802.11 Wireless

Review of Wi-Fi

Sniffing Wi-Fi

WEP

802.11i

IEEE 802.11 Wireless LAN

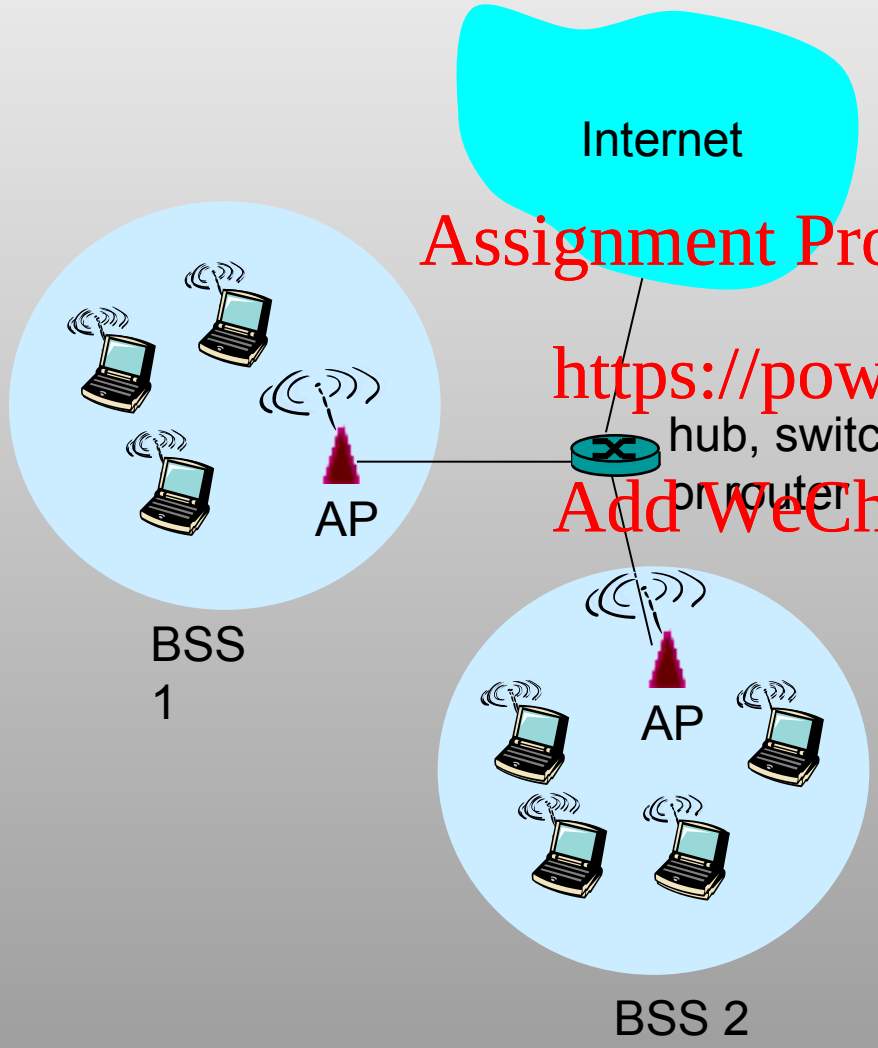
802.11b
- 2.4-2.485 GHz unlicensed radio spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer: all hosts use same chipping code

802.11a
- 5-6 GHz range
- up to 54 Mbps
- Physical layer: orthogonal frequency division multiplexing (OFDM)

802.11g
- 2.4-2.485 GHz range
- up to 54 Mbps
- OFDM

- All use CSMA/CA for multiple access
- All have base-station and ad-hoc versions
- All allow for reducing bit rate for longer range

