FIB Facultat d'Informàtica de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

CONCEPTES AVANÇATS DE SISTEMES OPERATIUS

Departament d'Arquitectura de Computadors

Vulnerabilitats del protocol 802.11

(Seminaris de CASO)

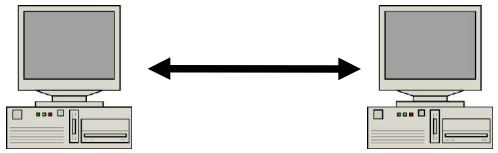
Autors

Albert Sànchez Casals i Daniel Pérez Alcázar

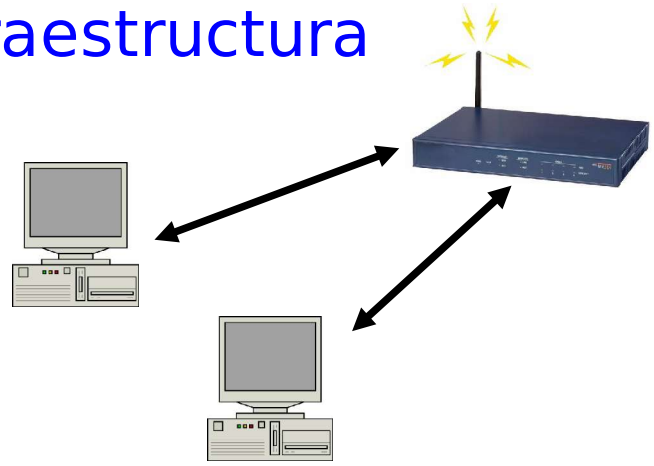
El protocol 802.11

- És un protocol de nivell 2 (enllaç).
- Utilitza un medi sense cablejar (*wireless*). Opera principalment a la banda dels 2,4Ghz.
- D'1 Mbps fins a 54 Mbps.
- Creixent popularitat.

