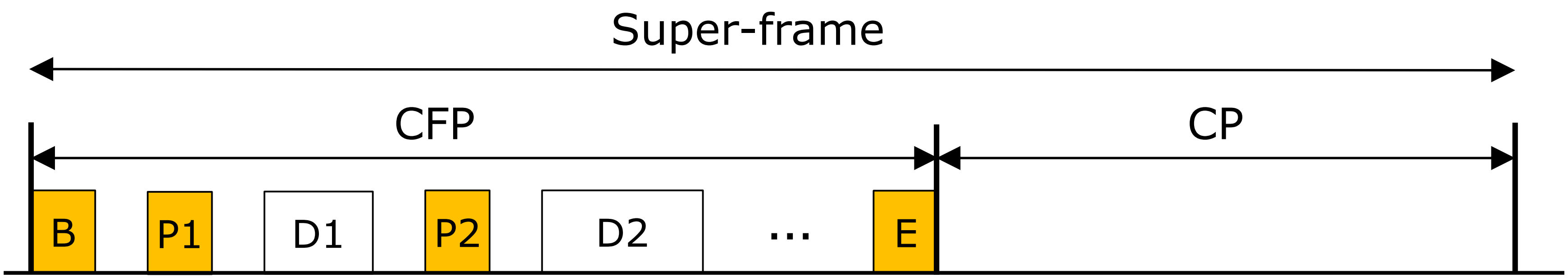
- Distributed and centralized MAC components
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)



B: beacon
CFP: contention free period
CP: contention period

IEEE 802.11 Wireless MAC

- Point Coordination Function (PCF)
  - polling to reserved nodes by AP (master)
  - super-frame structure

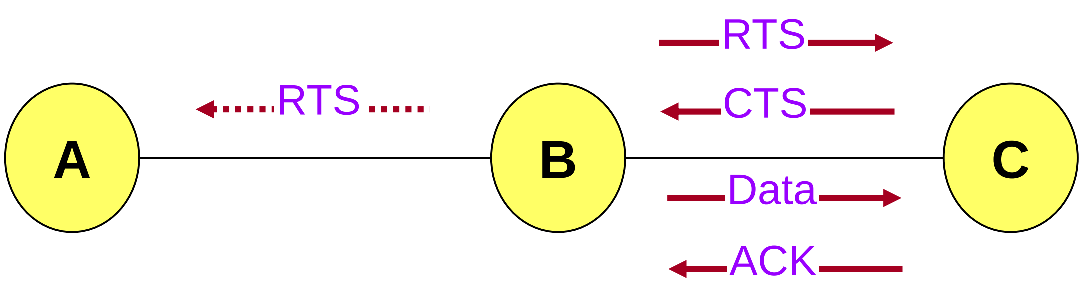


IEEE 802.11 Wireless MAC

- DCF suitable for multi-hop ad hoc networking
- DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol

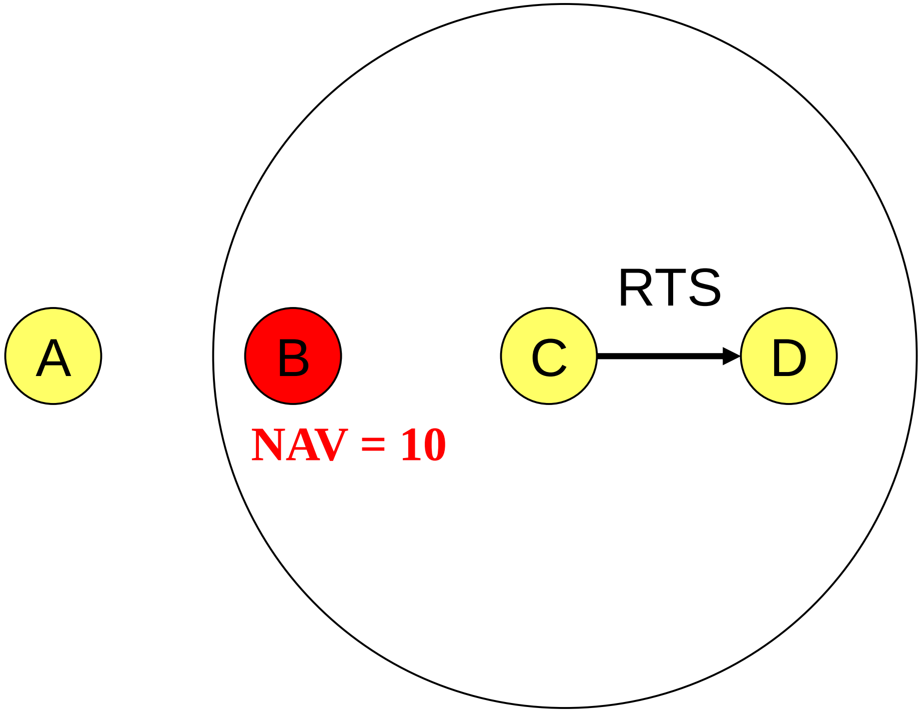
IEEE 802.11 DCF

- Carrier sensing
- RTS-CTS to avoid hidden terminal problem
  - Any node overhearing a CTS does not transmit for the duration of the transfer
- Uses ACK for reliability
- Virtual carrier sensing: any node receiving RTS or CTS cannot transmit during the transfer



