



UNIVERSITÀ  
DEGLI STUDI DI BARI  
ALDO MORO

*CDS IN INFORMATICA E  
COMUNICAZIONE DIGITALE*

Anno Accademico 2015-2016

**Corso di**

***“Reti di Calcolatori e Comunicazione Digitale”***

***Modulo 7: Le comunicazioni wireless***

*Prof. Sebastiano Pizzutilo  
Dipartimento di Informatica*

# Wireless

Si riferisce ad una tipologia di comunicazione, monitoraggio o sistema di controllo in cui i segnali viaggiano nello spazio e non su fili o cavi di trasmissione

*Le due tecnologie di trasmissione utilizzate sono :*

- La radio frequenza (RF)
- I raggi infrarossi (IR)

## Vantaggi

- Mobilità
- Portabilità
- Riduzione dei costi
- Risparmio di tempo

## Svantaggi

- Le comunicazioni tra le stazioni wireless **sono facilmente intercettabili**

VerificaFTP - Ethereal

No. -	Time	Source	Destination	Protocol	Info
300	39.705893	192.168.19.12	192.168.19.1	TCP	3610 > 8369 [SYN] Seq=0 Ack=0
301	39.708275	192.168.19.1	192.168.19.12	TCP	8369 > 3610 [SYN, ACK] Seq=0
302	39.708409	192.168.19.12	192.168.19.1	TCP	3610 > 8369 [ACK] Seq=1 Ack=1
303	39.708839	192.168.19.12	192.168.19.1	MSproxy	Client message: Unknown
304	39.711177	192.168.19.1	192.168.19.12	FTP	Response: 220 Benvenuto nel s
305	39.711367	192.168.19.12	192.168.19.1	FTP	Request: USER maria
306	39.714363	192.168.19.1	192.168.19.12	FTP	Response: 331 Please specify
307	39.714546	192.168.19.12	192.168.19.1	FTP	Request: PASS giovanna
308	39.735953	192.168.19.1	192.168.19.12	FTP	Response: 230 Login successfu
309	39.736290	192.168.19.12	192.168.19.1	FTP	Request: opts utf8 on
310	39.739197	192.168.19.1	192.168.19.12	FTP	Response: 500 Unknown commanr

Frame 307 (69 bytes on wire, 69 bytes captured)

- Ethernet II, Src: 00:02:a5:2d:64:b7, Dst: 00:d0:b7:0a:b5:ef
- Internet Protocol, Src Addr: 192.168.19.12 (192.168.19.12), Dst Addr: 192.168.19.1 (192.168.19.1)
- Transmission Control Protocol, Src Port: 3610 (3610), Dst Port: 8369 (8369), Seq: 13, Ack: 1
- MS Proxy Protocol
- File Transfer Protocol (FTP)
  - PASS giovanna\r\n
    - Request command: PASS
    - Request arg: giovanna

0000 00 00 07 0a 03 e1 00 02 a3 2d 04 b7 08 00 43 00 .....-U...E.  
0010 00 37 50 bf 40 00 80 06 02 a4 c0 a8 13 0c c0 a8 .7P.@... ..  
0020 13 01 0e 1a 20 b1 23 73 db 87 ab ed 35 45 50 18 ...#s...5EP.  
0030 62 26 19 f8 00 00 50 41 53 53 20 67 69 6f 76 61 b&...PA SS giova  
0040 6e 6e 61 0d 0a nna..

Filter: / Add Expression... Clear Apply P: 968

# Comunicazione wireless

*Si riferisce ad una tipologia di comunicazione, monitoraggio o sistema di controllo in cui i segnali viaggiano nello spazio e **non** su fili o cavi di trasmissione*

*Le due tecnologie di trasmissione utilizzate sono :*

- **La radio frequenza (RF)**
  - **I raggi infrarossi (IR)**
- 
- **DECT (Digital Enhanced Cordless Telecommunication)** standard digitale criptato per telefonini cordless
  - **IrDA (Infrared Device Application)** Tecnologia di interconnessione dati tramite infrarossi bidirezionale point-to-point tra dispositivi posizionati in visibilità reciproca LoS (Line to sight)
    - *Range di 1 o 2 metri*
    - *Bit rate di 4 Mbps*
  - **Bluetooth**, tecnologia per PAN (Personal Area Network)
  - **IEEE 802.11**, tecnologia per WLAN

# Bluetooth

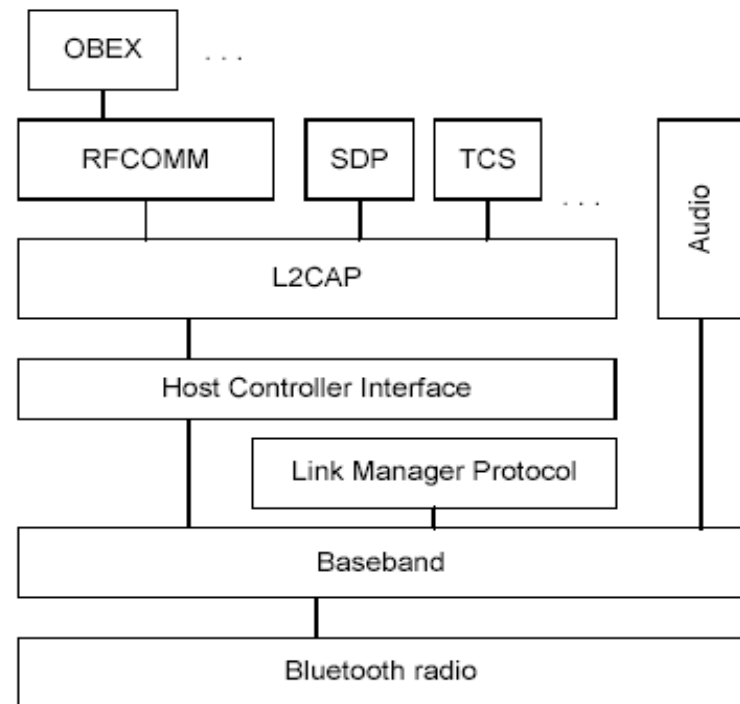


**Bluetooth**, il cui nome deriva da Harald Blatant Re di Danimarca nel 911 DC (detto “Bluetooth”), è stato sviluppato a partire dal 1994 e la sua trasformazione in standard avviene ad opera di un gruppo di imprese, il *Bluetooth Special Interest Group (BSIG)*, fondato nel 1998 da Ericsson Mobile Communications, Intel corporation, IBM corporation, Toshiba corporation, Nokia Mobile Phones, Microsoft, Lucent, 3Com, Motorola.

- Realizza una **WirelessPAN** per apparecchi di piccole dimensioni (**piconet**)
- Ha la capacità di far dialogare ed interagire fra loro dispositivi diversi (telefonini, stampanti, notebook, etc)
- Opera sulla frequenza di 2.4 GHz
- Raggiunge la velocità di 1 Mbps

# Bluetooth

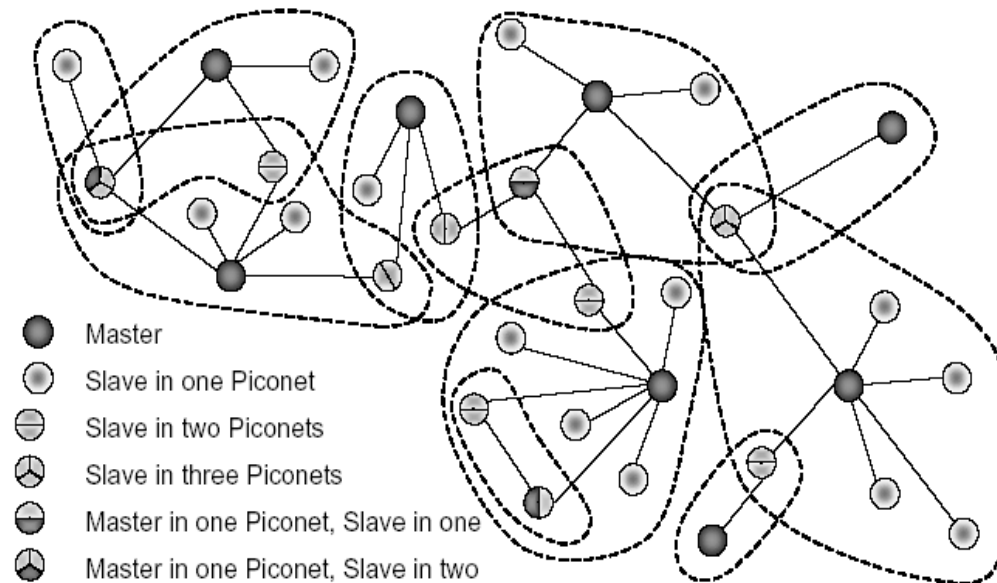
- La “Bluetooth Specification 1.2” definisce una velocità massima di trasmissione di 1 Mbit/s ed una copertura massima nominale di **cento metri**.
- Lo stack del protocollo Bluetooth:



*La IEEE sta definendo lo standard 802.15.1 per le WPAN al fine di integrare il Bluetooth con il Wi-fi all'interno della suite ISO/OSI.*

# Le topologie Bluetooth

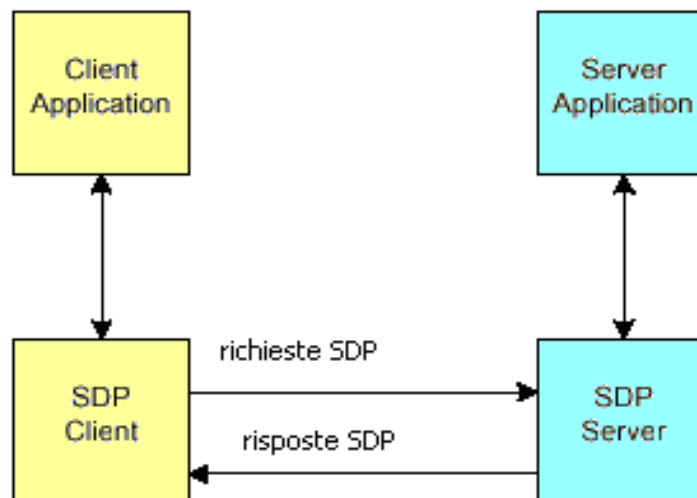
- In ogni **Piconet** un terminale Bluetooth assume la funzione di **master** scegliendo la sequenza con cui cambiare la frequenza portante radio, mentre gli altri assumono il ruolo di **slave** nella interazione tra di loro e con il master.
- Più **piconet** collegate tra loro dai relativi master formano una struttura più ampia chiamata **Scatternet**.
- In una **scatternet** le comunicazioni tra le piconet sono filtrate dai master ed è possibile includere fino a **10 piconet** con al loro interno un numero massimo di 79 dispositivi bluetooth.



# Il *Service Discovery Protocol*

- I dispositivi comunicano tra loro creando e riconfigurando dinamicamente le picoreti.
- Il *Service Discovery Protocol* permette a un dispositivo **bluetooth** di determinare quali siano i servizi che gli altri apparecchi presenti nella picorete ( a distanza di 10-100m) mettono a disposizione

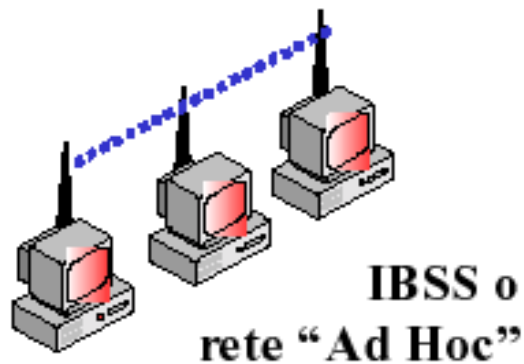
*Quando un dispositivo si inserisce per la prima volta in una **picorete** effettuerà una "scansione" di tutti i nodi presenti per capire come può interagire con essi. Tale modalità di interconnessione dinamica consente di sincronizzare automaticamente i dati tra due apparecchi Bluetooth.*



# Possibili architetture wi-fi

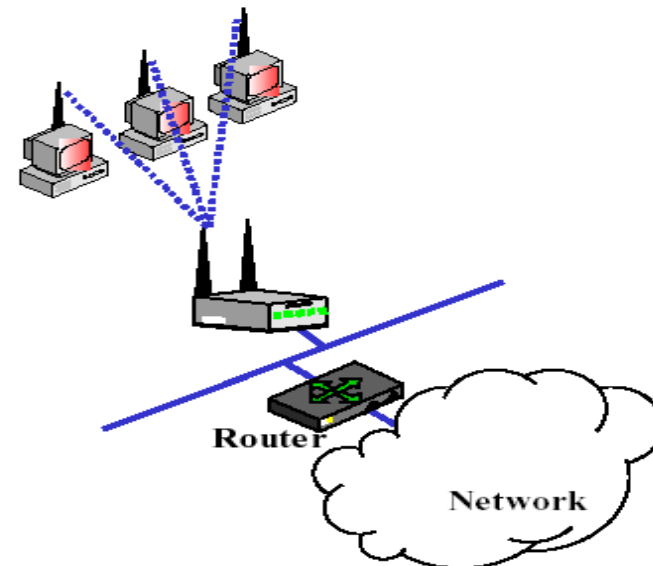
## ■ Ad Hoc

- *È composta solo da terminali wireless*
- *Non necessita di punti d'accesso ( IBSS= Independent Basic Service Set)*
- *Non supporta l'accesso alla rete cablata*



## ■ Infrastrutturale

- *È composta da una o più celle o dispositivi (stazioni di lavoro + AP = chiamate Basic Service Set = BSS )*
- *Ogni cella è controllata da un AP (Access Point)*





# **Le reti *MANET*** ***Mobile Ad hoc NETWORK***

Una rete che utilizza il modello *ad hoc*, composta da terminali mobili prende il nome di *MANET*.

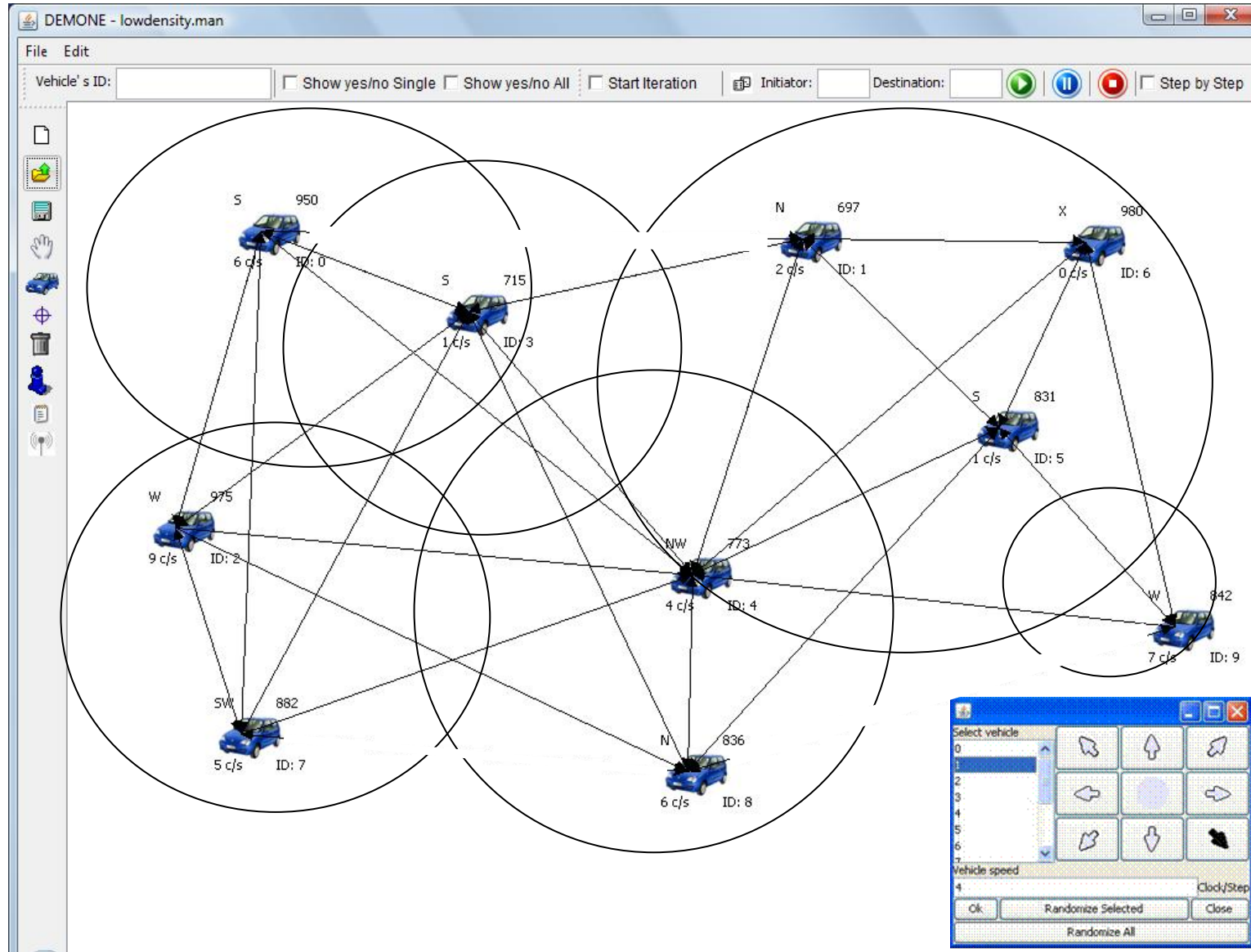
Una *Mobile Ad hoc NETWORK* è un sistema autonomo di *nodi mobili* connessi tra loro mediante collegamenti wireless "*ad hoc*", *che non richiedono una infrastruttura* fissa per la comunicazione

## *Caratteristiche:*

- Tipologia dinamica
- Topologia gerarchica o piatta
- Capacità variabile dei link
- Operazioni limitate dalle risorse energetiche
- Limitata sicurezza a livello fisico

*I nodi mobili fungono sia da host che da router e fanno ricorso a particolari algoritmi di routing.*

# Esempio di MANET



## Un esempio di protocollo di routing per Manet: **AODV**

**AODV** (*Ad hoc On demand Distance Vector*) è il protocollo di routing per reti mobili ad hoc e supporta l'instradamento unicast e broadcast. Si basa su un protocollo di tipo **reattivo** (la ricerca dei percorsi nella rete sono solo su richiesta).