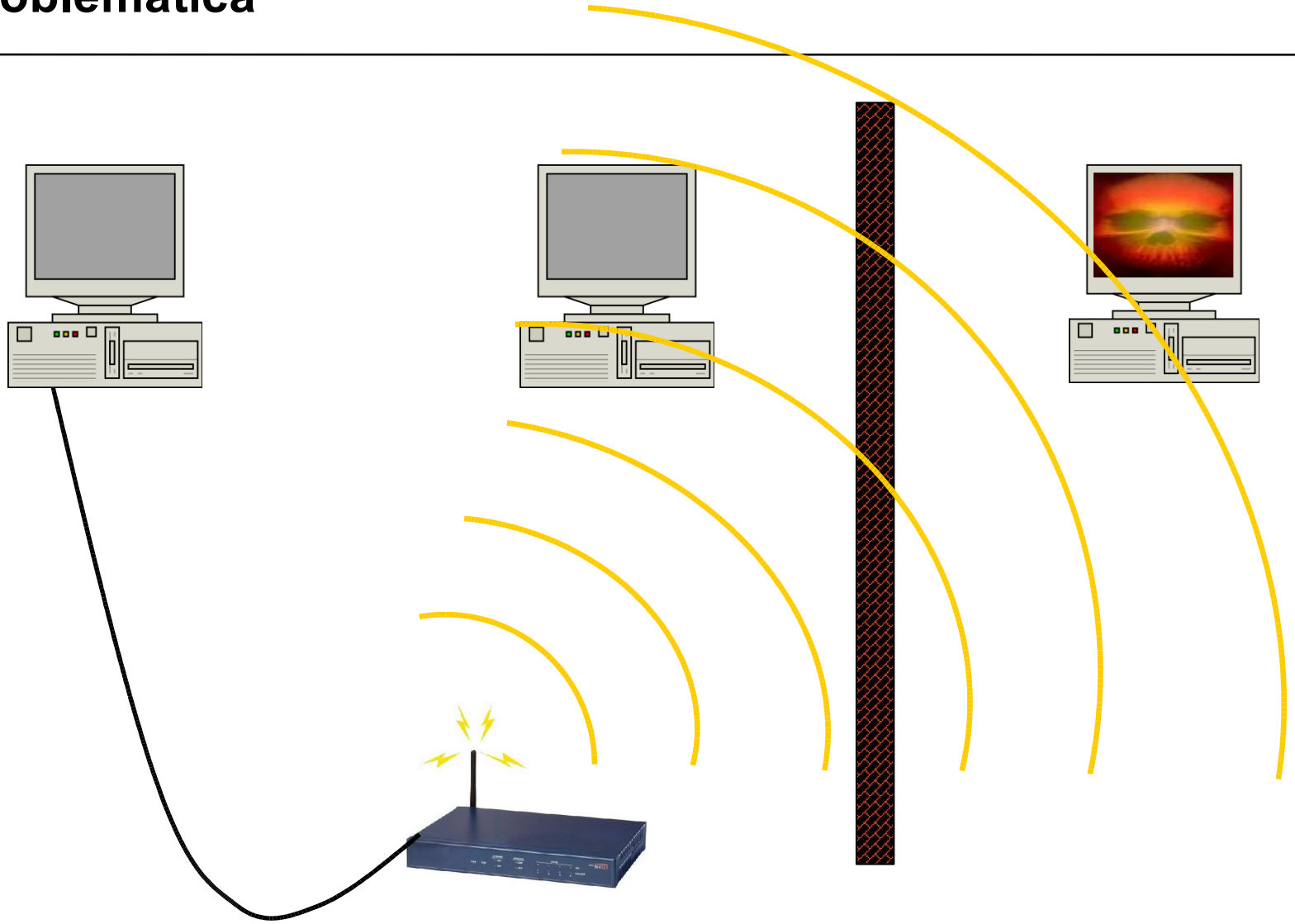
Mode ad-hoc



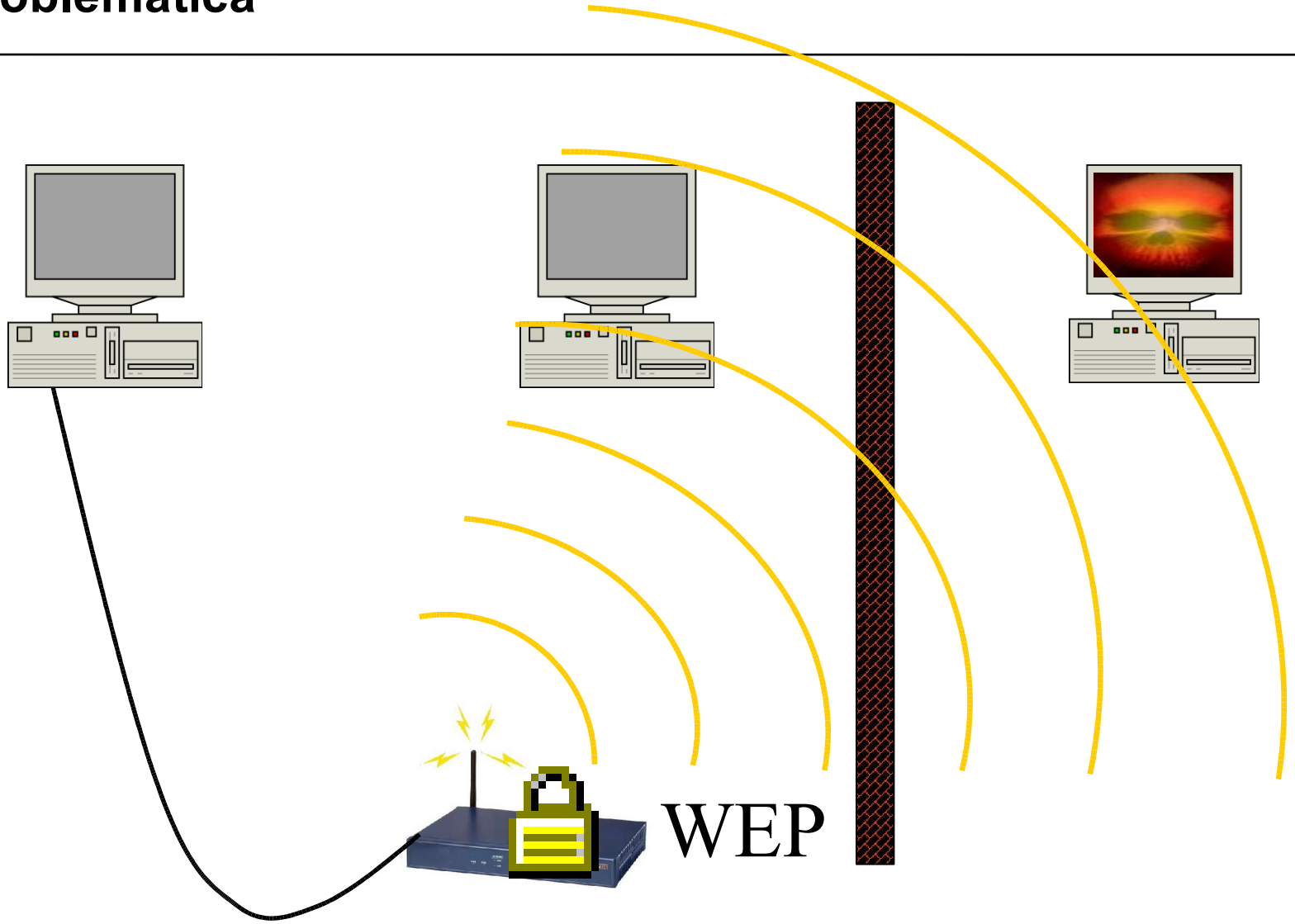
Mode infraestructura



Problemàtica



Problemàtica



WEP (wired equivalent privacy)(I)

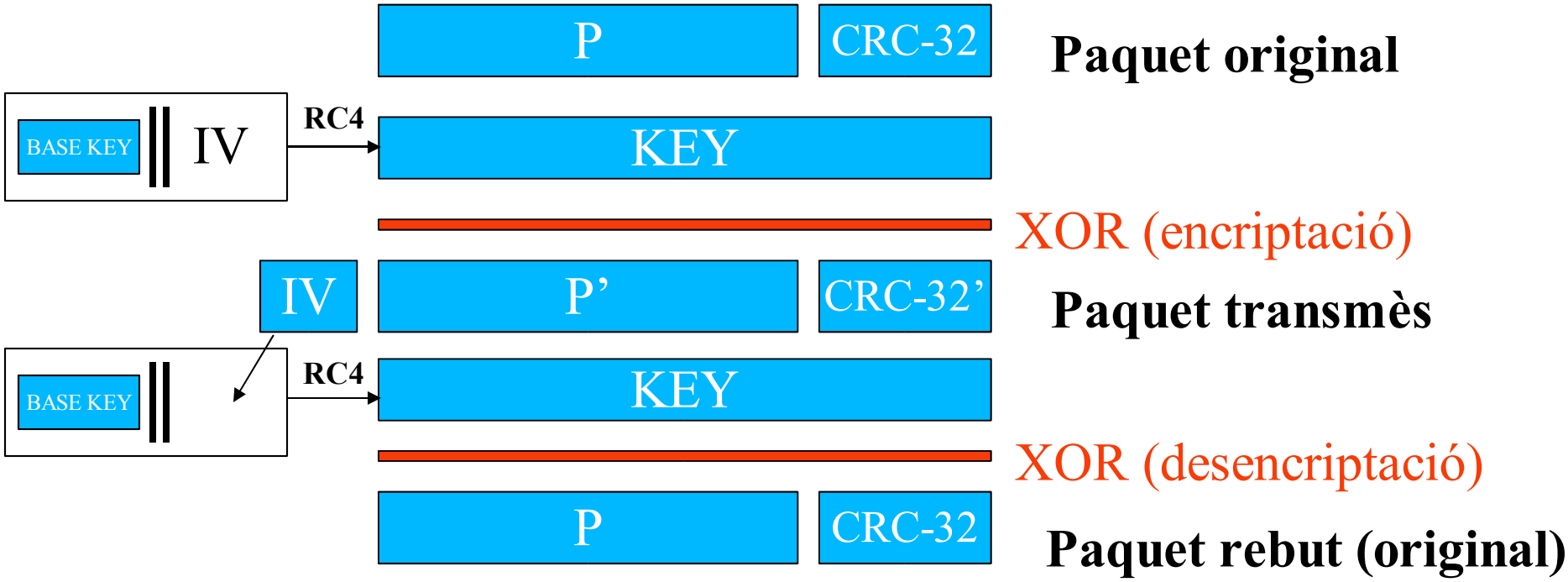
- WEP és un standard d'encriptació implementat a nivell d'enllaç (MAC).
- El seu ús és opcional → utilitzar-lo sempre!
- Utilitza l'algorisme RC4 (de RSA Security).
- Fa servir claus de 40 i 64 bits, posteriorment augmentat a 128 i 256 bits.
- S'utilitza perquè és simple d'implementar i d'execució ràpida, però massa insegur.