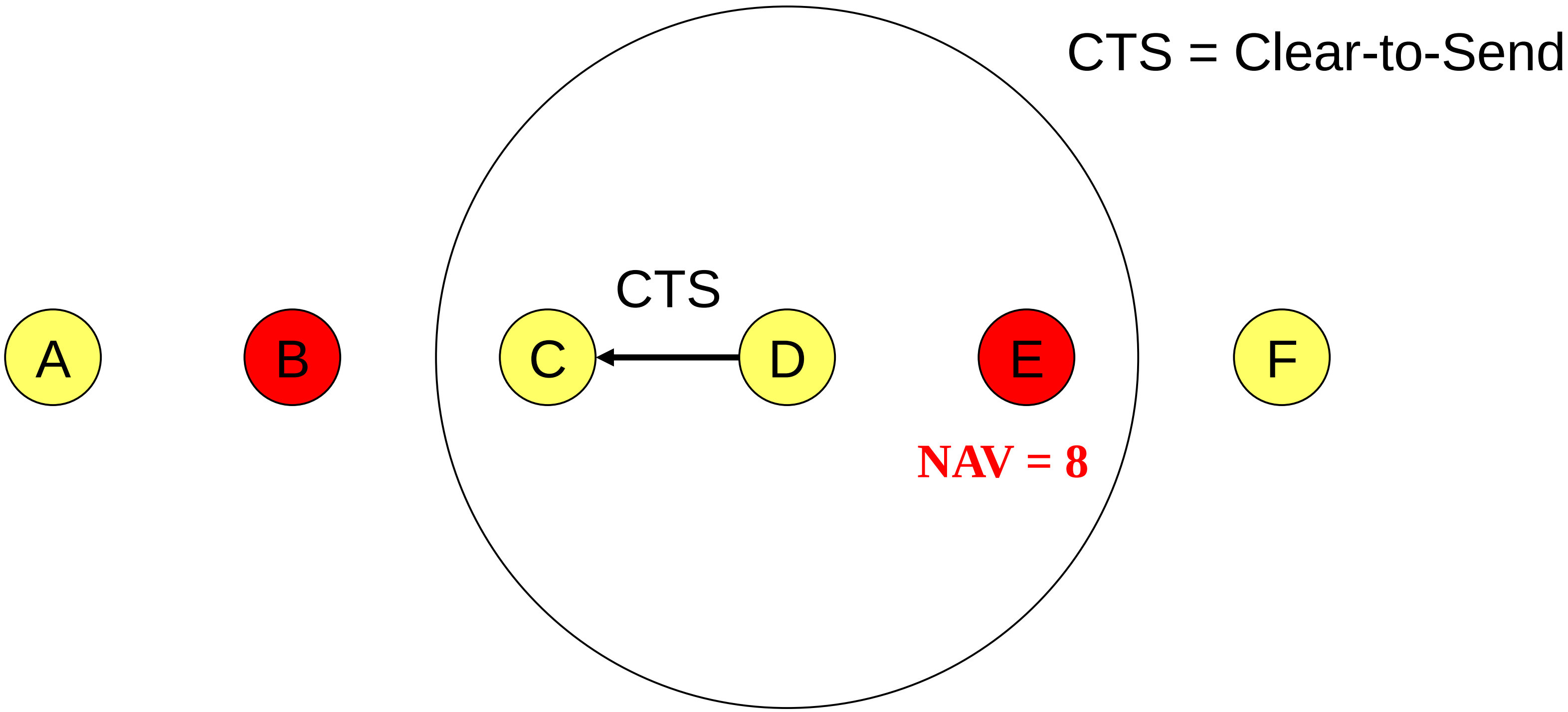
IEEE 802.11 DCF

RTS = Request-to-Send



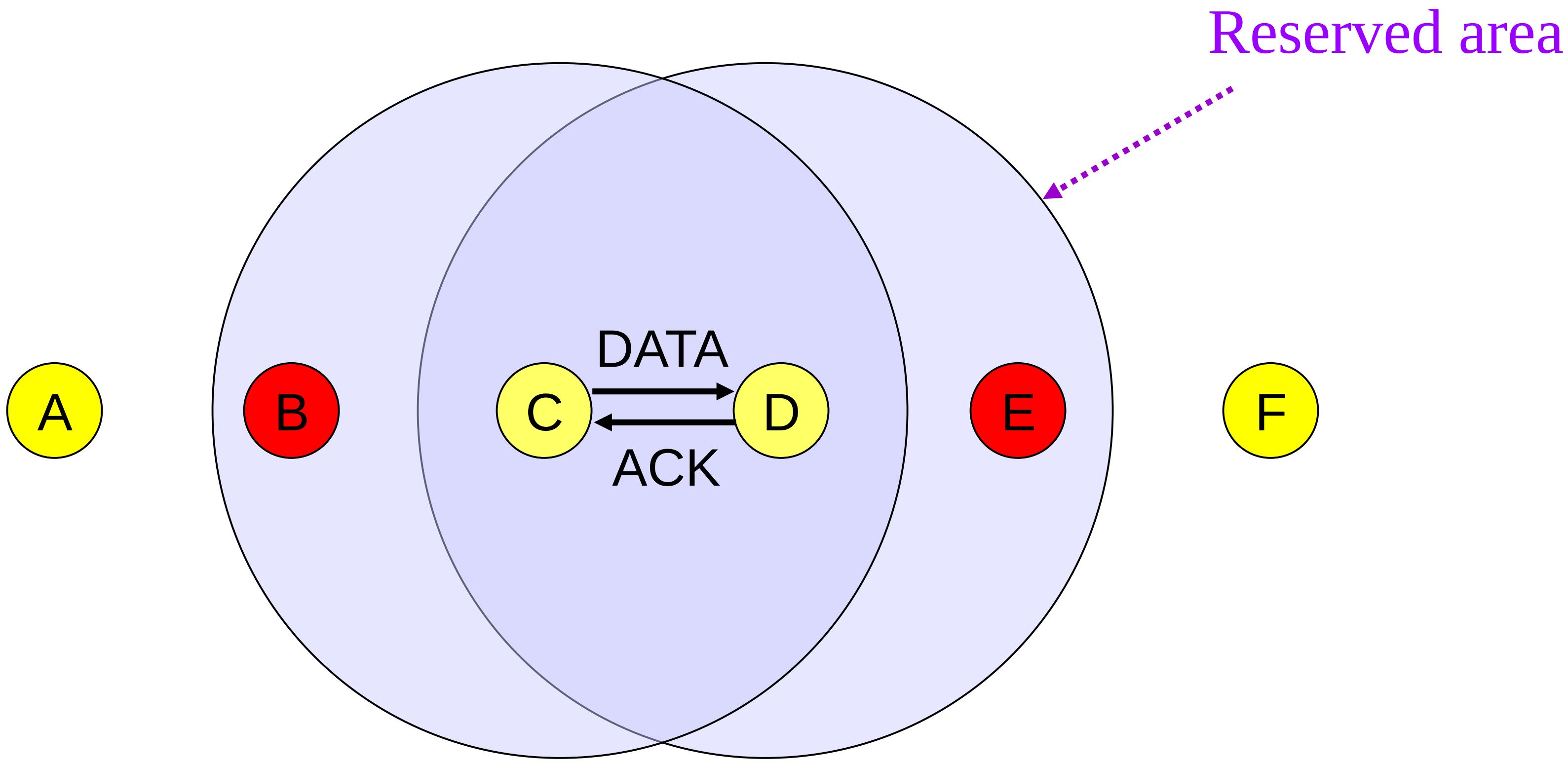
NAV = remaining duration to keep quiet

IEEE 802.11 DCF



IEEE 802.11 DCF

DATA packet follows CTS. Successful data reception acknowledged using ACK.