802.11 LAN architecture

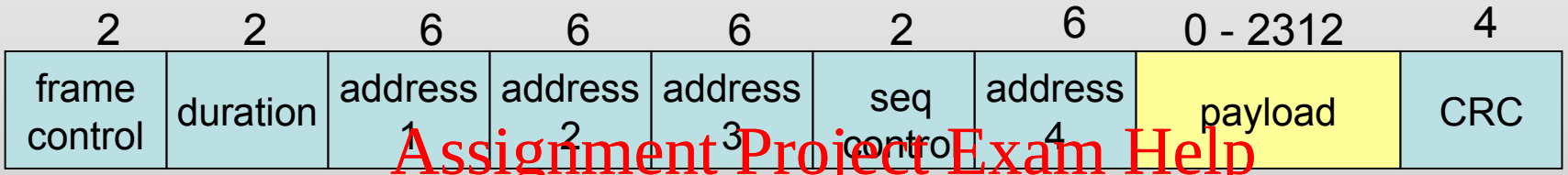


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

Channels, beacon frames & association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies; 3 non-overlapping
- AP admin chooses frequency for AP
- Interference possible: channel can be same as that chosen by neighboring AP!
- AP regularly sends beacon frame
- Includes SSID, beacon interval (often 0.1 sec)
- host: must associate with an AP
- scans channels, listening for beacon frames
- selects AP to associate with; initiates association protocol
- may perform authentication
- After association, host will typically run DHCP to get IP address in AP's subnet

802.11 frame: addressing



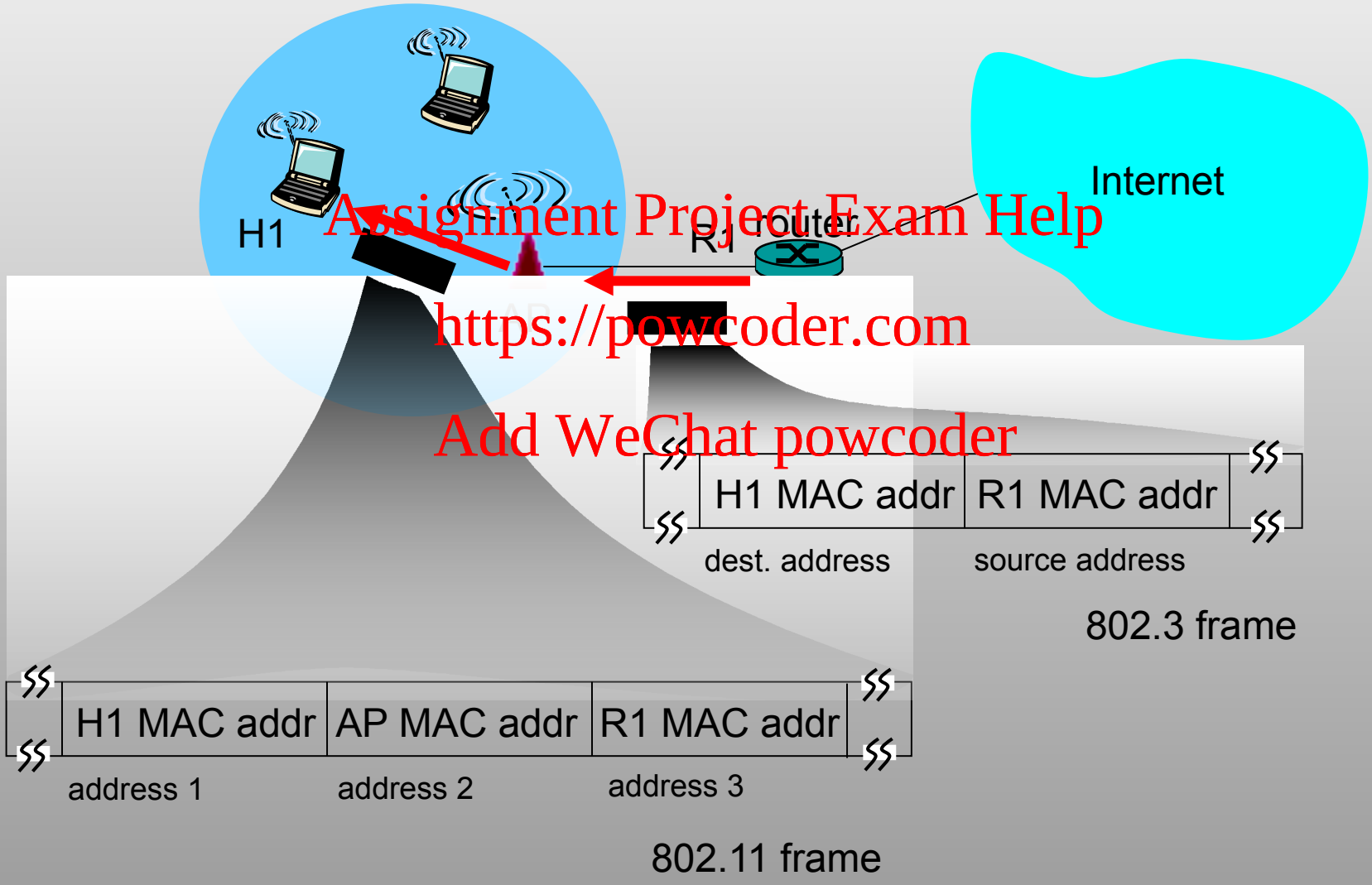
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