Ogni componente della rete è abilitato alla funzioni di routing, dispone infatti di una **tabella di routing** che contiene: 1) l'indirizzo del prossimo nodo in direzione della destinazione (**next hop**), 2) il suo numero di sequenza (**sequence number** che cresce nel tempo e che garantisce l'assenza di cicli nei percorsi utilizzati) e 3) la distanza complessiva indicata in **salti (hops)**.

**Dynamic Source Routing (DSR)** è un altro protocollo di routing per reti MANET.


È reattivo come AODV, ma è più vicino al Link State Routing, in quanto utilizza il **source routing** invece di affidarsi alla routing table di ogni nodo intermedio. DSR ha due fasi primarie, **Route Discovery** e **Route Maintenance**. La **Route Reply** verrà generata solo se il messaggio avrà raggiunto il nodo destinazione (la rotta registrata all'interno della **Route Request** verrà ovviamente inserita nella **Route Reply**)

Per determinare le rotte sorgente (**source routes**) DSR accumula gli indirizzi dei nodi intermedi a partire dalla sorgente verso la destinazione. Questo accumulo di informazioni è **memorizzato in cache** dai nodi che processano la **route discovery** e il percorso ottenuto verrà usato per inoltrare pacchetti. Ciò porta necessariamente ad un aumento di risorse.

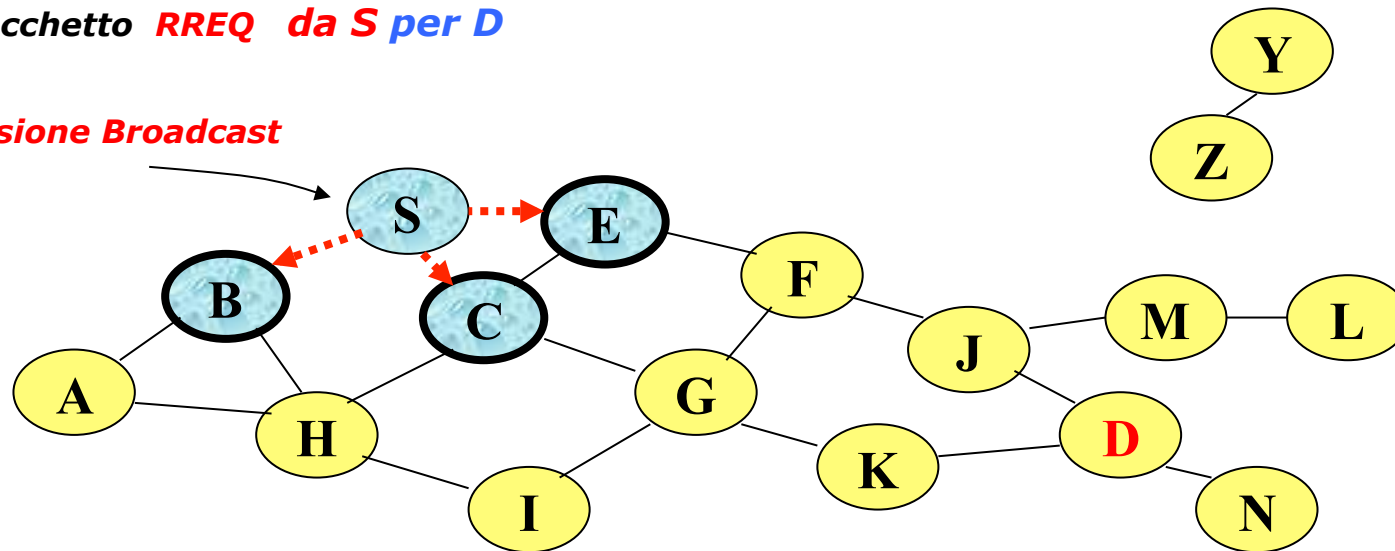
# AODV: route discovery

I pacchetti **RREQ** vengono inviati in broadcast dal nodo sorgente. Un nodo della rete che riceve un pacchetto di richiesta invia un pacchetto di **RREP** attraverso un percorso temporaneo fino al nodo richiedente, che potrà dunque sfruttare l'informazione ricevuta. Ogni nodo confronta i diversi percorsi in base alla loro lunghezza e sceglie il più conveniente.

Se un nodo non è più raggiungibile viene generato un messaggio di **RERR** per avvertire il resto della rete.

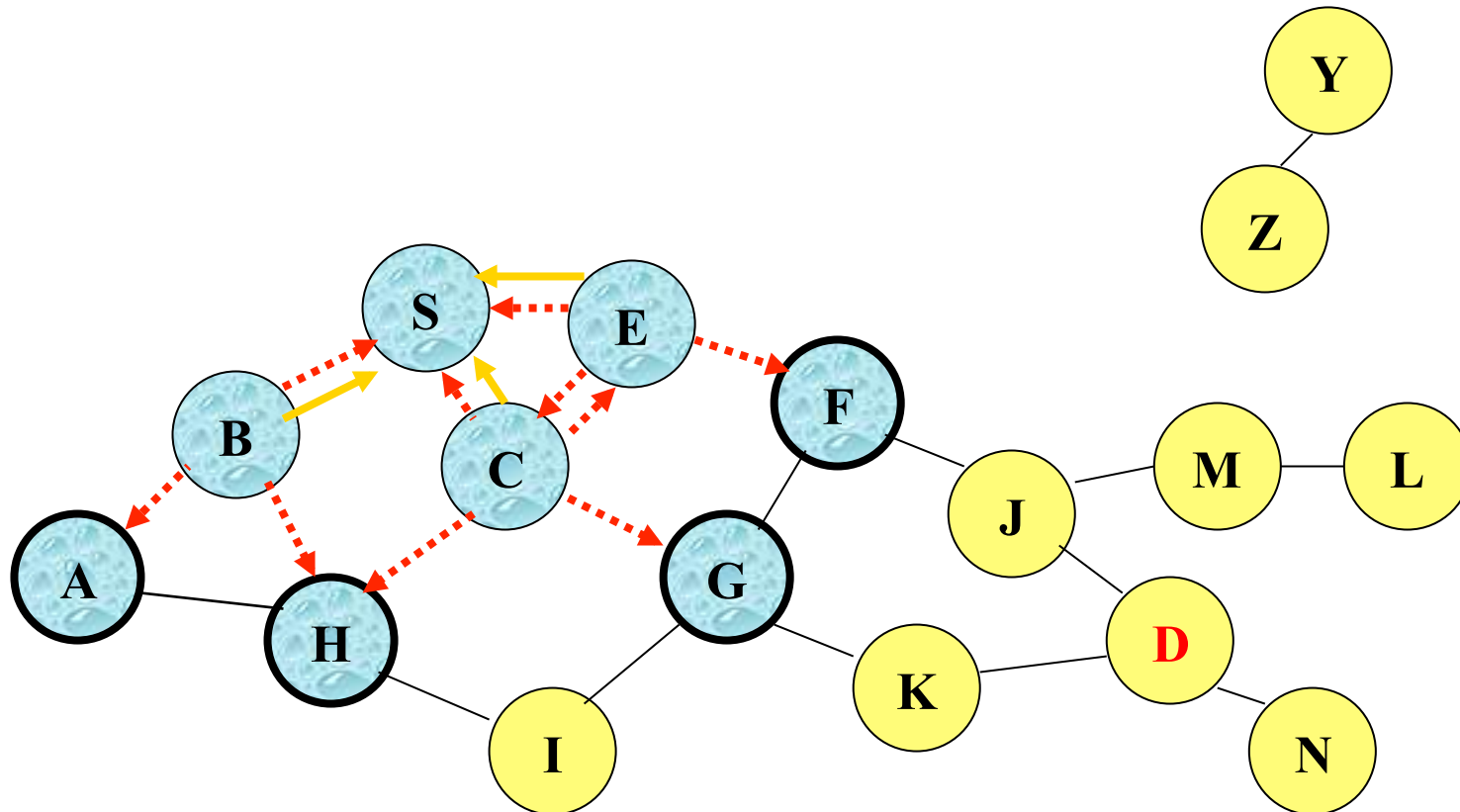
 **Rappresenta un nodo che ha ricevuto un pacchetto RREQ da S per D**