CSMA/CA

- Physical carrier sense, and
- Virtual carrier sense using Network Allocation Vector (NAV)
- NAV is updated based on overheard RTS-CTS-DATA-ACK packets

- Nodes stay silent when carrier sensed
- *Backoff intervals*
  - wait for random time if channel is busy
  - used to reduce collision probability

Backoff Interval

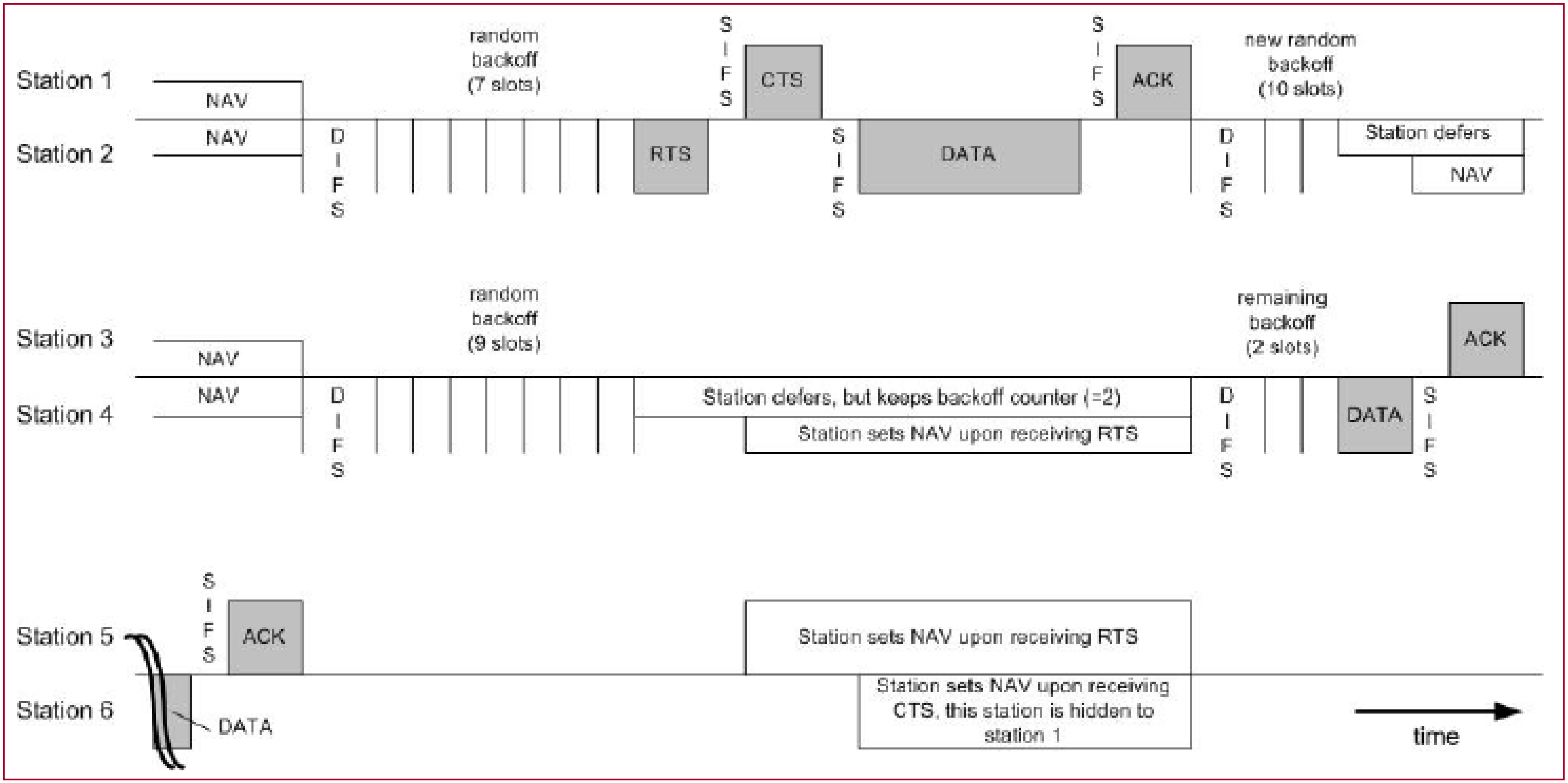
- When transmitting a packet, choose a backoff interval in the range [0,cw]
  - cw : contention window

- Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy

- When backoff interval reaches 0, transmit RTS

4-way Handshaking Protocol

- DCF mode: RTS → CTS → Data → ACK



Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
  - Choosing a *large cw* leads to large backoff intervals and can result in larger overhead
  - Choosing a *small cw* leads to a larger number of collisions (when two nodes count down to 0 simultaneously)

Backoff Interval

- The number of nodes attempting to transmit simultaneously may change with time $\rightarrow$ some mechanism to manage contention is needed