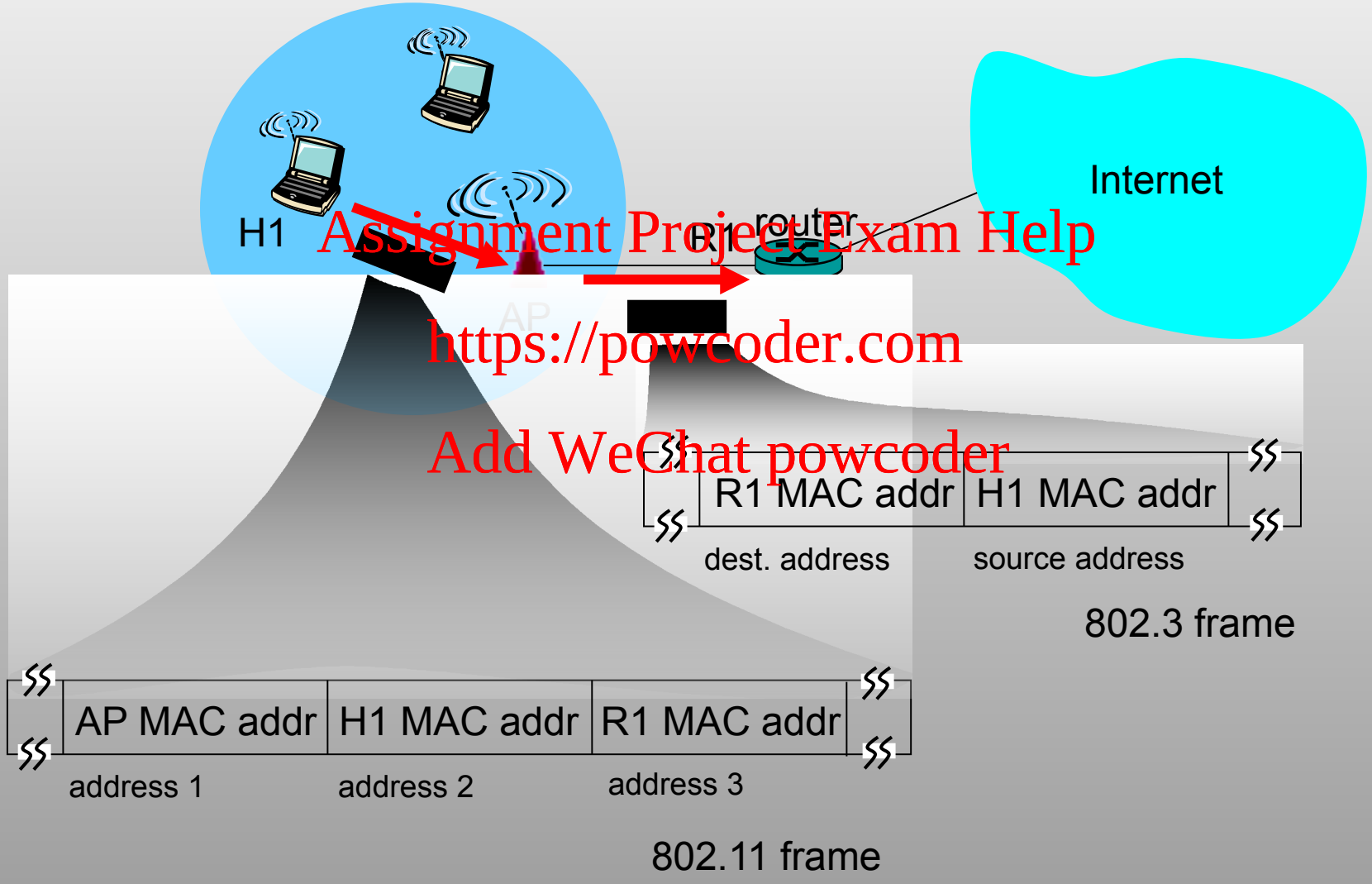
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