WEP (wired equivalent privacy)(II)

- Les estacions sense fil comparteixen la clau secreta de la xarxa amb el punt d'accés.
- Cada paquet està encriptat amb la clau compartida + un vector d'inicialització (IV) de 24 bits generat aleatoriament.
- Cada paquet inclou un control d'integritat.
- IC falla → paquet rebutjat.

WEP (wired equivalent privacy)(III)

- Funcionament:

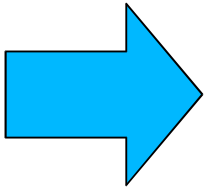


Vulnerabilitats

- Presentarem 5 vulnerabilitats:
  - Atac actiu per introduir transit
    → CRC vs control d'integritat
  - Atac passiu per desencriptar el transit
    → Reutilització del IV
  - Atac actiu desde dos extrems
    → Dos extrems
  - Atac actiu per desencriptació pràctica
    → IP forwarding
  - Atac actiu de denegació de servei
    → DOS

Vulnerabilitats – CRC vs control d'integritat (I)

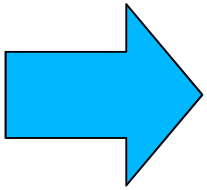
- CRC-32 utilitzat com a control d'integritat

  Bo per errors aleatoris

  Però que passa si són errors forçats?

- CRC i RC4 són linials:

  CRC(X^Y) = CRC(X)^CRC(Y)

  RC4(k,X^Y) = RC4(k,X)^Y

Vulnerabilitats – CRC vs control d'integritat (I)

- CRC-32 utilitzat com a control d'integritat

  Bo per errors aleatoris

  Però que passa si són errors forçats?

- CRC i RC4 són linials:

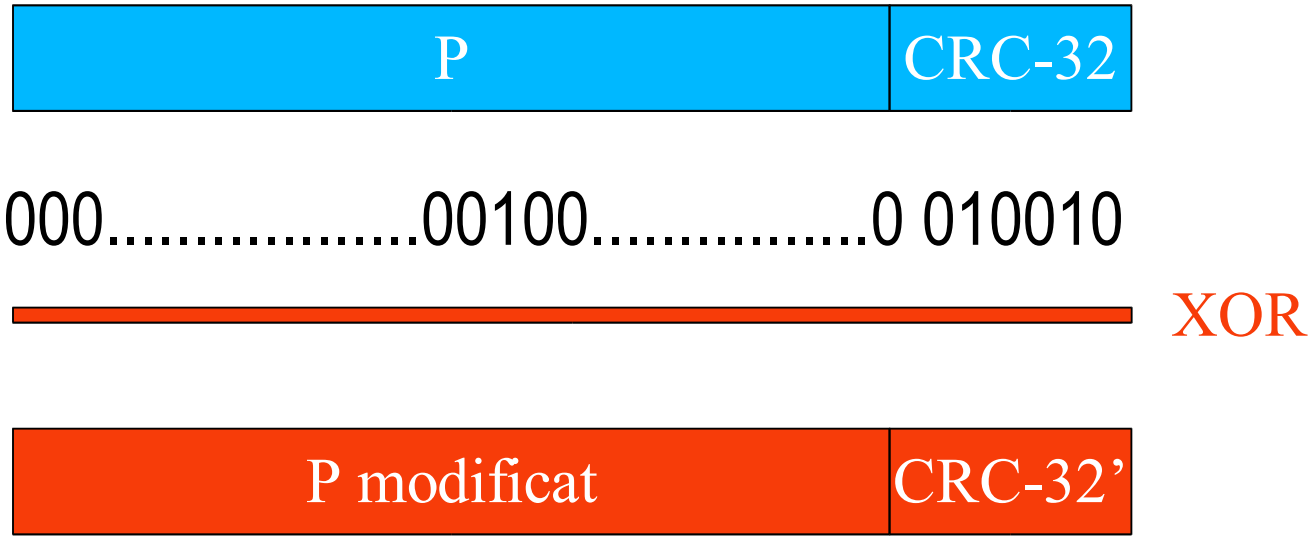
  CRC(X^Y) = CRC(X)^CRC(Y)