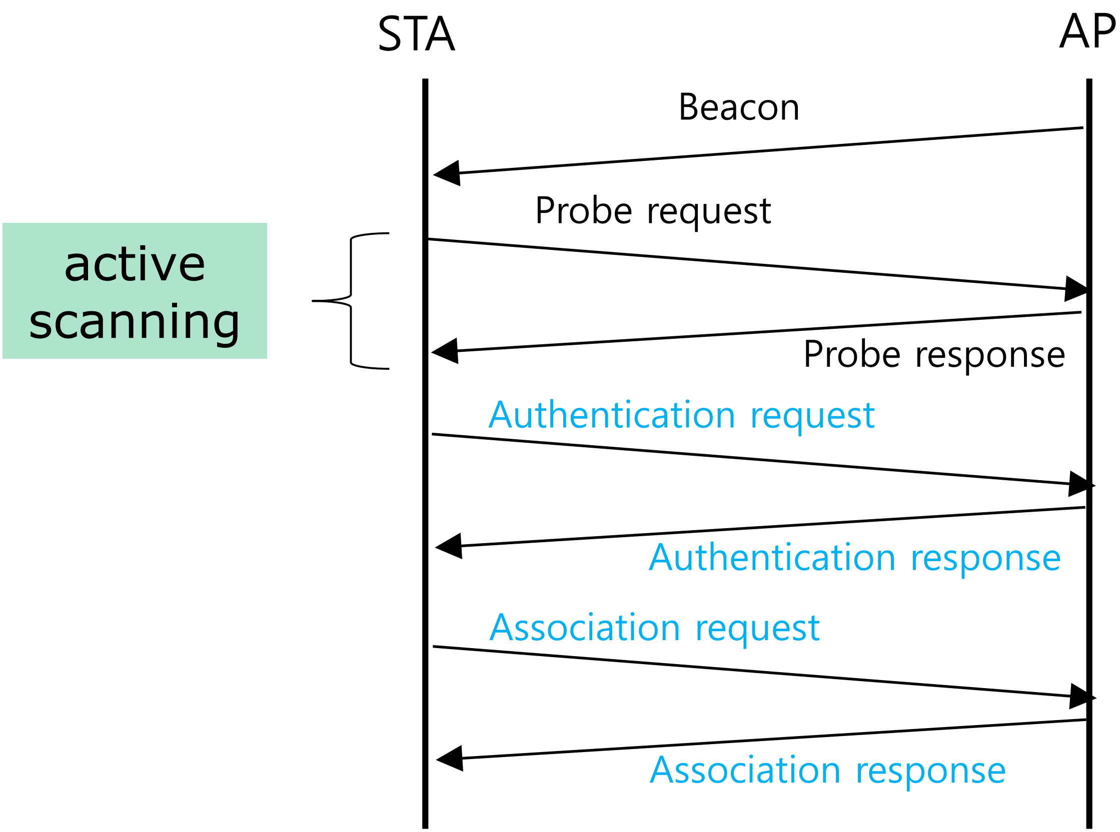
- IEEE 802.11 DCF: contention window *cw* is chosen dynamically depending on collision occurrence (the amount of traffic)

Binary Exponential Backoff in DCF

- When a node fails to receive CTS in response to its RTS, it increases the contention window
  - *cw* is doubled (up to an upper bound CW_{max})
- When a node successfully completes a data transfer, it restores *cw* to CW_{min}
- *cw* follows a saw-tooth curve
- *cw* denotes the amount of contention around the node

WiFi Communication

- Message exchange after association



Wired Equivalent Privacy (WEP)

- goal
  - make the WiFi network at least as secure as a wired LAN (that has no particular protection mechanisms)
  - WEP has never intended to achieve strong security

- services
  - access control to the network: association after authentication
  - message confidentiality
  - message integrity

WEP – Access Control

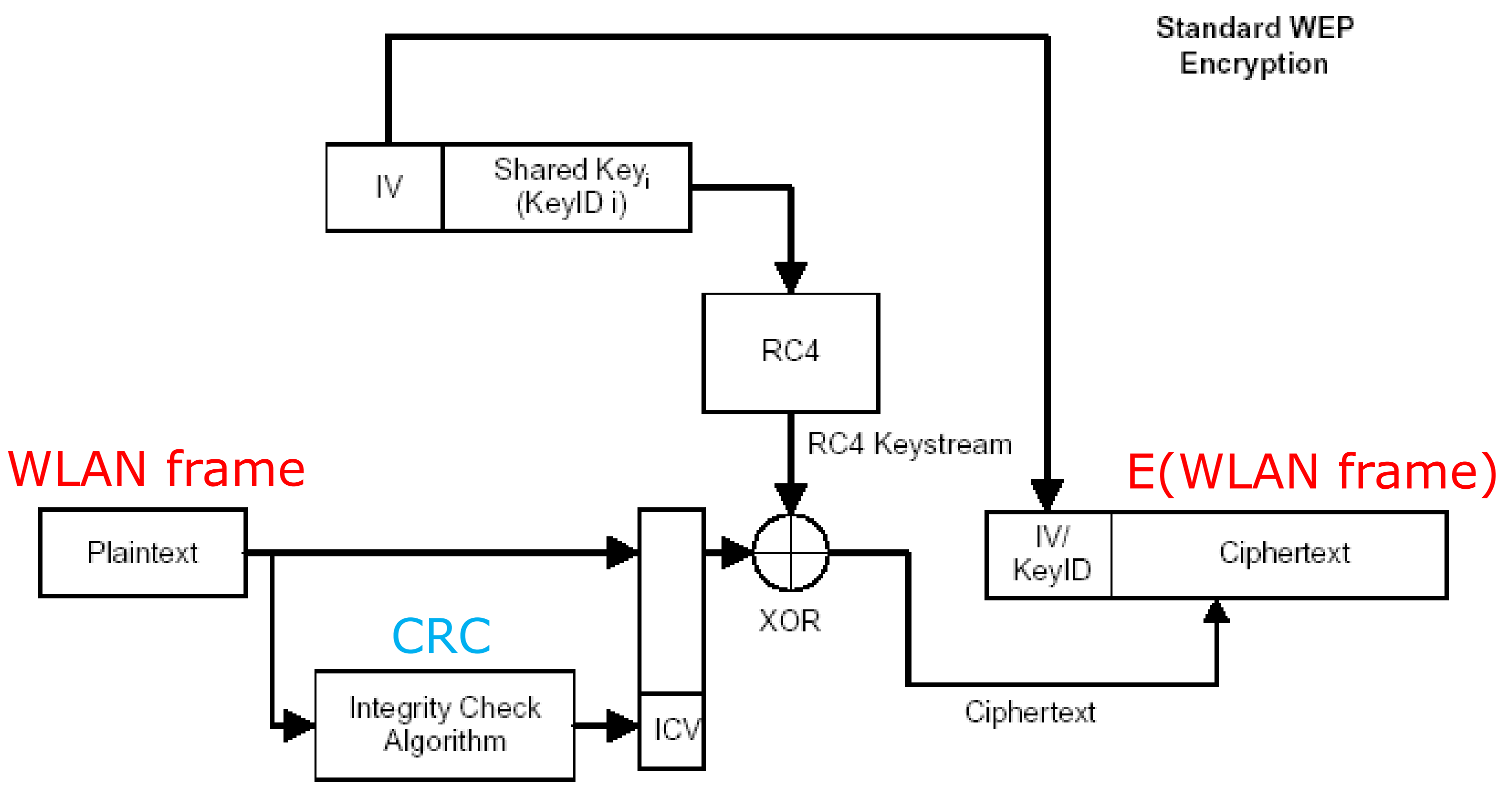
- before association, the STA needs to authenticate itself to the AP
- authentication based on challenge-response protocol:
  - STA → AP: authenticate request
  - AP → STA: r (authenticate challenge) // r is 128 bits long
  - STA → AP: $E_K(r)$ (authenticate response) // K: shared key
  - AP → STA: authenticate success/failure
- once authenticated,
  - the STA can send an association request, and the AP will respond with an association response
- if authentication fails, no association is possible