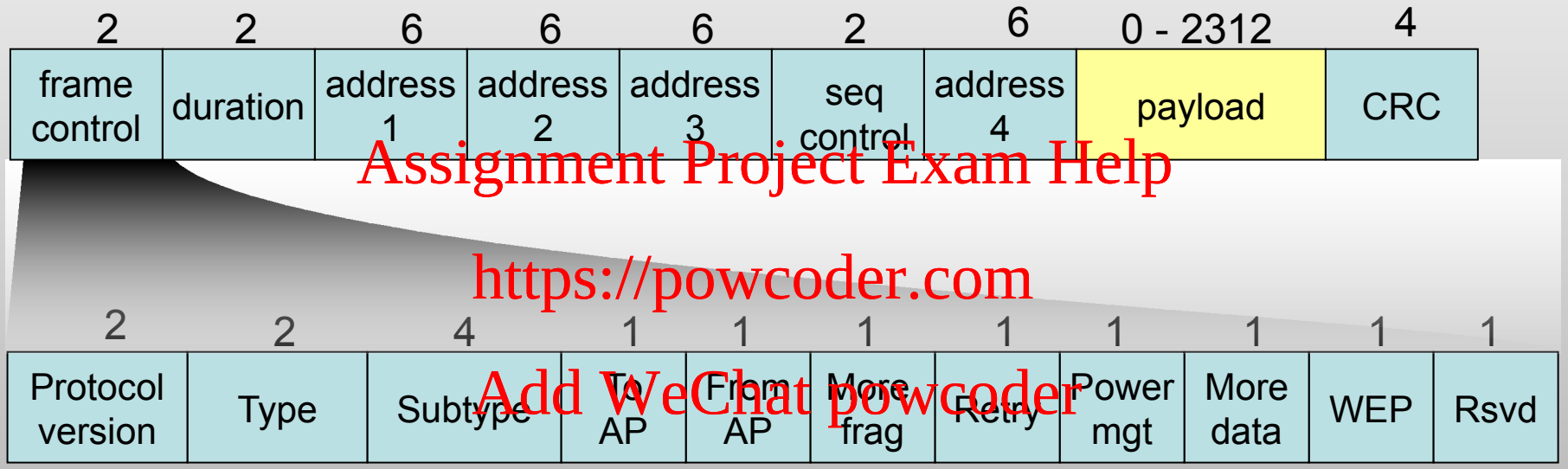


802.11 frame: addressing



802.11 frame (more)

frame:



frame control field expanded:

- Type/subtype distinguishes beacon, association, ACK, RTS, CTS, etc frames.
- To/From AP defines meaning of address fields
- 802.11 allows for fragmentation at the link layer
- 802.11 allows stations to enter sleep mode
- Seq number identifies retransmitted frames (eg, when ACK lost)
- WEP = 1 if encryption is used

Sniffing Encrypted 802.11 traffic

Suppose:

Traffic encrypted with symmetric crypto

Attacker can sniff but can't break crypto

What's the damage?