  RC4(k,X^Y) = RC4(k,X)^Y

PODEM MODIFICAR ELS PAQUETS!!!

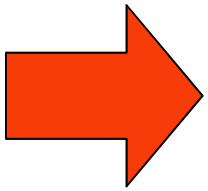
Vulnerabilitats – CRC vs control d'integritat (II)

- Com?



Vulnerabilitats – Reutilització del IV (I)

- WEP combina una clau privada amb un vector d'inicialització de 24 bits generat aleatòriament per a cada paquet.
  - Key = base_key || IV
  - 24 bits aleatoris → es reutilitzen valors del vector
- A més,
  - en algunes instal·lacions, totes les estacions utilitzen la mateixa clau
  - Claus repetides en ambdues direccions
  - Algunes implementacions posen el IV a 0 un cop inicialitzat

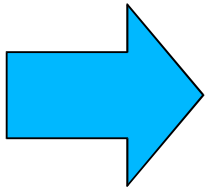


La repetició de IVs facilita atacs estadístics.

Vulnerabilitats – Reutilització del IV (II)

- La clau del RC4 no s'hauria de reutilitzar ja que

  RC4(k,X)^RC4(k,Y) = X^Y



Tenim dos paquets amb el mateix IV

C1 = P1 xor RC4(k||IV)

C2 = P2 xor RC4(k||IV)