WEP – Encryption

- WEP encryption based on RC4 stream cipher
  - Encryption:
    - RC4 is initialized with the shared secret and IV (between STA and AP)
    - RC4 produces a pseudo-random byte sequence (key stream)
    - this pseudo-random byte sequence is XORed to the message
  - IV : use different 24-bit IV for each message
    - each message is encrypted with a different key stream
- WEP integrity protection based on encrypted CRC value
  - ICV (integrity check value) is computed and appended to the message
  - the message and the ICV are encrypted together to check integrity

WEP – Encryption

- WEP encryption based on RC4 stream cipher



WEP – Encryption

- two kinds of keys
  - default key : shared key or group key
  - key mapping keys : individual key or per-station key
- in practice, often only default keys are supported
  - the default key is manually installed in every STA and the AP
  - each STA uses the same shared secret key → any STA can decrypt other's messages
  - the default key is a group key, and group keys need to be changed when a member leaves the group → practically impossible to change the default key in every device simultaneously

WEP Flaws

- authentication is one-way
  - STA may associate to a rogue AP
- the same shared secret key is used for authentication and encryption
  - different keys for different functions are desirable
- no session key is established during authentication
  - access control is not continuous → once a STA has authenticated and associated to the AP, an attacker can send messages using the MAC address of STA
  - The attacker cannot decrypt the messages, but replay of STA messages is still possible

WEP Flaws

- STA can be impersonated
- authentication based on a challenge-response protocol:
  - (1) STA → AP ; authenticate request
  - (2) AP → STA: r ; authenticate challenge
  - (3) STA → AP: [IV | r ⊕ K] ; authenticate challenge

    where K is a 128 bit RC4 output on IV and shared secret
- an attacker can compute key: r ⊕ (r ⊕ K) = K
- then it can use T to impersonate STA later:
  - (1) attacker(STA) → AP ; authenticate request
  - (2) AP → attacker: r' ; authenticate challenge
  - (3) attacker → AP: [IV | r' ⊕ K] ; re-use the previous IV

WEP Flaws

- Integrity mechanism
  - [IV | (M | CRC(M)) $\oplus$ K] where K is the RC4 output on IV and shared secret
  - IV is not mandated to be changed for each message → ICV mechanism and encryption cannot protect from replay attack

WEP Flaws

Replay attack

- CRC is a linear function in terms of XOR:

  $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$

  $(A \mid B) \oplus (C \mid D) = (A \oplus C) \mid (B \oplus D)$

  | : concatenation

- attacker eavesdrops $[(M \mid CRC(M)) \oplus K]$ where K is the RC4 output; K is the RC4 output on IV and shared secret
- Attacker wants to change M to M' (= $M \oplus \Delta M$)
- for any ΔM, the attacker can compute $CRC(\Delta M)$
- hence, the attacker can compute:

  $\underline{((M \mid CRC(M)) \oplus K) \oplus (\Delta M \mid CRC(\Delta M))} =$

  $((M \oplus \Delta M) \mid (CRC(M) \oplus CRC(\Delta M))) \oplus K =$

  $((M \oplus \Delta M) \mid CRC(M \oplus \Delta M)) \oplus K = (M' \mid CRC(M')) \oplus K$

WEP Flaws

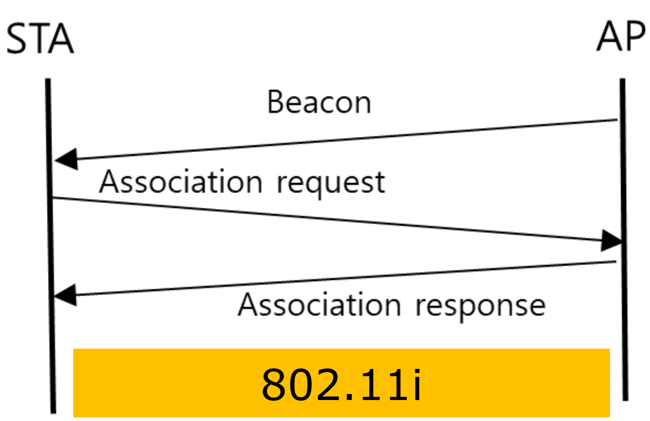
- RC4 encryption
  - weak keys: for some IVs, the beginning of the RC4 output is not really random and reveals key information

  - IV: 24bits is too small - there are 16,777,216 possible IVs
  - after around 17 million messages, IVs are reused
  - an AP at 54 Mbps is capable for transmitting 3400 packets per second → IV space is used up in around 1.5 hours
  - same IVs → same key streams; WEP encryption can be broken by capturing a few million messages