SSID, Mac addresses

Manufacturers of cards from MAC addrs

Count # of devices

Traffic analysis:

Size of packets

Timing of messages

Determine apps being used

But cannot see anything really useful

Attacker needs the keys !

Attacks on keys

- Attacker can get keys from disgruntled employee or sloppy administration.
- Possible solution: put key in hardware or software & don't make key visible to humans. Problems:
- Attacker gets access to equipment with key
- With good technical skills, attacker can extract key
- Ex: large corporation puts key in flash memory of all its devices
- Someone clever extracts key, publishes it on Web, destroying corporate security solution

WEP Feature Goals:

- Authentication
- AP only allows authorized stations to associate
- Data integrity
- Data received is the data sent
- Confidentiality
- Symmetric encryption

WEP Design Goals

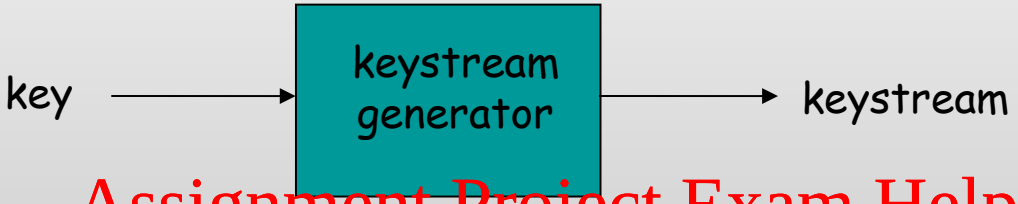
- Symmetric key crypto
- Confidentiality
- Station authorization
- Data integrity
- Self synchronizing: each packet separately encrypted
- Given encrypted packet and key, can decrypt; can continue to decrypt packets when preceding packet was lost
- Unlike Cipher Block Chaining (CBC) in block ciphers
- Efficient
- Can be implemented in hardware or software

WEP Keys

- 104 bits
- Key distribution not covered in standard
- Configure manually:
- At home
- Small organization with tens of users
- Nightmare in company >100 users
- Four default keys: 0,1,2,3
- Key 0 is initially active at AP and hosts.

- Administrator tells users: "must change to key 1 before date Z"
- During transition: old key users and new key users.
- AP encrypts with old key but decrypts with both old and new.
- Node advertises its key ID in keyID field
- At deadline, AP encrypts and decrypts only with new key
- Four keys allow for *directional key use*
- AP can use different key than hosts

Review: Symmetric Stream Ciphers

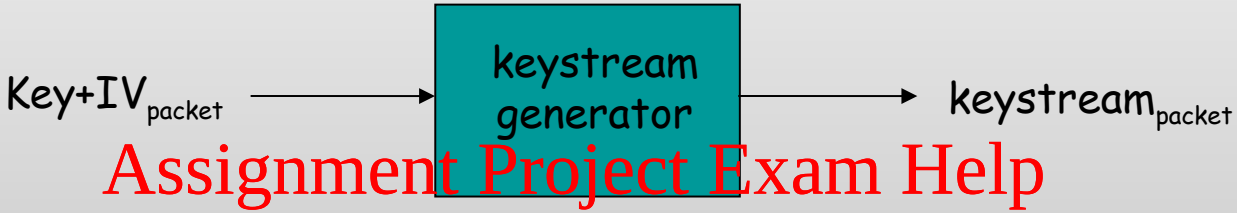


Combine each byte of keystream with byte of plaintext to get ciphertext

m(i) = ith unit of message
ks(i) = ith unit of keystream

c(i) = ith unit of ciphertext
$c(i) = ks(i) \oplus m(i)$ ($\oplus$ = exclusive or)
$m(i) = ks(i) \oplus c(i)$
WEP uses RC4