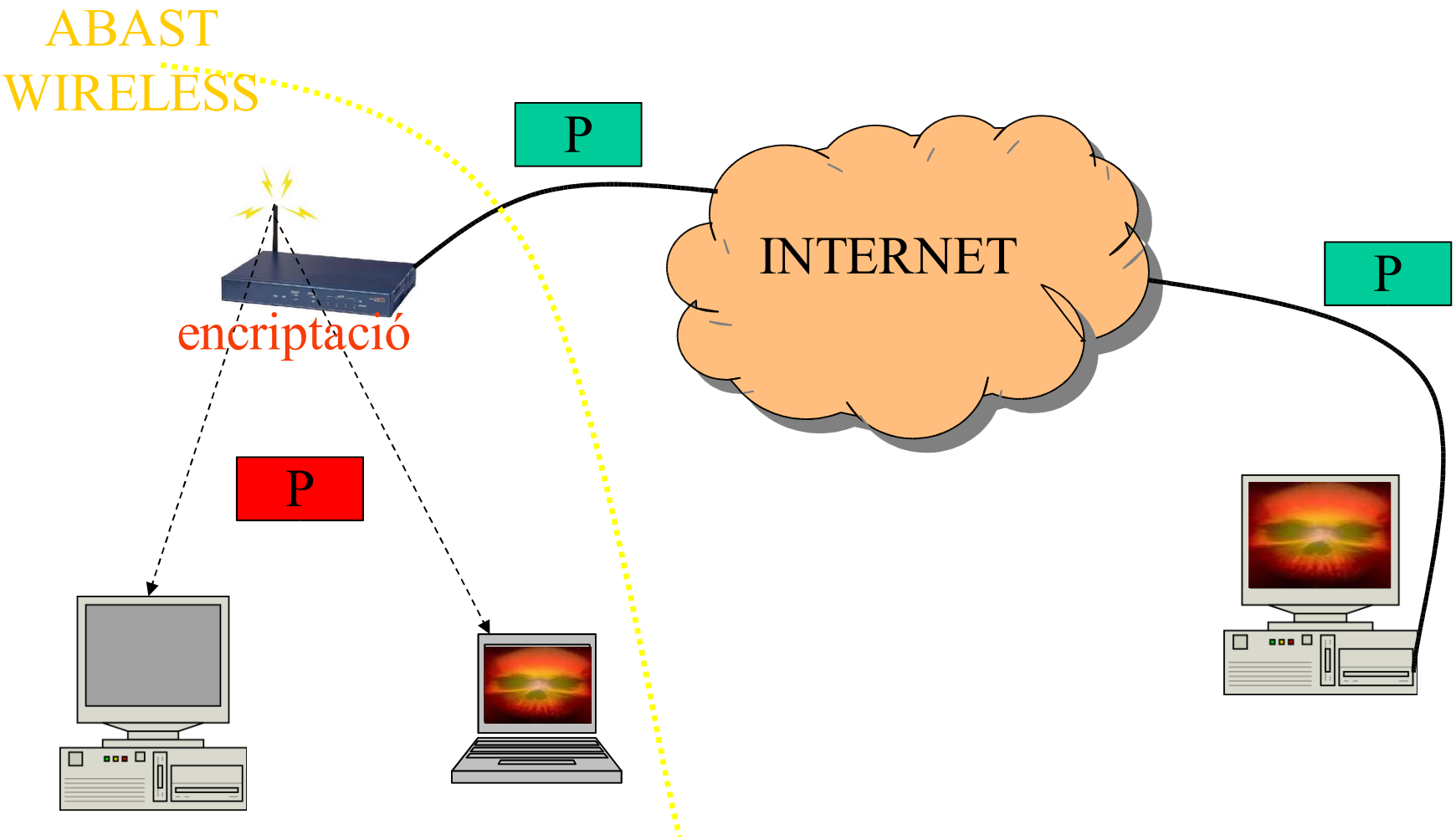
C1 xor C2 = P1 xor P2

→ Coneixent el text de P1, tenim P2

→ Anàlisi estadistic per trobar P1 i P2

→ Encara més facil amb 3 paquets …

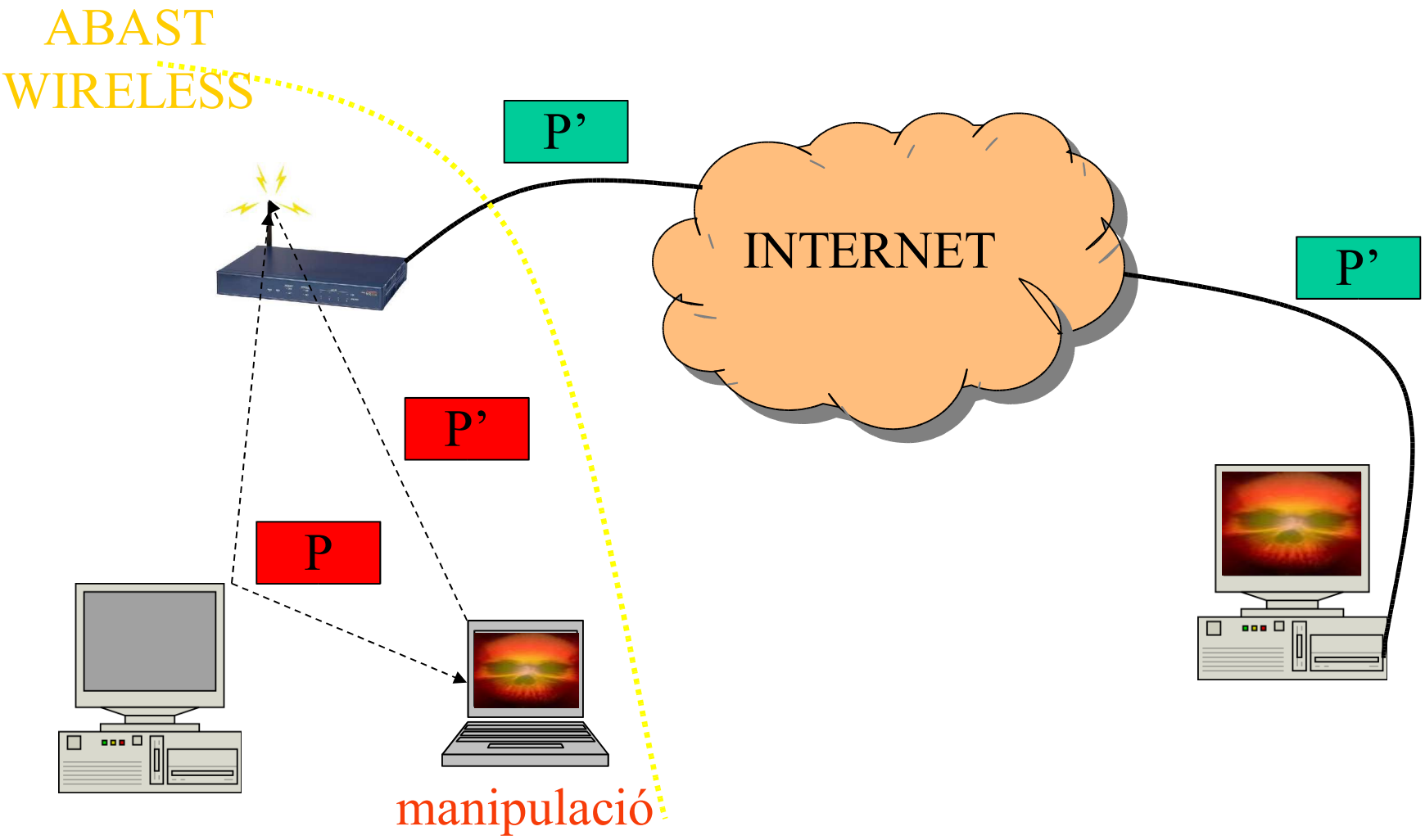
Vulnerabilitats – Dos extrems (I)