**Trasmissione Broadcast**

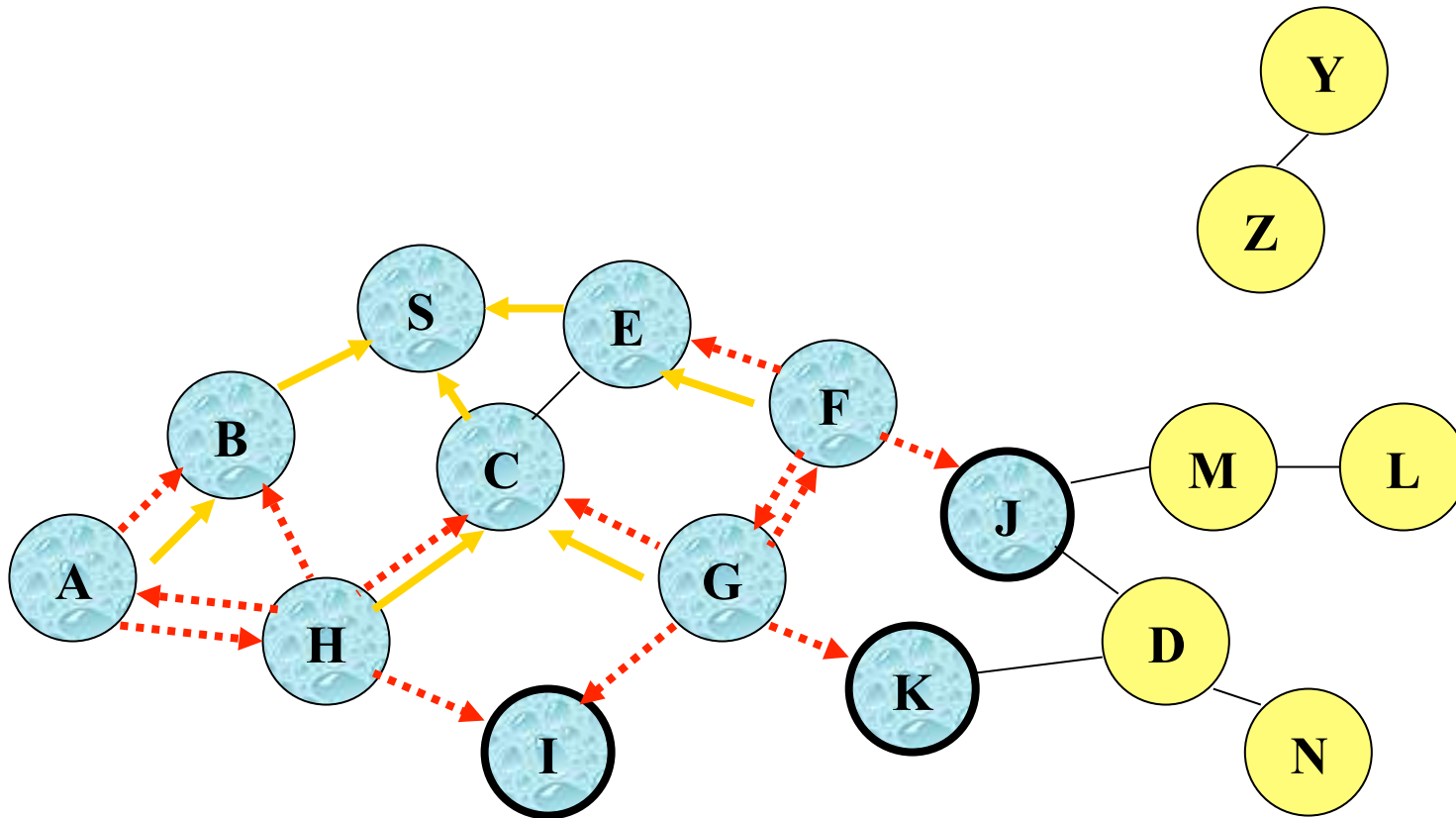


 **Trasmissione di un pacchetto RREQ**  
 **messaggi HELLO**

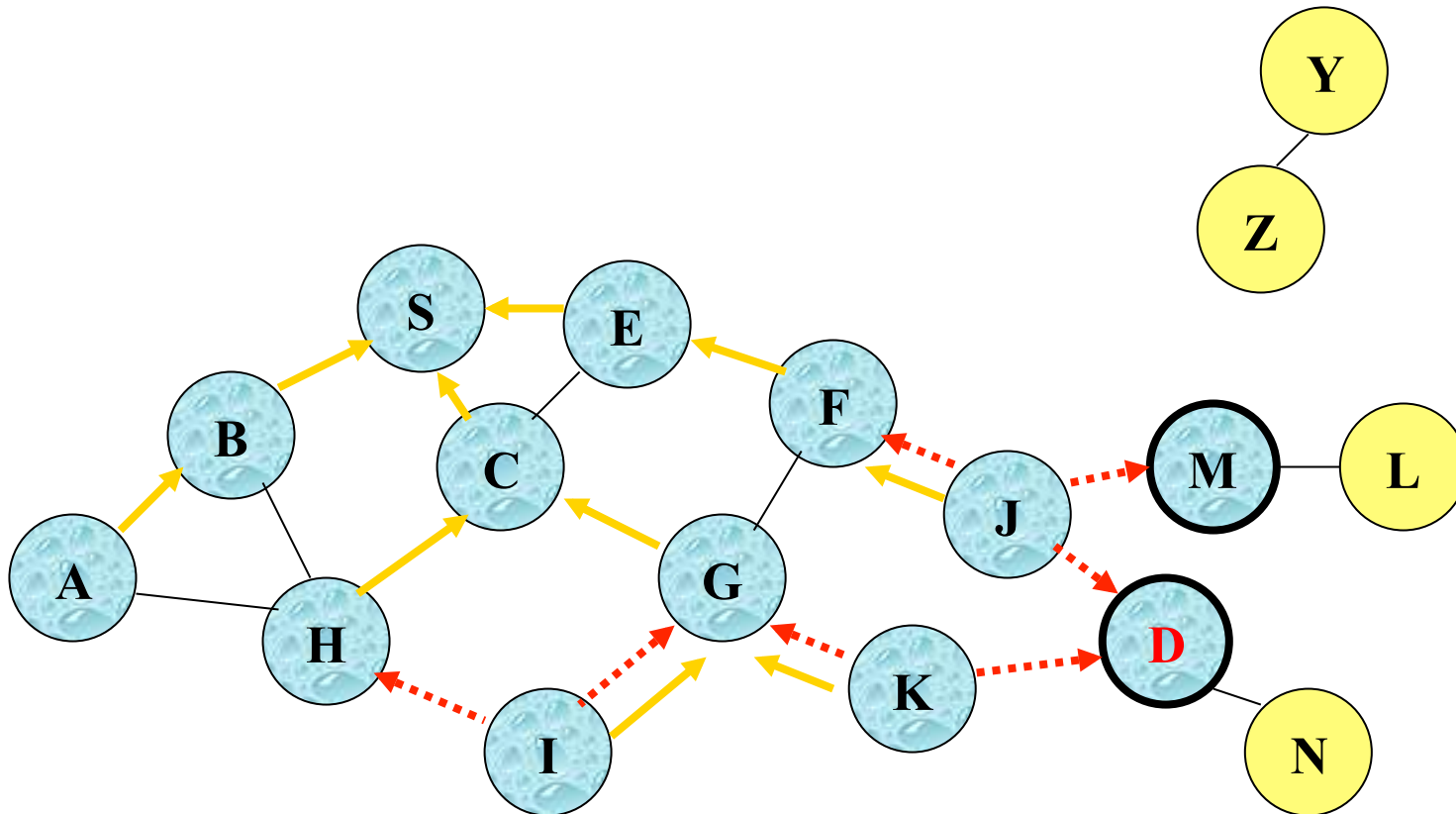
# AODV: route discovery



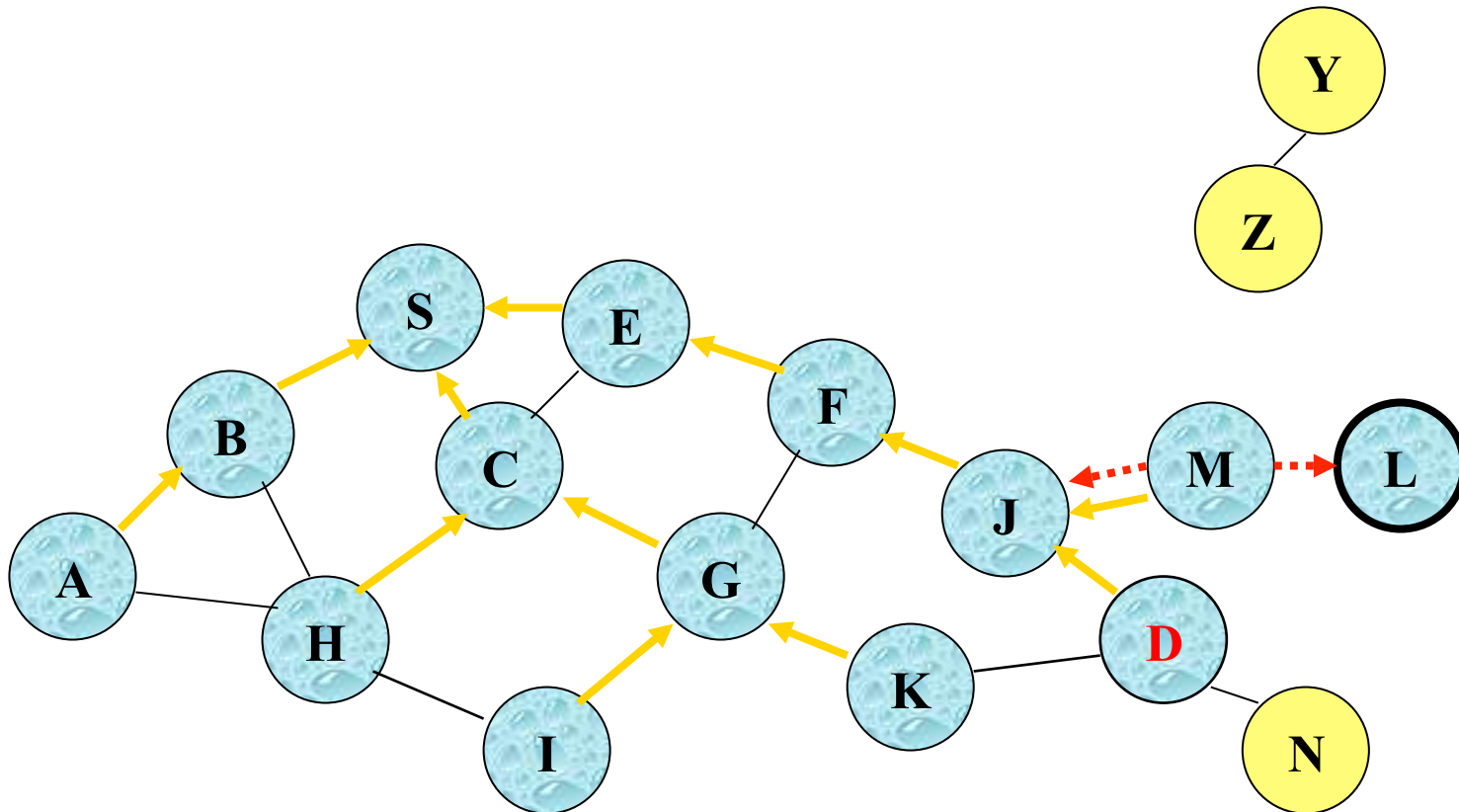