Stream cipher and packet independence

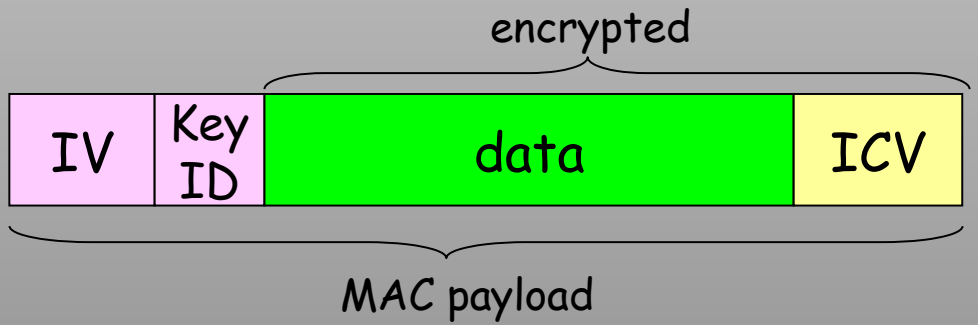


- Recall design goal: each packet separately encrypted
- If for frame n+1, use keystream from where we left off for frame n, then each frame is not separately encrypted

- Need to know where we left off for packet n
- WEP approach: initialize keystream with key + new IV for each packet:

WEP encryption (1)

- Sender calculates Integrity Check Value (ICV) over data
- four-byte hash/CRC for data integrity
- Each side has 104-bit shared key
- Sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key
- Sender also appends keyID (in 8-bit field)
- 128-bit key inputted into pseudo random number generator to get keystream
- data in frame + ICV is encrypted with RC4:
- Bytes of keystream are XORed with bytes of data & ICV
- IV & keyID are appended to encrypted data to create payload
- Payload inserted into 802.11 frame



WEP encryption (2)