Vulnerabilitats – IP forwarding (I)

- Recordem que hem vist que podem modificar els bits dels paquets.
- Modifiquem la IP destí de la capçalera, fàcil d'obtenir.
- Modificació posant una IP d'un host que controlem.
- L'enviem a l'Access Point (AP), que té connexió a Internet.
- L'AP desencripta el paquet, i fa "forwarding".
  → Rebem el paquet amb el text desencriptat!!!
- Si modifiquem la capçalera TCP, podem posar el port 80 per saltar-nos els firewalls.

Vulnerabilitats – IP forwarding (II)



Vulnerabilitats – DOS (I)

- Ja era possible provocar una DOS saturant la banda dels 2,4Ghz de determinada manera, però calia equips potents.

  → Però el Maig 2004 es descobreix com fer-ho... amb una Palm!!!!

- Afecta a l'IEEE 802.11, 802.11b i 802.11g de baixa velocitat (per sota dels 20Mbps). No es veuen afectats l'IEEE 802.11a ni l'802.11g d'alta velocitat (>20 Mbps).

- Afecta a tots els clients dins del rang de l'atacant.

Vulnerabilitats – DOS (II)

- Descripció de l'atac:

→No ha sortit una descripció precisa! ☹... o ☺?

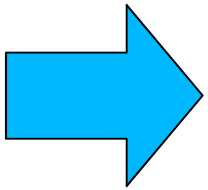
→Estaria basat en l'explotació d'un error de disseny del MAC (control d'accés al medi):

- S'utilitza CSMA/CA per evitar col·lisions a la transmissió, que a la seva vegada utilitza un procediment anomenat Clear Channel Assessment (CCA) per assegurar que el transmissor pot transmetre perquè el canal està lliure.

- L'atac fa que el CCA sempre vegi el canal com a "ocupat" i per tant no es puguin establir communiacions.

Conclusions

- Llancem la nostra xarxa wireless a la paperera????
  - No!!



Simplement evaluar riscos i utilitzar-la amb el pensament de què és insegura:

- Utilitzar encriptació a nivells superiors.
- Delimitar accés físic a la xarxa (evitar tafaners).
- No basar la infraestructura de xarxa en aquesta tecnologia.
- Utilitzar una política de claus exigent.

Bibliografia

- http://standards.ieee.org/getieee802/802.11.html (estàndar wifi)
- http://www.wi-fiplanet.com/tutorials/article.php/1368661 (seguretat wireless)
- http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (seguretat WEP)
- http://www.auscert.org.au/render.html?it=4091 (la darrera vulnerabilitat)
- Google 802.11 + security