# AODV: route discovery



# AODV: route discovery

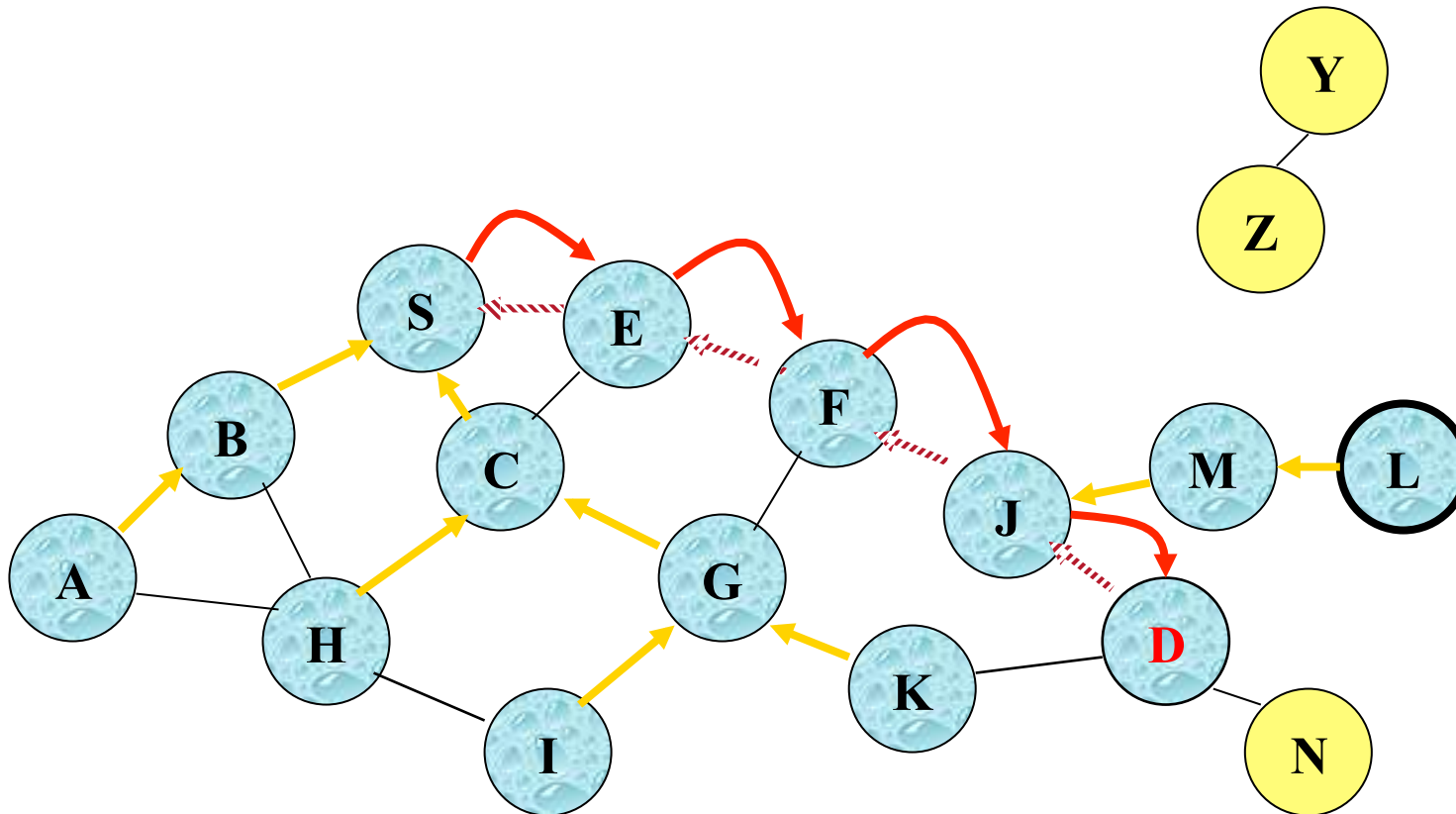


# AODV: route discovery





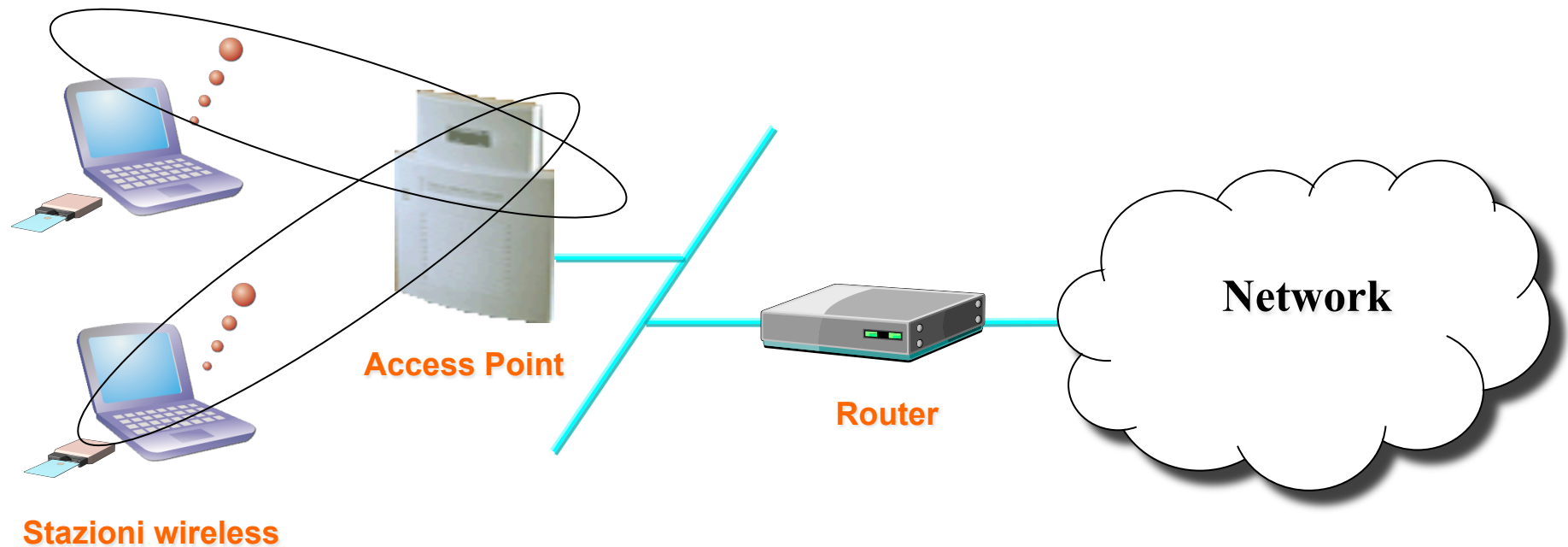
# AODV: route discovery



# IEEE 802.11

Il primo standard IEEE 802.11 “*Wireless LAN*” è stato approvato nel 1997 come alternativo all’802.3 “Ethernet”.