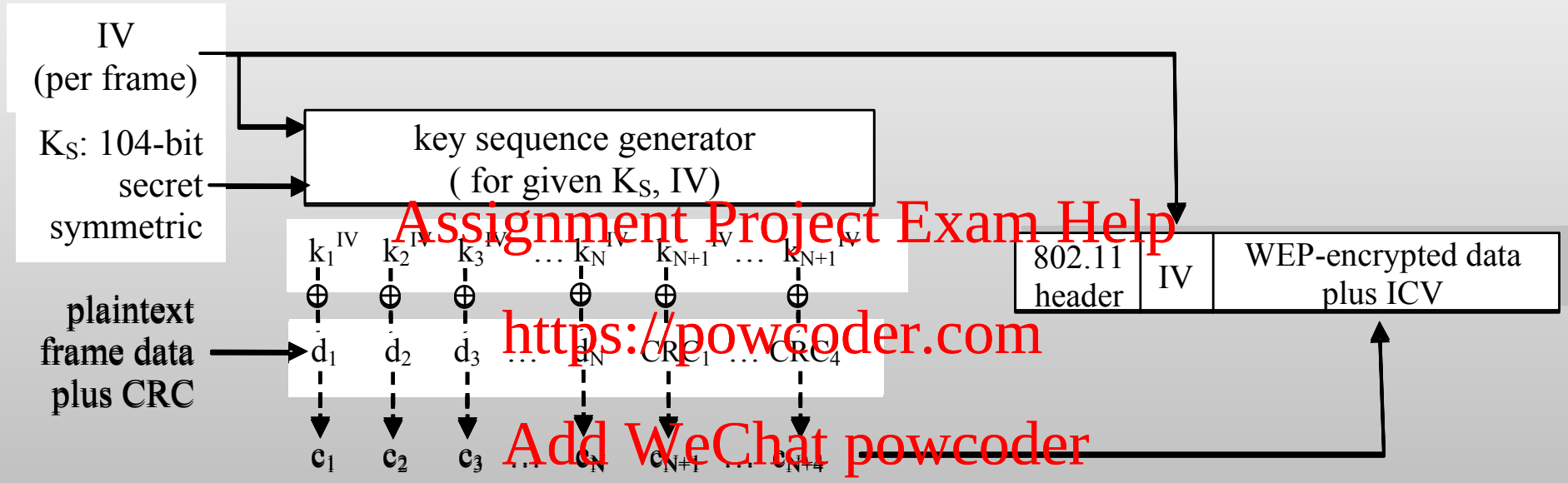


Figure 7.8-new1: 802.11 WEP protocol

New IV for each frame

WEP decryption overview

Receiver extracts IV

Inputs IV and shared secret key into pseudo random generator, gets keystream

XORs keystream with encrypted data to decrypt data + ICV

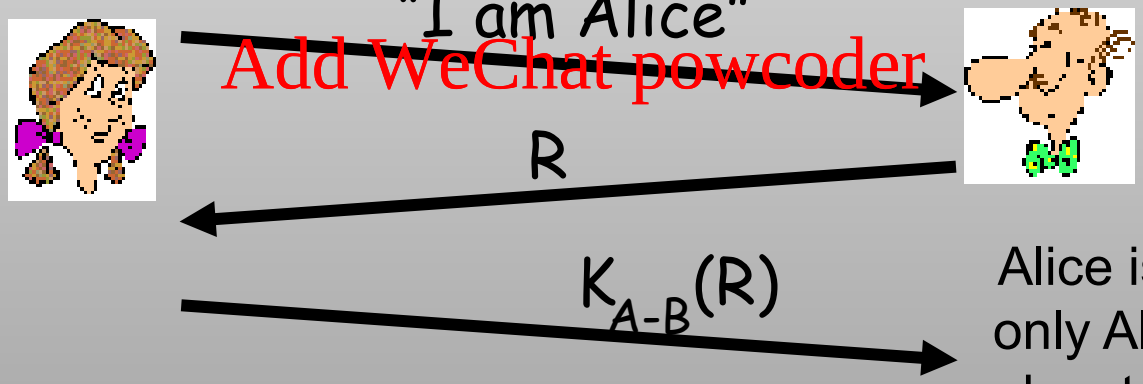
Verifies integrity of data with ICV

Note that message integrity approach used here is different from the MAC (message authentication code) and signatures (using PKI).

End-point authentication w/ nonce

Nonce: number (R) used only *once –in-a-lifetime*

How: to prove Alice "live", Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

WEP Authentication

Not all APs do it, even if WEP is being used. AP indicates if authentication is necessary in beacon frame. Done before association.

AP

authentication request

nonce (128 bytes)

nonce encrypted shared key

success if decrypted value equals nonce

WEP is flawed

Message integrity problems

Message privacy problems

WEP authentication problems

Plaintext attack

- Attacker sniffs nonce, m, sent by AP
- Attacker sniffs response sent by station:
- IV in clear
- Encrypted nonce, c
- Attacker calculates keystream ks = m ⊕ c, which is the keystream for the IV.
- Attacker then requests access to channel, receives nonce m'
- Attacker forms response c' = ks ⊕ m' and IV
- Server decrypts, matches m' and declares attacker authenticated !

Problems with Message Integrity

- ICV (Integrity Check Value) supposed to provide data integrity
- ICV is a hash/CRC calculation, but a flawed one.
- Can predict which bits in ICV change if you change single bit in data.
- Suppose attacker knows that flipping bit 3244 of plaintext data causes bits 2,7,23 of plaintext ICV to flip
- Suppose attacker intercepts a frame:
- In intercepted encrypted frame, attacker flips bit 3244 in data payload and ICV bits 2,7,23
- Will ICV match after decryption at the receiver?
- After decryption, cleartext bit 3244 is flipped (stream cipher)
- Also after decryption, cleartext bits 2,7, 23 also flipped.
- So cleartext ICV will match up with data!