IEEE 802.11i

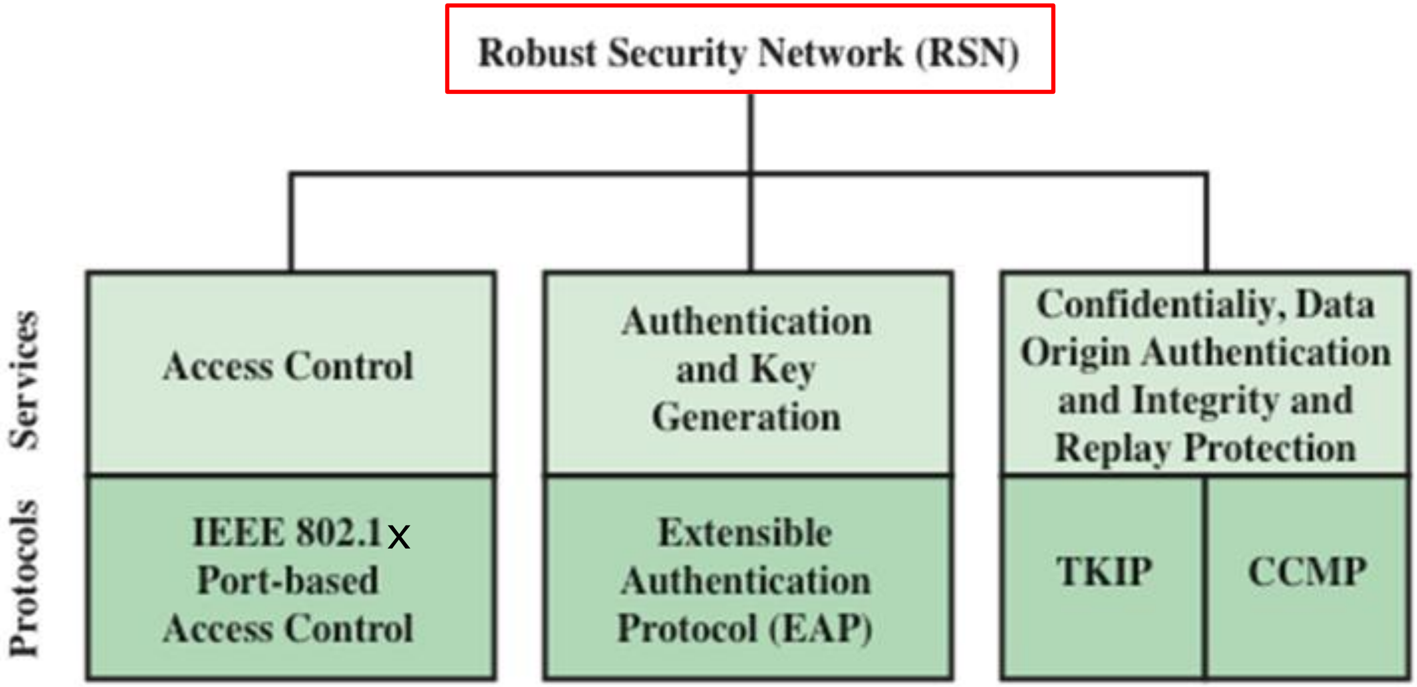
- Wi-Fi Protected Access (WPA)
  - A set of security mechanisms that eliminates WEP security issues
  - Based on the current state of the 802.11i standard