Lo standard *dettava le specifiche a livello fisico e datalink per l’implementazione di una rete LAN wireless*

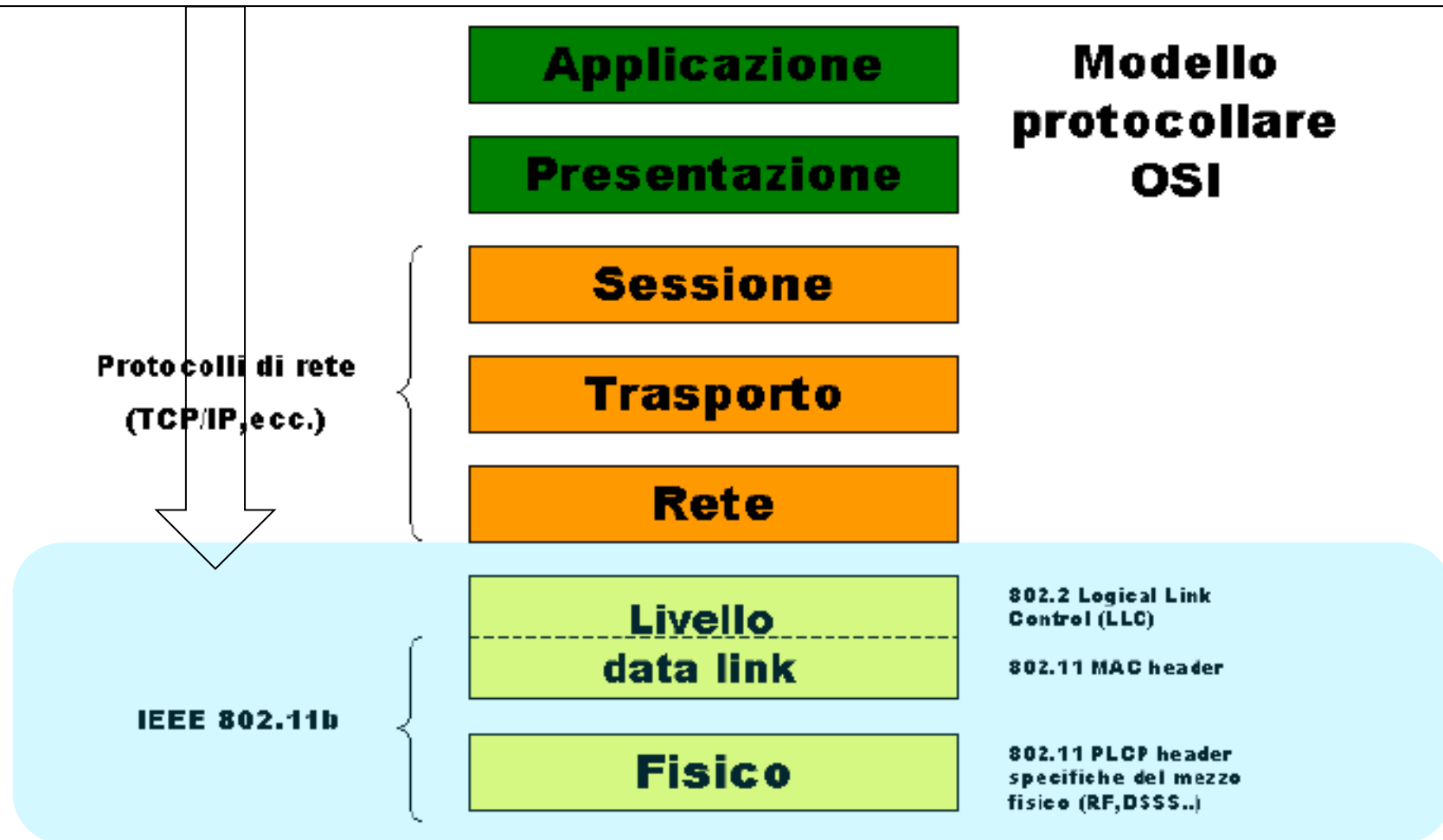


# *La famiglia IEEE 802.11*

Standard	Descrizione	Stato dello standard
802.11	WLAN; fino a 2 Mb/s; 2,4 Ghz	Approvato nel 1997
802.11a	WLAN; fino a 54 Mb/s; 5 Ghz	Approvato nel 1999
802.11b	WLAN; fino a 11 Mb/s; 2,4 Ghz	Approvato nel 1999
802.11g	WLAN; fino a 54 Mb/s; 2,4 Ghz	Approvato nel 2003
802.11e	Nuovo coordinamento per QOS	In fase di sviluppo
802.11f	IAAP (Inter-AP Protocol)	Approvato nel 2003
802.11h	Uso della banda 5 Ghz in Europa	Approvato nel 2003
802.11i	Nuovi standards per la criptazione	Approvato nel 2004
802.11n	MIMO physical layer	In fase di sviluppo

# Lo Standard 802.11

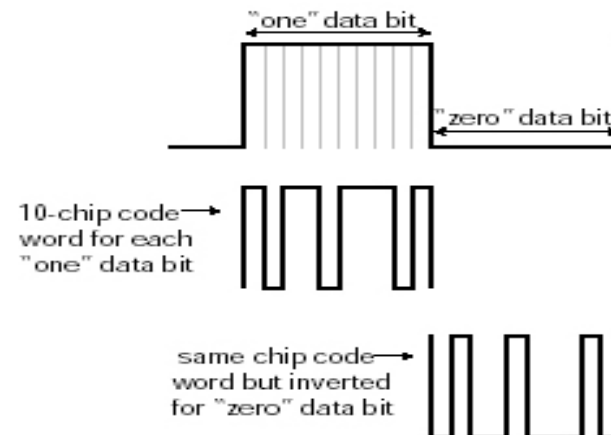
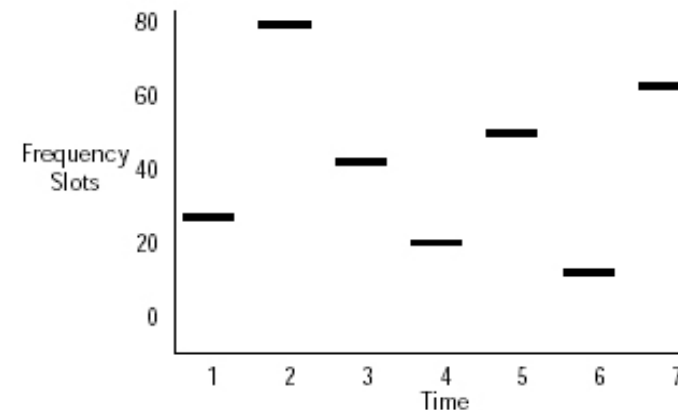
*È una famiglia di protocolli a livello di data link e fisico per le reti wireless*



# Il livello fisico di IEEE 802.11

A livello fisico le tecniche permesse sono:

- **FHSS, Frequency Hopping Spread Spectrum**, basato su salti di frequenza pseudocasuali. Solo le stazioni che conoscono la sequenza di *hopping* ricevono correttamente le informazioni.
- **DSSS, Direct Sequence Spread Spectrum**, ogni singolo bit viene codificato in base ad un *chipping code* ed inviato su una banda più ampia rispetto a quella richiesta. La stazione ricevente decodifica il segnale.



# Il livello MAC di Wi-Fi

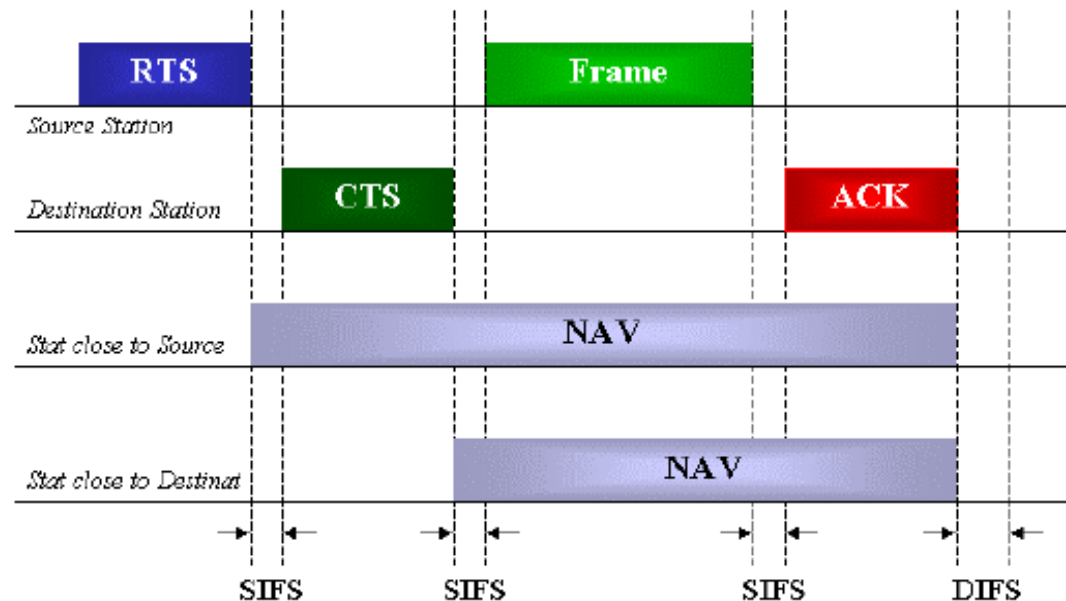
*Il livello MAC del Wi-fi utilizza i metodi:*

- **DCF, Distributed Coordination Function**, protocollo obbligatorio presente sia su reti *ad hoc* che *con infrastruttura*.