Problems with WEP confidentiality (1)

- IV is 24 bits; incremented by 1 for each packet
- 2^{24} (approx 17 million) different IV values
- If you know keystream for every IV, can decrypt all frames
- 1500-byte keystream for all possible IVs: 23 Gybytes of storage – feasible
- How do you get the keystream for an IV ?

Problems with WEP confidentiality (2)

IV reuse

- With 17 million IVs and 500 full-length frames/sec, collisions start after 7 hours
- Worse when multiple hosts start with IV=0
- IV reuse:
- Trudy guesses some of Alice's plaintext $d_1\ d_2\ d_3\ d_4\ \ldots$
- Trudy sniffs: $c_i = d_i \oplus k_i^{IV}$
- Trudy computes keystream $k_i^{IV} = c_i \oplus d_i$
- Trudy knows encrypting keystream k_1^{IV} $k_2^{IV}\ k_3^{IV}\ \ldots$
- Next time IV is used, Trudy can decrypt!

Worse: Weak Key Attack

- Mathematical, complicated,
- For certain key values (weak keys), disproportionate number of bits in first few bytes of the keystream are determined by just a few key bits.
- As the IV cycles, wait for weak keys
- Exploit weak keys to crack the key
- Effort is only linear in key size!
- Cracker script tool available

Summary of WEP flaws

One common shared key
- If any device is stolen or compromised, must change shared key in all devices
- No key distribution mechanism
- Infeasible for large organization: approach doesn't scale

Crypto is flawed
- Early 2001: Integrity and authentication attacks published
- August 2001 (weak-key attack): can deduce RC4 key after observing several million packets
- AirSnort application allows casual user to decrypt WEP traffic

Crypto problems
- 24 bit IV to short
- Same key for encryption and message integrity
- ICV flawed, does not prevent adversarial modification of intercepted packets
- Cryptanalytic attack allows eavesdroppers to learn key after observing several millions of packets

IEEE 802.11i

- Much stronger encryption
- TKIP (temporal key integrity protocol)
- But use RC4 for compatibility with existing WEP hardware
- Extensible set of authentication mechanisms
- Employs 802.1X authentication
- Key distribution mechanism
- Typically public key cryptography
- RADIUS authentication server
- distributes different keys to each user
- also there's a less secure pre-shared key mode
- WPA: Wi-Fi Protected Access
- Pre-standard subset of 802.11i

TKIP: Changes from WEP

- Message integrity scheme that works
- IV length increased
- Rules for how the IV values are selected
- Use IV as a replay counter
- Generates different message integrity key and encryption key from master key
- Hierarchy of keys derived from master key
- Secret part of encryption key changed in every packet.

- Much more complicated than WEP!

TKIP: Message integrity

- Uses message authentication code (MAC); called a MIC in 802.11 parlance
- Different key from encryption key
- Source and destination MAC addresses appended to data before hashing
- Before hashing, key is combined with data with exclusive ors (not just a concatenation)
- Computationally efficient

TKIP: IV Selection and Use

- IV is 56 bits
- 10,000 short packets/sec
- WEP IV: recycle in less than 30 min
- TKIP IV: 900 years
- Must still avoid two devices separately using same key
- IV acts as a sequence counter
- Starts at 0, increments by 1
- But two stations starting up use different keys:
- MAC address is incorporated in key

802.11 security summary

- SSID and access control lists provide minimal security
- no encryption
- WEP provides encryption, but is easily broken
- Emerging protocol: 802.11i
- Back-end authentication server
- Public-key cryptography for authentication and master key distribution
- TKIP: Strong symmetric crypto techniques