- Robust Security Network (RSN)
  - Final form of 802.11i standard
  - complex



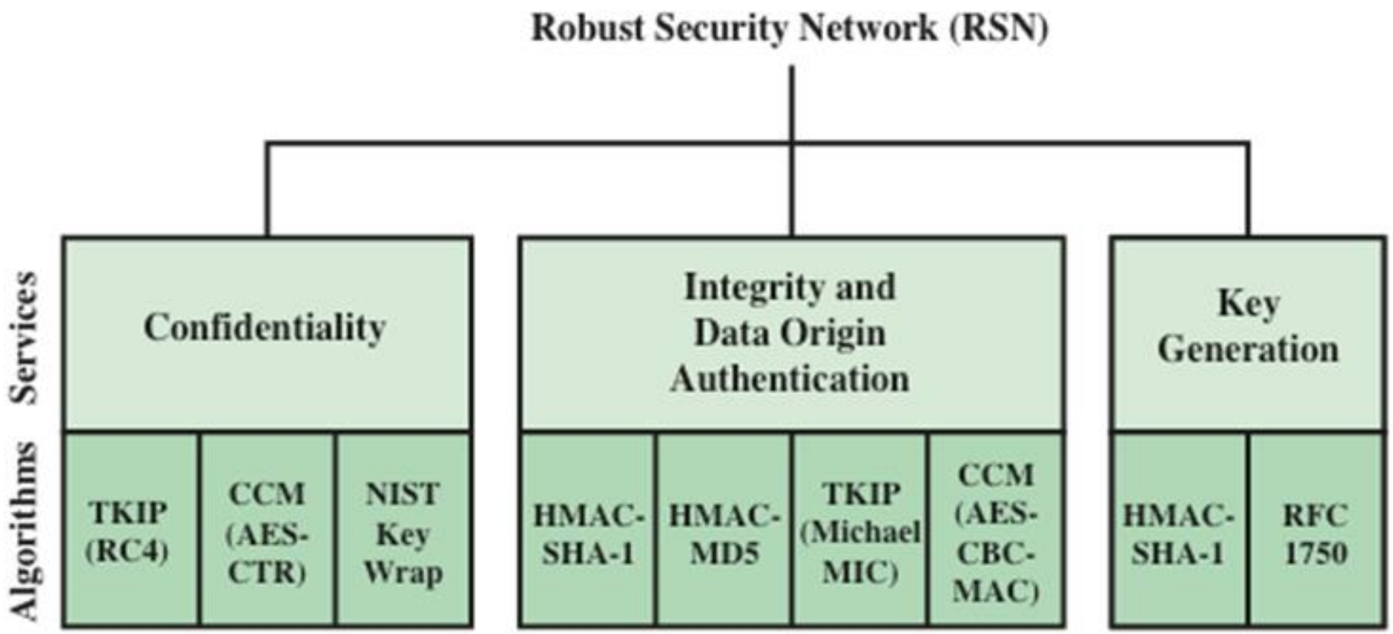
IEEE 802.11i

- Services and protocols



IEEE 802.11i

- Cryptographic algorithms

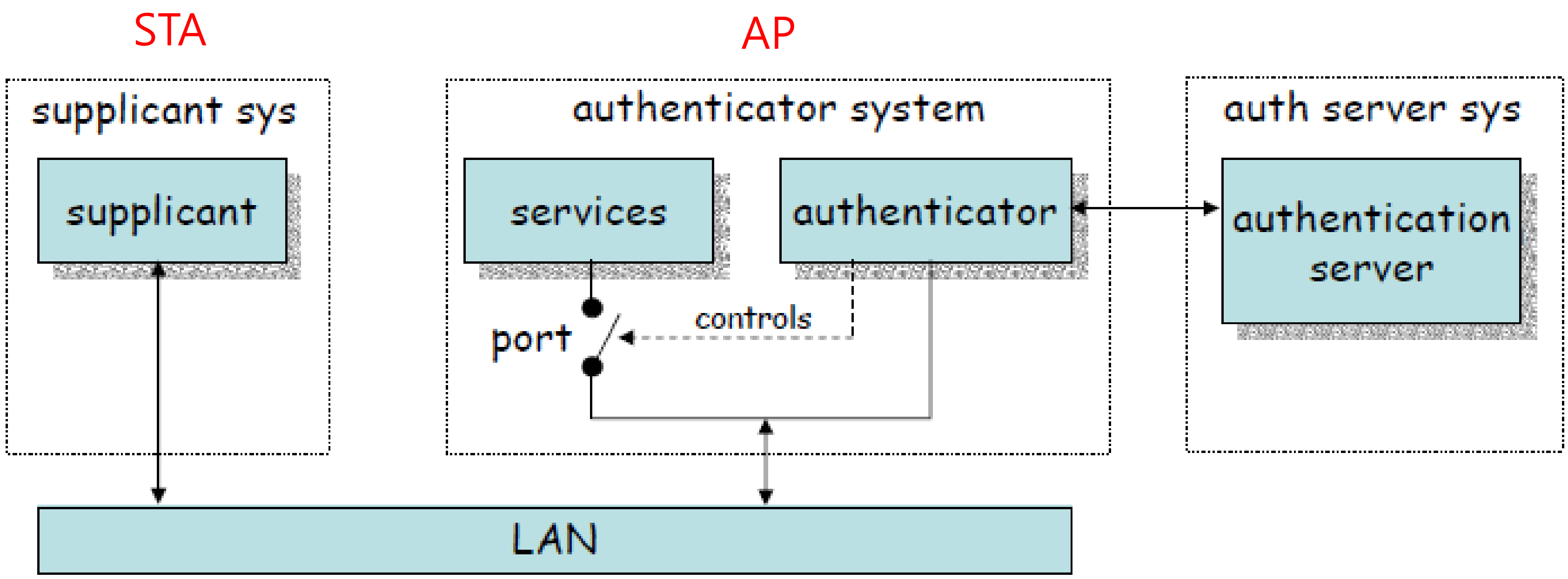


(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

IEEE 802.11i

- Port-based access control



IEEE 802.11i

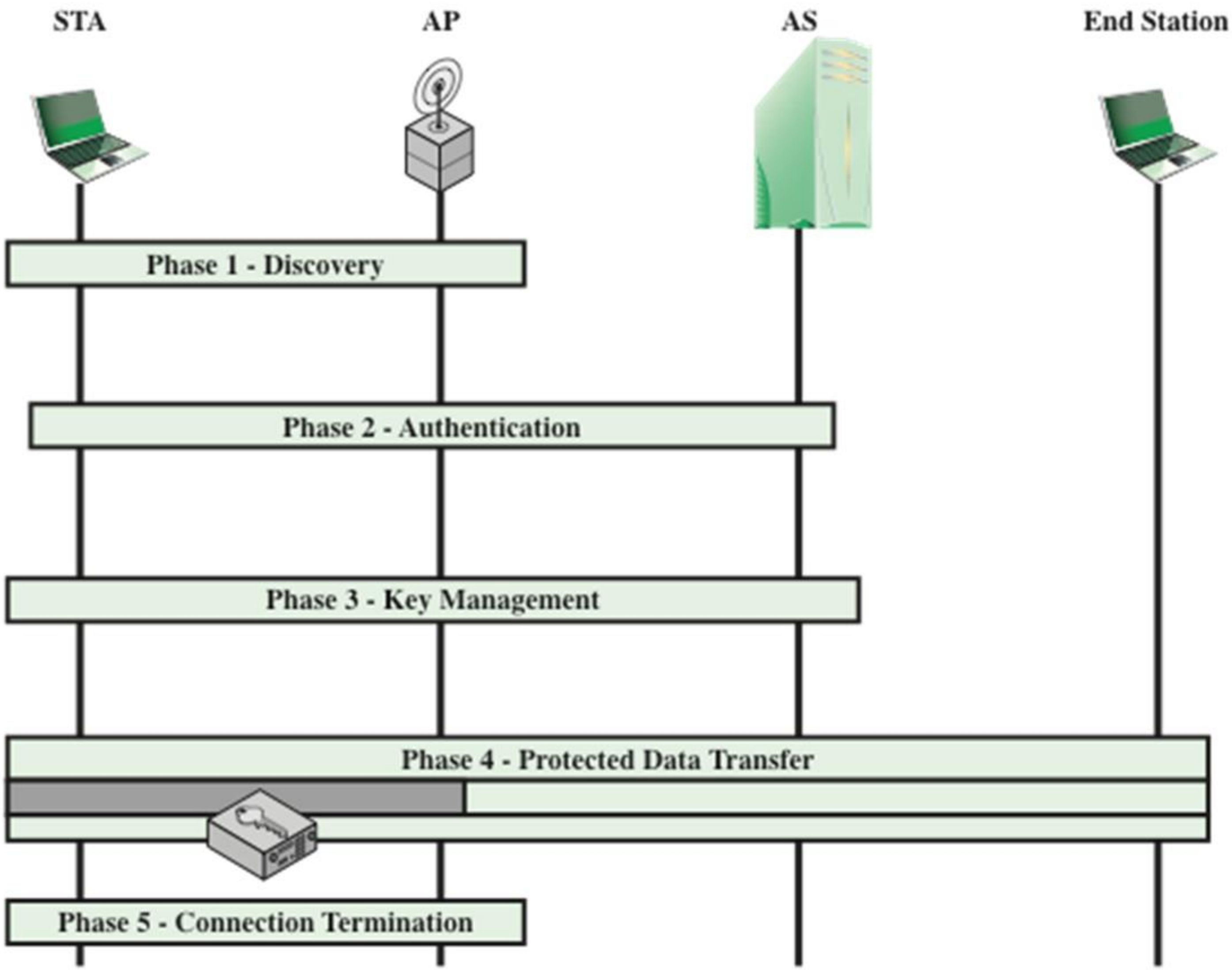
- supplicant requests access to the services
- authenticator
  - controls access to the services
  - controls the state of a port – port-based access control
- authentication server (AS) authorizes access to the services
  - the supplicant authenticates itself to the AS
  - if the authentication is successful, the AS instructs the authenticator to switch the port ON
  - the AS informs the supplicant that access is allowed
  - The AS sends a session key after encrypting using the shared secret key b/w the supplicant and the AS