E' basato su **CSMA/CA** = CSMA/CD con l'aggiunta di due nuovi messaggi **RTS** (Request To Send) e **CTS** (Clear To Send) .

Così la stazione che intende trasmettere attende per un **InterframeSpaceFrame** allo scopo di **evitare** le collisioni.

- **PCF, Point Coordination Function**. Si basa su un Point Coordinator, (Access Point) che sincronizza le trasmissioni all'interno della WLAN.

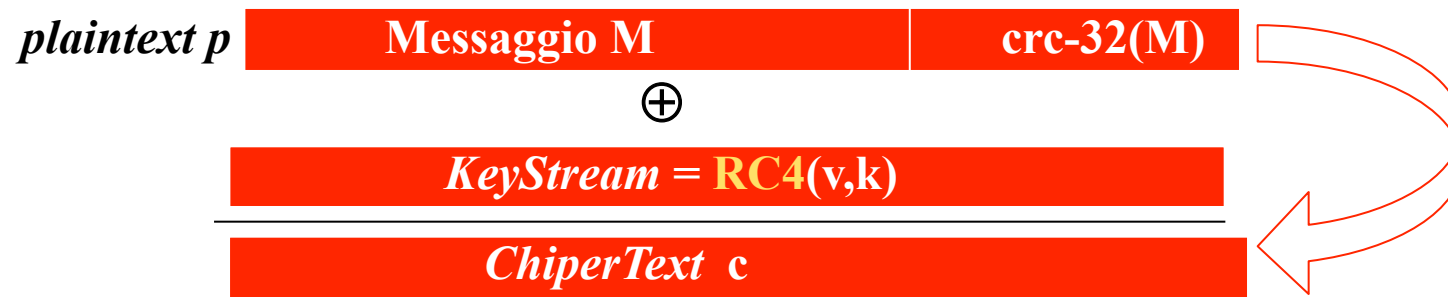


# Meccanismi di sicurezza wi-fi



L'algorithmo di cifratura **WEP** (**W**ired **E**quivalent **P**rivacy)

- Assicura la **confidenzialità** attraverso la crittografia dei segnali radio (effettuata con il protocollo RC4)
- Fornisce un meccanismo di autenticazione all'interno della rete con una chiave di 10 o 26 cifre esadecimali
- Evolve nel 2003 in WPA (Wi-fi Protected Access) e WPA2 con chiave di criptazione di 64-bit o 128-bit



*L' RC4 è uno tra i più famosi e diffusi algoritmi di **cifratura a flusso a chiave simmetrica***

Per decifrare il pacchetto, il ricevente deve applicare il processo di cifratura all'inverso:  $p' = c \oplus RC4(v,k)$   
 $= (p \oplus RC4(v,k)) \oplus RC4(v,k) = p$

# WEP- Vulnerabilità

- **Accessi non autorizzati**  
*Vengono autenticati solo i dispositivi e non gli utenti*
- **Access Point “abusivi”**  
*Manca di mutua autenticazione*
- **Riuso del keystream**  
*il 50% di probabilità di collisione esiste dopo l’invio di 4823 pacchetti*
- **CRC non è sufficiente**  
*Un malintenzionato può apportare opportune modifiche al ciphertext senza che la validità del checksum sia compromessa*
- **Esistono tool in grado di calcolare la chiave**

## Meccanismi di autenticazione wi-fi

- tramite **SSID** (Service Set Identifier)
- tramite Indirizzi **MAC**
- accesso aperto
- a chiave condivisa

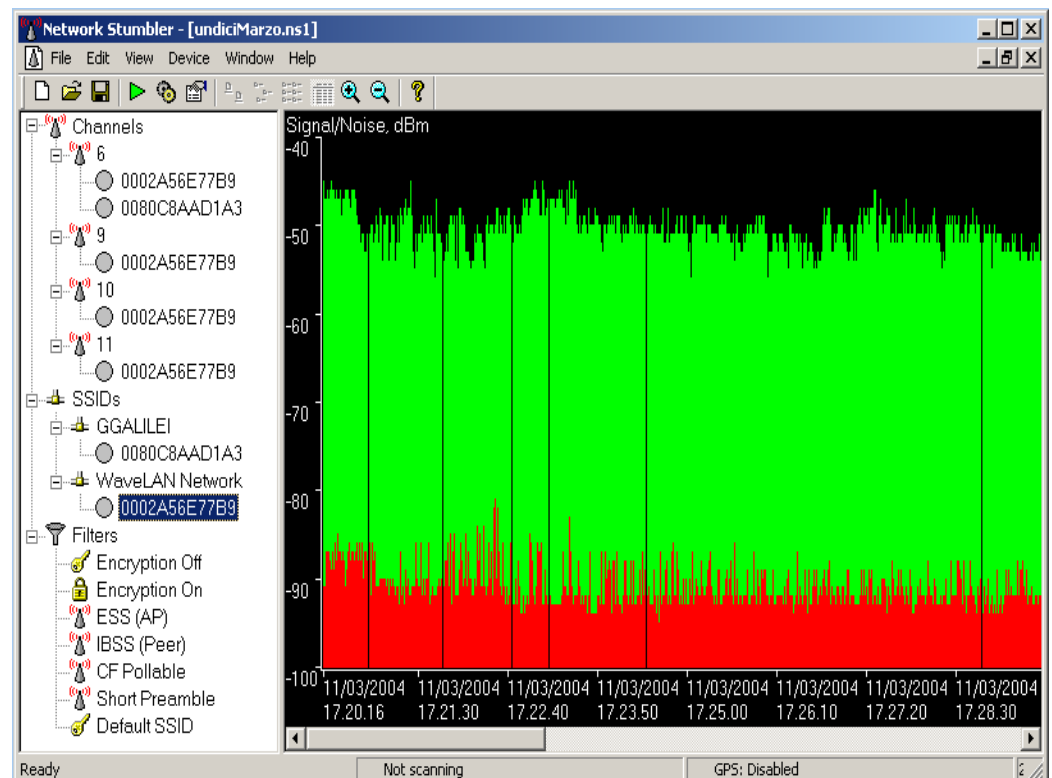


# *SSID (Service Set Identifier)*

- **SSID** è una chiave assegnata a ciascun dispositivo della rete
- Solo gli utenti che utilizzano la corretta SSID possono comunicare con gli AP

*Esistono tool in grado di identificare:*

- **SSID**
- **Indirizzi MAC**
- **Canale**
- **Esistenza o meno del WEP**



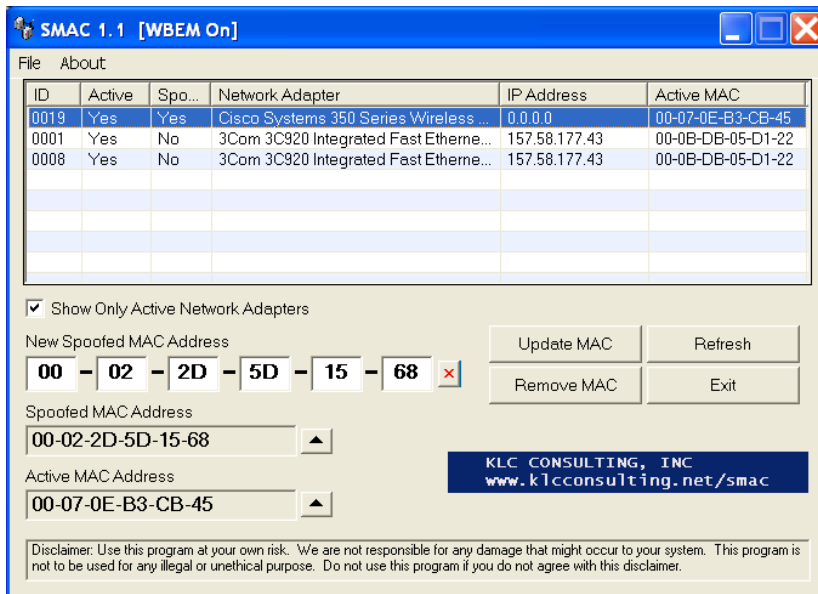
# Indirizzi MAC

# Accesso Aperto

- L'Access Point controlla se l'indirizzo MAC del client che richiede l'accesso alla WLAN fa parte dell'elenco di quelli abilitati (**ACL**)
- I dispositivi il cui indirizzo MAC non appartiene alla lista non possono accedere alla rete