IEEE 802.11i

- Port-based access control
  - Port - logical state implemented in software in the AP
  - Uncontrolled ports
    - Allows the exchange of only the authentication-related PDUs between the supplicant and the AS
  - Controlled ports
    - Allows the exchange of PDUs between a supplicant and other systems on the LAN after the supplicant is authenticated by AS

IEEE 802.11i

- Operation steps

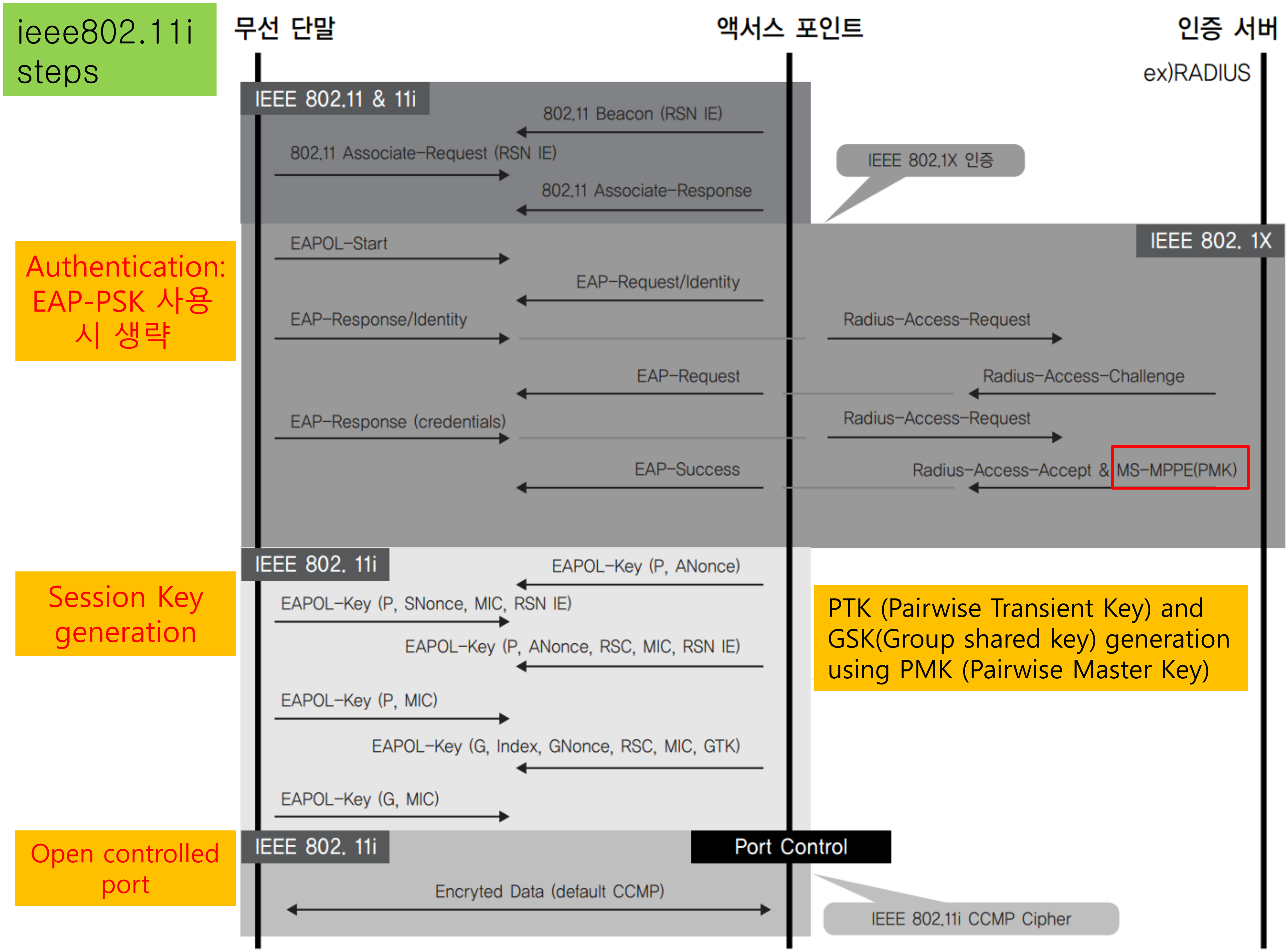


IEEE 802.11i

- Discovery
  - STA and AP recognize each other, agree on a set of security capabilities
  - Establish an association for future communication using the security capabilities
- Authentication
  - STA and AS prove their identities to each other
  - AP blocks non-authentication traffic b/w STA and AS until the authentication is successful

IEEE 802.11i

- Key generation and distribution
  - After the authentication, AP and STA perform some operation and message exchange to generate and share the session key
- Protected data transfer
  - Encrypted frames exchanged b/w STA and end stations thru AP



ieee802.11i steps
무선 단말
액세스 포인트
인증 서버
ex)RADIUS
IEEE 802.11 & 11i
802.11 Beacon (RSN IE)
802.11 Associate-Request (RSN IE)
802.11 Associate-Response
IEEE 802.1X 인증
IEEE 802. 1X
Authentication: EAP-PSK 사용 시 생략
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Radius-Access-Request
EAP-Request
Radius-Access-Challenge
EAP-Response (credentials)
Radius-Access-Request
EAP-Success
Radius-Access-Accept & MS-MPPE(PMK)
IEEE 802. 11i
Session Key generation
EAPOL-Key (P, ANonce)
EAPOL-Key (P, SNonce, MIC, RSN IE)
EAPOL-Key (P, ANonce, RSC, MIC, RSN IE)
EAPOL-Key (P, MIC)
EAPOL-Key (G, Index, GNonce, RSC, MIC, GTK)
EAPOL-Key (G, MIC)
PTK (Pairwise Transient Key) and GSK(Group shared key) generation using PMK (Pairwise Master Key)
Open controlled port
IEEE 802. 11i
Port Control
Encryted Data (default CCMP)
IEEE 802.11i CCMP Cipher