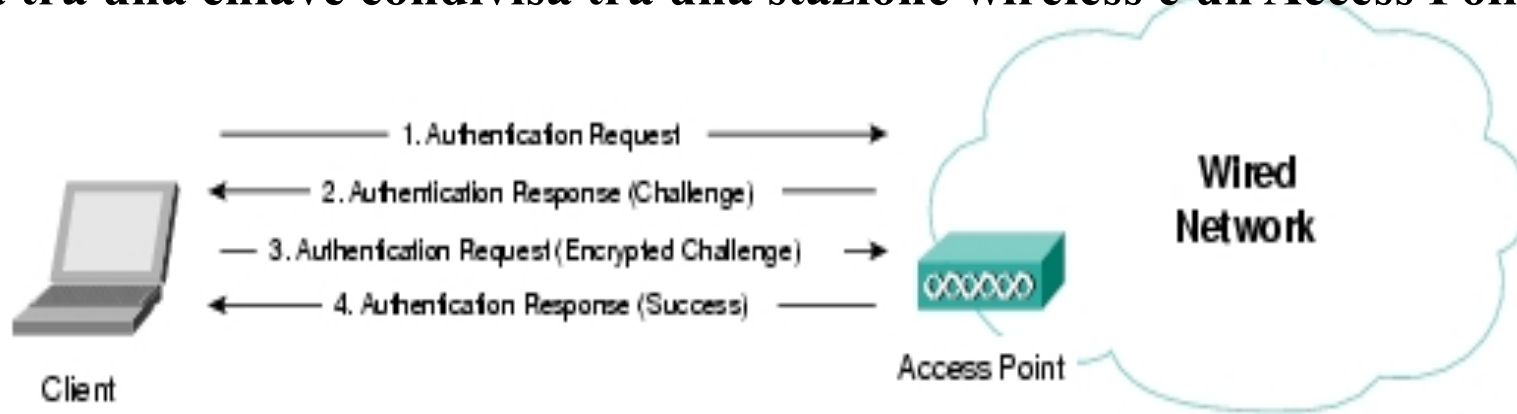
L'accesso alla rete è aperto a tutti i richiedenti senza che venga fatto alcun controllo sulla loro identità

- È progettato per l'accesso veloce alla rete
- Consiste di due messaggi
  - La richiesta di autenticazione
  - La risposta di autenticazione

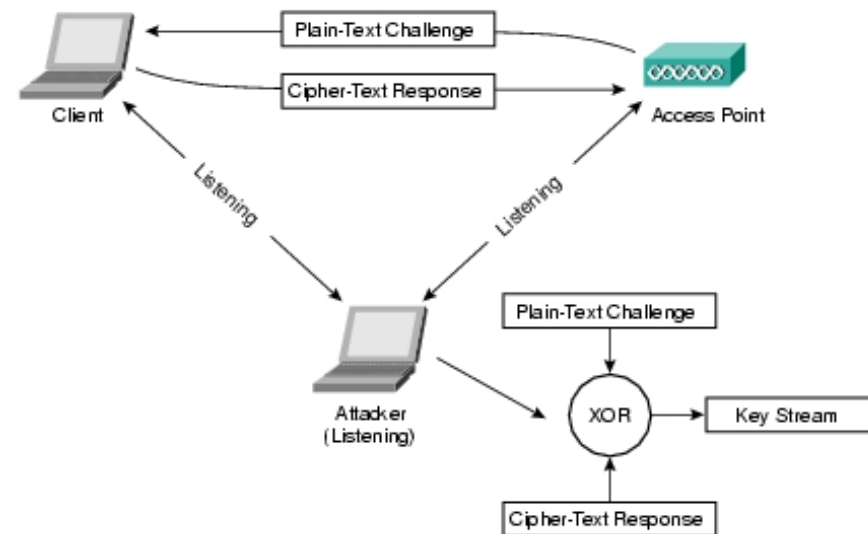


# A Chiave Condivisa

Si basa tra una chiave condivisa tra una stazione wireless e un Access Point



*Sfortunatamente, la chiave può essere facilmente decifrata*



# Miglioramento della configurazione



- **Accorgimenti**
  - ✓ *Cambiare spesso la chiave WEP*
  - ✓ *Minimizzare l'intensità del segnale*
  - ✓ *Proteggere il client*
  - ✓ *Disabilitare il broadcast SSID*
  - ✓ *Disabilitare il DHCP*
  - ✓ *Limitare il traffico broadcast*
  
- **Non è sufficiente a proteggere la rete wireless**
  
- **Ma rende più difficile la violazione della rete wireless**

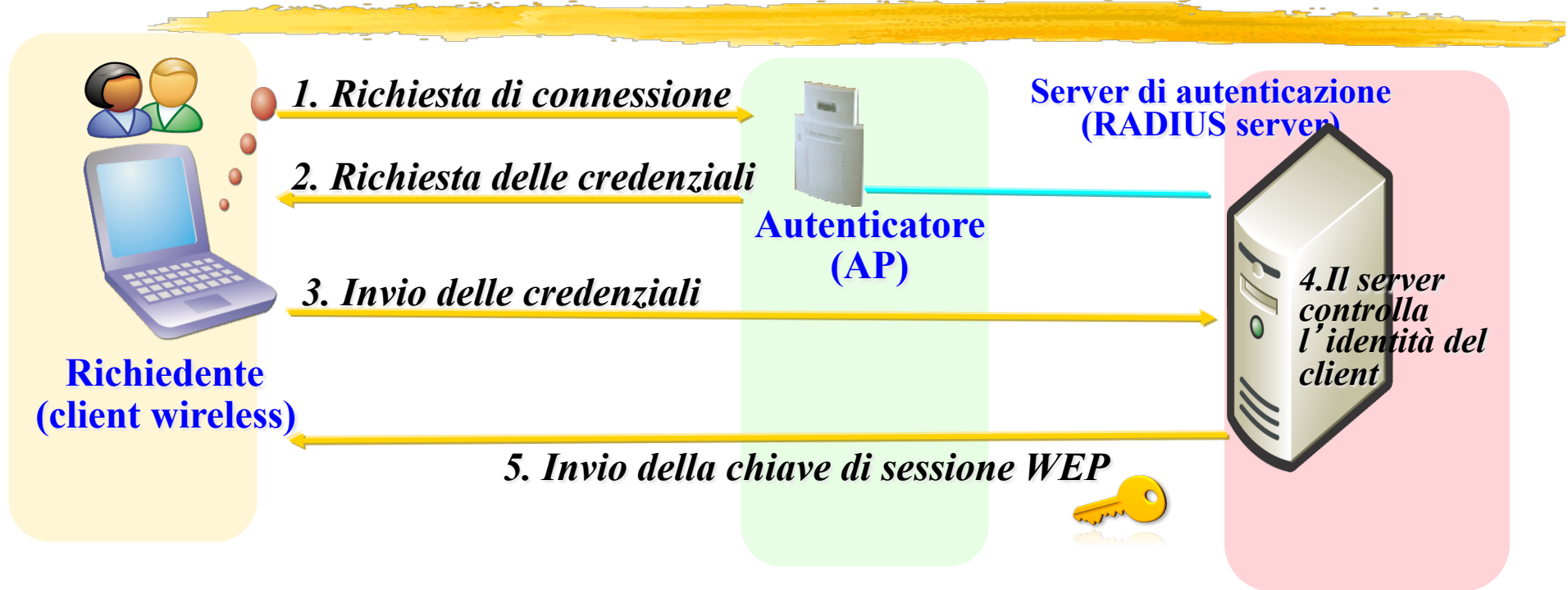
# Standard 802.1x



- ◆ Basa l'autenticazione su elementi indipendenti dai dispositivi,
- ◆ Supporta l'autenticazione reciproca tra client e Access Point,
- ◆ Supporta le chiavi basate sulla sessione,
  
- ◆ Sfrutta tecnologie esistenti come:

**EAP (Extensible Authentication Protocol)** prevede che non sia l'Access Point ad autenticare il client: *esso reindirizza la richiesta di autenticazione avanzata dal client ad uno specifico server, configurato per questo scopo come un **RADIUS (Remote Authentication Dial-In User Service)**.*

# Processo di autenticazione 802.1x



## Per concludere

- *Sia l'algoritmo di cifratura WEP sia i meccanismi di autenticazione non sono sufficienti.*
- *Una corretta configurazione può solo limitare i rischi di attacchi alla sicurezza.*
- *L'802.1x è la soluzione ottimale al problema del controllo degli accessi.*
- *Non esiste un'unica soluzione ma varie tecniche e componenti che permettono congiuntamente di proteggere la rete.*